IMPERVA REPORT

How Bots Affect Airlines

Executive Summary of Findings

Bots by the numbers

Bad bot traffic percentage - All industries	21.8%[1]
Bad bot traffic percentage - Airlines	43.9%[1]
Highest bad bot traffic percentage on an airline	94.58%
Number of airline domains with greater than 50% bad bot traffic	51

Five Groups Attack Airlines With Bots

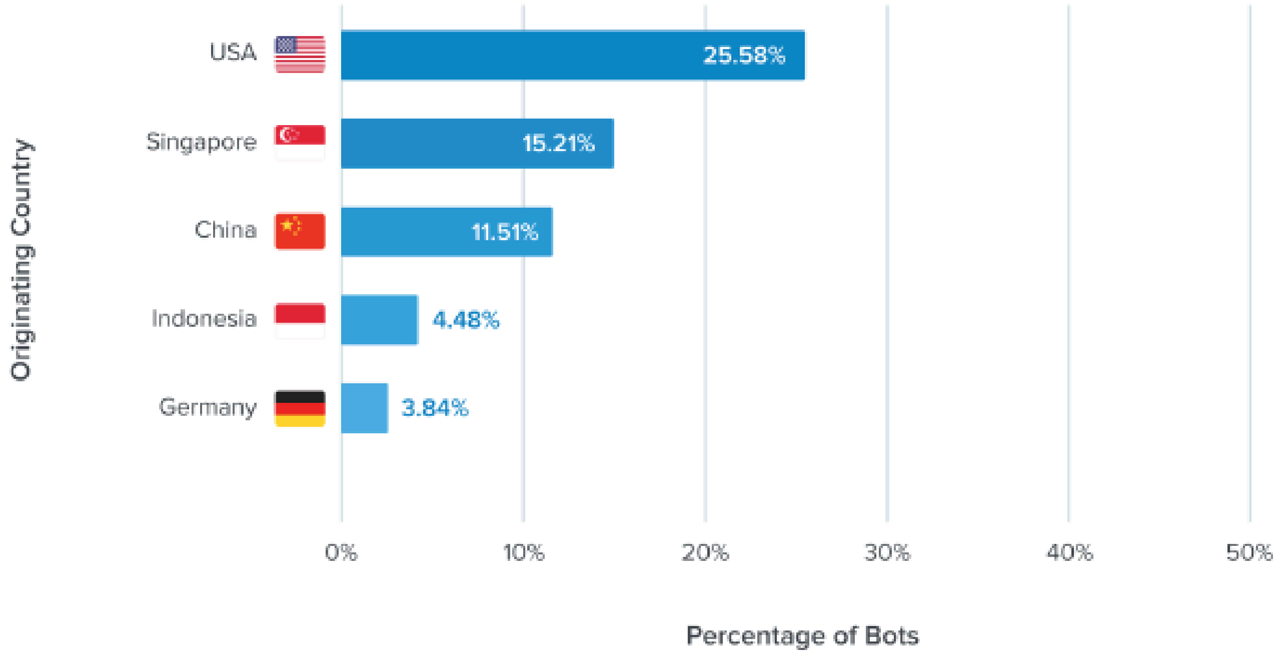
Who Launches Bots	Bot Objectives
Online travel agencies	Scrape flight information and fares. Seat spinning to hold seats to re-sell.
Competitors	Scrape flight information and fares to gain market intellience. Hold seats to block real purchases.
Criminals	Loyalty program account takeover to steal loyalty points. Fraud (Credit card and loyalty program).

Bot Sophistication on Airlines Rises

Bot Sophistication	Airline Domains 2017[1]	Airline Domains 2018
Sophisticated	19.10%	31.40%
Moderate	52.93%	52.90%
Simple	27.37%	15.70%

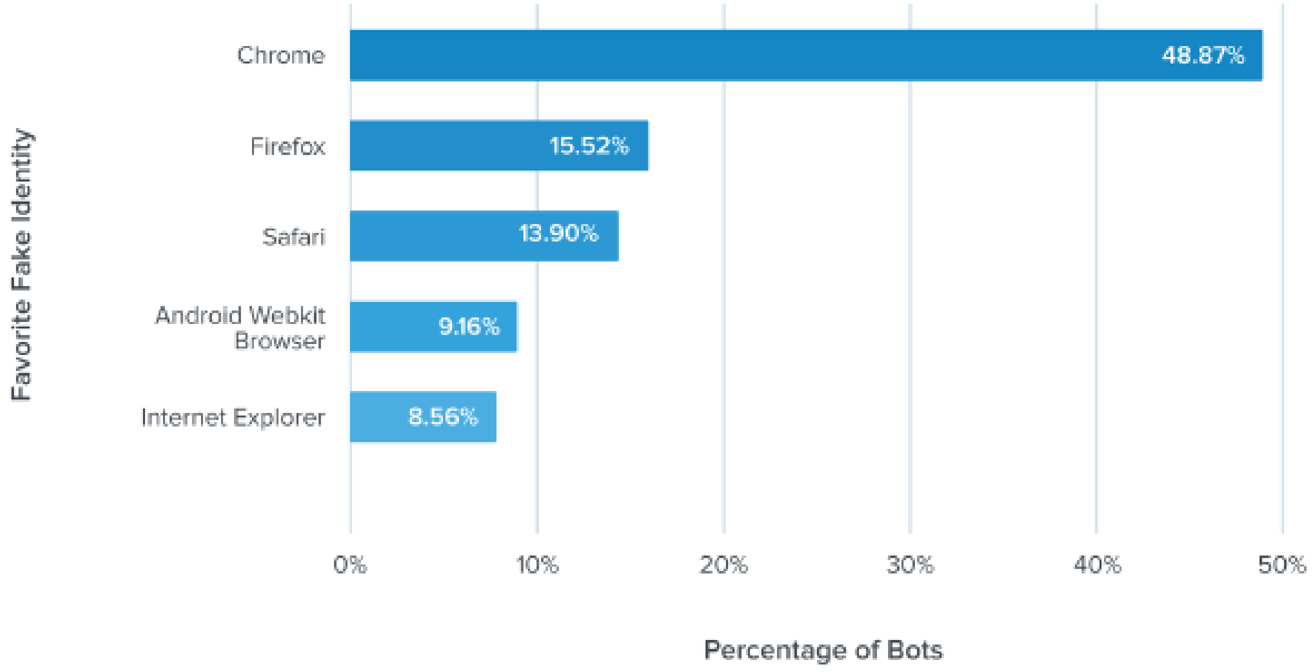
TOP 5

Airline Bot Traffic Originating Country



TOP 5

Airlines Bots Favorite Fake Identity

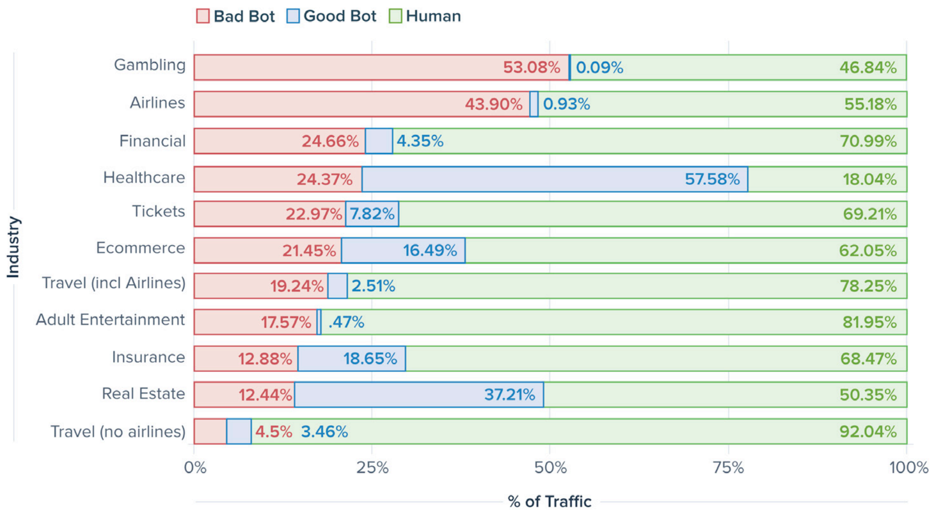


Introduction to the Bad Bot Problem

Bad bots are a problem faced by every business with an online presence. Every website, mobile app, and the APIs that power them are attacked by bots around the clock. According to the annual Bad Bot Report, only 57.8 percent of web traffic comes from actual humans—the rest are bots. While some bots are welcomed by businesses, such as search engines, there are other nefarious bots that are dangerous to the success of organizations. These bad bots comprise 21.8 percent of all web traffic.

