reCAPTCHA and Anti-Bot Overview

Christian Bada and Randy Gingeleski
DTC Security Office Hours
2022 July 19

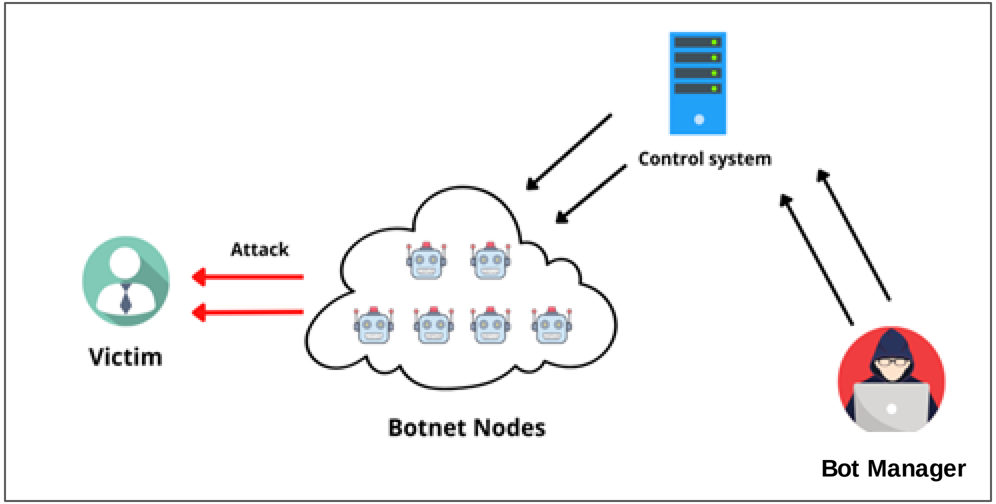
WARNER BROS.
DISCOVERY

Agenda

- Why bot or script versus HBO Max?
- How to bot
- How to stop bots
- Current anti-bot program
- Why reCAPTCHA?
- reCAPTCHA alternatives
- Current weaknesses
- In-flight initiatives and foreseeable future
- Utopian future
- Q&A

Why do attackers use bots/scripts against HBO Max?

- **Why use bots/scripts?**
  - Can conduct high volume of attacks against an application
  - Not sitting at a keyboard doing manual work



Why do attackers use bots/scripts against HBO Max?

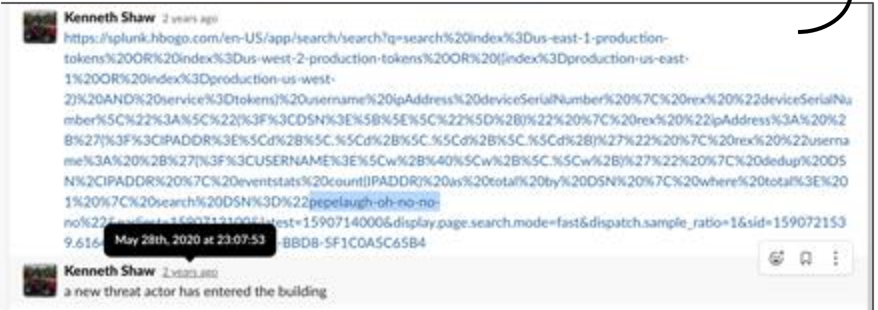
- **Why attack the HBO Max application?**
  - ○ Resell accounts and/or get free service
  - ○ Check stolen credit cards
  - ○ Possible ad fraud for AVOD
  - ○ Piracy and content scraping
  - ○ Stock price manipulation?

99.9%

  - ○ Trolling

“Pepe laugh oh no no no”

0.1%



Kenneth Shaw 2 years ago

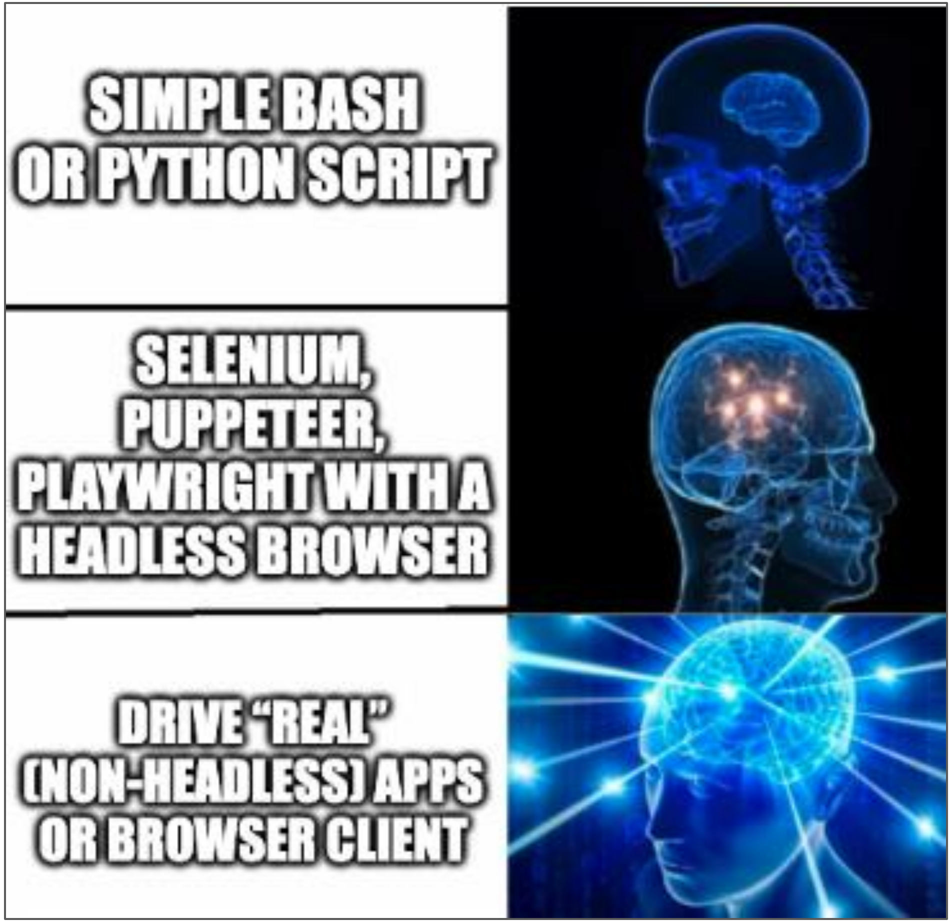
https://splunk.hbogo.com/en-US/app/search/search?q=search%20index%3Dus-east-1-production-tokens%20OR%20index%3Dus-west-2-production-tokens%20OR%20((index%3Dproduction-us-east-1%20OR%20index%3Dproduction-us-west-2)%20AND%20service%3Dtokens)%20username%20ipAddress%20deviceSerialNumber%20%7C%20rex%20%22deviceSerialNumber%5C%22%3A%5C%22(%3F%3CDSN%3E%5B%5E%5C%22%5D%2B)%22%20%7C%20rex%20%22ipAddress%3A%20%2B%27(%3F%3CIPADDR%3E%5Cd%2B%5C.%5Cd%2B%5C.%5Cd%2B%5C.%5Cd%2B)%27%22%20%7C%20rex%20%22username%3A%20%2B%27(%3F%3CUSERNAME%3E%5Cw%2B%40%5Cw%2B%5C.%5Cw%2B)%27%22%20%7C%20dedup%20DSN%2CIPADDR%20%7C%20eventstats%20count(IPADDR)%20as%20total%20by%20DSN%20%7C%20where%20total%3E%201%20%7C%20search%20DSN%3D%22pepelaugh-oh-no-no-no%22&earliest=1590712100&latest=1590714000&display.page.search.mode=fast&dispatch.sample_ratio=1&sid=1590721539.616 -BBDB-5F1C0A5C65B4

