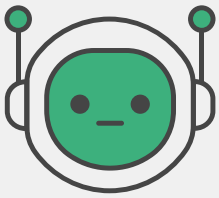
POINT OF VIEW

Bot or Not?

Sophisticated, Malicious Bots Can Bypass Security by Mimicking Human Behavior

Executive Summary

Over the past few years, bots have become more sophisticated. They can now mimic human internet users' behavior, making it more difficult for older security solutions to detect and block malicious bots. Organizations need new tools that distinguish bots from human users and good bots from bad bots. The weaponization of bots has become a major threat to websites, APIs, and mobile applications, so selecting the right advanced protection solution is critical.



According to recent studies, roughly half of internet traffic is bot-generated. And about half of this half is bad bots.[1]

The Risks Associated with Automated Threats

The Open Web Application Security Project (OWASP) has mapped 21 categories of automated threats with adverse impacts that affect the privacy and security of individuals, applications, and system components, causing financial, operational, security, and reputational damage.

As bots get more advanced, organizations struggle to separate them from real humans. For example, bots are increasingly used for online fraud, which causes direct revenue loss for businesses. Activities like gift card fraud, account takeovers, inventory scalping, and digital skimming can rob companies of millions in sales. Bots also commonly spread spam and phishing scams, further damaging brand trust and reputation.

Organizations face destructive downtime issues when bot floods are used for crushing servers with traffic to severely downgrade website response times or even take sites offline completely. These denial-of-service attacks also hurt site performance indirectly by hogging bandwidth and resources.

Bots are often used to harvest user accounts and confidential data through web scraping and unauthorized access. They probe sites for vulnerabilities and can infiltrate backend systems to steal financial information, intellectual property, and other sensitive assets. This infiltration often leads to dangerous data breaches.

Organizations can also face regulatory compliance risks related to data protection from bot activity, and comment spamming by bots can ruin the user experience and damage a brand's reputation. An organization's SEO rankings can also be affected when bots copy and redistribute content.

A few other real-life examples of bad bot activity include:

- Users are unable to buy concert or airline tickets because of bots hoarding the inventory
- Coupon scraping by a bot that leaves club members frustrated
- Copied and repurposed websites that compete with the original
- Cracking user credentials to break into banking or e-commerce accounts
- Inflating digital marketing campaign budgets through fictitious clicks

The Evolution of Bot Attacks

In cybersecurity, threat actors are typically one step ahead. When a new threat or attack vector emerges, the security industry then follows with a solution. In the past, bots were simple scripts that could be identified by network firewalls based on an IP address or by using reputation or signature feeds. The next generation of bots used IP rotation tools to bypass these defenses, so a bot came from a different IP address in each request. Bots then escalated and began rotating web browsers until web application firewalls started to fingerprint devices and user agents to detect and block these attacks.

However, bots now can mimic user behaviors, such as fictitious mouse movements or keystrokes. Threat actors have learned, for example, that real users type their password characters much slower than bots do, so they adapted their approach. And they figured out that fixed intervals between bot actions are easy to program but also easy to detect, so they randomized the intervals.

Some bots now are sophisticated enough to bypass CAPTCHA, which uses the Turing heuristic to tell a human from a machine. Bot operators sometimes hire individuals to solve the CAPTCHA and let the bot do the rest.

Defend against Bot Attacks

With various use cases, bot behaviors, and threat indicators, today's solutions to protect against bots must be intelligent. They need to be able to identify, correlate, and analyze all suspicious traffic to an application. Unfortunately, many organizations still spend time and resources attempting to enhance web security by creating their own scripts and customized rules to complement the shortcomings of older solutions. Generally, their efforts are unsuccessful because attempting to address all the possible scenarios is next to impossible. Rotating IP addresses and device IDs, changing browsers, generating fictitious keystrokes and mouse movements, operating at random intervals rather than fixed, and even solving CAPTCHA have all fooled legacy solutions.

In the face of these challenges, a new bot management category of solutions has emerged in the cybersecurity industry. This new wave of solutions takes a more methodical approach to distinguishing between humans and good and bad bots.

These new solutions first look at indicators of known bots or simple bot behaviors. In parallel, they build a data lake of bot attack patterns and good bot behaviors that can be used for training machine learning models. These models bring together the metadata from each incoming request (IP, user agent, device history) with biometric challenges and behavioral factors. As the models grow, they improve the detection accuracy, with the ultimate goal being to determine whether a request is coming from a human, a good bot, or a bad bot that poses a threat.

The Impact of Bad Bots

Although good bots can automate tedious tasks and accelerate business operations, bad bots are programmed to take over user accounts, steal data, and disrupt services. Bad bots are a serious cybersecurity concern because they can easily bypass common defense strategies. In the face of these threats, organizations must reevaluate the impact of bot attacks on their business and the investments in security they need to make. To protect against bots, organizations must move away from legacy options and secure their digital assets and activities with advanced solutions.

[1] CPO Magazine, Bad Bots Account for 30% of Internet Traffic and Are More Frequent in Account Takeover and API Attacks, May 30, 2023.

January 12, 2024 2:21 PM

2510872-0-0-EN