



DTC Security
Advanced Signal Sciences Investigation/Blocking
01 December 2021



Agenda

Not-so-clean blocks

Last time we just looked at “happy path”

“The QA environment is broken!”

*Or, how to tell if *we’re* blocking something*

“What are all these 403s”

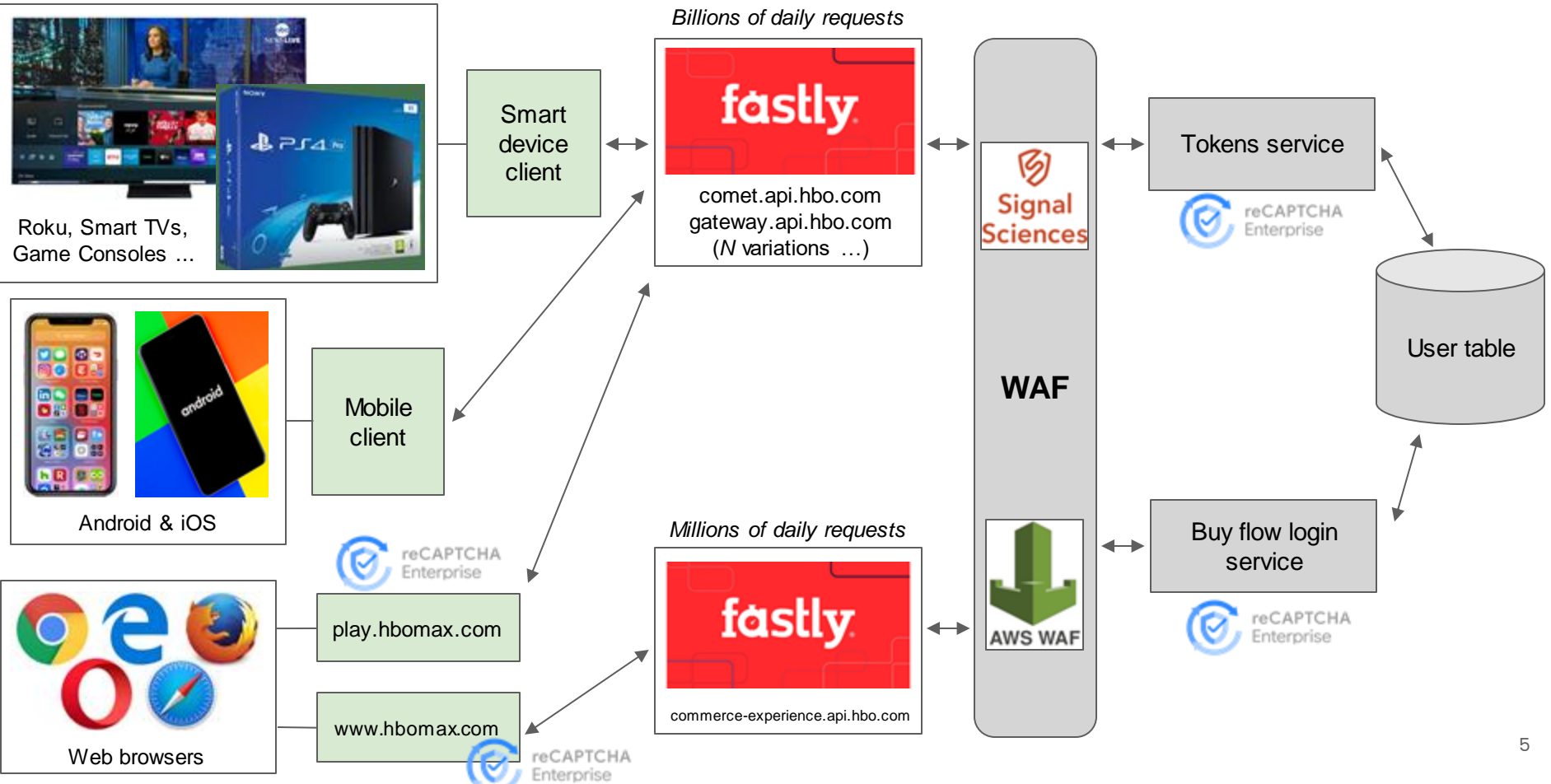
When your starting point is just request count of certain statuses...