May 28th, 2020 at 23:07:53

Kenneth Shaw 2 years ago

a new threat actor has entered the building

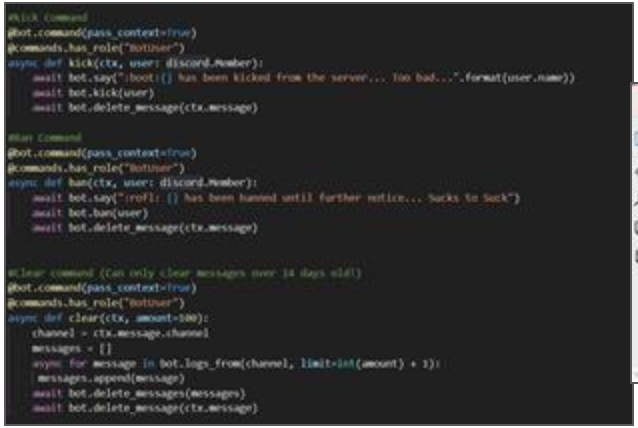
How to bot


SIMPLE BASH OR PYTHON SCRIPT
SELENIUM, PUPPETEER, PLAYWRIGHT WITH A HEADLESS BROWSER
DRIVE "REAL" (NON-HEADLESS) APPS OR BROWSER CLIENT

How to bot

- Different levels of bot attack
  - Simple: A Bash or Python Script, OpenBullet config
  - Advanced: Selenium, Puppeteer, Playwright with a headless browser
  - Ultimate: Drive “real” (non-headless) apps or browser client
    - Possibly using real devices
      - “Device Farming”
    - Swapped fingerprints to feign larger volume of uniques

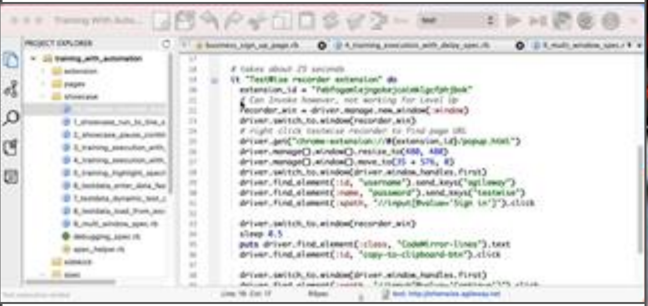
https://github.com/HBOCodeLabs/bot-zoo



```python
#Kick Command
@bot.command(pass_context=True)
@commands.has_role("BotUser")
async def kick(ctx, user: discord.Member):
    await bot.say(":boot: {} has been kicked from the server... Too bad...".format(user.name))
    await bot.kick(user)
    await bot.delete_message(ctx.message)

#Ban Command
@bot.command(pass_context=True)
@commands.has_role("BotUser")
async def ban(ctx, user: discord.Member):
    await bot.say(":rofl: {} has been banned until further notice... Sucks to Suck")
    await bot.ban(user)
    await bot.delete_message(ctx.message)


#Clear command (Can only clear messages over 14 days old!)
@bot.command(pass_context=True)
@commands.has_role("BotUser")
async def clear(ctx, amount=100):
    channel = ctx.message.channel
    messages = []
    async for message in bot.logs_from(channel, limit=int(amount) + 1):
     messages.append(message)
    await bot.delete_messages(messages)
    await bot.delete_message(ctx.message)
```

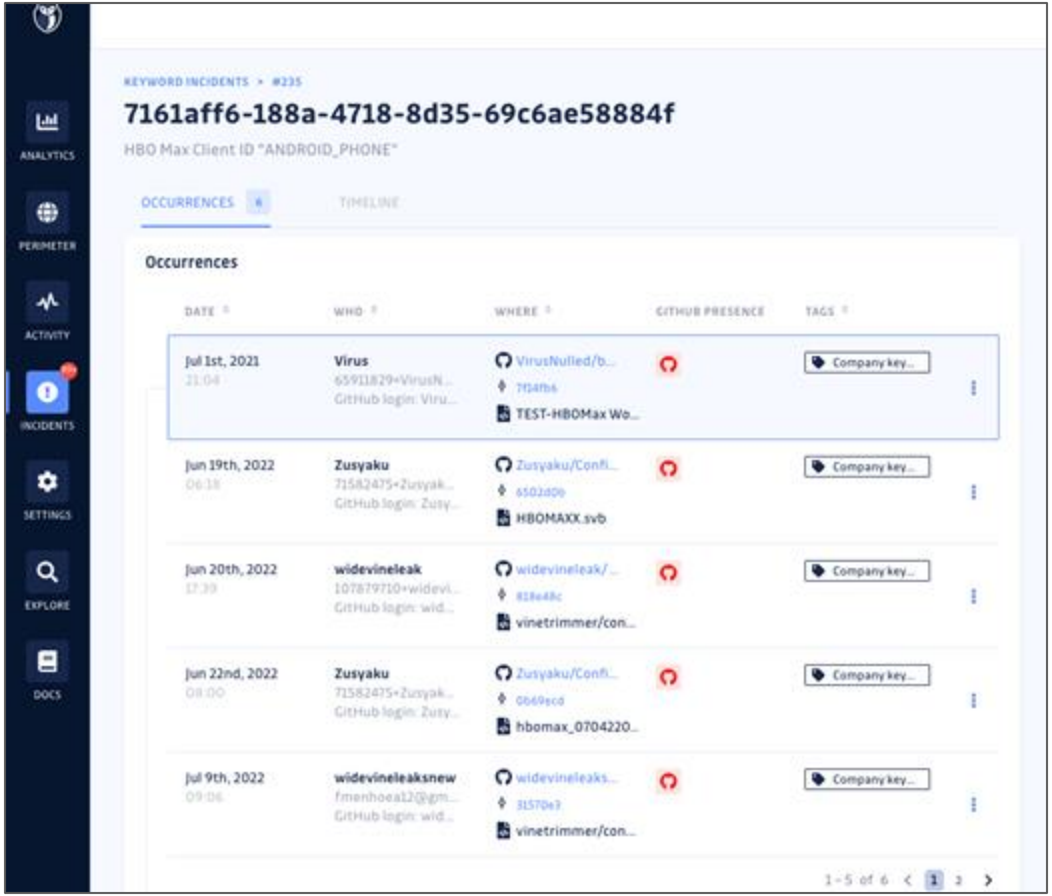


```ruby
  # takes about 25 seconds
  it "TestWise recorder extension" do
    extension_id = "[illegible]"
    # Can Invoke however, not working for Level Up
    recorder_win = driver.manage.new_window(:window)
    driver.switch_to.window(recorder_win)
    # right click testwise recorder to find page URL
    driver.get("chrome-extension://#{extension_id}/popup.html")
    driver.manage().window().resize_to(480, 480)
    driver.manage().window().move_to(35 + 576, 0)
    driver.switch_to.window(driver.window_handles.first)
    driver.find_element(:id, "username").send_keys("agileway")
    driver.find_element(:name, "password").send_keys("testwise")
    driver.find_element(:xpath, "//input[@value='Sign in']").click

    driver.switch_to.window(recorder_win)
    sleep 0.5
    puts driver.find_element(:class, "CodeMirror-lines").text
    driver.find_element(:id, "copy-to-clipboard-btn").click

    driver.switch_to.window(driver.window_handles.first)
```

How to bot



KEYWORD INCIDENTS > #235

7161aff6-188a-4718-8d35-69c6ae58884f

HBO Max Client ID "ANDROID_PHONE"

