Bad Bots: The First Step To Committing Fraud

Bots can be beneficial to businesses, automating repetitive tasks and providing faster customer service. But, in the wrong hands, bots can also be a powerful weapon for cybercriminals to mount attacks and commit fraud. The ever-evolving digital threat landscape requires that security and fraud teams be able to identify and block "bad" bots before they can steal data, steal money, or cause other harm. So, how well do you know your bots?

Beneficial Bots

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

Aggregator Bots
Collect and consolidate multiple data sources (or bots) into a single bot.

Commercial Bots
Monitor news feeds, customer reviews, ad networks, etc. to gain additional customer insights.

Chatbots
Provide real-time, interactive customer service through text or voice responses.

Malicious Bots

Credential Stuffing
Leverage stolen credentials to automate large-scale account takeovers.

Fake Accounts
Perform money laundering via online banking or 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 cards that have a positive balance.

Scraping
Collect proprietary data that can lead to intellectual property theft or other negative outcomes.

Application Denial of Service (DoS)
Degrade application performance and impact user experiences that can lead to lost customer trust and lost revenue.

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

How to Block Bad Bots

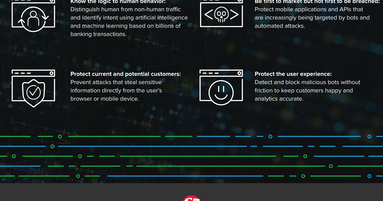
Security and fraud teams don't need to fight an army of bots alone. By joining forces and partnering with F5 Shape to bolster their real-time bot defenses, they can mitigate bot attacks before those attacks compromise security, commit fraud, or degrade customer experiences. Here are ten ways that F5 Shape can help today:

1. **Rate-limit traffic** to keep legitimate traffic flowing on your website while you investigate suspicious traffic.
2. **Identify** known bots against a vast and continuously updated library of real-time attack signatures.
3. Use **Reverse Domain Name System (DNS)** lookups to instantly 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 unauthorized attempts to access restricted files or data using non-compliant searches.
6. **Assign risk scores to sessions** based on trusted/suspicious behavior, 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, and variations in IP addresses, user agents, or session data.
8. **Detect human behavior** using artificial intelligence and machine learning based on organizations with similar attack profiles and risk surfaces.
9. **Adapt** to attacks that attempt to bypass countermeasures.
10. **Extend protections to APIs and mobile apps** – a growing target for automated bot attacks.

It Isn't Easy to Beat the Bots

In the example of an online ticket purchase, 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, fraudsters can then sell them at a higher price at a later date.

THE RACE FOR ONLINE TICKETS



Fraud Prevention, Security, and F5 Shape: Stronger Together

Now, more than ever, financial services organizations need to embrace new innovations such as digital banking and mobile apps without compromising security, compliance, or convenience. Fraud prevention and security teams can't fight the battle against the bots alone, but together with F5 Shape they can present a united, resilient front that helps them:

Deliver a Better Banking Experience...

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 Being Smarter than the Bots

Know the logic to human behavior:
Distinguish human from non-human traffic and identify intent using artificial intelligence and machine learning based on billions of banking transactions.

Be first to market but not first to be 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 on how F5 Shape's proactive, powerful bot protection can help your organization securely deliver the financial services of the future, visit f5.com/bots.