What is Bot Traffic?

perimeterx.com/resources/learning-center/block-bots

When people visit your site to view your products and make purchases, that's human traffic. When automated software — also called a bot — visits your site, that's bot traffic.

Bot traffic can be both good and bad. Google, for example, has bots catalog your site and its contents, so that it appears in search results. Here are some examples of good bots:

- Search engine web crawlers for enhanced indexing
- Chatbots for customer service
- Monitoring bots for website analytics
- Testing bots for website performance
- Marketing bots for optimizing display ads
- Virtual assistants for boosting productivity

But bots aren't all positive. Cybercriminals leverage bad bots to validatel your consumers' credentials, payment card data and other personal information for use in credential stuffing, carding and account takeover (ATO) attacks. Malicious bots extract your pricing and product content in web scraping attacks, giving your competitors an edge. They buy up your inventory and resell at inflated prices in scalping and denial of inventory attacks.

How to Identify Bot vs. Real Human Traffic

Bot traffic is different from human traffic. Bots can execute tasks much faster than people, and bot traffic comes in much higher volumes than human traffic. You'll see bots produce record-high numbers of page views in an instant. Human users usually do several different actions and clicks at a more moderate pace.

Bots spend both significantly more and less time on your site than human visitors do. If web sessions start and end very quickly, it's typically a sign that a bot is crawling your site much faster than a human ever would. Exceptionally long sessions mean that a bot is browsing the site very slowly. Web sessions for humans are more consistent in duration than for bots.

Next is their behavior once they land on your site. Bots often visit a page, but do nothing once they get there. Instead of navigating predictably through your site or purchasing products, they might just visit a page and leave. This can be seen in unusually high bounce rates and, sometimes, lower conversion rates as well.

Another way to identify bots is through the use of honeypots. This might mean adding a hidden HTML input element to a page that legitimate human users are not able to see — so if a user accesses the element, you can be sure it's a bot. Another technique is to stack two

clickable elements in the same place on a page. A legitimate user can only click on the upper element, while a bot automatically will click on both.

In addition, you can consider the source of suspect traffic. Bots may invade your site from geographies where your customers don't live, and the inhabitants don't use the language on your site. This is an indication that visitors aren't human.

Website owners can analyze server logs to identify malicious bot traffic hiding inside legitimate site traffic. Specific signals can help you to flag bot activity on your site. For example:

- When bots test usernames and passwords by stuffing long lists of credentials into your login screens, you'll see an increase in login failures and password reset requests from real customers whose accounts have been part of the test.
- When bots test credit and debit card numbers, you'll see a surge in failed transactions.
- When bots create high volumes of fake accounts, you'll see new accounts appearing at a rapid pace.

Impact of Bot Traffic on Your Business

Bot traffic negatively affects your organization by driving flawed business decisions, diminished site performance and lower search engine rankings — which can all lead to competitive disadvantages.

Automated traffic taxes your infrastructure and increases your costs for bandwidth and compute cycles. Bot traffic can overwhelm your network and slow site performance, which frustrates customers and negatively impacts user experience.

Search engines consider your site's speed as a factor in positioning your site among search results. Your site can appear lower in search due to the effects of bot traffic, which can keep consumers from finding you.

In addition, bot traffic skews your analytics — for example, by appearing to show an increase in consumer demand. Flawed metrics on user behavior can lead you to make poor business decisions about pricing, stocking goods, and investing in marketing and advertising.

These outcomes are byproducts of bot traffic itself. But perhaps more damaging is what cybercriminals can use bots to do. Malicious bot traffic means bot attacks to validate stolen information on your site. These include:

- Credential stuffing - Bots attempt logins across popular sites using stolen credentials. Validated credentials can be used in future account takeover attacks or sold on the dark web.

- Carding - Bots test stolen credit and debit card numbers by making small purchases on e-commerce sites. Validated payment details can be used to make larger purchases of gift cards and high value goods.
- Account takeover (ATO) - Cybercriminals use stolen credentials to gain unauthorized access to user accounts. This allows them to make fraudulent purchases with stored payment data, steal gift card balances or loyalty points, and commit other types of fraud.
- Scalping and inventory hoarding - Bots buy up high-demand products and sell them at inflated prices on third party sites. This frustrates users and drives them off your site to shop elsewhere.
- Web scraping attacks - Hackers use bots to scrape your pricing information, product descriptions and other content to gain a competitive edge. This can also harm your SEO rank.

Successful bot attacks drive financial losses due to chargebacks, credit processing fees, infrastructure costs, and the need for more internal resources from engineering, security and customer service teams — not to mention potential lawsuits and regulatory fines. Furthermore, bot attacks damage brand reputation and consumer trust, which negatively impacts long-term revenue, stock value and business growth.

Learn how to beat bad bots!

Read E-book

How to Block Bots from Attacking Your Web and Mobile Apps and APIs?

You can do several things to prevent bots from crawling your web and mobile apps and APIs.

Monitor your site for malicious bot traffic

You can gain visibility by monitoring your site for malicious activity. Once you establish a baseline of typical human behavior, you can compare and contrast suspected bot activity. When visitors and accounts reach a threshold of likely bot behavior, you can trigger alerts and automated responses to block them.

Challenge the bots to prove they are human

You can challenge bots to prove they are human when you suspect malicious behavior using a problem that only real people can solve. A CAPTCHA is one example of this, though sophisticated bots can beat those tests. Furthermore, CAPTCHAs often frustrate human users, driving abandonment. Human Challenge, an alternative human verification system, keeps bots out while preserving the user experience.

Limit the rate of bots' illicit behaviors

You can frustrate malicious bots by limiting the rate of their repetitive behaviors. Bots often make many login or payment attempts in a short amount of time. Rate limiting slows the process, so cybercriminals move to easier targets with quicker payoffs. However, using something like a web application firewall (WAF) to rate-limit traffic is not enough to block bots on its own. WAFs cannot detect bots that piggyback on real users' identities and mirror their behavior, nor can they recognize botnets that rotate through thousands of different IP addresses to bypass IP-based rules.

Require proof of work

The proof of work (PoW) technique requires computational effort to be expended before logging in, verifying a payment method or executing another task. PoW consumes a large amount of energy and CPU cycles at scale, which places a cost burden on attackers trying to do many fraudulent activities at once. Because of this, PoW makes it expensive for hackers to complete their attacks and disincents them from launching future attacks against your site.

Block the connection

Once you confirm malicious bot activity, you can block bot access using block pages, redirect the malicious traffic or block the internet address responsible for the bot traffic.

How can PerimeterX Bot Defender Help with Blocking Bots?

PerimeterX Bot Defender detects and blocks bots with unparalleled accuracy. The solution uses machine learning, behavioral analysis and predictive methods to protect against bot traffic to web and mobile apps and APIs. The algorithms evolve in real time, becoming more sophisticated as bots do.

By blocking unwanted bot traffic at the edge and optimizing the use and performance of your web infrastructure, Bot Defender preserves page load performance, and optimizes security resources and infrastructure costs. The solution enables your team to focus on innovation and growth, instead of chasing down bad bot traffic.

Bot Defender offers a layered barrier against bots attacks, wherever they happen along your users' digital journey. Learn more about how PerimeterX can help you manage bot traffic.