[eBook]

CDNetworks

Beating the Bots: The Most Common Issues Impacting the Online Travel Industry and How to Combat Them

The Prevalence of Scraper Bots in the Travel Industry

The tourism and travel sector has seen a significant uptick across the world ever since the end of 2020, once the pandemic lockdown restrictions began to be eased. However, this change has also resulted in a surge of bot attacks on industries in these sectors and those associated with them. According to the State of Web Application and API Protection 2022 report from CDNetworks, the three industries most severely affected by bot attacks are software information services, transportation services, and information and consulting services. In fact, bot attacks in these industries account for as many as **25% of all bot attacks** in 2022.

These bot attacks are much more than a distraction for businesses in the travel and tourism sector. They can cause direct harm to your systems, network and infrastructure and affect your business in a number of hidden ways as well.

The Biggest Challenges Caused by Scraper Bots

Ticket Scalping

Ticket scalpers use web crawling programs to continuously and rapidly extract ticket information, enabling them to purchase large quantities of in-demand or special air and train tickets. This not only undermines the dynamic pricing system and disrupts the normal market operations but can also lead to ticket servers crashing due to a sudden surge in demand, thereby affecting the regular functioning of the platform.

A perfect example of this was seen during the COVID-19 pandemic in 2020, as the domestic epidemic prevention and control situation stabilized and improved in China. The tourism market was gradually improving and flight operations of domestic airlines were being resumed. Various promotional methods such as "Fly as You Want" and instant discounts were being launched to boost consumption. But in this return to activity in the aviation and travel market, there was also a resurgence of another wave of the "dark army" – Bots. According to data from CDNetworks Cloud Security Platform, in July and August 2020, the number of malicious bot attacks against airlines surged 446% compared to the previous two months.

Seat Spinning

Denial of Inventory, or seat spinning as it is commonly called, refers to a malicious practice where bots or automated scripts are used to hold or reserve seats on flights, trains, or buses without actually completing the purchase. This practice can cause several problems:

Artificial Demand: By reserving a large number of seats without actually purchasing them, bots can create artificial demand, which can lead to increased prices as the booking system responds to the perceived scarcity of seats.

Lost Revenue: Genuine customers may be unable to purchase tickets if bots are holding all the available seats, leading to lost revenue for the travel operator.

Operational Disruption: The travel operator may need to adjust schedules, capacities, or pricing in response to the artificial demand created by seat spinning bots, leading to operational disruption.

Increased Operational Costs: Travel operators may need to invest in additional cybersecurity measures to detect and block seat spinning bots, leading to increased operational costs.

Customer Dissatisfaction: Genuine customers may become frustrated or dissatisfied if they are unable to purchase tickets or if they have to pay higher prices due to the artificial demand created by seat spinning bots.

Price and Data Scraping

Travel platform competitors 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.

Account Takeover to Compromise Reward Programs

The bots that criminals launch at airlines and travel platforms 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 airlines and travel platforms. Once a customer's account has been hacked, the platform has a customer service problem to solve. They also have the added cost of forensics and reimbursement of stolen points or credit card fraud.

Overloading of Servers

Scalping ticket requests will lead to a server load spike, which may affect the business response speed, or cause the system to fail to operate normally, and more seriously affect the normal operation of ticketing organizations, causing the relevant companies to make incorrect judgments about the market, which will affect a series of decisions in the future. The inability of normal ticket buyers to purchase tickets will also have a negative impact on the operation and reputation of the ticketing organization.

Bot Trends to be Wary of

Malicious bots have always been a concern, what makes it worse is that bots in the tourism industry are evolving towards trends of intelligence, anthropomorphism, and mobility, which makes them even more dangerous.

For example, some malicious bots forge normal User-Agents and use automated frameworks that simulate a normal browser to launch their attacks. They can also disguise themselves as bona fide search engine bots to confuse fixed-rule-based detection schemes and elude the "heavy siege" of traditional protection methods.

These ever-evolving bots are becoming capable of dynamically adjusting through distributed architecture or IP address pool to bypass rate limiting and IP blocking. Sophisticated bots can also use machine learning to identify images to bypass CAPTCHA.

