Shape
Part of F5

BAD BOTS: THE FIRST STEP TO COMMITTING FRAUD

Bots reduce costs for basic and repetitive tasks and can improve business intelligence and customer engagement. Bots also reduce costs and scale attacker arsenals. The question becomes intent – is this a human and potential customer, a search engine bot part that could improve SEO, or is this bot part of an automated credential stuffing attack that may lead to account takeover, fraud losses, and poor business outcomes?

Benign Bots

Search Engine Bots
Crawl the Internet fetching data used by search engines.

Aggregator Bots
Collect and propagate information from 3rd parties.

Commercial Bots
Monitor news reports or customer reviews or ad networks to help marketers optimize their audience.

Chatbots
Provide human-like service through text or voice to responses to your queries.

Malicious Bots

Credential Stuffing
Leverage stolen credentials to automate large scale account takeover.

Fake Accounts
Perform money laundering via online banking and abuse customer loyalty/reward programs.

Credit Application Fraud
Impersonate identities and perform fraudulent transactions that could result in chargeback losses.

Gift Card Cracking
Identify and steal gift card balances with value.

Scraping
Collect proprietary data that can lead to negative business outcomes like intellectual property theft.

Application Denial of Service (DoS)
Degrade performance and impact user experience that could lead to revenue and customer loss.

Aggregator Fraud
Leverage aggregators as a backdoor into banks in order to implement fraud.

Detecting Bot Attacks

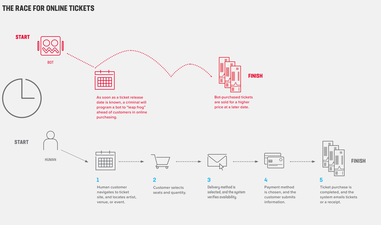
Benign bots can benefit the business. Bad bots can break the business. Blocking all bots is not a realistic option. How can you detect and block the bad bots before they disrupt operations and commit fraud without causing friction for real or potential customers?

1. **Rate-limit traffic** to keep legitimate traffic flowing on your website while you investigate suspicious ones
2. **Identify** known bots using dynamically updated signatures
3. Use **Reverse Domain Name System (DNS)** lookups to validate search engine requests
4. **Challenge requests** to verify they are not from an automated script
5. **Look for suspicious behavior** such as high or irregular traffic patterns and attempts to access restricted files or data using non-compliant searches
6. **Assign risk scores to sessions** by using a combination of these methods to add or subtract points to a risk score - then decide when and what type of action you want to take against risky clients
7. **Analyze device, network, and environment signals** to uncover anomalous behavior such as login success rates, devices per user, users per device, and variations in IP addresses, user agents, session data
8. **Detect human behavior** using artificial intelligence (AI) and machine learning (ML) based on organizations with similar attack profiles and risk surfaces
9. **Adapt** to attackers that attempt to bypass countermeasures while maintaining full efficacy
10. **Extend protections to APIs and mobile apps** which are a growing target for automated attacks that use bots

Let Humans and Benign Bots in and Keep Malicious Bots Out!

In this online ticket purchasing scenario, the deck is stacked against a human trying to get to the finish line of making a purchase before a bot can grab tickets. When the tickets are sold out, a fraudster can sell them at a higher price at a later date.

THE RACE FOR ONLINE TICKETS



Winning in the Age of Bots

Filter out malicious bot traffic to get good business intelligence and prevent fraud while maximizing customer experience.

Focus on the Business...

1. Prevent excessive cloud charges and security team distractions due to bot traffic.
2. Stop credential stuffing attacks that can lead to data breaches and account takeovers.
3. Mitigate sophisticated fraud that uses bots and automation to imitate human behavior.

...By Beating the Bots

Know the logic to Human Behavior: Detect human and non-human traffic and identify intent using artificial intelligence and machine learning based on organizations with similar attack profiles and risk surfaces.

Be first to market but not first to breached: Protect mobile applications and APIs that are increasingly being targeted by bots and automated attacks.

Protect current and potential customers: Prevent attacks that steal sensitive information directly from the user's browser or mobile device.

Protect the user experience: Detect and block malicious bots without friction to keep customers happy and analytics accurate.

For more information about how proactive, multi-layered bot protection can help your organization deliver optimal application security, visit f5.com/bots.