Anti-Bot in Online Handel/Websites

By Nicolas Trussardi and Anton Urbanek

Inhaltsangabe

Einleitung

Allgemeine Informationen

"An Anti-Bot system is a technology or process put in place to stop bad Bots."

"A 'Bot' – short for robot – is a software program that performs automated, repetitive, pre-defined tasks."

"It detects bad Bots by using machine learning algorithms."

The rise of Anti-Bots

- Bots machen ca. 50 % des Internetverkehrs aus
- 50 % dieser Bot-Aktivitäten sind böswillig
- Anti-Bots können solch böswillige Aktivitäten erkennen und diesen Zugriff sperren
- Relevanz für E-Commerce und auch Website-Betreiber

Anwendungsbereiche

- E-Commerce Websites

- Internet of Things (IOT)

- Spam

- Standard Websites
  - Educational Websites
  - Blogs
  - Entertainment Websites
  - Forums
  - Social Media
  - Institutional Websites

Bot Detection

1. Delay between actions
2. IP address
3. Action patterns
4. Cookies
5. Number of requests
6. User-agent

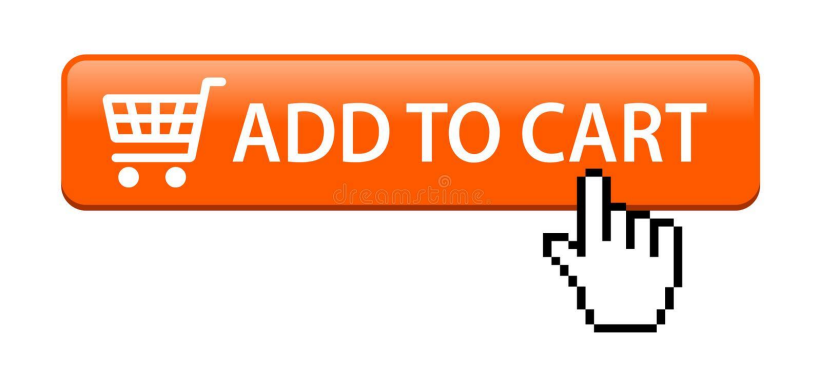

Abb. 1: Add to Cart

Abb. 2: Cookies

Abb. 1: https://thumbs.dreamstime.com/z/add-to-cart-201101236.jpg
Abb. 2: https://www.footlocker.at/

Damage/Bot Prevention

1. IP ban/rate-limit
2. Limit gleichzeitige user (Queue)
3. Log in authentification
4. User-agent
5. Obfuscation of scripts

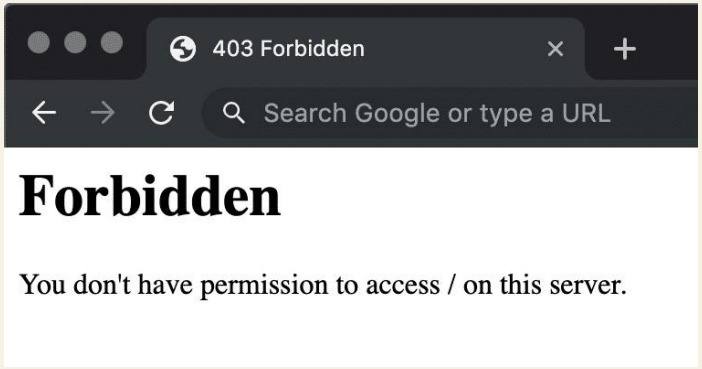

Abb. 3: Permission to Access

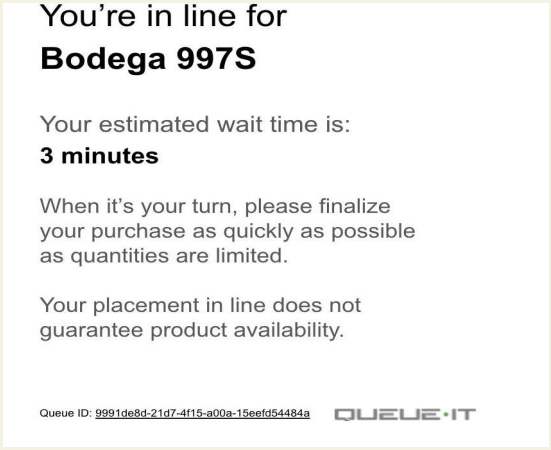

Abb. 4: Access Queue

Abb. 4: https://bdgastore.com/

Anti-Bot Systeme von Drittanbietern

- DataDome
- Kasada
- Akamai
- Perimeterx
- CloudFlare
- reCAPTCHA / hCaptcha
- Queue-it
- Cequence

Abb. 5: Akamai Logo

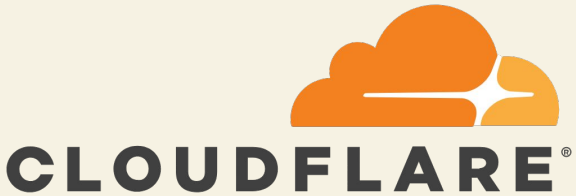

Abb. 6: CloudFlare Logo

Abb. 7: reCAPTCHA

Abb. 5: https://upload.wikimedia.org/wikipedia/commons/thumb/8/8b/Akamai_logo.svg/1200px-Akamai_logo.svg.png
Abb. 6: https://upload.wikimedia.org/wikipedia/de/a/a2/Cloudflare_logo.svg
Abb. 7: https://upload.wikimedia.org/wikipedia/commons/thumb/a/ad/RecaptchaLogo.svg/800px-RecaptchaLogo.svg.png

