TRAVEL & HOSPITALITY

Master Bot Attacks without Breaking a Sweat

Travel sites depend on a safe, reliable, and highly-available online environment for customers to browse and buy. What makes a site attractive to customers, also makes it a paradise for automated attacks.

Malicious bots make up an average of 30% of the traffic on your website with spikes up to more than 50%—about a third of them are headless browsers and infected users—which are difficult to detect and stop. Bots are extremely adept at mimicking human behavior—acting like real users interested in your offerings without following through.

Bots make an average of 30% of the traffic on your website

AUTOMATED BOT ATTACKS DRAMATICALLY DISTURB YOUR REVENUE STREAM

- **Scraping your data for competitive-enabling intelligence:** Bots constantly scrape your website, steal pricing and availability data to compete with you in garnering customers. This data may be used for customer and partner acquisition or to resell to competitors.
- **Negative look-to-book ratios affect revenue:** Maintaining high look-to-book ratios are drivers for measuring the effectiveness and ROI for the travel and hospitality industry. If bots are attacking your inventory, your look-to-book ratios will be greatly affected and search charges will occur. Bots aren't looking to convert.
- **Inflated traffic data on search queries increases expenditures:** Travel and hospitality businesses are charged on GDS searches. If bots are accessing this database mimicking an authorized user, your query limits will be reached creating expensive overages.
- **Distorted open-to-buy availability shifts customers to the competition:** Reservations can be made online with no cancellation fee. Bots can be used to book your entire inventory causing customers to go elsewhere for the service leaving you with a distorted sense of inventory availability and sell-through. In reality, bots are hoarding your inventory—reserving cars, booking hotel rooms, etc.—without the intention of buying while preventing you from selling the service to a paying customer.
- **Increase in online fraud and loyalty account transactions:** Bots try username/password combinations leaked from other attacks until they "crack" a customer or loyalty account to fraudulently book rooms, reserve rental cars or redeem loyalty points—to get free services. The majority of customer accounts contain payment cardholder data which is now easily accessible to the attacker to create fraudulent transactions.
- **Tainted data impacts your marketing decision making:** Bots waste marketing expenditures and skew your business decisions. Bot traffic in A/B test and analytics data impacts business decisions through undesirable site layout/design changes, retargeting campaigns and product promotions are less effective to human visitors. By detecting and removing bot activity, conversion stats will be more accurate and trusted indicators for accurately revealing successful and underperforming programs, experiments, and campaigns.

PerimeterX Bot Defender is a highly scalable and extremely accurate solution to detect and mitigate automated bot attacks against travel and hospitality sites. The sophisticated real-time detection and mitigation defends against the full range of automated bot attacks, both known and unknown.

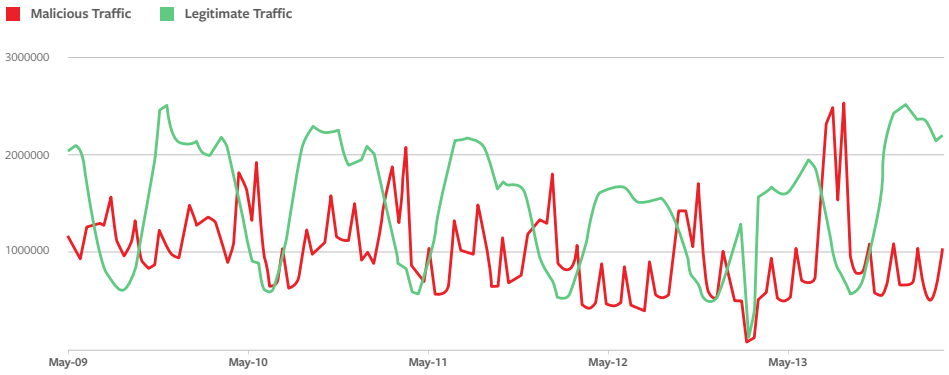
Scraping
Bots constantly scrape website and booking engine for product prices and availability, increasing costs & reducing revenue

Account Abuse
Bots hijack customer accounts, place orders, redeem loyalty points for free products or services

Hoarding/Inventory Exhaustion
Bots reserve inventory never intending to purchase, preventing customers from buying products or services

Skewed Analytics
Bots distort look-to-book ratios and skew promotions, A/B testing, retargeting campaigns and conversion rates

Total Traffic Overview Malicious vs. Legitimate



HOW PERIMETERX HELPS TRAVEL AND HOSPITALITY

PerimeterX developed behavior-based threat protection technology that advances state-of-the-art detection of automated bot attacks. Our approach is focused on dynamic behavior profiles of real customers—what a good customer looks like. We target the behavior and environment of users, rather than historical signatures of bad bots, focusing on interactions with applications, fingerprints from devices and profiling of the network characteristics. This approach leads to highly effective identification of bad bot traffic including new threats not previously seen. PerimeterX Bot Defender catches, in real-time, automated attacks with unparalleled accuracy, autotuning to improve detection while easily integrating into your existing infrastructure enabling detection and blocking within seconds.

About PerimeterX

PerimeterX protects the world's largest and most reputable websites from malicious activities, future-proofing your digital business from automated bot attacks. PerimeterX Bot Defender, bot protection-as-a-service, safeguards web, mobile applications and APIs from account takeover attacks, checkout abuse, carding attacks, marketing/click fraud and scraping through a scalable, out-of-band solution easily integrated into your existing infrastructure for a scalable, easy to manage and performance solution.

perimeterx
www.perimeterx.com
info@perimeterx.com