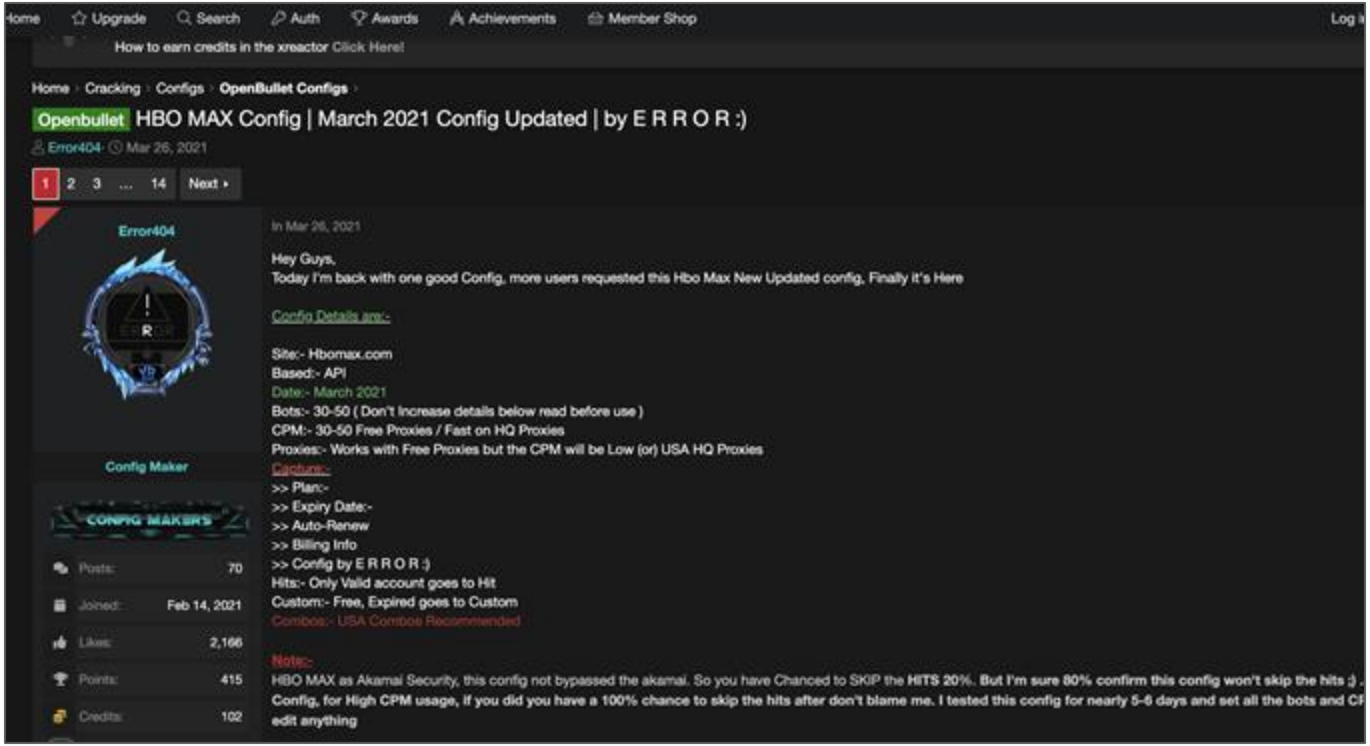
OCCURRENCES 6 TIMELINE

Occurrences

DATE	WHO	WHERE	GITHUB PRESENCE	TAGS
Jul 1st, 2021 21:04	Virus 65911829+VirusN... GitHub login: Viru...	VirusNulled/b... 7f14fb6 TEST-HBOMax Wo...		Company key...
Jun 19th, 2022 06:18	Zusyaku 71582475+Zusyak... GitHub login: Zusy...	Zusyaku/Confi... 6502d0b HBOMAXX.svb		Company key...
Jun 20th, 2022 17:39	widevineleak 107879710+widevi... GitHub login: wid...	widevineleak/... 818e48c vinetrimmer/con...		Company key...
Jun 22nd, 2022 08:00	Zusyaku 71582475+Zusyak... GitHub login: Zusy...	Zusyaku/Confi... 0b69ecd hbomax_0704220...		Company key...
Jul 9th, 2022 09:06	widevineleaksnew fmenhoea12@gm... GitHub login: wid...	widevineleaks... 31570e3 vinetrimmer/con...		Company key...

1 - 5 of 6 < 1 2 >

How to bot



How to earn credits in the xreactor Click Here!

Openbullet HBO MAX Config | March 2021 Config Updated | by E R R O R :)

Error404 · Mar 26, 2021

In Mar 26, 2021

Hey Guys,
Today I'm back with one good Config, more users requested this Hbo Max New Updated config, Finally it's Here

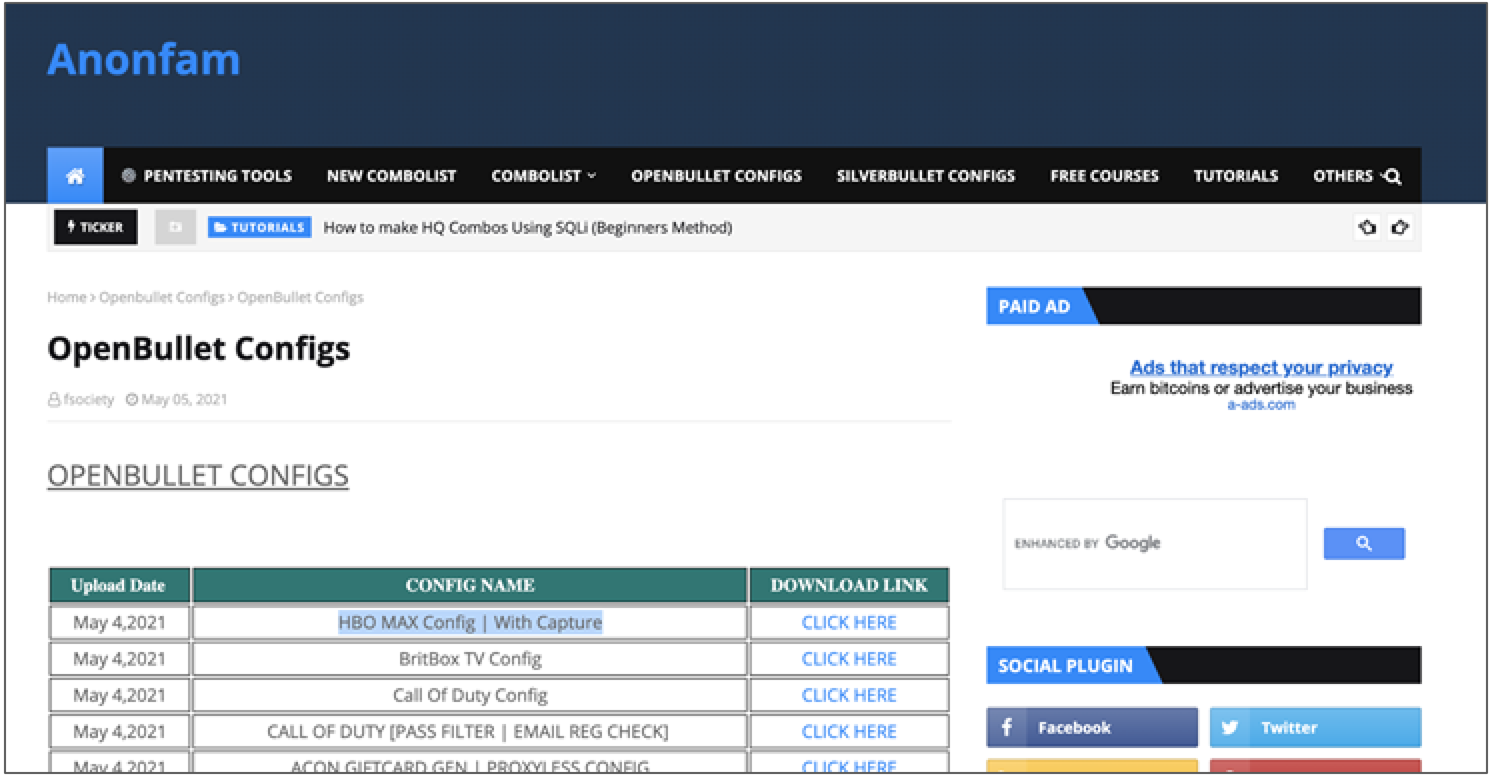
Config Details are:-

Site:- Hbomax.com
Based:- API
Date:- March 2021
Bots:- 30-50 (Don't Increase details below read before use)
CPM:- 30-50 Free Proxies / Fast on HQ Proxies
Proxies:- Works with Free Proxies but the CPM will be Low (or) USA HQ Proxies
Capture:-
>> Plan:-
>> Expiry Date:-
>> Auto-Renew
>> Billing Info
>> Config by E R R O R :)
Hits:- Only Valid account goes to Hit
Custom:- Free, Expired goes to Custom
Combos:- USA Combos Recommended