The Airline Bot Problem

The airline industry bot problem is significantly worse than the cross-industry average. In 2017, the proportion of bad bots traffic to airline websites was 43.9 percent. Only one industry – gambling – had a higher proportion of bad bot traffic.



Bots in the Airline Ecosystem

This report is the first industry-specific study examining the round-the-clock damage caused by bots on airline websites, APIs and mobile apps. Before delving into the statistical data, it is helpful to understand why bots are used, what kinds of bot operators use them, and the business impact on airlines.

Airline Web Property Structure

At the heart of the bot problem is the airline website and mobile app. This is the online home for all flight information where customers can review prices and discounts, make purchase decisions, choose their seat, and book their flight. For simplicity, an airline website can be thought of as having two distinct areas: the booking engine and the rest of the website, sometimes known as the portal.

While some airlines build their own proprietary booking engine, others use the services of a third-party partner to manage the entire booking process. The specifics of each website vary, but the underlying structure chosen by airlines is typically one of three models:

AIRLINE MANAGED	OUTSOURCED WEBSITE	OUTSOURCED BOOKING ENGINE ONLY
Portal and booking engine managed by airline.	Fully managed portal and booking engine by third party vendor	Booking engine managed by third party vendor, and portal managed by airline.

Regardless of the model adopted, consistent bot problems plague all airlines. In general, they are launched from four main groups of bot operators.

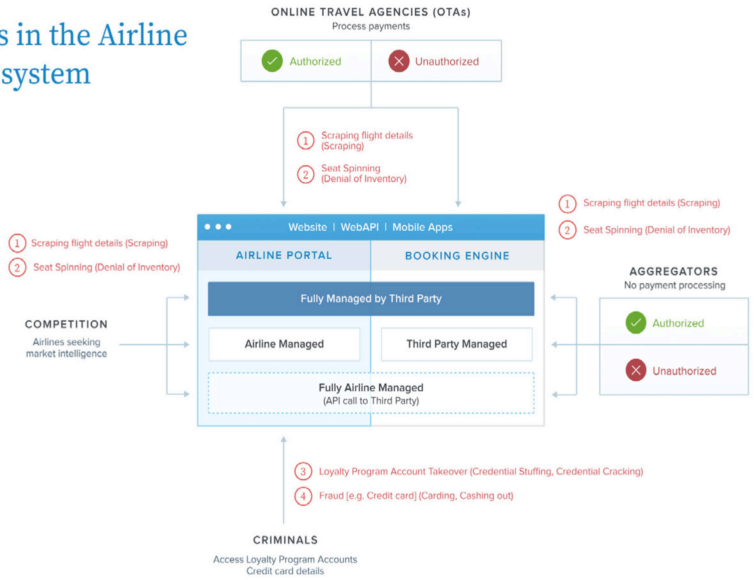
Bot Operators: Online Travel Agencies & Aggregators

Airlines rely on the online travel agency (OTA) channel to distribute and sell its flights. OTAs like Expedia and Booking.com help customers find flights and process payments on their own website. Travel aggregators such as Kayak and Skyscanner are similar to OTAs but for one difference: aggregators don't process bookings or payments on their website. Instead, aggregators typically redirect a customer to the airline's web portal to complete their purchase.

Authorized OTAs and aggregators are allowed to scrape data about flight information from an airline under agreed upon terms, such as how frequently they access the website in exchange for associated fees. To scrape the data, OTAs and aggregators can either access the airline or booking engine through an API or use an automated script that runs when programmed – otherwise known as a bot.

Unauthorized OTAs and aggregators also use bots to scrape prices and flight information. The difference here is that they do so with no agreement in place, and no stated frequency of bots crawling on the airline's site. Unauthorized OTAs and aggregators seek to gather free information from the airline rather than pay associated fees by entering into a commercial arrangement that would require a service level agreement. Without visibility into its traffic, an airlines has no way to discern which OTA or aggregator bot activity is sanctioned and which is unauthorized.

Bots in the Airline Ecosystem


ONLINE TRAVEL AGENCIES (OTAs)
Process payments
Authorized
Unauthorized
1 Scraping flight details (Scraping)
2 Seat Spinning (Denial of Inventory)
1 Scraping flight details (Scraping)
2 Seat Spinning (Denial of Inventory)
Website | WebAPI | Mobile Apps
AIRLINE PORTAL
BOOKING ENGINE
Fully Managed by Third Party
Airline Managed
Third Party Managed
Fully Airline Managed
(API call to Third Party)
1 Scraping flight details (Scraping)
2 Seat Spinning (Denial of Inventory)
COMPETITION
Airlines seeking market intelligence
AGGREGATORS
No payment processing
Authorized
Unauthorized
3 Loyalty Program Account Takeover (Credential Stuffing, Credential Cracking)
4 Fraud [e.g. Credit card] (Carding, Cashing out)
CRIMINALS
Access Loyalty Program Accounts
Credit card details

Bot Operators: Competitive Airlines

Competing airlines soften launch bots against each other in order to gather up-to-the-minute market intelligence. They use bots that identify competitor prices, count seat inventories, and identify discounted fares. Competitive bots add to the volume of bots on a website and serve no valuable purpose to the business that falls victim to them.

Bot Operators: Criminals

The bots that criminals launch at airlines are primarily intended to compromise loyalty rewards programs. These bots run brute-force credential stuffing and credential cracking attacks on login pages in order to gain access to accounts and, once inside, steal loyalty points, transfer them to other accounts, or use them for fraudulent purchases. They can also steal personal information such as credit card numbers and passport numbers.

Account takeovers can shake consumer confidence so much that customers change their preferred airline. Once a customer's account has been hacked, the airline has a customer service problem to solve. They also have the added cost of forensics and reimbursement of stolen points or credit card fraud.

How Bots Affect Airlines

While no two airlines are identical, no two bot problems are the same either. That said, bots cause business problems that impact nearly all airlines. These include unauthorized scraping, seat spinning, loyalty program account takeover, and fraud. Each of these problems alone is enough to have a significant impact on customer experience and, ultimately, the reputation of the airline. Collectively, these bot activities add up to a significant headache for the business, especially the IT team. Left unaddressed, they lead to poor website performance and even downtime.