Q&A

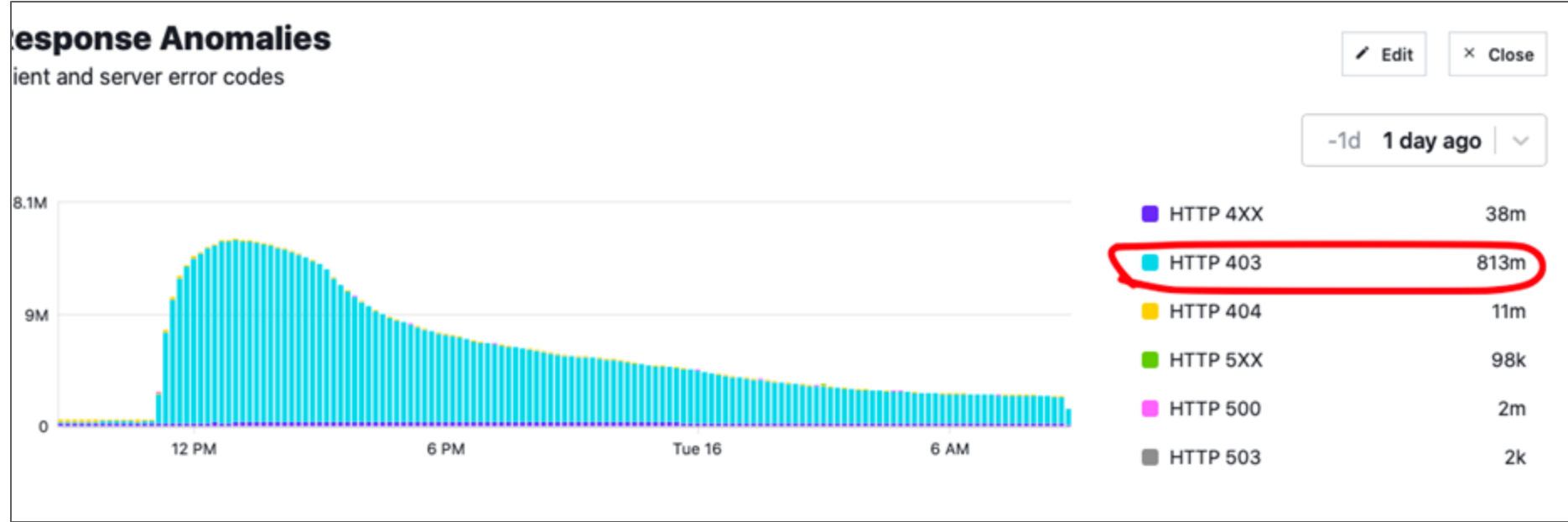
- **Success rate is suspiciously high for a given header order**
 - Subjective but let's say north of 5%
 - What paths are they hitting?
 - What do User-Agents look like?
 - Do not make decisions off UA alone though
 - LOGINATTEMPT-tagged traffic versus not
 - Are compromised usernames being hit an outsized number of times to obfuscate "true" success rate?
 - Follow traffic all the way to other supporting logs
 - Such as reCAPTCHA or tokens

"The QA environment is broken!"

