WHITE PAPER

A comprehensive guide to bad bots

What you need to know to protect your digital business from costly bot attacks

White paper in partnership with PerimeterX

perimeterx

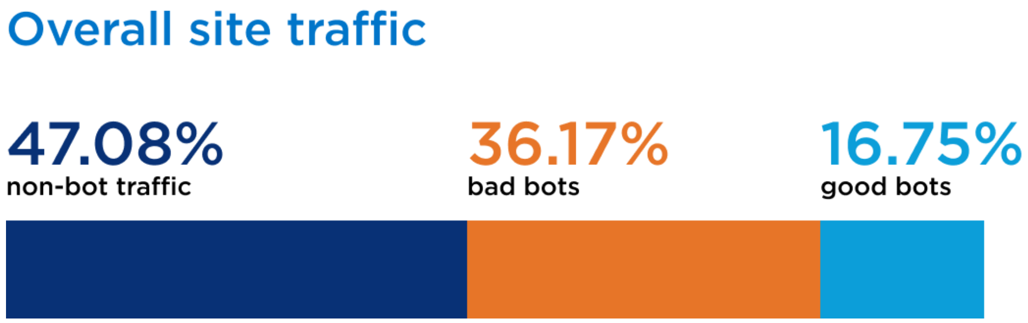
LUMEN®
TECHNOLOGIES

Introduction: what you need to know about bots

Did you know that there are likely more bots than real people using your company's website? According to the PerimeterX research team, good bots constitute 16.75% of overall site traffic, while bad bots account for 36.17%.

Cybercriminals have developed bots to be more sophisticated and difficult to decipher, giving them humanlike fluidity through your site. It is therefore important to understand what they are, how they've evolved and the impact of bots to your digital business. Your competitors may even be utilizing bots to scrape your content to compromise your competitive edge.

This white paper covers various concepts around bots. After differentiating good bots from the bad ones, we shed light on how bad bots can compromise a business. We will then discuss seven key capabilities required to battle today's sophisticated bots.



Getting familiar with bots

What is a bot?

The term bot is short for robot and is a generic term for software that runs automated tasks over the internet. There are many different types of bots, both good—used for productive purposes—and bad—used for malicious activities. The inability to identify them and to block malicious attacks can cause more harm to your online business than you may realize.

What is a botnet?

A botnet is a network of internet-connected devices infected with malicious software and controlled as a group without the device owner's knowledge.

The business impact of bad bots

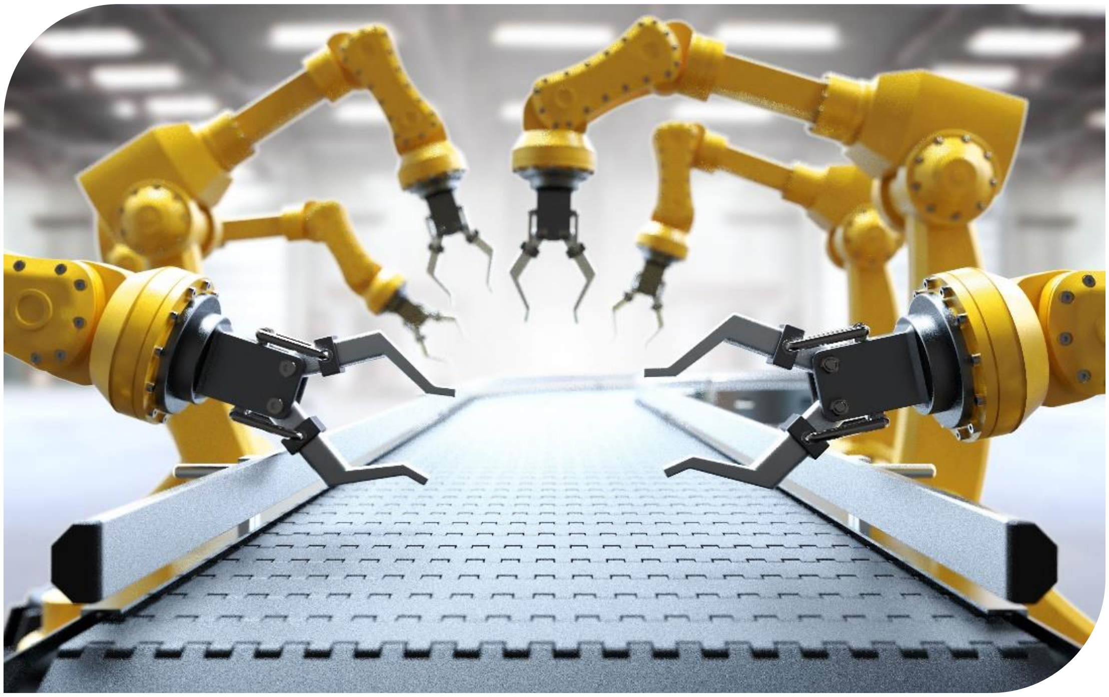
- Lost revenue
- Tarnished brand reputation
- Declining customer loyalty
- Faulty business decisions
- Loss of competitive edge
- Risk of data breaches
- Loss of PII user data
- Non-compliance of governing regulations
- Decreased operational efficiency
- Increased operational and support costs
- Mounting customer complaints

What are examples of good bots?