The Primary Problem is the Volume of Scraping

Every airline has some combination of authorized and unauthorized scraping that occurs on its web properties. The volume of scraping bots launched from OTAs, aggregators, and competitors is significant for many reasons, not least of which is that high volumes damage business insights such as look-to-book ratios, and increase fees incurred by third-party booking vendors. Any dramatic changes in the look-to-book ratio indicates an increase in bot traffic actively scraping flight information. This is a primary business case for many airlines to seek solutions that address the bot problem.

Seat Spinning: An Asia Pacific Problem

While all airlines experience seat spinning, those in the Asia Pacific region see a higher proportion because in some countries a seat can be held at no cost for 24 hours before requiring payment. This allows the bot operator, for example an OTA, to hold seats and re-sell the held booking without any investment. The problem is most visible to an airline as departure time draws closer. When a flight that was previously fully booked suddenly sees increasing numbers of empty seats appear it is a good indication of bot activity. No airline likes empty seats at take-off, especially if unauthorized bots are the culprit.

Bots Attack Loyalty Rewards Accounts

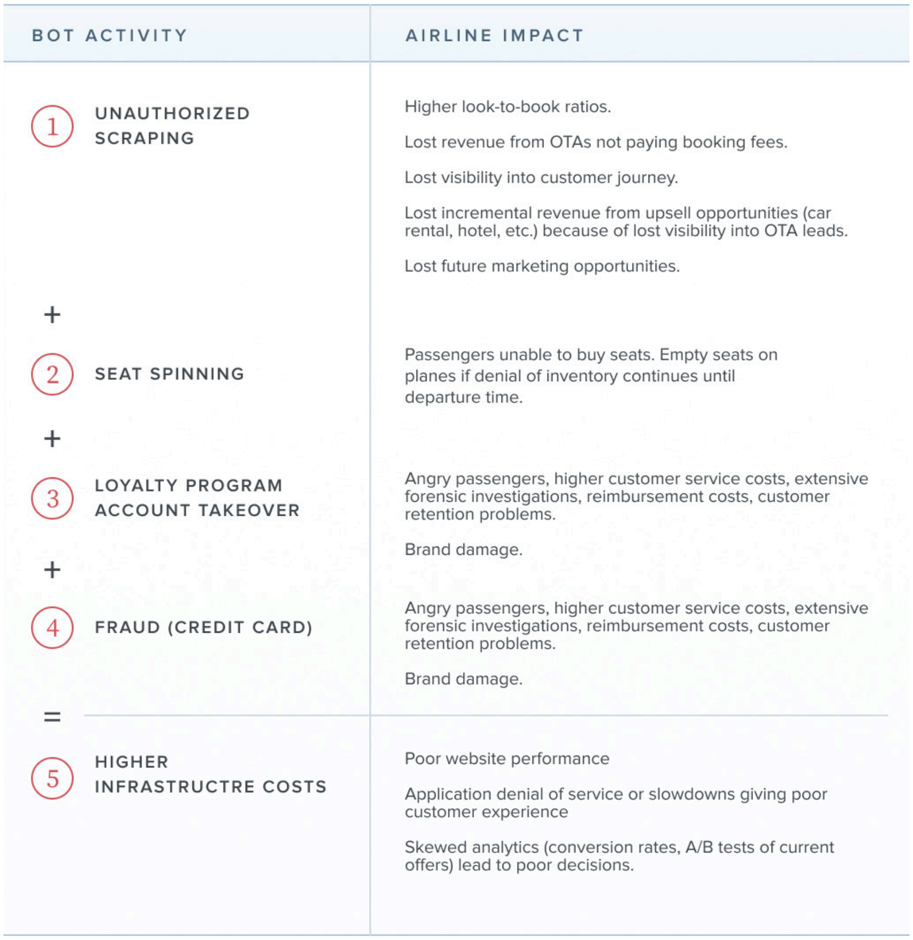
Using bots to perform account takeover attacks of loyalty rewards accounts is prevalent within airlines where the loyalty reward points or miles are treated as currency. For this reason, larger North American and European airlines see more bots attempting credential stuffing attacks against their login pages. A noticeable spike in requests to a login page combined with a rise in the typical proportion of failed login attempts is a key indicator that an account takeover attack is underway.

Fraud: A Cost of Doing Business?

Credit card fraud is a constant problem for any ecommerce business and airlines are no different. Card-not-present transactions are necessary but lead to an increase in options for criminals attempting to commit fraud using stolen or incomplete credit card details. Bots are used to run carding and card cracking scams. Any increase in customer complaints about account lockouts or increase in credit card fraud is a good indicator of the presence of malicious bots. Reducing the total volume of bot traffic on the website or mobile app typically reduces the amount of attempted automated fraud during transactions.

The Equation of How Bots Affect Airlines

A summary of business problems that the bombardment by bots causes airlines is shown below.



BOT ACTIVITY	AIRLINE IMPACT
1 UNAUTHORIZED SCRAPING	Higher look-to-book ratios. Lost revenue from OTAs not paying booking fees. Lost visibility into customer journey. Lost incremental revenue from upsell opportunities (car rental, hotel, etc.) because of lost visibility into OTA leads. Lost future marketing opportunities.
+	
2 SEAT SPINNING	Passengers unable to buy seats. Empty seats on planes if denial of inventory continues until departure time.
+	
3 LOYALTY PROGRAM ACCOUNT TAKEOVER	Angry passengers, higher customer service costs, extensive forensic investigations, reimbursement costs, customer retention problems. Brand damage.
+	
4 FRAUD (CREDIT CARD)	Angry passengers, higher customer service costs, extensive forensic investigations, reimbursement costs, customer retention problems. Brand damage.
=	
5 HIGHER INFRASTRUCTRE COSTS	Poor website performance Application denial of service or slowdowns giving poor customer experience Skewed analytics (conversion rates, A/B tests of current offers) lead to poor decisions.

Bots Affect Every Department

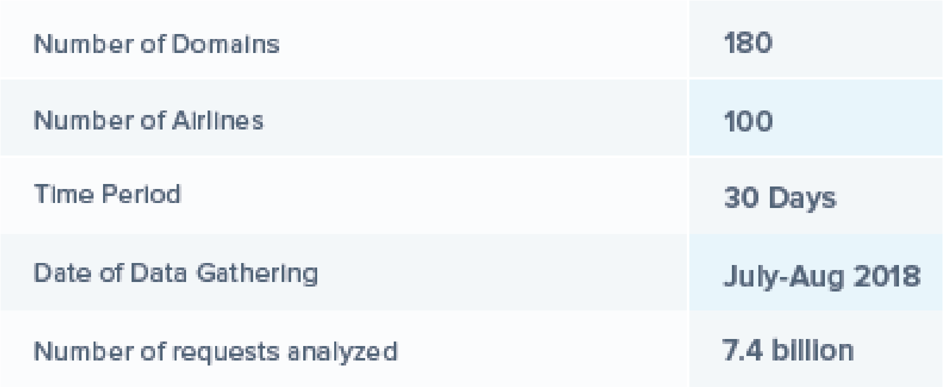
Minimizing the bot problem as solely the domain of the IT or Security department is too simplistic. While the performance and security of the website falls under the IT remit, the effect of bots on the airline is much wider. While the bot problem is typically managed by a technology solution deployed by the IT or Security departments, the result for the airline is usually a positive return-on-investment for all departments.

Poor look-to-book metrics and empty seats are a concern of leadership and airline business management. Commercial and marketing departments care about conversion rates, traffic sources, and campaign effectiveness. But with bots dirtying the traffic, decision making based upon skewed results is significantly flawed.

Credit card and loyalty program fraud is an ongoing concern of an airline's finance department while angry passengers locked out of their loyalty account or seeking reimbursement from fraud will contact the customer service department. Bots affect the entire airline business.