Note:-
HBO MAX as Akamai Security, this config not bypassed the akamai. So you have Chanced to SKIP the **HITS 20%. But I'm sure 80% confirm this config won't skip the hits :) .**
Config, for High CPM usage, If you did you have a 100% chance to skip the hits after don't blame me. I tested this config for nearly 5-6 days and set all the bots and CP
edit anything

https://xreactor.org/threads/hbo-max-config-march-2021-config-updated-by-e-r-r-o-r.2379/

How to bot



How to make HQ Combos Using SQLi (Beginners Method)

Home › Openbullet Configs › OpenBullet Configs

OpenBullet Configs

fsociety May 05, 2021

OPENBULLET CONFIGS

Upload Date	CONFIG NAME	DOWNLOAD LINK
May 4,2021	HBO MAX Config | With Capture	CLICK HERE
May 4,2021	BritBox TV Config	CLICK HERE
May 4,2021	Call Of Duty Config	CLICK HERE
May 4,2021	CALL OF DUTY [PASS FILTER | EMAIL REG CHECK]	CLICK HERE
May 4,2021	ACON GIFTCARD GEN | PROXYLESS CONFIG	CLICK HERE

https://www.anonfam.com/2021/05/openbullet-configs.html - **CONFIG FILE LINK**

How to stop bots

https://github.com/prescience/dark-knowledge

https://github.com/IPL/fraud-detection-papers

https://github.com/safe-graph/DGFraud

https://getipintel.net

https://antoinevastel.com/bots/ip

https://github.com/Umkus/ip-index

https://github.com/FlUxIuS/p0f3plus

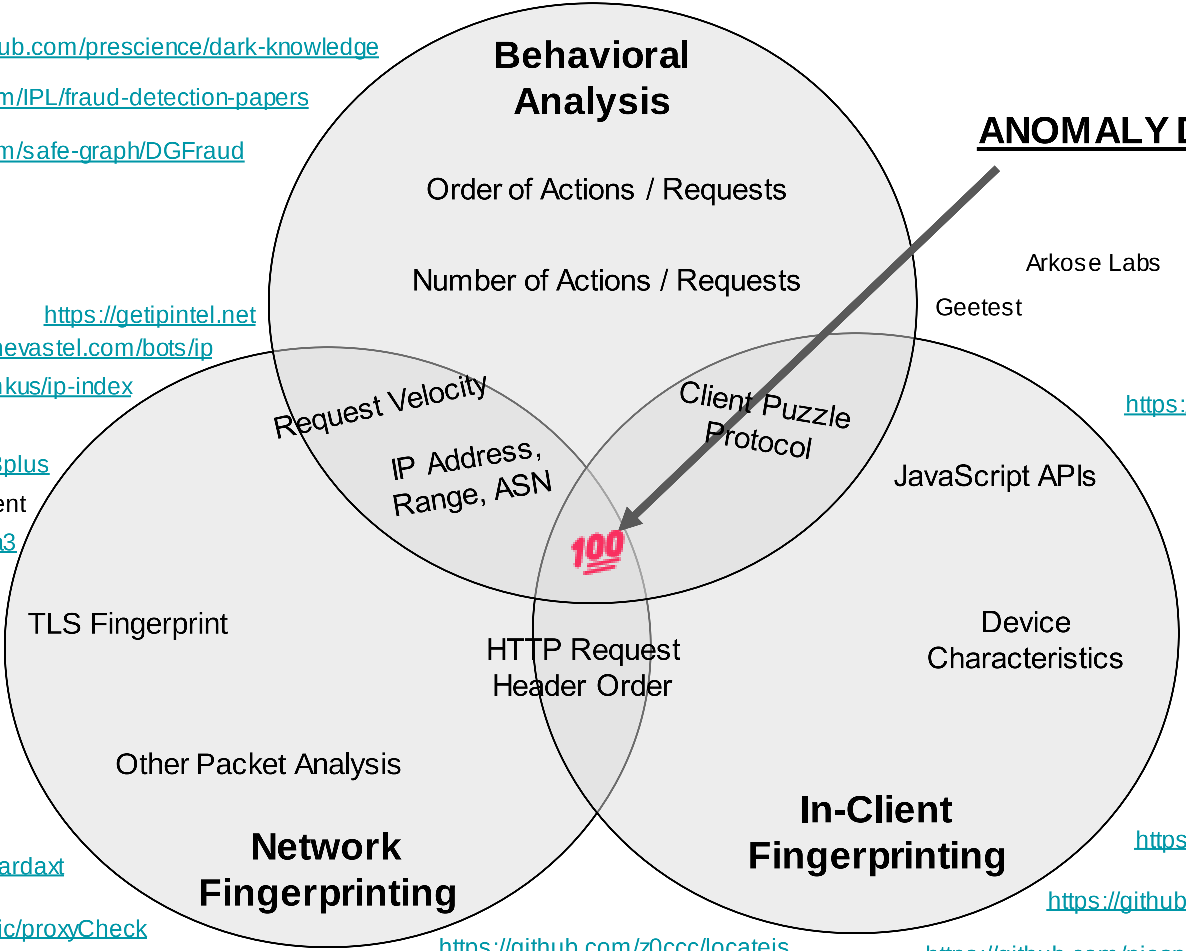
Cloudflare Bot Management

https://github.com/salesforce/ja3

Google "reCAPTCHA Lite"
Add-on at CDN

https://github.com/NikolaiT/zardaxt

https://github.com/Ivan-Markovic/proxyCheck



ANOMALY DETECTION

Behavioral Analysis

Order of Actions / Requests

Number of Actions / Requests

Request Velocity

IP Address, Range, ASN

Client Puzzle Protocol

💯

TLS Fingerprint

HTTP Request Header Order

Other Packet Analysis

Network Fingerprinting

JavaScript APIs