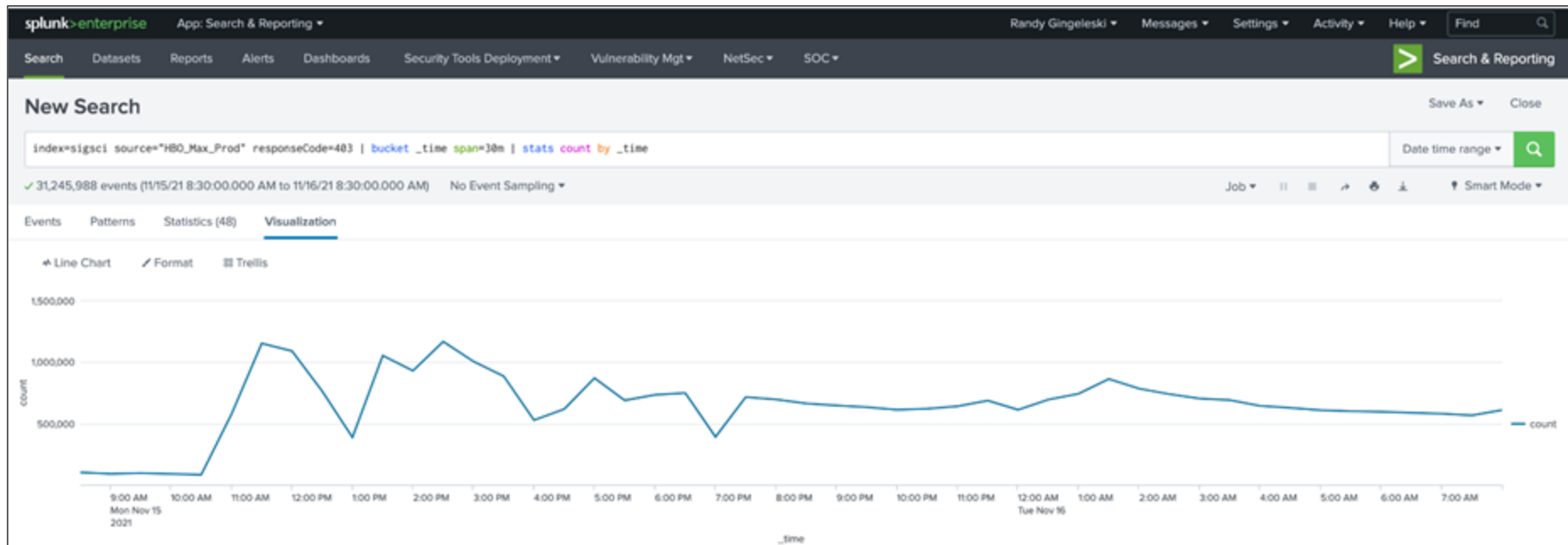
- **Need (IP address OR username) and approx. timestamp at a minimum**
- **Is traffic showing up in Signal Sciences?**
 - Not blocked by Fastly then
 - Decreasingly relevant but still
 - Response code 403 typically suggests Magellan denial
 - MaxMind geo, MaxMind VPN, or ASN block that differed from Fastly edge
- **index=*prod* <IP_ADDRESS_OR_OTHER_IDENTIFIER_HERE> for HBO Splunk**
 - [Example Splunk via Slack thread](#)
 - Some [Kibana starters](#) too
 - Just throw the unique string on the end in both cases, basically



“What are all these 403s”



“What are all these 403s”



“What are all these 403s”

splunk enterprise App: Search & Reporting Randy Gingeleski Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Security Tools Deployment Vulnerability Mgt NetSec SOC Search & Reporting

New Search

Save As Close

index=sigsci source="HBO_Max_Prod" responseCode=403 path="*/tokens" OR path="/content" | stats count by userAgent

Date time range

✓ 8,941,302 events (11/15/21 11:00:00.000 AM to 11/15/21 4:00:00.000 PM) No Event Sampling Job

Events Patterns **Statistics (4,641)** Visualization

100 Per Page Format Preview

< Prev 1 2 3 4 5 6 7 8 ... Next >

userAgent	count
Dalvik/2.1.0 (Linux; U; Android 9; AFTSS Build/PS7242)	2461674
Dalvik/2.1.0 (Linux; U; Android 7.1.2; AFTM Build/NS6281)	2097821
Dalvik/2.1.0 (Linux; U; Android 9; AFTSSS Build/PS7242)	1899688
Dalvik/2.1.0 (Linux; U; Android 5.1.1; AFTT Build/LYY48F)	706341
Dalvik/2.1.0 (Linux; U; Android 9; Xview Build/PI)	241665
Dalvik/2.1.0 (Linux; U; Android 9; Orion Build/PI)	231742
Dalvik/2.1.0 (Linux; U; Android 9; SKYWORTH-HY4002 Build/PI)	208497
Dalvik/2.1.0 (Linux; U; Android 9; AFTKA Build/PS7255)	169322
Dalvik/2.1.0 (Linux; U; Android 9; AFTB Build/PS7242)	140527
Dalvik/2.1.0 (Linux; U; Android 9; B820C-A15 Build/PI)	117944
Dalvik/2.1.0 (Linux; U; Android 9; MIBOX4 Build/PI)	117057
Dalvik/2.1.0 (Linux; U; Android 9; MIBOX3 Build/PI)	86007
Dalvik/2.1.0 (Linux; U; Android 9; BRAVIA 4K G8 Build/PTT1.190515.001.543)	45375
Dalvik/2.1.0 (Linux; U; Android 10; X96Q Build/QPIA.191105.004)	37838
Dalvik/2.1.0 (Linux; U; Android 9; DECO ENTEL Build/PI)	37625
Dalvik/2.1.0 (Linux; U; Android 9; B826C-A12 Build/PI)	37265
Dalvik/2.1.0 (Linux; U; Android 9; SHIELD Android TV Build/PPR1.180610.011)	36377
Dalvik/2.1.0 (Linux; U; Android 9; BRAVIA 4K UR3 Build/PTT1.190515.001.5104)	36079
Dalvik/2.1.0 (Linux; U; Android 8.0.0; BRAVIA 4K 2015 Build/OPR2.170623.027.516)	33165

