



CUSTOMER SUCCESS STORY

StubHub Prevents Content Scraping, Account Takeover, and Skewed Conversion Rates

StubHub

Overview

StubHub (an eBay company), headquartered in San Francisco, California, was founded in 2000 with the mission to help fans find fun. As one of the world’s largest ticket marketplaces, StubHub enable fans to buy and sell tens of thousands of tickets, whenever they want, through desktop and mobile experiences, including apps for iPhone, iPad, Apple Watch and Android.

Bad bots were wreaking havoc on StubHub’s business. Competitors were scraping pricing information and inventory data, customer accounts were taken over by cyber thieves, and bot requests doubled the load on the site causing downtime and skewed analytics.

“Competitive data mining for ticket prices and inventory information was a constant threat.”

Competitor Price Scraping

“Competitive data mining for ticket prices and inventory information was a constant threat.”

As an online ticket marketplace, StubHub exposes proprietary information on its website. Unaffiliated actors go to great lengths to scrape this information, so they can turnaround and sell it to other large ticket brokers or repost it on their own web properties.

How does Price Scraping affect Ecommerce?

If you own an ecommerce site, your website is your business. Competitors use bots to scrape pricing, content, and inventory data. The data shows up on competitor sites improving their page rank, luring your customers away, and costing you revenue.



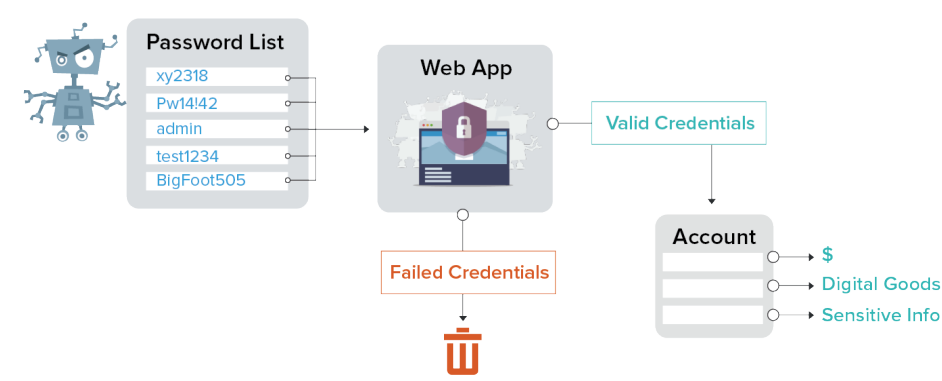
CHALLENGES	IMPERVA SOLUTION
Pricing/inventory information stolen and reposted elsewhere	Pro-actively blocked persistent web scraping campaigns.
Proprietary information sold to competitors	Protected pricing and inventory information
Competitors undercut StubHub’s pricing	Maintained competitive pricing advantage

Account Takeover

StubHub accounts have a lot of value to cyber thieves because of the ease and velocity of purchasing and selling tickets on its platform. The problem is exacerbated by the general availability of stolen login information and password reuse, which gives thieves access to accounts.

How is Account Takeover Performed Using Bots?

This diagram shows a process, known as ‘credential stuffing,’ whereby attackers continuously test login combinations purchased off the dark web, looking for instances of password/username reuse among your customer base.



“Imperva helped us greatly reduce transaction fraud and account takeovers.”

CHALLENGES	IMPERVA SOLUTION
Credential stuffing using Ashley Madison stolen credential list	Prevented credential stuffing bots from accessing site
Account takeover leading to buyer and seller fraud	Lowered fraud
High fraud costs impacting revenue	Improved brand and reputation with customers

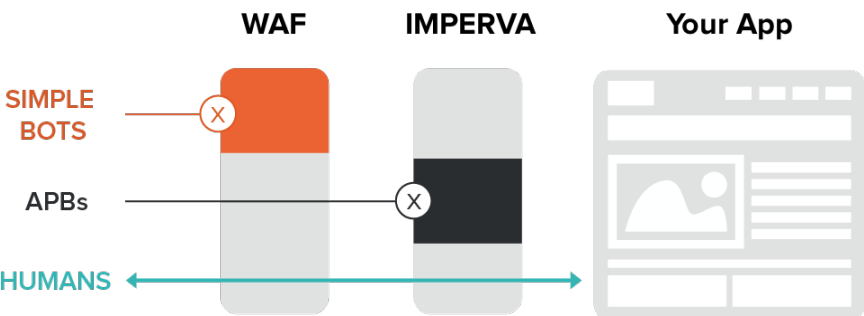
Advanced Persistent Bots (APBs)

“Until recently, bots were fairly unsophisticated. People used cURL or some other non browser based tools to just mine a lot of data off our site. That has morphed into browser based plugins, Selenium, dejaclick—things like that.”

Not all bots are created equal. Advanced persistent bots (APBs) are configured with software that allows them to attack sites from browsers, imitate human-like interactions, and load JavaScript—enabling them to blend in with human traffic. StubHub knew IP blacklisting and rate limiting wasn’t enough to stop these bots.

Am I Protected if I Use a WAF?

WAFs can’t stop APBs, which makeup nearly 90% of all bad bot traffic. Stopping APBs requires advanced fingerprinting technology, behavioral analysis, machine learning, and dynamic access controls. If you are just using a WAF, you’re still an easy target for APBs.