Device Characteristics

In-Client Fingerprinting

https://github.com/z0ccc/locatejs

Arkose Labs

Geetest

https://github.com/abrahamjuliot/creepjs

https://supercookie.me

Google reCAPTCHA Enterprise

hCaptcha

https://github.com/Cleafy/refingerprint

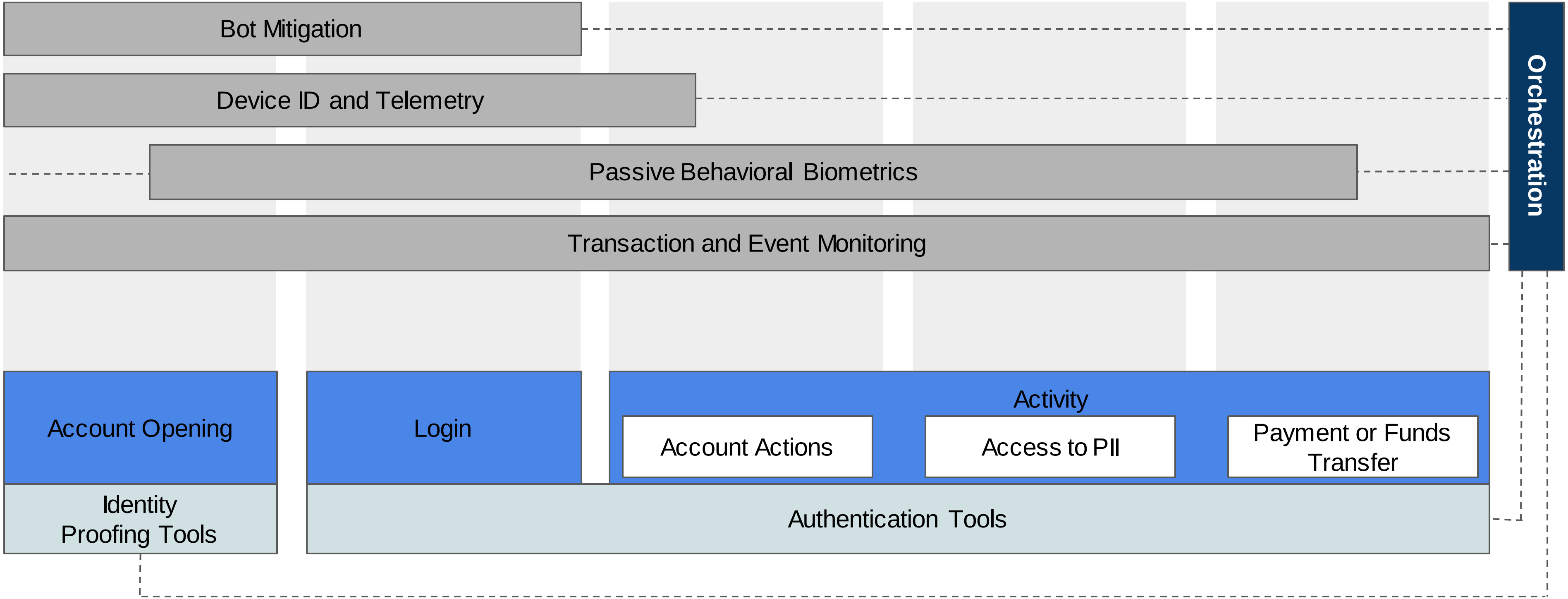
https://github.com/antoinevastel/fp-collect

https://github.com/niespodd/browser-fingerprinting

How to stop bots

- https://incolumitas.com/pages/BotOrNot/
    - Bot or not? Start here for exploration into the logic
- https://github.com/abrahamjuliot/creepjs
    - General browser fingerprinting
        - Does test for 35 browser extensions, but that is not best-in-class at this
- https://github.com/z0ccc/extension-fingerprints
    - Browser extension fingerprinting
        - Purportedly tests for >=1,000 browser extensions
- https://bot.incolumitas.com/proxy_detect.html
    - Proxy- or VPN-focused network fingerprinting
        - Not exactly open-source but from https://incolumitas.com blog posts much of the inner-workings can be deduced
- https://incolumitas.com/pages/TLS-Fingerprint/
    - TLS network fingerprinting
- https://incolumitas.com/pages/TCP-IP-Fingerprint/
    - TCP/IP network fingerprinting
- https://incolumitas.com/pages/Datacenter-IP-API/
    - Datacenter IP network fingerprinting

How to stop bots

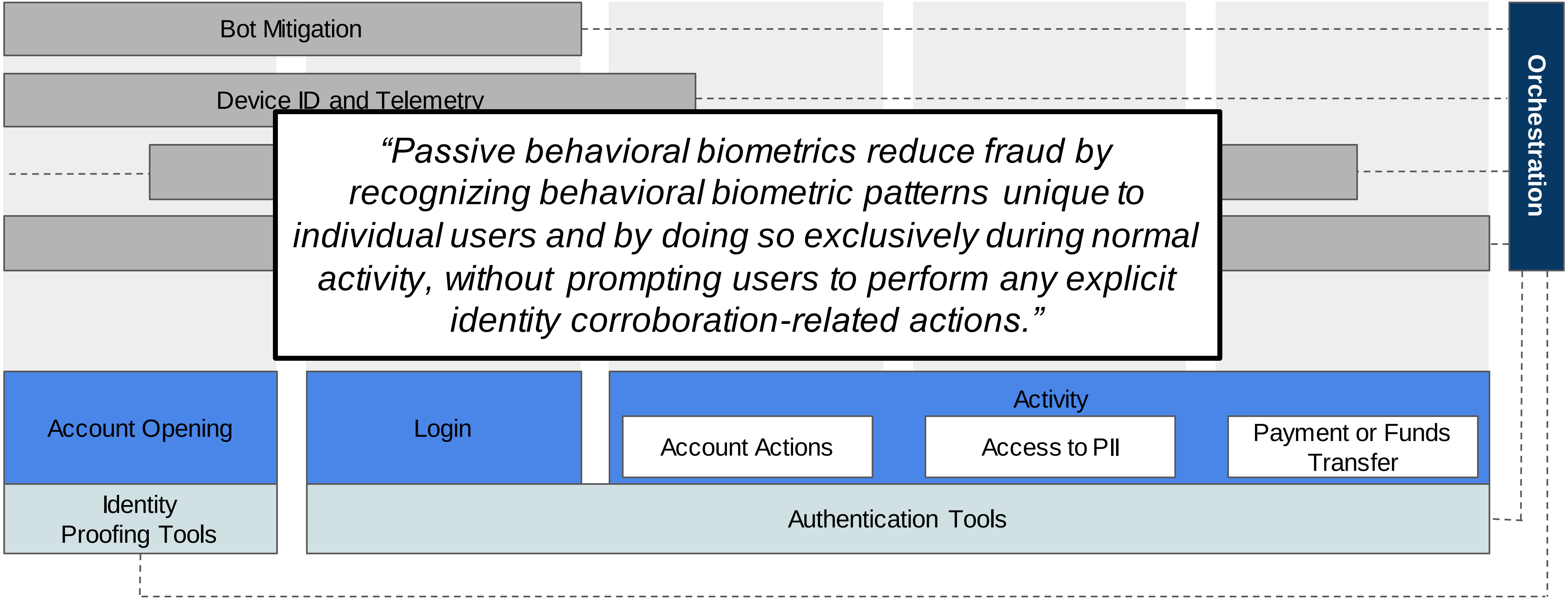


“Online Fraud Detection” (OFD)

Adapted from Gartner

https://gartner.com/document/4015931?ref=solrResearch&refval=331205008

How to stop bots



> *“Passive behavioral biometrics reduce fraud by recognizing behavioral biometric patterns unique to individual users and by doing so exclusively during normal activity, without prompting users to perform any explicit identity corroboration-related actions.”*

“Online Fraud Detection” (OFD)