“What are all these 403s”

splunk enterprise App: Search & Reporting

Randy Gingeleski Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Security Tools Deployment Vulnerability Mgt NetSec SOC

Search & Reporting

New Search

Save As Close

index=sigsci source="HBO_Max_Prod" responseCode=403 path="tokens" OR path="/content" | stats count by headersIn.x-HO

Date time range

✓ 8,941,302 events (11/15/21 11:00:00.000 AM to 11/15/21 4:00:00.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (246)** Visualization

100 Per Page Format Preview

1 2 3 Next

headersIn.x-HO	count
Authorization x-hbo-headwater x-hbo-client-version Accept x-hbo-device-name x-b3-traceId Accept-Language x-hbo-device-os-version Content-Type User-Agent Host Connection Accept-Encoding Content-Length	5486281
x-hbo-headwater x-hbo-client-version x-b3-traceId x-hbo-device-name Accept x-hbo-device-os-version Accept-Language Authorization Content-Type User-Agent Host Connection Accept-Encoding Content-Length	2262629
x-hbo-headwater x-hbo-client-version x-b3-traceId Accept x-hbo-device-name x-hbo-device-os-version Accept-Language Authorization Content-Type User-Agent Host Connection Accept-Encoding Content-Length	686644
Accept x-hbo-client-version Content-Type Content-Length Authorization Accept-Language User-Agent Host Connection Accept-Encoding	171158
Accept x-hbo-client-version Content-Type Content-Length Authorization User-Agent Host Connection Accept-Encoding	76953
:authority content-type x-hbo-device-name accept authorization x-hbo-client-version x-b3-traceId accept-encoding accept-language content-length user-agent x-hbo-headwater x-hbo-device-os-version	52924
Accept x-hbo-client-version Content-Type Content-Length Authorization x-hbo-headwater Accept-Language User-Agent Host Connection Accept-Encoding	47757
:authority content-length authorization origin x-b3-traceId accept-language user-agent content-type x-hbo-device-name accept x-hbo-device-os-version x-hbo-client-version x-hbo-headwater accept-encoding	31935
Authorization x-hbo-client-version Accept x-hbo-device-name x-b3-traceId Accept-Language x-hbo-device-os-version Content-Type User-Agent Host Connection Accept-Encoding Content-Length	29178
Accept x-hbo-client-version Content-Type Content-Length Authorization x-hbo-headwater User-Agent Host Connection Accept-Encoding	21164
x-hbo-headwater x-hbo-browie x-hbo-client-version x-b3-traceId x-hbo-device-name Accept x-hbo-device-os-version Accept-Language Authorization Content-Type User-Agent Host Connection Accept-Encoding Content-Length	19975
Authorization x-hbo-headwater x-hbo-client-version Accept x-hbo-device-name x-b3-traceId Accept-Language x-hbo-device-os-version x-hbo-browie Content-Type User-Agent Host Connection Accept-Encoding Content-Length	18911
Accept Content-Type Content-Length User-Agent Host Connection Accept-Encoding	9795
X-Hbo-Client-Version x-b3-traceId x-hbo-device-name Accept x-hbo-device-os-version Accept-Language Authorization Content-Type User-Agent Host Connection Accept-Encoding Content-Length	7994
Host Connection Accept-Encoding Content-Type Content-Length User-Agent Accept Accept-Language x-hbo-client-version x-hbo-device-os-version x-hbo-device-name x-b3-traceId Origin DNT Referer	7838
x-hbo-headwater x-hbo-browie x-hbo-client-version x-b3-traceId Accept x-hbo-device-name x-hbo-device-os-version Accept-Language Authorization Content-Type User-Agent Host Connection Accept-Encoding Content-Length	3342
:authority content-type x-hbo-device-name accept authorization x-hbo-client-version x-b3-traceId accept-encoding accept-language content-length user-agent x-hbo-device-os-version	3294
Authorization x-hbo-client-version Accept x-hbo-device-name x-b3-traceId Accept-Language x-hbo-device-os-version x-hbo-browie Content-Type User-Agent Host Connection Accept-Encoding Content-Length	2956

Questions?