“Until recently, bots were fairly unsophisticated. People used cURL or some other non browser based tools to just mine a lot of data off our site.

That has morphed into browser based plugins, Selenium, dejaclick—things like that.”

CHALLENGES	IMPERVA SOLUTION
User agent string/IP blocking and rate limiting not enough	Behavioral analysis and machine learning
Frequently attacked by bots using browsers and JavaScript	Advanced fingerprinting technology
One attacker used more than 10k IPs in a scraping campaign	World’s largest known violators database

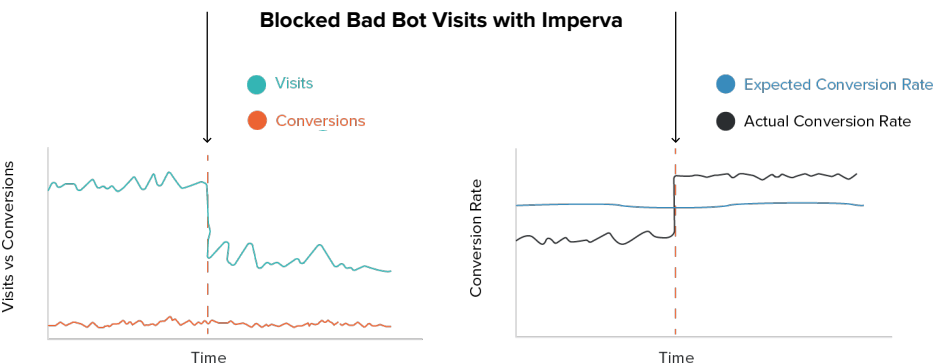
Skewed Conversion Tracking

“The number of conversions were greatly deflated because of bad bot traffic. Now that we’re filtering bad bot traffic out, we’re able to see what the real data is and make decisions based on real visitors.”

As an ecommerce company, StubHub relies on accurate site conversion (number of uniquevisitors vs. number of people that buy) data to run its business. However, half of StubHub’s page views were coming from bad bots, which skewed analytics and lowered conversion rates.

How Do Bots Impact Conversion Tracking?

APBs have gotten so human-like they even trick analytics tools into counting them as visitors. Because these bots create traffic, but aren’t actual customers, they skew the data that goes into your funnel reporting.



“The number of conversions were greatly deflated because of bad bot traffic. Now that we’re filtering bad bot traffic out, we’re able to see what the real data is and make decisions based on real visitors.”

CHALLENGES	IMPERVA SOLUTION
Bad bots doubled the traffic on the site	99.9% of bad bots blocked
Analytics and tracking numbers skewed	Lowered page view traffic by 50%
Artificially low conversion rates and bad funnel reporting	Higher conversion rates and improved sales funnel reporting

Recapturing the Economic Impact of Bad Bots

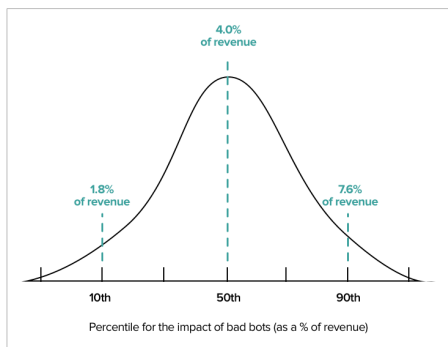
Automated attackers have an impact on the top and bottom lines of online businesses. Their actions add costs to operations, cause data breaches and with them compliance penalties, interrupt current revenue streams, and interfere with future revenue potential. In order to quantify the economic impact of bad bots, Imperva (formerly Distil Networks) worked with research and analyst firm The Aberdeen Group to identify and quantify several bot related issues that effect most online businesses including:

- Over provisioning of website infrastructure (which is wasted on bad bots).
- Wasted web marketing spend and skewed KPI data.
- The cost of data breaches.
- Website slowdowns and downtime due to bot activity.
- Fraudulent online transactions such as account take over and theft.

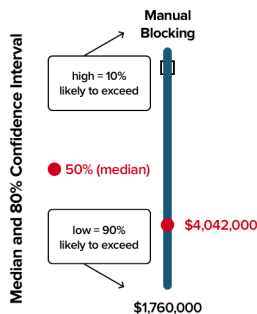
**ABERDEEN
GROUP**

For a web site contributing \$100M / year in revenue

	80% Confidence Interval (\$ / year)		Median (\$ / year)
Manual Blocking	\$1,760,000 1.8%	\$7,600,000 7.6%	\$4,042,000 4.0%



Quantifying the Risk of Bad Bots



ABOUT IMPERVA BOT MANAGEMENT

Imperva Bot Management, the global leader in bot mitigation, protects websites, mobile apps, and APIs from automated threats. Fraudsters, hackers, and competitors use bots to commit online fraud, break into customer accounts, and gain an unfair competitive advantage. As the sheer volume, sophistication, and business damage of these attacks grow, bots put a costly strain on IT staff and resources. Only Imperva Bot Management's unique, more holistic approach provides the vigilant service, superior technology, and industry expertise needed for full visibility and control over this abusive traffic. The Imperva Bot Management team pioneered bot mitigation in 2011, and has been leading the way ever since. With Imperva Bot Management, there is finally a defense against automated attacks that is as adaptable and vigilant as the threat itself.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 [866] 926-4678
imperva.com