Adapted from Gartner

https://gartner.com/document/4015931?ref=solrResearch&refval=331205008

How to stop bots

There’s a middle ground between **ALLOW** and **BLOCK** 🥺

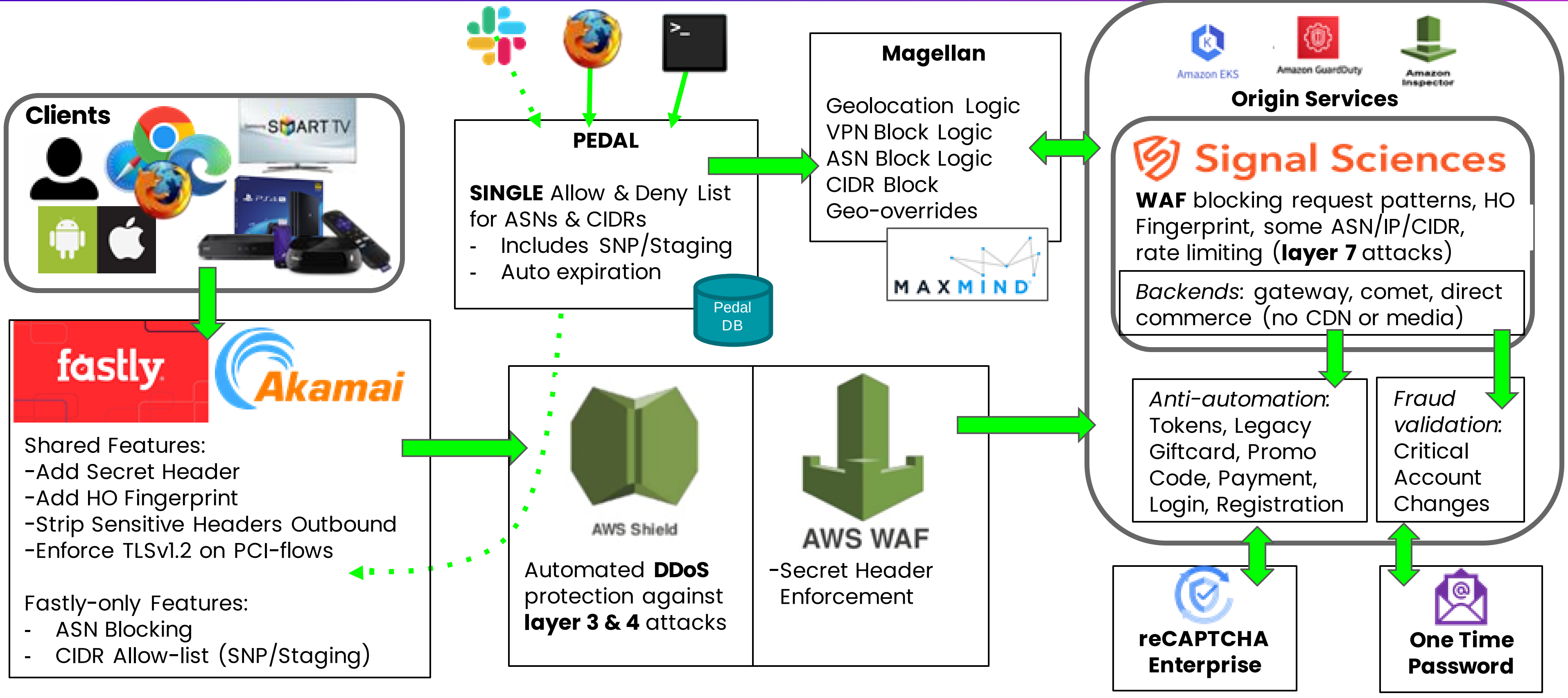
ALLOW

- Block the input and/or don’t deliver the output
- Terminate the active user session
- Lock the user account from additional logins
- Present the user with an in-session cognitive challenge
- Challenge the user with an MFA/2FA request
- Block the IP address that performed the submission
- Heighten logging associated with the active user session
- Flag transactions performed by the user for review by your security or fraud personnel
- Place the user into a “virtual waiting room” and/or introduce a time delay between allowed transactions
- Adjust the user’s in-app permissions and/or available application features
- Increment a counter towards some decision you make after collecting more evidence of automation or abuse
- Notify the end user via email, text message, or otherwise that their account appears to be compromised
- Request or force user account password reset
- Limit the number and/or size of transactions that can be performed within the user account or active session

BLOCK

Doesn’t all necessarily make sense for a consumer streaming app though 🥺

Current anti-bot program



Clients

PEDAL

SINGLE Allow & Deny List for ASNs & CIDRs

- Includes SNP/Staging
- Auto expiration

Magellan

Geolocation Logic
VPN Block Logic
ASN Block Logic
CIDR Block
Geo-overrides

Origin Services

WAF blocking request patterns, HO Fingerprint, some ASN/IP/CIDR, rate limiting (**layer 7** attacks)

Backends: gateway, comet, direct commerce (no CDN or media)

Anti-automation: Tokens, Legacy Giftcard, Promo Code, Payment, Login, Registration

Fraud validation: Critical Account Changes

reCAPTCHA Enterprise

One Time Password

Shared Features:
-Add Secret Header
-Add HO Fingerprint
-Strip Sensitive Headers Outbound
-Enforce TLSv1.2 on PCI-flows

Fastly-only Features:

- ASN Blocking
- CIDR Allow-list (SNP/Staging)

Automated **DDoS** protection against **layer 3 & 4** attacks

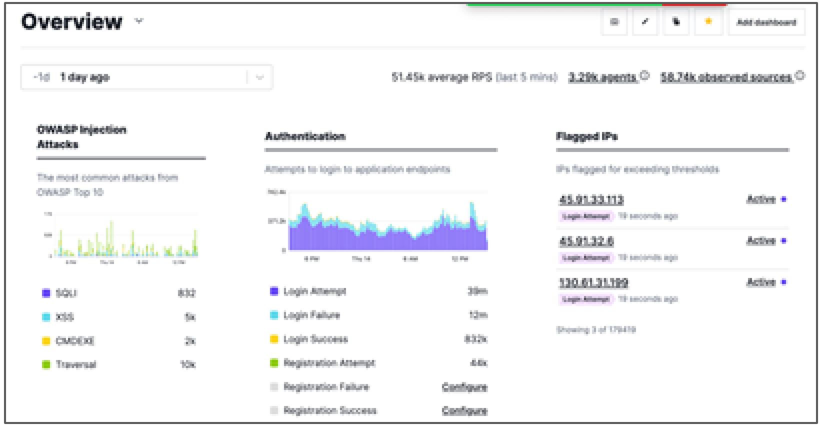
AWS WAF

-Secret Header Enforcement

Current anti-bot program

- **Signal Sciences**
  - Web application firewall
  - “Wraps” API endpoints
  - Can identify ‘signals’ of incoming requests
  - Security Controls
    - Rate limiting
    - Anomalous request behavior blocks
    - Header order blocks

Signal Sciences



Overview

Add dashboard

-1d 1 day ago

51.45k average RPS (last 5 mins) 3.29k agents 58.74k observed sources

OWASP Injection Attacks

The most common attacks from OWASP Top 10

SQLI	832
XSS	5k
CMDEXE	2k
Traversal	10k

Authentication

Attempts to login to application endpoints

Login Attempt	39m
Login Failure	12m
Login Success	832k
Registration Attempt	44k
Registration Failure	Configure
Registration Success	Configure

Flagged IPs

IPs flagged for exceeding thresholds

45.91.33.113 Active
Login Attempt 19 seconds ago

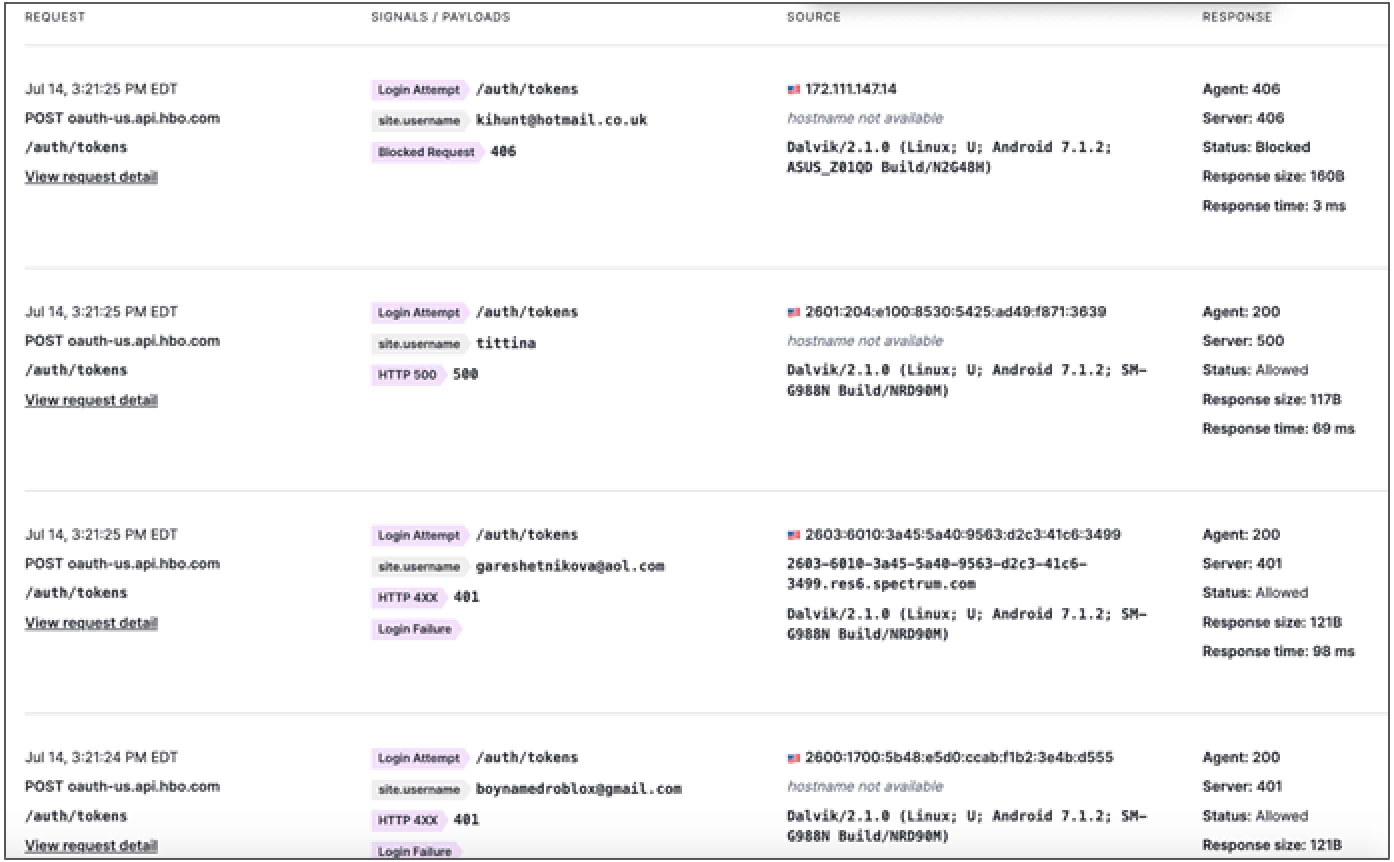
45.91.32.6 Active
Login Attempt 19 seconds ago