Methodology

This report is the first industry-specific study into the round-the-clock damage caused by bad bots on airline websites, APIs and mobile apps. This report is an aggregate of data gathered and is not intended to reveal the data for any specific airline.



Number of Domains	180
Number of Airlines	100
Time Period	30 Days
Date of Data Gathering	July-Aug 2018
Number of requests analyzed	7.4 billion

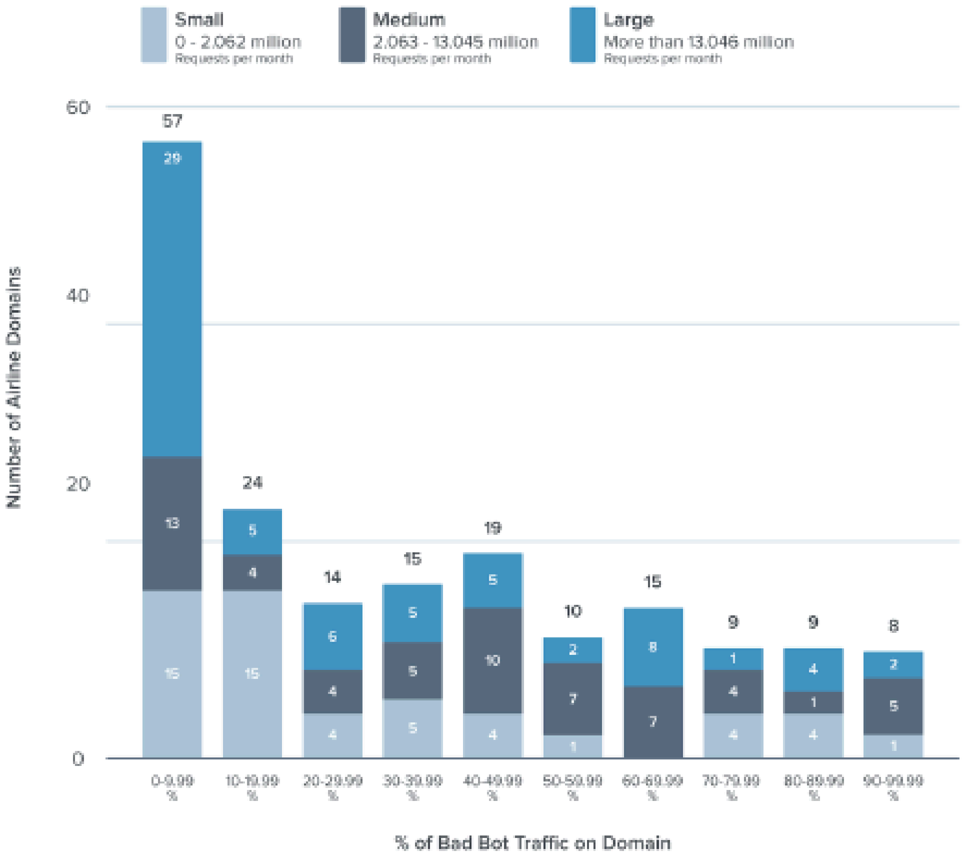
The Bots on Airlines How Bad is Bad?

The domain identified as suffering from the highest proportion of bot traffic was a European airline—94.58 percent of its traffic was bots. Humans accounted for only 5.42 percent of its traffic.

On 51 of the domains, bots accounted for greater than 50 percent of all traffic—80 percent of these were from medium and large traffic sites.

The average amount of bad bots seen was 21.8 percent3 across all industries. In this study, 94 airline domains exceed this average proportion of bad bot traffic.

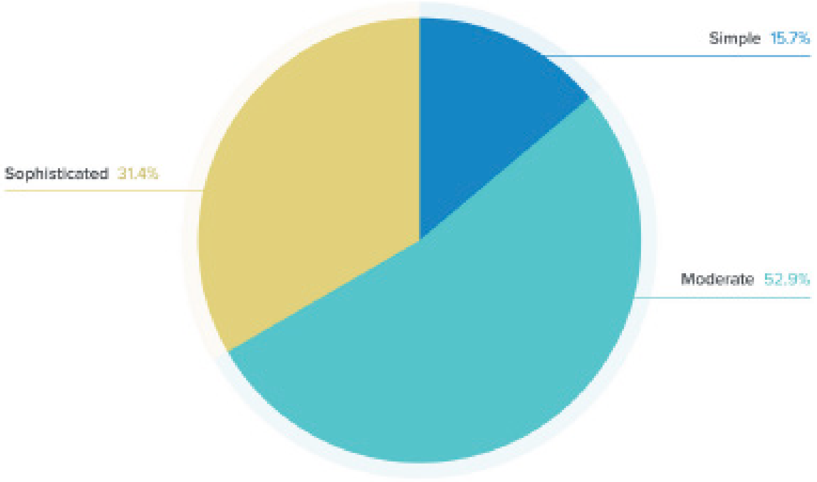
Number of Airline Domains by Percentage of Bot Traffic



Airline Bot Sophistication

Nearly a third (31.40 percent) of bots on airlines were classified as sophisticated. Only 15.70 percent were simple bots. The remaining (52.90 percent) were moderately sophisticated.

Sophistication of Bots

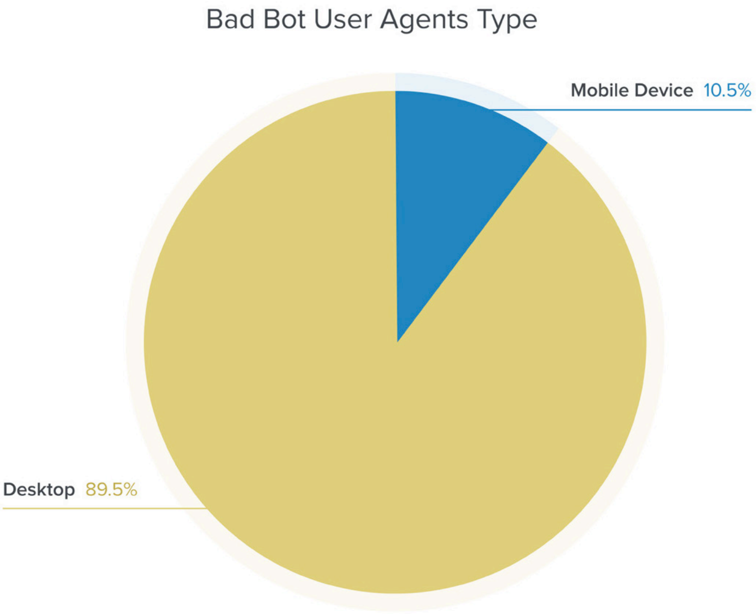


The sophistication level of bots on airlines is significantly higher than previously seen in the 2018 Bad Bot Report. In that research, 19.70 percent of bots on airlines were sophisticated compared with 31.40 percent now. This increasing sophistication is explained by the arms race at play between bot operators and bot detection technology. Once bots are detected and blocked, the challenge to the bot operator is to create another bot to achieve the same goal. Because the financial viability of unauthorized OTAs and aggregators is based upon bots scraping airline data, the cycle continues ad infinitum.

