SEO Title: Top 5 Bot Threats for the Online Retail Industry | DataDome

Description: The online retail e-commerce industry is under constant attack from malicious bots. Learn about the most dangerous threats and how to stop them in their tracks.

Top 5 bot threats for the online retail industry

Around 30 percent of all web traffic is made up of bad bots[1]. Online retail and e-commerce businesses are constant targets of bad bot attacks such as denial of inventory, scalping, scraping, credential stuffing, and Layer 7 DDoS attacks. What's more, bots are increasingly complex and sophisticated, making detection and deterrence extremely challenging.

Bot attacks can result in poor website performance, site downtime, exposure of sensitive customer data, and lost revenue. It is therefore imperative that online retailers implement and maintain robust security measures against malicious bots.

In this post, we'll examine five of the most dangerous bot threats that online retailers are facing today — and how to stop them.

1. Denial of inventory

In this type of attack, the bot selects items in the online store and adds them to the cart, but never completes the purchase. The result is that inventory gets tied up, and legitimate shoppers may get an "out of stock" message.

A denial of inventory bot will repeatedly add items to the cart on a periodic basis, so even if the cart automatically empties, the bot will return and put them in the cart again. This kind of activity can initiate from unscrupulous competitors trying to gain an unfair business advantage.

As a defense, online retailers may set limits on how long shoppers can hold items in their carts, and on the number of times the same item can be added. However, more advanced bot attacks override these limits by using large numbers of different IP addresses, thus appearing to be many individual shoppers instead of a single item hoarder.

A more effective countermeasure is a specialized bot detection solution which identifies and blocks malicious bots before they can even access the store.

2. Scalping

[1] *Average figure observed over the past 30 days from a traffic sample based on a selection of e-commerce, marketplace and classified ads websites*

Like real world event ticket scalpers, malicious scalper bots buy up limited-edition items to sell them later at a higher price.

Let's say an eagerly anticipated new game console is due to be released. On release date, scalper bots use the power of computer speed to buy up as much stock as possible as quickly as possible. Human customers get an "out of stock" message, with can occur within seconds of the product release, and have no choice but to pay the bot operator's marked-up resale price.

For instance, on launch day, the $80 Super Nintendo Entertainment System Classic Edition sold for an average of $165 on eBay - more than double the original price.

Scalper bots are hard to beat, but a specialized bot protection solution will detect and block them. Malicious attempts are automatically detected 24/7, and can be mapped on a dashboard which enables retailers to monitor bot activity in real time. Also, when a new undesirable bot is identified on one retailer's website, the best solutions will automatically protect all their users against it.

3. Scraping

Bot-driven listing scraping are high-volume attempts to steal listings from online retailer websites. Without asking for end-user consent, dishonest competitors can then add the stolen content to their own listings, or the data can be sold on the Deep Web. In the end, the victim's e-commerce portal receives fewer genuine visitors, which cuts into revenue and damages brand value.

TheFork (TripAdvisor) was experiencing unexplained traffic spikes that didn't match their normal activity peaks (holidays, special offers, etc.). The company knew these were malicious bots attempting to steal value-added content such as user reviews and table availability.

To thwart these bad bots, TheFork implemented the DataDome bot protection solution to ensure that only human visitors and good bots can access the site. As a result, content scraping is no longer a problem, and TheFork has also been able to reduce its hosting and maintenance costs.

4. Credential Stuffing & Credential Cracking

In credential stuffing attacks, malicious bots take stolen credentials (usernames and passwords) from one site and attempt to log in to other sites. Credentials are typically obtained after a massive data breach, and the stolen data is either published online or sold. More sophisticated credential stuffing attacks recruit a large number of bots so that login attempts appear to come from many different devices.

Credential cracking, also known as brute force attacks, use huge attempt volume to "guess" the right combination of credentials. For instance, in a dictionary-type attack, all the words in a dictionary (word list) are tried, one-by-one, to gain access. Cyber criminals use bots to be able to run through such massive numbers of attempts.

Credential cracking and credential stuffing are two means to the same end: accessing and abusing user accounts, also known as account takeover.

With 40 million members, BlaBlaCar is the world’s largest carpool community. The company’s massive database is a tempting target for those seeking personal data for criminal purposes. At one point, BlaBlaCar detected huge abnormal load spikes identified as brute force attacks. The criminals were trying to access user accounts in order to steal credit card numbers and retrieve coupons which could be used or resold.

Advanced bot protection technology makes it possible for BlaBlaCar to block both known bots and new threats, so that their users stay safe. Even better, this does not require any daily intervention by the company’s technical team.

5. DDoS Layer 7

Layer 7 DDoS attacks are designed to target the application layer in the Open Systems Interconnection (OSI) model. The intent is to overwhelm and crash a website with a flood of traffic.

Celio is a leading men’s ready-to-wear brand, present in more than 50 countries with over 1100 stores. The Celio team used to handle bot traffic on a case-by-case basis, monitoring traffic and manually blocking unwanted bots. This was very labor intensive, however, and it is ineffective against attacks using large numbers of varied IP addresses.

Unexpectedly, the company experienced a massive DDoS Layer 7 attack. The bot traffic broke through manual defense efforts, overwhelmed the hard disk logs, and crashed the platform.

Thanks to the DataDome bot protection solution, Celio has been able to eliminate unwanted bot traffic, reduce server load, and stop downtime incidents. A custom rules function also enables them to block human traffic from specific countries or manage access for partner bots, but for the most part, Celio’s team doesn’t worry much about bots anymore.

Discover the DataDome bot protection solution

Ready to put an end to bot-related security issues for good? Try DataDome for free for 30 days!

Set up the trial up at your own pace (it typically takes less than an hour), and start observing your bot traffic in real time today.