130.61.31.199 Active
Login Attempt 19 seconds ago

Showing 3 of 179419

Current anti-bot program

- **Signal Sciences**

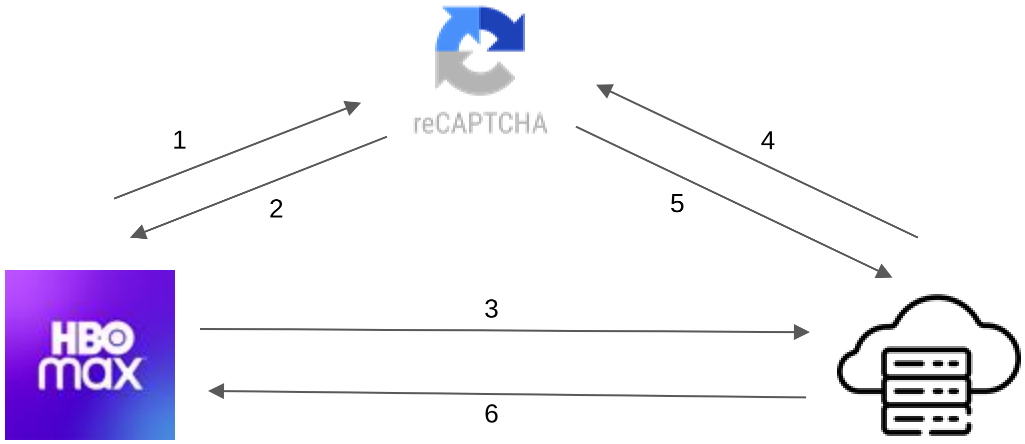


REQUEST	SIGNALS / PAYLOADS	SOURCE	RESPONSE
Jul 14, 3:21:25 PM EDT POST oauth-us.api.hbo.com /auth/tokens View request detail	Login Attempt /auth/tokens site.username kihunt@hotmail.co.uk Blocked Request 406	172.111.147.14 *hostname not available* Dalvik/2.1.0 (Linux; U; Android 7.1.2; ASUS_Z01QD Build/N2G48H)	Agent: 406 Server: 406 Status: Blocked Response size: 160B Response time: 3 ms
Jul 14, 3:21:25 PM EDT POST oauth-us.api.hbo.com /auth/tokens View request detail	Login Attempt /auth/tokens site.username tittina HTTP 500 500	2601:204:e100:8530:5425:ad49:f871:3639 *hostname not available* Dalvik/2.1.0 (Linux; U; Android 7.1.2; SM-G988N Build/NRD90M)	Agent: 200 Server: 500 Status: Allowed Response size: 117B Response time: 69 ms
Jul 14, 3:21:25 PM EDT POST oauth-us.api.hbo.com /auth/tokens View request detail	Login Attempt /auth/tokens site.username gareshetnikova@aol.com HTTP 4XX 401 Login Failure	2603:6010:3a45:5a40:9563:d2c3:41c6:3499 2603-6010-3a45-5a40-9563-d2c3-41c6-3499.res6.spectrum.com Dalvik/2.1.0 (Linux; U; Android 7.1.2; SM-G988N Build/NRD90M)	Agent: 200 Server: 401 Status: Allowed Response size: 121B Response time: 98 ms
Jul 14, 3:21:24 PM EDT POST oauth-us.api.hbo.com /auth/tokens View request detail	Login Attempt /auth/tokens site.username boynamedroblox@gmail.com HTTP 4XX 401 Login Failure	2600:1700:5b48:e5d0:ccab:f1b2:3e4b:d555 *hostname not available* Dalvik/2.1.0 (Linux; U; Android 7.1.2; SM-G988N Build/NRD90M)	Agent: 200 Server: 401 Status: Allowed Response size: 121B

Current anti-bot program

- **reCAPTCHA Enterprise**
    - Invisible implementation
        - Does not require user interaction
    - Two endpoints protected
        - Commerce/Commerce-Experience
            - Login
            - Registration
            - Payment
            - Promo code
        - Gateway
            - Login
    - Active blocks on web client
        - Block activation on iOS & Android pending verification of client bug fix

Current anti-bot program



Score	Google Says	Our Description
0.0 - 0.2	High Risk	Seems Bot-like
0.3 - 0.8	Medium Risk	*~ Meh ~*
0.9 - 1.0	Low Risk	Seems Human

How it works:

1. Call is made via javascript to reCAPTCHA API containing information about user
2. reCAPTCHA generates and sends back a token with score and other information
3. App sends token to server with other login information
4. Back-end server sends token to reCAPTCHA to verify the token is valid
5. reCAPTCHA sends response to server with token information
6. Server response sent to application based on reCAPTCHA information received

Why do we use reCAPTCHA?

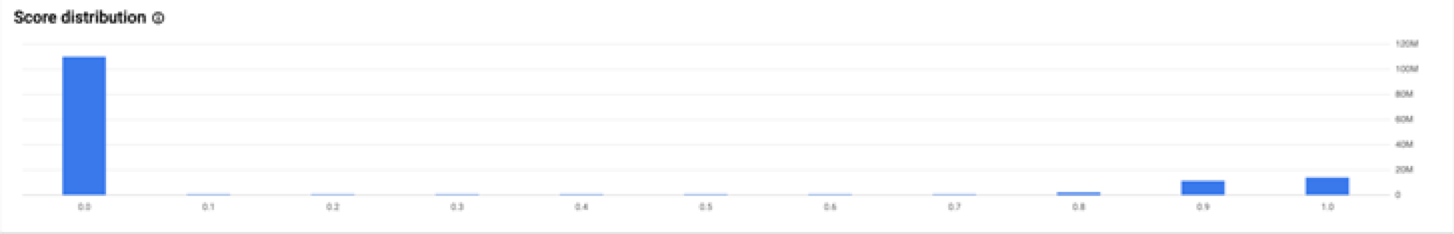
- **Initially implemented as a rate limiting solution in commerce**
  - reCAPTCHA V3 (Free version)
- **Met product team's desire for an 'invisible' anti-bot solution**
  - Hard no regarding user friction
- **Signed big deal across all of WarnerMedia**