Bot Sophistication	Airline Domains 2017[1]	Airline Domains 2018
Sophisticated	19.10%	31.40%
Moderate	52.93%	52.90%
Simple	27.37%	15.70%

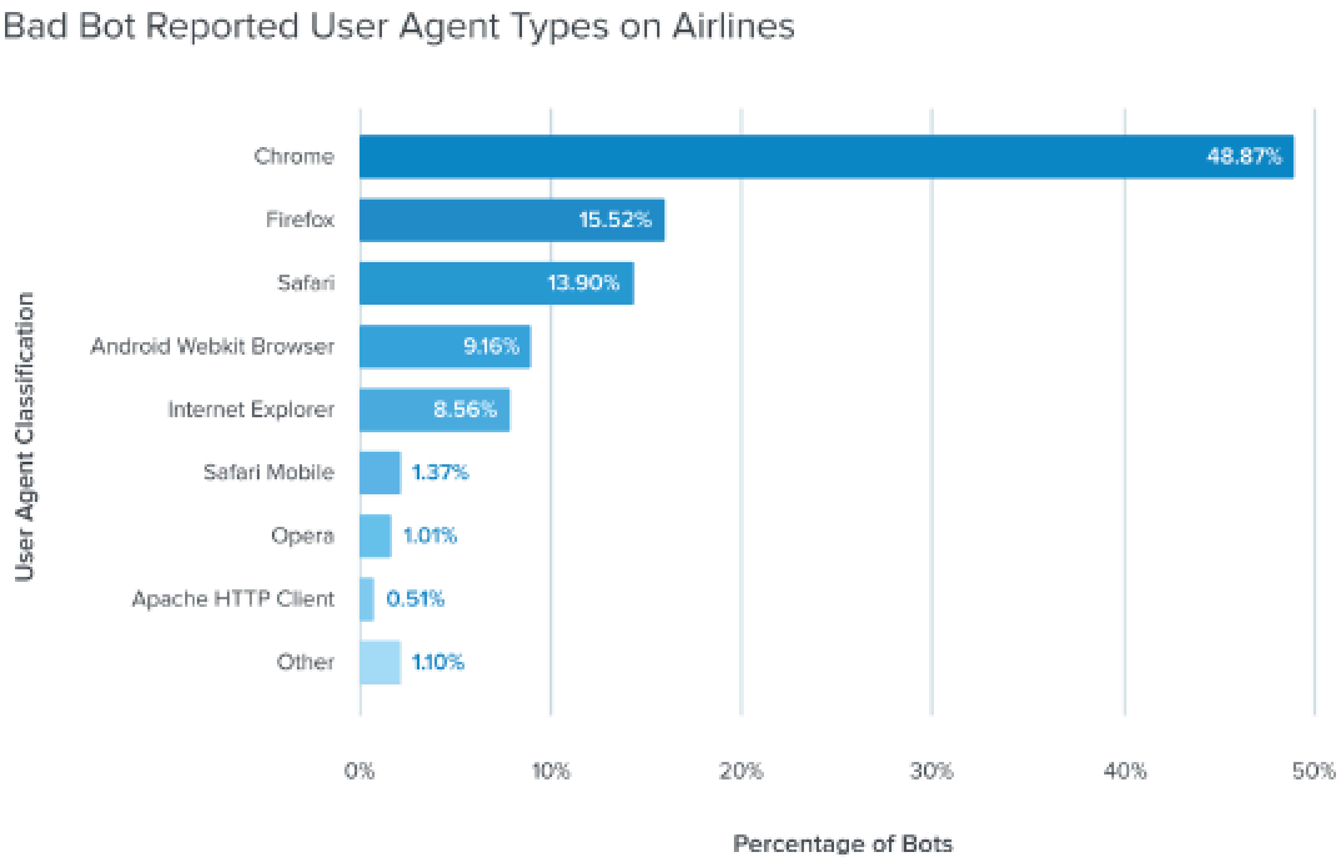
Mobile versus Desktop Bots

10.50 percent of bots on airlines identify as a user agent from a mobile device. The rest all claim a user agent associated with a desktop browser. While this proportion of mobile impersonators is currently small, it is consistently growing and this trend is expected to continue.



Top Self Reporting Browsers

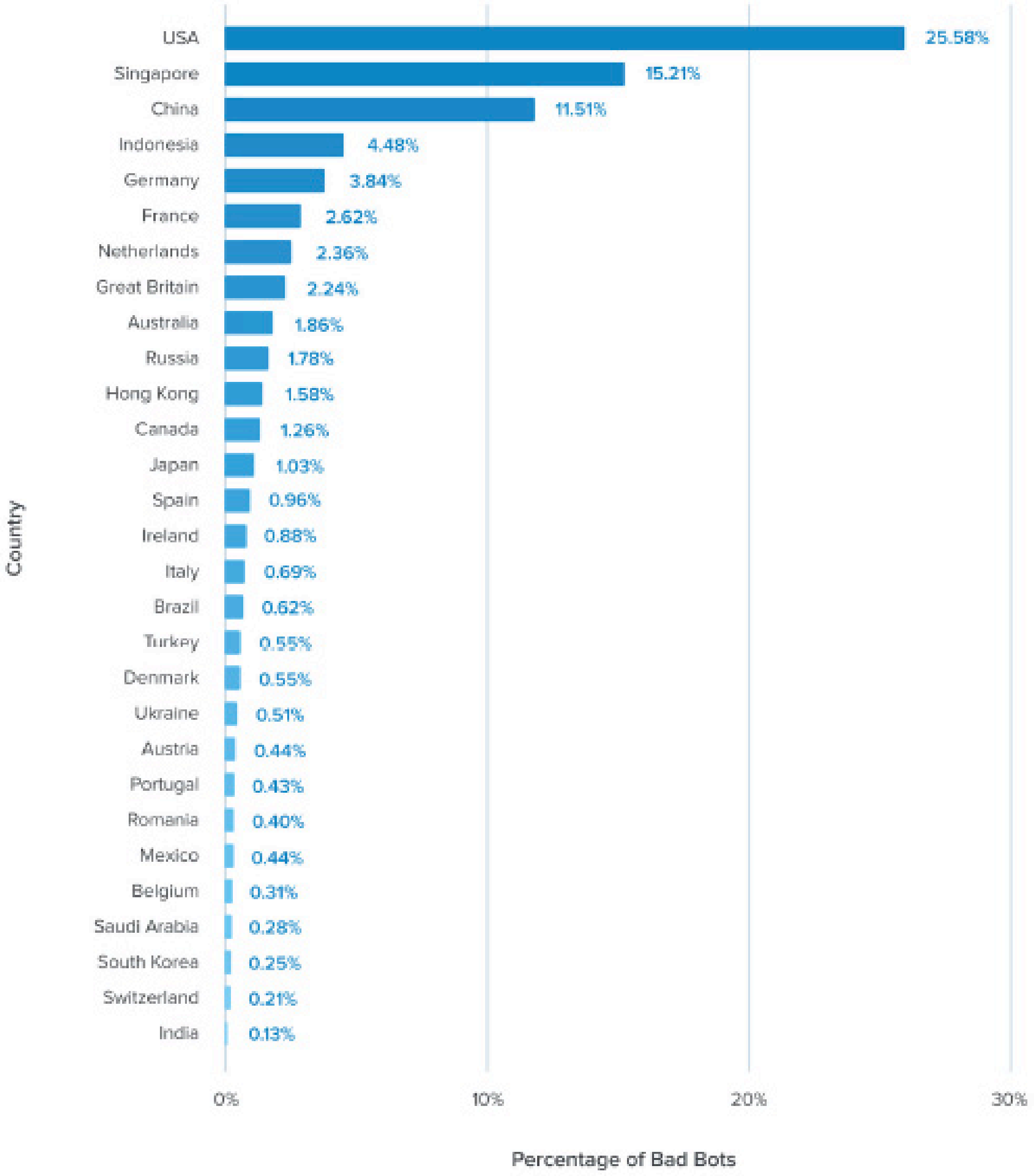
Across all airlines, bad bots identified themselves as one of 270 unique user agents. However, almost half (48.87 percent) of all bad bots claim to be Chrome. Clearly bots are attempting to hide in plain sight by impersonating the most popular browser. Firefox at 15.52 percent and Safari at 13.90 percent are the distant second and third. Mobile browsers, Android and Safari Mobile, occupy the fourth and sixth most popular user agent for bots.