Good bots are used for beneficial, automated tasks such as:

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

More than 50% of web traffic comes from bots.



What are examples of bad bots?

Bad bots are used to run automated malicious tasks or competitive research schemes, including:

Account takeover (ATO)

Bots perform credential stuffing, hijack user accounts or create new fake accounts to commit fraud, such as retrieving funds or goods without payment, both online and offline, using cloned gift cards or prepaid loyalty cards.

Scalping

Bots buy or hoard limited availability and highly sought-after products, forcing customers into secondary markets where these sellers can create higher demand and generate large profit margins.

Carding and gift card cracking

Bots test stolen credit card data or try to guess and validate gift cards on merchant sites, then, armed with legitimate card data, make large unauthorized purchases. APIs can experience different types of attacks and abuses versus a web app or webpage.

Skewed analytics

Bots repeatedly click on online ads, attempt logins, create fraudulent accounts, browse product pages and add items to cart without completing checkouts, which distorts the web analytics that are necessary for making business decisions and reduces the effectiveness of marketing spend.

Denial of inventory

Bots continuously add best-selling products to carts or hoard perishable products like movie or concert tickets, airline seats or hotel rooms, artificially depleting availability, denying products to legitimate customers, blocking sales by keeping inventory out of stock and forcing customers to competitive sites.

Web scraping

Bots from competitors steal prices, curated content, product reviews, inventory data and more to capture your business prospects in their direction.

Identifying a bad bot problem

Bad bots can harm any online business. They have become so sophisticated that they often go undetected because of the human-like behavior built into them today. And the development of malicious bots will continue to evolve as cyber criminals continue to look at ways to infiltrate online businesses. There are a number of signs that may indicate that your business is under attack from bots.

Increased shopping cart abandonment

Denial of inventory is a malicious attack. Cybercriminals unleash automated scalping bots to buy sought-after products, tying up your inventory and preventing sales to legitimate customers. By hoarding a high-demand product, bots keep it out of stock, annoying customers, taxing your infrastructure, reducing conversions and revenue.

Your original content displayed on non-approved sites

Web scraping bots continuously capture pricing data and product descriptions at scale that can give your competition an advantage. Competitors or scammers scrape your content and publish it to steal search traffic away from your site and offer potential customers better pricing.

Reduced website conversation rates

With bots often accounting for more than half of web traffic, lost revenue and investments from bad business decisions made due to skewed analytics can be significant, ranging from millions to a few billion dollars. Bots skew many KPIs and web metrics, including user tracking and engagements, session durations, bounce rates, ad clicks, look-to-book ratios, campaign data and conversion funnels.

Increased login failures

Attackers typically buy a list of credentials on the dark web and launch an army of bots across popular retail, travel, social media and e-commerce sites to test username and password combinations and spiking login attempts to gain access.

Spike in account creations

Another type of ATO happens when bots create new accounts that are not linked to real users. Fake accounts are leveraged for other attacks or fraudulent transactions.

Unknown geographical traffic

If a wave of web traffic comes from locations where your customers don’t live or where you don’t offer your service, then you may be under attack.

Increased gift card or point validation failures

A rapid rise in gift card validation failures often means that bots are trying to identify which gift card accounts have large balances that can be stolen and sold on the dark web. Similarly, travel or account points are often under attack to be stolen and sold illegally.

> **“Up to 95% of all login attempts during significant account takeover (ATO) attacks are malicious.”**
>
> **- PerimeterX, 2022**

Traditional techniques no longer work: it’s time to upgrade

Given the rapidly evolving bot landscape, many solutions available today are ineffective in identifying and blocking bot attacks.

Technique	Description	Why it’s not enough
Rate limiting	Limits the number of times that any given device or user, represented by an IP address, can request information or otherwise access the application.	Rate limiting can’t detect more sophisticated attacks coming from many different IP addresses, typical of today’s botnet-powered attacks. Bots are effective at finding the limit and remaining below it, which lets them operate and cause cumulative damage for long periods of time.
IP reputation	Identifies the likelihood that any given IP address has been compromised by a bot, relying on historical malicious activity seen from that IP address.	Sophisticated bots operate from infected devices and from within legitimate networks. IP reputation is ineffective at identifying infected users. Moreover, relying on IP address only leads to false positives, as a single, infected device can “burn” all other (legitimate) users in that network.
Signature-based	Relies on signature databases that contain information on the characteristics of historical bot attack software	More advanced attackers overcome signature-based detection by changing the parameters of the attack. Using historical, static signatures is not effective against new, never-before-seen attacks.
Network-based	Evaluates different characteristics of network traffic such as network statistics, types of communication protocols, suspicious traffic behavior and malicious action types	Low-and-slow and widely scaled-out attacks are difficult for network based behavioral algorithms to detect. By recording a legitimate user and then replaying the recording with modifications, bots can easily copy network-based identifiers.