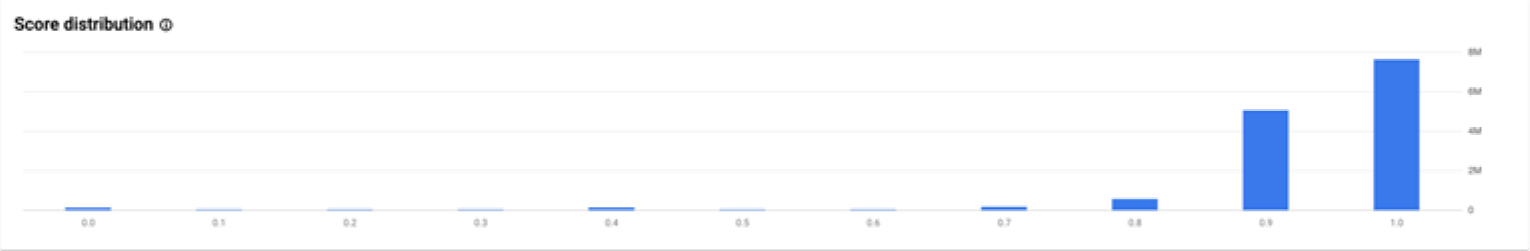
reCAPTCHA Alternatives

- **Several alternative technologies**
- **Why reCAPTCHA over other alternatives?**
  - reCAPTCHA invisible implementation
    - Product team specified
  - Used by other major streaming services
    - Netflix
    - Hulu
  - Price
    - High volume of requests
    - Budget-friendly
  - Costly to switch
    - Would require hours of manpower to switch
    - reCAPTCHA implementation not complete
      - Requires tuning - alternatives would require same tuning

Current weaknesses

- **Threshold tuned to 0.5 (based on score distribution could be higher)**
- **No visibility into how reCAPTCHA scores**
  - known/hypothesized? Factors
    - IP Address
    - Previous reCAPTCHA interactions
    - User behavior on the page
- **Implemented with focus on good user experience**





In-flight initiatives and foreseeable future

“Quality of life”

- **Client bug fix for IAP flow**
- **Developers’ (and other trusted devices) bypass**
  - ~Instant IP-based bypassing versus present-state that requires Gateway restart

Increasing friction for bad actors

- **Block (re-)activation on iOS & Android**
- **Score tuning**
  - Labeling known bot or known human traffic to improve model
    - https://github.com/HBOCodeLabs/bot-zoo
  - Threshold increase(s)

Latency / performance

- **“reCAPTCHA Lite” (maybe?)**
  - Edge-based consideration of traffic (Fastly or other)

Utopian Future (HBO Max)

- **reCAPTCHA**
  - Bypass feature for internal use with immediate effectiveness
  - Blocks activated for mobile devices
  - Tuning reCAPTCHA with known bot traffic and known human traffic
  - Score threshold raised to at least 0.6

- **Signal Sciences alternative ?**
  - Other competing products bring built-in anomaly detection
    - + Improve on traffic ⇔ user/account correlation

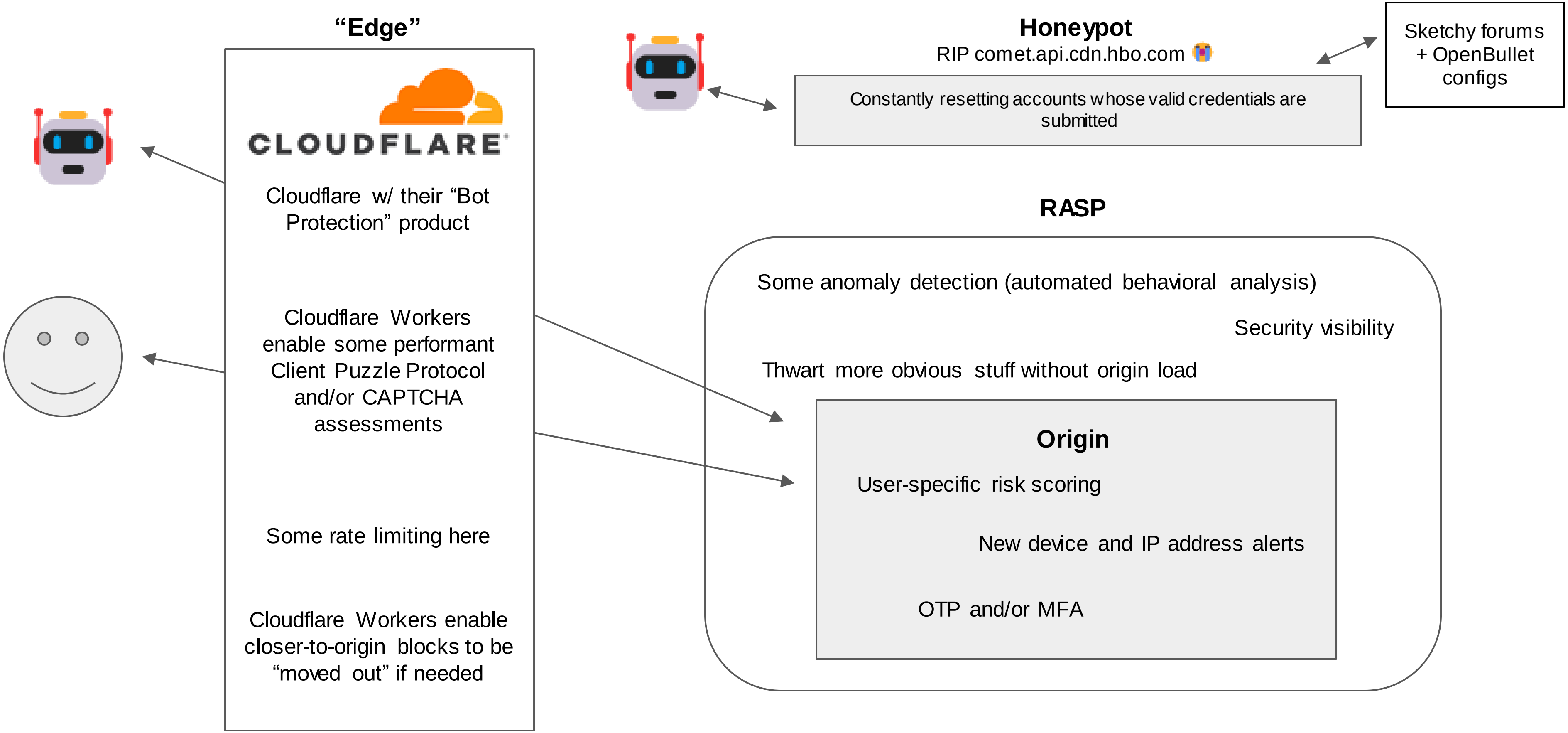
Utopian Future (Brand New Platform)

- **Edge-based blocking**
  - Network fingerprinting
  - In-client fingerprinting ??

- **More processing and levels of user friction, within or closer to origin**
  - In-client fingerprinting
  - Behavioral analysis

- **Security appliances augmenting and/or wrapping all traffic**
  - RASP **R**untime **A**pplication **S**elf-**P**rotection 😇
    - Signal Sciences, Traceable, etcetera

Utopian Future (Brand New Platform)



"Edge"

Cloudflare w/ their "Bot Protection" product

Cloudflare Workers enable some performant Client Puzzle Protocol and/or CAPTCHA assessments

Some rate limiting here

Cloudflare Workers enable closer-to-origin blocks to be "moved out" if needed

Honeypot

RIP comet.api.cdn.hbo.com 😭

Constantly resetting accounts whose valid credentials are submitted

Sketchy forums + OpenBullet configs

RASP

Some anomaly detection (automated behavioral analysis)

Security visibility

Thwart more obvious stuff without origin load

Origin

User-specific risk scoring

New device and IP address alerts

OTP and/or MFA

Questions? / Open Forum

🍿 🍿 🍿

Contact Us

- Contact DTC Security Team for general inquiries in #security-team slack channel:
  - @dtc-security-team to notify all security team members
  - @appsec application security (SigSci, Web, etc.)
  - @cloudsec cloud security (AWS, infra, etc.)

DTC Security

Agents Of Change