INDUSFACE™

BAD BOTS ARE ON THE ATTACK, WHAT IS YOUR BOT PREVENTION PLAN?

You've probably heard the terms bots and botnets in recent news about cybersecurity risks. But what exactly are they?

A bot is an application, which automatically performs tasks that humans might otherwise do. Not all bots are bad, but some bots out there use their powers for malicious activities or attackers do it through them.

Botnets are a collection of connected devices that typically comprises compromised servers or servers, affected by a set of malware or malicious software.

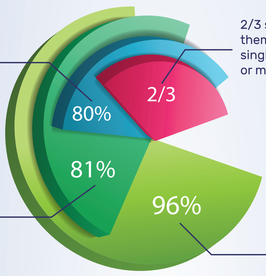
Botnets are capable to carry out various kinds of attacks including:

1. Malspam campaigns
2. Click Fraud
3. Bitcoin Mining
4. Distributed Denial of Service
5. Account Takeover
6. Payment Card Fraud
7. Application Abuse
8. Scraping and Data Theft

Impacts of Bot Attacks

80% of organization faced financial loss because of more sophisticated bot attacks

2/3 say a single bot attack has cost them $100,000 or more and 1/4 say a single attack has cost them $500,000 or more in the past year



Businesses often face issues related to bad bots

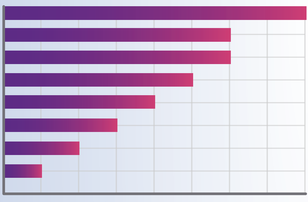
The organization say good bots are vital to their company's eCommerce success, yet 80% have lost revenue to malicious bots

Data source: kount.com

What Are the Consequences of Bot Attacks?

Malicious bots can steal customer information, crash a website, create fake accounts, frozeninventory, stop order fulfillment, and cripple customer service.

Consequences of Bot-Related Attacks



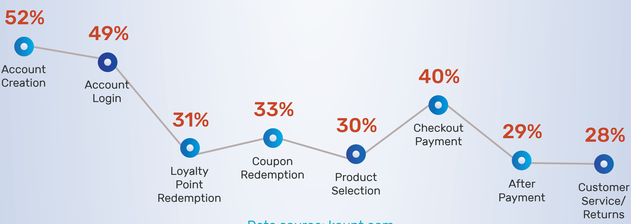
59% Crashed website
46% Compromised customer information
46% Influx of fake customer/user accounts
44% Frozen Inventory
38% User/Customer account hacks
29% Halted order fulfillment
12% Proprietary information leaks
1% Others

46% say malicious bots have led to an influx of fake customer accounts

Data source: kount.com

Where Do Malicious Bots Occur in the Customer Journey?

Bad bots concentrate every part of the customer journey:



Data source: kount.com

5 Signs That You're Under Bot Attack

1. Abnormally high web-server CPU load
2. Non-native traffic profiles
3. Devices crash for no apparent reason
4. Internet connection slowed down significantly
5. Browsers in your network feature unknown components

How to Prevent Your Business from Bot Attacks?

1. Monitor Incoming Traffic and Analyze Its Sources
2. Practice least privilege principles among employee
3. Protect every bat bot access point
4. Monitor for failed login attempts
5. Keep your software up to date

Implement Advanced Bot Mitigation Solution with Indusface

AppTrana's bot mitigation gives you full control over legitimate and malicious bots

Indusface's Advanced Web Application Firewall protect mission-critical websites, applications, and APIs from automated attacks without affecting the entry of legitimate traffic.

Our holistic approach offers the superior technology, industry expertise, and vigilant service needed for complete visibility and control over human and automatic traffic.

Advanced bot management is a component of Indusface's market-leading, fully managed web application firewall, AppTrana, which brings defense-in-depth to a new level.

DATA REFERENCE

https://go.kount.com/industry-report-bot-impact.html
https://www.indusface.com/web-application-firewall.php