Seven key capabilities for battling today’s sophisticated bots

Once you’ve noticed signs or have evidence that bad bots may be impacting your online business, the next question is how to stop them. And perhaps the bigger question long term is how do you ensure you have the capability to keep up with the evolving sophistication of bot attacks? Unfortunately, bad bots and the people who use them continue to gain the upper hand on unprotected websites.

Today’s bots, unlike the more crude, basic bots of the past, are becoming more adept at **mimicking actual users** and disguising their true purpose. Protecting your digital business against sophisticated bots requires advanced bot detection and mitigation software that incorporates machine learning and predictive analytics to achieve high levels of detection accuracy. A comprehensive solution that incorporates the various elements outlined below is key to beating bad bots.

Seven key capabilities required

Capabilities	Description
Attack detection	At the very minimum, platform with the ability to identify bot attacks on any channel - i.e., websites, mobile apps and APIs – is required. To combat bots, the solution needs to identify today's sophisticated bots that have human-like behavior using advanced techniques and utilizing data collected over time that continually tune its algorithm. The detection techniques should be accurate in identifying good bots vs. bad bots with optimal accuracy and with few to no false positives in the detection process.
Attack response	While accurate attack detection is important, it doesn't do much to help if the solution isn't able to respond. An effective solution must be able to provide alerts to attacks, cut off attacking sessions, deny entry, and protect the website or mobile app effectively. The solution should have built in capabilities to foresee bot attacks and to mitigate risks automatically.
Ongoing threat detection	Bots' sophistication will only grow as criminal minds are always in the market to infiltrate businesses. The challenge is staying ahead of the game, and the ability to detect and mitigate future attacks automatically is key.
Bot management / ease of use	Bot management through a centralized UI for creating customized rules to modify attack detection and responses is essential. The bot management interface should be intuitive and easy to set up, without adding any complexity to the security operations or site recovery roles.
Scalability without loss of performance	When implementing any solution, the first imperative is ensuring your website or mobile application doesn't suffer the consequences from your bot protection software. Users are easily distracted and will leave your site if they think performance is slow. The ability to have little to no website and application performance impact is a top requirement.
Low latency out-of-bond approach	Addressing latency requires a new approach to bot management processing user traffic metadata out-of-band in real-time and performing enforcement inline as close to the edge as possible. This out-of-band approach has the added advantage of enabling bot management solutions to work with existing web technology stacks without adding any additional layers of traffic processing.
Key integrations	Out-of-the-box integrations with your platforms and applications is important for fast and easy deployment into your existing infrastructure. Your bot management solution should come with the ability to translate bot detection to other applications that rely heavily upon the data.

Protecting your business with comprehensive bot management

PerimeterX Bot Defender on Lumen uses machine learning and behavior-based analytics to help ensure that your website or application is protected against bot threats by tracking attack patterns, fingerprinting devices and monitoring network characteristics to stop attacks at the source.

Pre-integrated into the Lumen global edge, PerimeterX Bot Defender can be up and running in a matter of hours without complex development work. Your properties can be protected around the cloud while preserving end-user experience and page response times.

PerimeterX Bot Defender on Lumen provides a comprehensive solution that goes beyond the required capabilities to battle today's sophisticated bots so that you can focus on growing your business. Bot Defender can help your business grow stronger against sophisticated bot attacks now and in the future. Get started today!

> “PerimeterX Bot Defender is the best fit for companies that interact with users across multiple channels - web, mobile and API.”
>
> The Forrester New Wave™: Bot Management. Q1 2020

PerimeterX is the leading provider of solutions that detect and stop the abuse of identity and account information on the web. Its cloud-native solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world’s largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers’ digital experience while disrupting the lifecycle of web attacks.

PerimeterX is headquartered in San Mateo, California, and at www.perimeterx.com.

Why Lumen?

With global network scale and dedicated focus on improving business outcomes, Lumen is trusted by many of the world’s leading enterprises to help them create new and differentiating user experiences all over the globe. Whether you are delivering video streams, popular games, online storefronts, or next generation applications, the broad capabilities of Lumen edge security and delivery services enable businesses to stand out from the crowd.

Disclaimer: This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue.

lumen.com | application.delivery@lumen.com