Bad Bots on Airlines: A Global Problem

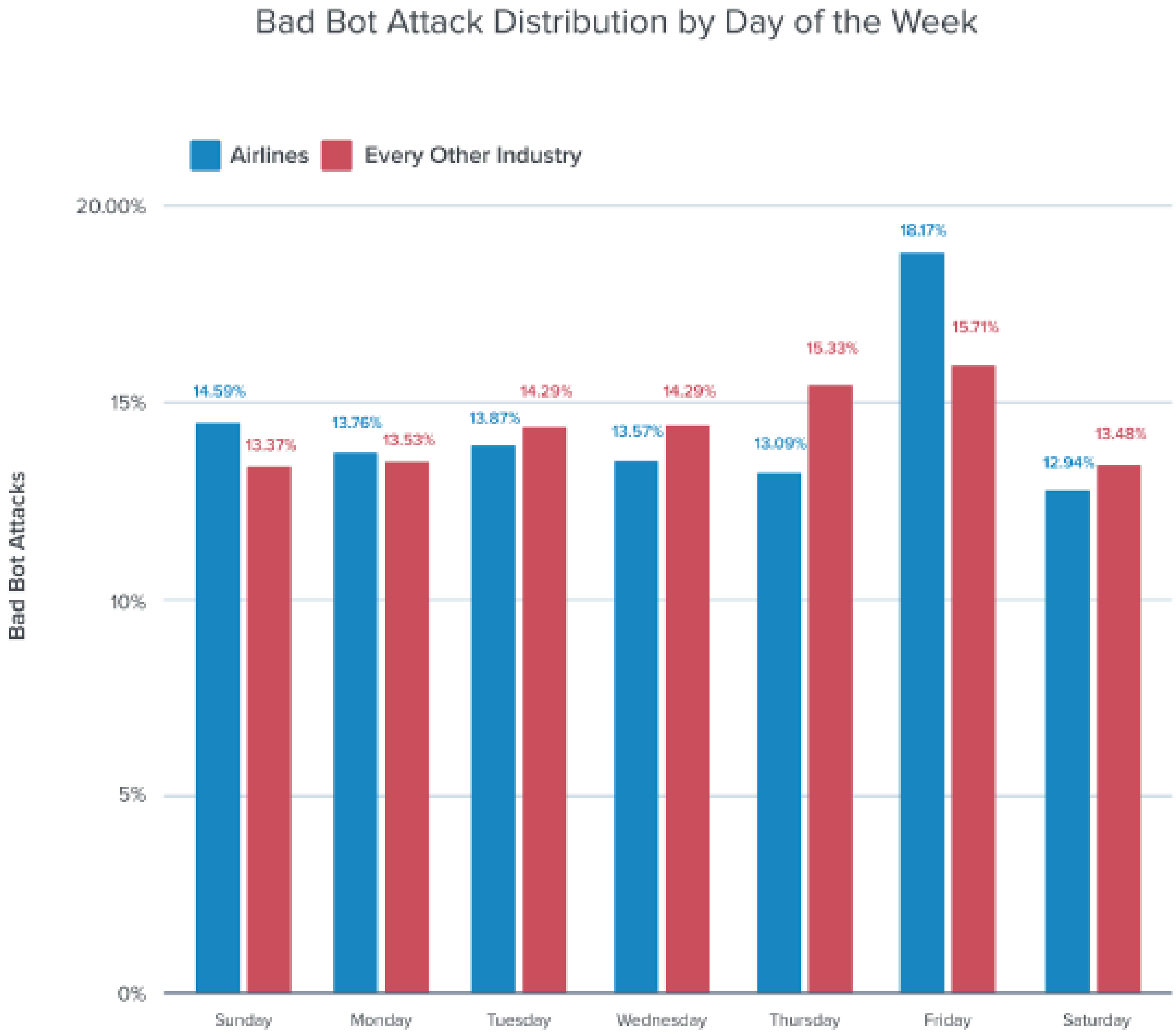
USA is the leading source of bad bots on airlines responsible for 25.58 percent of this traffic. Singapore is in second place with 15.21 percent and China is third with 11.51 percent. Reflecting the global distribution of airlines, OTAs and aggregators, the number of countries hosting bot traffic is high and is spread out across every region of the world.

Bad Bot Originating Countries on Airline Domains



Airline Bots By Day of the Week

The consistency of bad bot traffic on airlines is noticeable when examining the data by day of the week. Bots don't sleep and work around the clock, every day of the week. In general, they are consistent in volume every day except for Friday where there is a peak of bad bot traffic at 18.17 percent. This is explained by some airlines offering discounts on fares on Friday's and bots increasing activity to gather any new information.