Fallbeispiele

Fallbeispiel 1

- Eine Website mit Button, der einen Counter um 1 erhöht.
- Der “Anti-Bot” ist ein einfaches Skript
- Anti-Bot blockiert alle User die den Button mehr als 5 mal klicken
- Ähnliche Systeme finden im E-Commerce Verwendung

Fallbeispiel 1: Website Code

```html
<html>
<head>
    <title>Button_Counter</title>
</head>
<body>
    <h1>Button with Counter</h1>
    <button type="button" onclick="clicker(this)">Increase the Counter by one!</button>
    <p id="count">Count = 0</p>
    <script>
        let i = 0;
        function clicker(elmnt) {
            if (i >= 5) {
                document.writeln("Access Denied!");
            }
            i++;
            document.querySelector("#count").innerHTML = "Count = " + i;
        }
    </script>
</body>
</html>
```

Abb. 8: Button with Counter

Fallbeispiel 1: Bot Code

```python
import time
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.chrome.options import Options

options = Options()
options.add_argument('--headless')
driver = webdriver.Chrome(options=options)
driver.maximize_window()
driver.get("file:///C:/Users/ntrus/PycharmProjects/schoolproject/Fallbeispiel_01.html")


while(driver.find_element(By.XPATH, "/html/body").text != "Access Denied!"):
    print(driver.find_element(By.XPATH, '//*[@id="count"]').text)
    time.sleep(1)
    driver.find_element(By.XPATH, '/html/body/button').click()
print(driver.find_element(By.XPATH, '/html/body').text)
```

Abb. 9: Bot made with Python

Fallbeispiel 2

- Action pattern
- Button mit Vorhang: Button kann nur geklickt werden, wenn vorher ein anderer Button geklickt wurde.
- Im Fallbeispiel wird dies anhand eines simplen Skripts überprüft.
- Es werden User blockiert, welche zuerst den zweiten Button klicken.

Fallbeispiel 2: Website Code

```html
<html>
<head>
    <title>Field_and_Button</title>
</head>
<body>
    <h1>Field and Button</h1>
    <label for="username">Please enter your Username:</label><br />
    <input type="text" id="username" /><br />
    <button type="button" id="firstbutton" onclick="clicker(this)">Confirm Username!</button><br />
    <div id="myDIV">
        <p id="userText"></p>
        <button id="secondbutton" type="button" onclick="clicker2(this)">Click!</button>
        <p id="buttonClicked">The button has not been clicked.</p>
    </div>
    <script>
        var x = document.getElementById("myDIV");
        var clickedFirstButton = false;
        var clickedSecondButton = false;

        x.style.display = "none";

        function clicker(elmnt) {
            clickedFirstButton = true;
            document.querySelector("#userText").innerHTML = "Your Username: " + document.getElementById("username").value;
            x.style.display = "block"
        }

        function clicker2(elmnt) {
            clickedSecondButton = true;
            document.querySelector("#buttonClicked").innerHTML = "The button has been clicked.";
        }

        if (clickedFirstButton == false && clickedSecondButton == true) {
            document.writeln("Access Denied!")
        }
    </script>
</body>
</html>
```

Abb. 10: Button with Curtain

Fallbeispiel 3

- User-agent
- Dieser Sachverhalt wird anhand der Chrome Console vermittelt
- Website kann nur von einem bestimmten Gerätetypen aufgerufen werden
- User-agent kommt hier als Bot Damage/Prevention Konzept zum Einsatz

Fallbeispiel 3: Chrome Console

```
sec-ch-ua: " Not;A Brand";v="99", "Google Chrome";v="97", "Chromium";v="9
7"
sec-ch-ua-mobile: ?1
sec-ch-ua-platform: "Android"
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Mobile Safari/537.3
6
```

Abb. 11: Chrome Console

Abschließende Worte

- Gewinnt immer mehr an Bedeutung im E-Commerce Sektor
- Bereits in 2012: U.S. Anti-Bot Code of Conduct for ISPs
- Bedeutungsgewinn in IOT Security
- Anti-Bots sollen Angriffe erschweren, nicht komplett verhindern

Quellen

[1]:https://www.netacea.com/glossary/anti-bot-system/

[2]:https://www.kaspersky.com/resource-center/definitions/what-are-bots

[3]:https://www.netacea.com/glossary/anti-bot-system/

Design:https://slidesgo.com/theme/kuman-business-meeting#search-computer&position-13&results-103

Ergänzende Literatur

- https://par.nsf.gov/servlets/purl/10170537
- https://www.researchgate.net/profile/Elisa-Chiapponi-2/publication/351081653_HoPLA_a_Honeypot_Platform_to_Lure_Attackers/links/6083ca0f8ea909241e1f200c/HoPLA-a-Honeypot-Platform-to-Lure-Attackers.pdf
- https://www.profsandhu.com/confrnc/misconf/Malware2009.pdf
- https://conceptechint.net/index.php/CFATI/article/view/23/8

Danke für eure Aufmerksamkeit