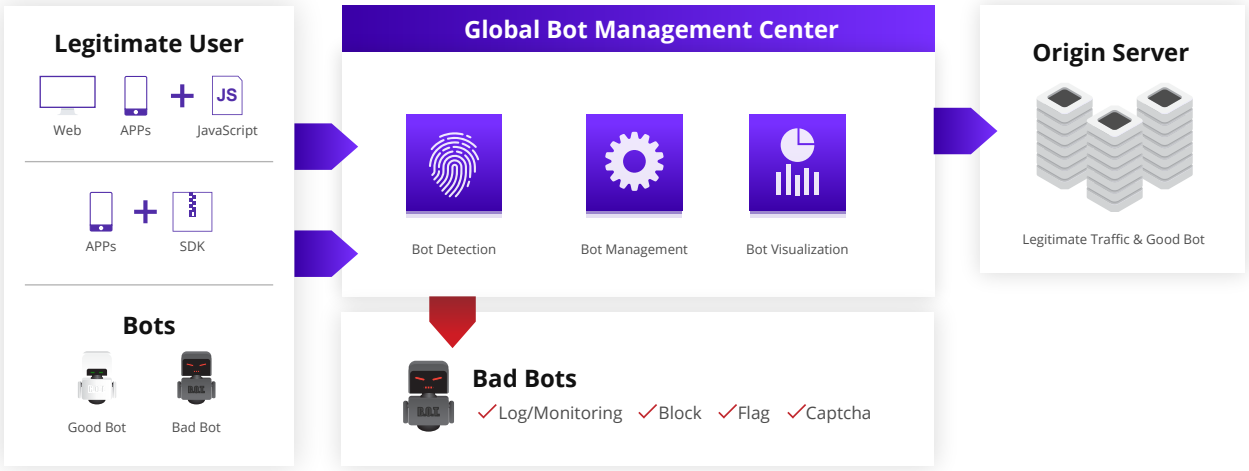
Additionally, they can mimic human behavioral characteristics, such as mouse movement, keyboard tapping and other interactive events. All of this makes it more difficult to accurately identify legitimate user traffics from malicious traffics with increasingly high simulation levels.

At the same time, various aviation and travel businesses are getting on the trends of mobile internet, which has given rise to the proliferation of device-based bot. Different from web bot, device-based bots mostly operate via emulators, and are often controlled by mobile group control software, automation tools, and device modification tools. To deal with these bots, one needs to use targeted defense strategies, which present a new challenge to the anti-bot capabilities of airline and travel platforms.

Time for Takeoff: Fighting Back Against the Bots

The concerning rise in bot attacks pose a serious danger to businesses in the travel and tourism industries, as well as related sectors. A practical approach would involve proactively exploring security solutions that comprehensively address all aspects of bot security and management, while also being capable of learning and adapting to emerging bot-based threats.

CDNetworks offers Bot Shield, a cloud-based comprehensive bot management solution to help you defend and fight back against bots. Bot Shield is based on multi-dimensional access control, request legitimacy verification, interaction verification and other protection strategies. At the same time, it imports the attack samples from the whole network into the big data analysis platform, and generates a variety of intelligent protection models by using AI deep learning technology, so as to accurately distinguish between the good bot and malicious bot traffics. This helps travel companies avoid the business risks and potential losses caused by malicious bots.



Three Steps to Protect Your Business

Bot Recognition

In defending against bots, it is important to be careful in analyzing traffic coming to your website to distinguish between authentic human behavior and malicious bots. Data from CDNetworks' Security Platform 2022 shows that only about 60% of the traffic to web applications and APIs really were made by human visits. The remaining 40% is mostly bot traffic, which includes search engine bots and malicious bots. CDNetworks adopts multiple protection means and intelligent protection technology to detect good bots and malicious bot traffic and distinguish between them in real time.

Preliminary Filtering Based on Intelligence Information

Using the worldwide bot intelligence database, covering more than 100 types of collaborative defense intelligence, CDNetworks Bot Shield filters the global traffic accessing airlines, hotels, and booking platforms, and performs preliminary identification of malicious bot attacks and the good bots that match intelligence information characteristics

Behavioral, Biometric-based Verification

Through observation over a period of time, CDNetworks carries out refined identification of abnormal behaviors such as overly high-frequency, overly single-target access and traversal behaviors that do not conform to the logic of normal browsing behavior. We also identify abnormal traffic that lacks biological features typically associated with normal browsing, such as UA information, cookie features, JS features, login information, referrer information, and operating environment features.

At this stage, CDNetworks also conducts follow-up tracking by uniquely fingerprinting each visiting client to further discover more advanced bots and disguised intelligent bots in the travel industry.

Bot Management

Relying on AI intelligent analysis engine, combined with threat intelligence, CDNetworks Bot Shield can accurately identify different categories of bots at the edge, differentiate between good and bad bot traffic, and provide multiple traffic control policies.

Good Bot Management

CDNetworks establishes a Good Bot Library, defining each category of good intentional bots, such as normal visiting users, search engines, data analytics and partners to ensure the normal operation of air travel and hotel business by formulating reasonable management strategies.

Bad Bot Mitigation

CDNetworks Bot Shield can mitigate bad bots, especially disguised bots, and blocking them at the edge. To this end, we define certain characteristics based on the difference in business workflow between normal user access and attack requests.