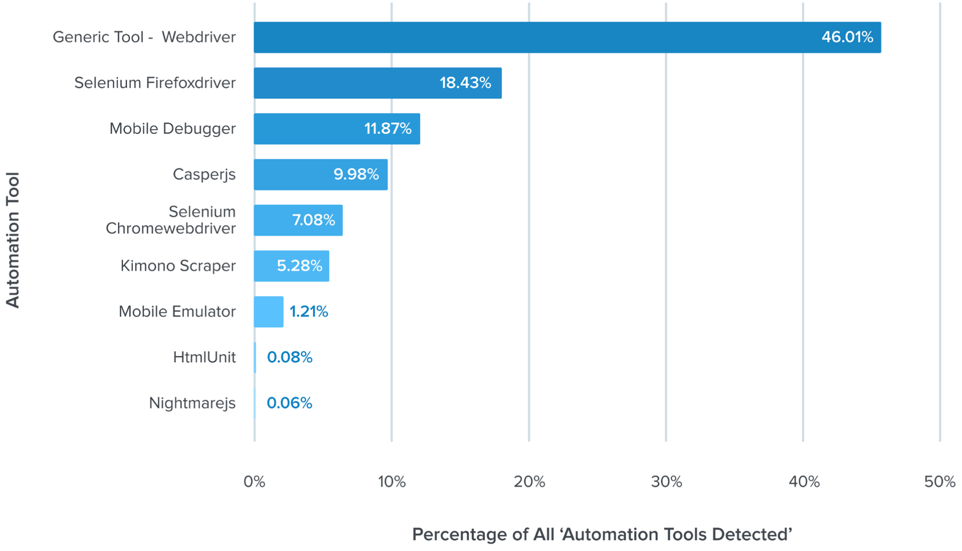


Popular Automated Tools Used on Airlines

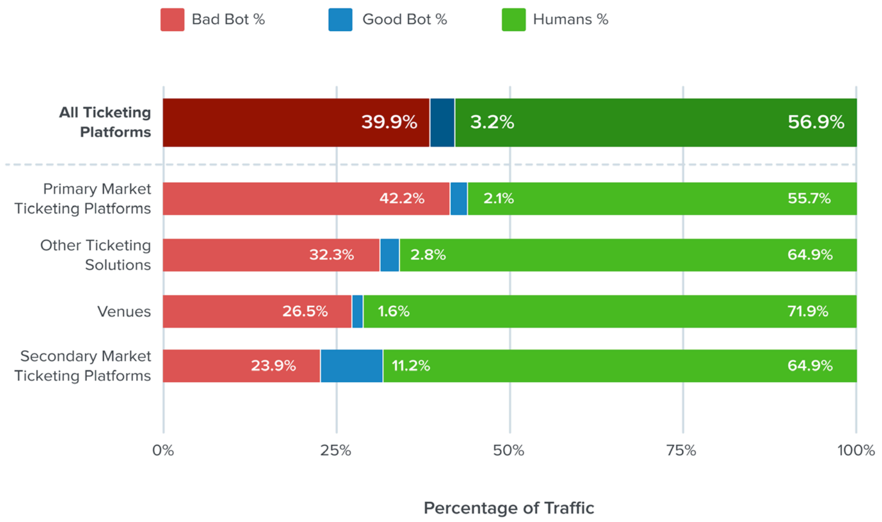
Of the bad bots identified as an Automated Tool, a generic automation framework (WebDriver) was the most popular accounting for 46.01 percent of those detected. Different versions of Selenium also saw significant usage—Selenium “Firefox” with 18.43 percent and Selenium “Chrome” with 7.08 percent.

Mobile tools were also detected. Mobile debugger’s accounted for 11.87 percent of automated tools and mobile emulators were 1.21 percent, which further indicates the increasing part that mobile bots are playing in attacking airlines.

Most Popular Automated Tools Detected on Airlines



Bad Bots v Good Bots v Human Traffic on Ticketing Platforms



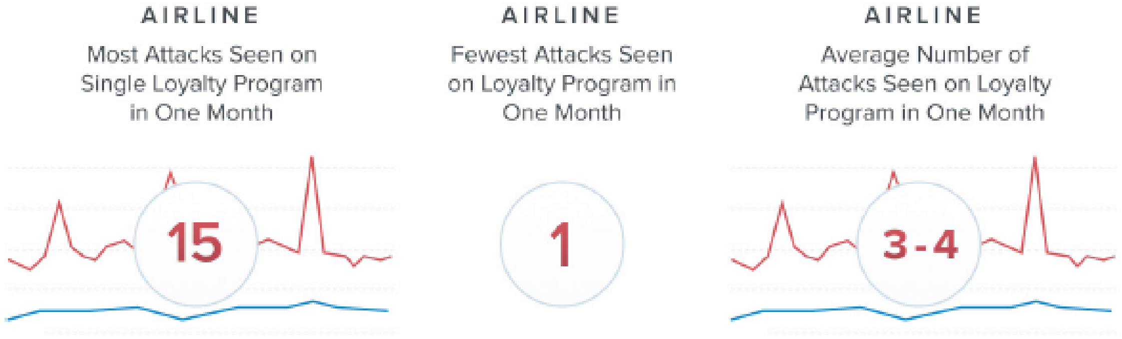
Loyalty Programs: Bots Perform Account Takeover

In 2016, $48 billion in airline miles and other rewards sat unredeemed in customer accounts according to Gartner's "Market Guide for Loyalty Marketing Platforms". With so much money hidden in loyalty programs, criminals understand that accessing those accounts is a potentially lucrative effort. Bots run credential cracking and credential stuffing attacks to identify which pairs of usernames and passwords gain access to any accounts.

Credential cracking attempts, where the bot is programmed to try common passwords with stolen email addresses in what is known as a 'dictionary attack', are typically low and slow and occur consistently around the clock.

Credential stuffing is when a criminal runs a list of stolen paired credentials against sites around the world hoping to gain access, and is volumetric in nature. These attacks are spikey and last for a short period, but if they are large enough can cause slowdowns or downtime due to the demands placed on the backend database during repeated authentication attempts.

The typical range of volumetric account takeover attacks for any industry is 2-3 per month5. For airlines, account takeover is more prevalent with 3-4. The most attacks seen on a single loyalty program during one month was fifteen, or one every two days. Larger airlines are a more high value target because they typically have a larger database of loyalty program members which increases the likelihood of finding a successful match from brute force credential stuffing.



Understanding Credential Stuffing Attacks

A typical airline loyalty program saw 6 volumetric credential stuffing attacks which lasted on average from 30-90 minutes. The largest attack saw ~50,000 login attempts and lasted 3 hours 30 minutes. Compared with similar attacks which are much larger in volume and duration, it is safe to assume that this bot operator was trying to avoid being too noisy for too long to evade detection.

Case Study: European Airline Loyalty Program

Bot Sophistication	Ticketing Domains 2017[1]	Ticketing Domains 2018
Sophisticated	19.10%	31.40%
Moderate	59.63%	46.60%
Simple	21.27%	21.90%

Because the vast majority of stolen credentials fail during a credential stuffing attack, it is sensible to conclude that any sudden spike of traffic to the login page combined with a higher than normal failed login rate is an indicator of account takeover attempts by bots.

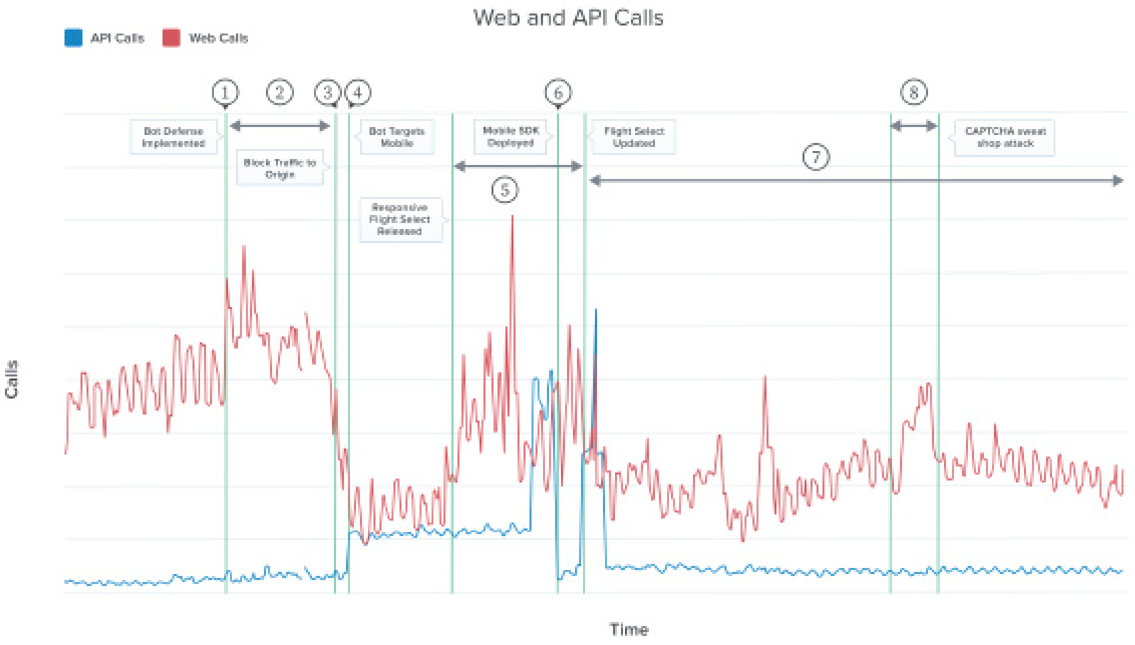
Scraping Bots and Look-to-Book Ratios

Bots sent from OTAs, aggregators and competitors to scrape prices and flight details are in themselves not malicious but the sheer volume of them on an airline website creates a multitude of business problems. This abundance of bot traffic skews important metrics designed to understand website and business performance. A key metric for airlines is the look-to-book ratio which is defined as the number of times a flight is requested per reservation made. Not every airline cares about look-to-book in the same way. Some are comfortable with look-to-book in the 1,000s while others are demanding a number below 100. The case study below illustrates the persistent problem of bots and demonstrates how this metric is affected.

Case Study: North American Airline

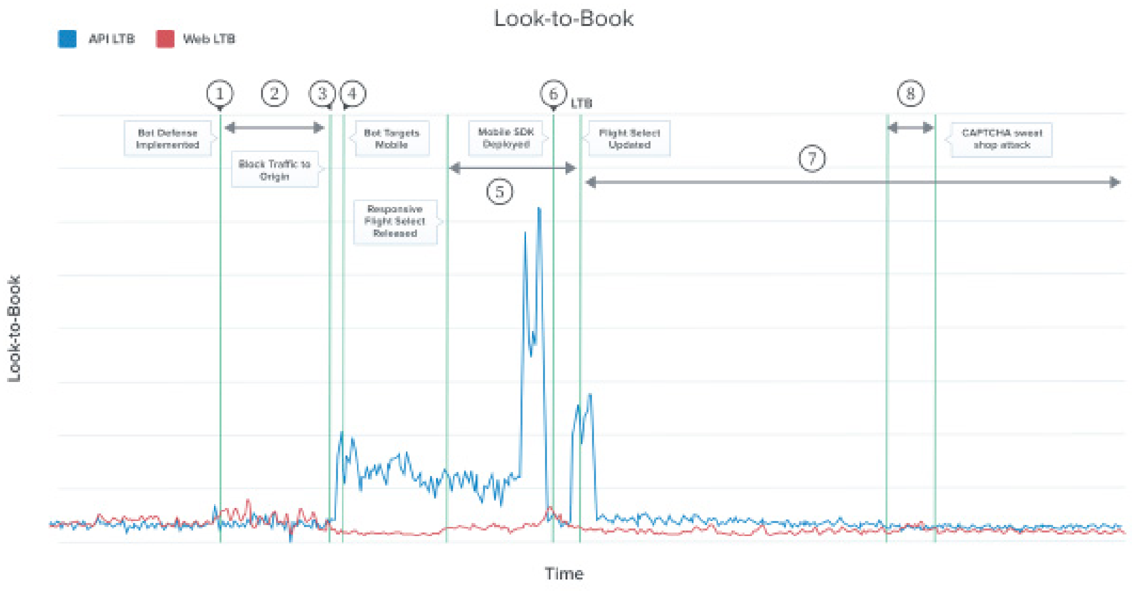
Understanding the effect of bots on web and API calls made to airlines servers is important. The chart below plots both the web and API calls over time as various bot management techniques were introduced. The numbers 1 through 8, shown below, describe the significant events on the following two charts.

1. Airline begins bot management deployment Technology is implemented to protect web calls but not API calls.
2. Bot management sees little effect Upon investigation, bot traffic was able to bypass bot detection and go directly to airline's origin servers.
3. Block traffic to origin server implemented After an infrastructure change is made, bot mitigation is effective, resulting in a dramatic drop in web calls.
4. Bot operator moves to Mobile API After seeing the drop in web calls, the bot operators change targets and move to the mobile API calls, which rise significantly.
5. Website feature changes allow easier bot access Airline updates website with new responsive flight selection feature which allows bots easy access until the website feature is updated.
6. Bot mitigation added to Mobile app SDK deployed on mobile app resulting in immediate drop in API calls as bot traffic is blocked.
7. Bot mitigation stabilizes on web & API calls Bots are removed from both website and mobile app.
8. CAPTCHA sweat shop attack Bot operators use an outsourced sweat shop of humans to defeat CAPTCHAs until blocked once again.



Look-to-book Effect

Examining the same steps (1 through 8), the impact of bots on look-to-book ratios on both the web and API traffic is significant. In the chart below, bot traffic causes the API look-to-book to spike up to 20 times its normal amount. If fees are associated with maintaining look-to-book thresholds, spikes like these may lead to significant financial overages.



Bot Management: A Way To Improve Look-to-Book Ratios

Preventing bots is a cat and mouse game. The problem is persistent and bot operators will use every available method to achieve their goal. They will move from website to mobile apps and APIs. But this case study shows that with diligence, the key look-to-book metric can be improved by removing bot traffic from an airlines site.

Lost Airline Revenue: Partners Not Paying Booking Fees

Revenue Generation by Blocking Bots

Authorized OTAs that sell a flight to a customer are typically required to use that airline's API to make the booking and the OTA pays a booking fee to the airline under the terms of the commercial agreement.

Unscrupulous OTAs circumvent these booking fees by using scraper bots to access the flight information and then manually booking the flight on the airline's website or mobile app. This saves the OTA from paying these additional booking fees but is lost revenue for the airline.

One of the quickest methods for airlines to improve revenue is by actively preventing scraper bots from unauthorized OTAs. Once these OTAs are denied free access to flight information, the alternatives are to scrape information from another website or enter into an authorized commercial arrangement with the airline and pay the required booking fee.

1. Block or CAPTCHA Outdated User Agents/Browsers: The default configurations for many tools and scripts contain user-agent string lists that are largely outdated. This step won't stop the more advanced attackers, but it might catch and discourage some. The risk in blocking outdated user agents/browsers is very low; most modern browsers force auto-updates on users, making it more difficult to surf the web using an outdated version. We recommend you block or CAPTCHA the following browser versions:
2. Block Known Hosting Providers and Proxy Services: Even if the most advanced attackers move to other, more difficult-to-block networks, many less sophisticated perpetrators use easily accessible hosting and proxy services. Disallowing access from these sources might discourage attackers from coming after your site, API, and mobile apps.

   Block these data centers: • Digital Ocean • DigitalOcean • OVH SAS

   • Choopa, LLC • OVH Hosting • GigeNET • Amazon.com
3. Protect Every Bad Bot Access Point: Be sure to protect exposed APIs and mobile apps—not just your website—and share blocking information between systems wherever possible. Protecting your website does little good if backdoor paths remain open.
4. Carefully Evaluate Traffic Sources: Monitor traffic sources carefully. Do any have high bounce rates? Do you see lower conversion rates from certain traffic sources? These can be signs of bot traffic.
5. Investigate Traffic Spikes: Traffic spikes appear to be a great win for your business. But can you find a clear, specific source for the spike? One that is unexplained can be a sign of bad bot activity.
6. Monitor for Failed Login Attempts: Define your failed login attempt baseline, then monitor for anomalies or spikes. Set up alerts so you're automatically notified if any occur. Advanced "low and slow" attacks don't trigger user or session-level alerts, so be sure to set global thresholds.

7. Monitor Increases in Failed Validation of Gift Card Numbers: An increase in failures, or even traffic, to gift card validation pages can be a signal that bots such as GiftGhostBot are attempting to steal gift card balances.

8. Pay Close Attention to Public Data Breaches: Newly stolen credentials are more likely to still be active. When large breaches occur anywhere, expect bad bots to run those credentials against your site with increased frequency.

9. Evaluate a Bot Mitigation Solution: The bot problem is an arms race. Bad actors are working hard every day to attack websites across the globe. The tools used constantly evolve, traffic patterns and sources shift, and advanced bots can even mimic human behavior. Hackers using bots to target your site are distributed around the world, and their incentives are high. In early bot attack days you could protect your site with a few tweaks; this report shows that those days are long gone. Today it's almost impossible to keep up with all of the threats on your own.