For highly disguised bots, the AI model performs machine learning based on device fingerprint tracking to build a dynamically updated business workflow analysis model. The request is analyzed in real time, and when behavior that does not conform to normal access logic is detected, it is blocked in a timely manner.

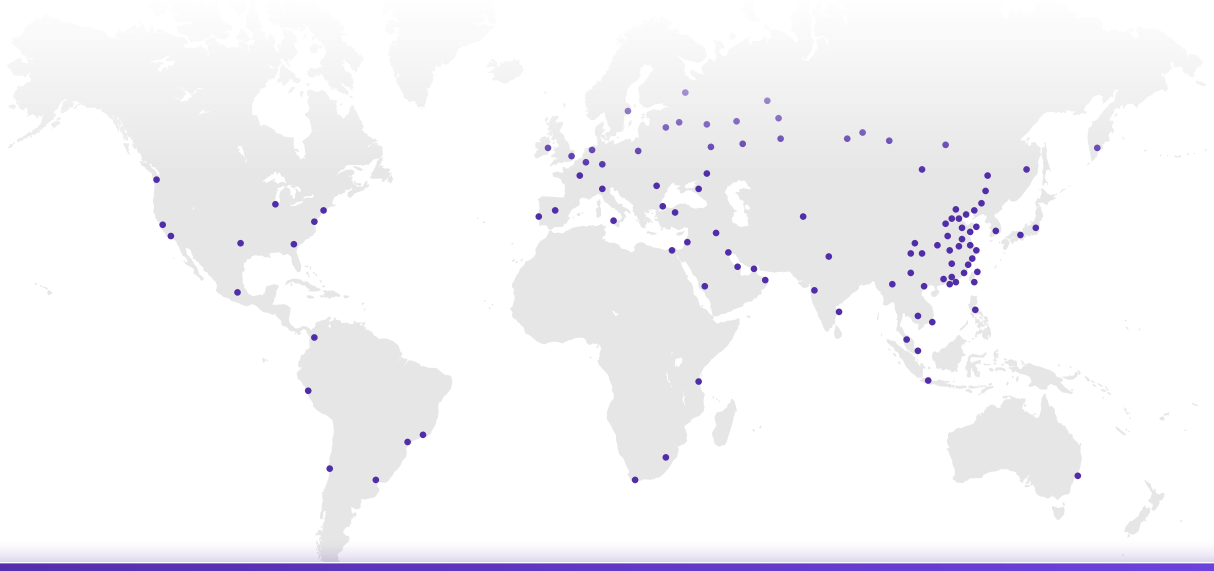
Due to the cost of attack, a well-disguised bot will inevitably adopt more efficient access behaviors than a real person, and these subtle differences can still be dynamically captured by CDNetworks' AI analysis model and blocked at the edge.

Monitoring and Strategy Optimization

CDNetworks Bot Shield provides visual dashboard of threat and professional data analysis, making it easy to help organizations gain insights of their security posture related to bots. In the field of airline, hospitality and ticket booking, the fight against malicious bot attacks is a continuous process.

CDNetworks has established a monitoring system capable of serving all kinds of travel platforms. The system is able to monitor the bot attack incidents, watching closely upon the interception rate, false negative rate, and all types of anomalies. In addition, CDNetworks utilizes an intelligent online operation system and the expertise of security professionals to dynamically modify protection strategies in real-time. This enables the establishment of a closed loop for the identification, management, blocking, monitoring, and optimization of the entire strategy.

Abundant Resources & Capabilities



200,000+	2,800+	270+	3.3B+	15Tbps+	20+
Global Servers	Global CDN PoPs	Cities in 70+ Countries	Daily attacks Mitigated	Scrubbing Capacity	Scrubbing Centers

Explore CDNetworks' Comprehensive Solutions

Web Performance

Deliver maximum web and application performance and reliability anywhere in the world – 24/7.

- Content Acceleration
- Dynamic Web Acceleration
- Cloud DNS+
- CDN Pro

WAAP

Keep your business safe from both malware and cybersecurity attacks with multi-layered security technology.

- DDoS Protection
- Web Application Firewall
- API Shield
- Bot Shield
- Security Services

Media Delivery

Deliver solid streaming experiences to consumers with ultra-low latency, high reliability and scalability.

- Media Acceleration VoD
- Media Acceleration Live Broadcast
- Low Latency Streaming
- Cloud Streaming Solution(VoD/Live)
- Object Storage

CDNetworks

As the APAC-leading network with over 2,800 global Points of Presence and more than 20 years of technology experience, CDNetworks embraces the new era of Edge and takes it to the next level by using the Edge as a service to deliver the fastest and most secure digital experiences to end users. Our diverse products and services include web performance, media delivery, cloud security, zero trust security, and colocation services— all of which are uniquely designed to spur business innovation.

Follow Us

Start Free Trial

Contact us at sales@cdnetworks.com or visit cdnetworks.com