HBO max

DTC Security ⇄ Fraud Management

Piracy / Content Security Investigation Overview

10 August 2021

Agenda

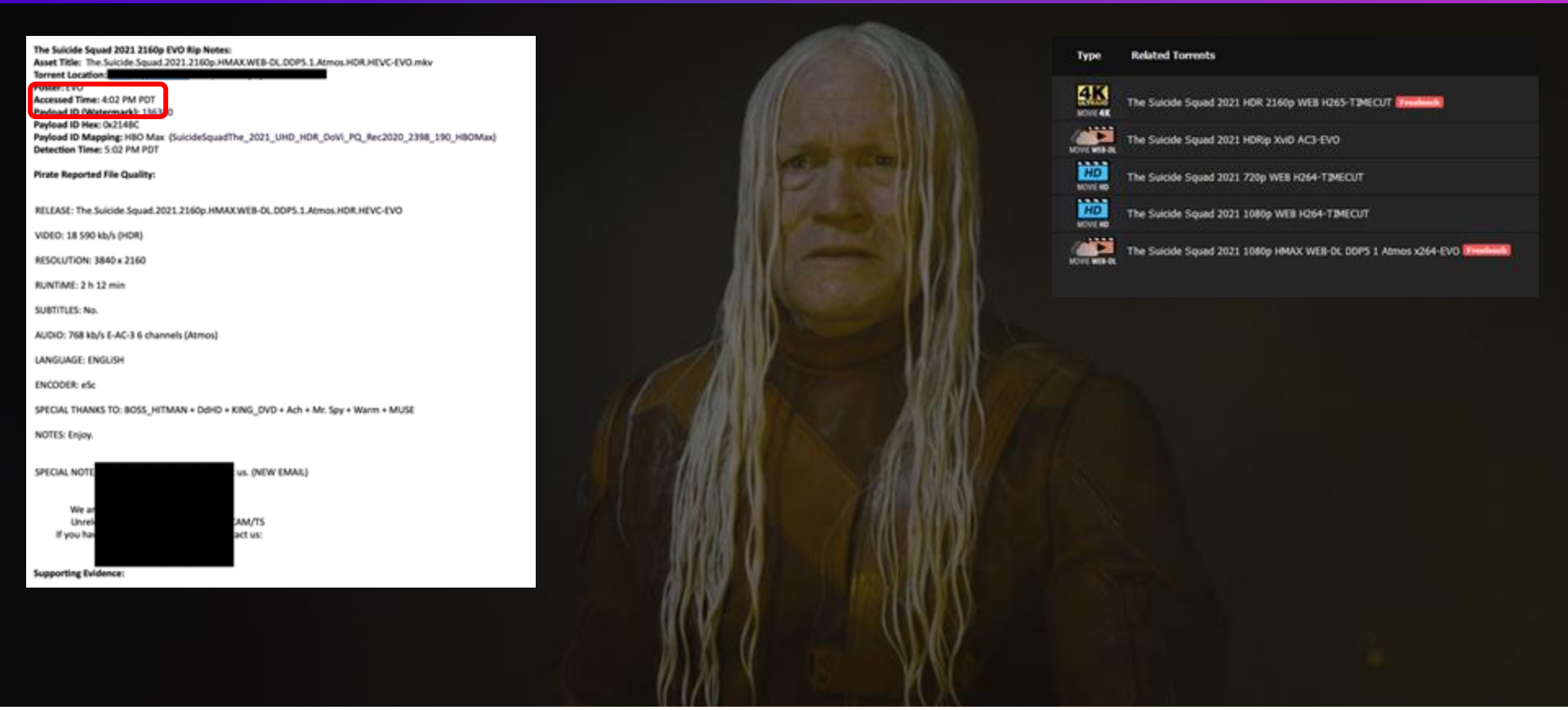
DTC/FM Joint Piracy Operations Overview

a. Popcorn Release Piracy Research Overview
b. Account Integrity as a Contributor to Piracy

Technical Overview, Challenges, and Roadmap

Questions and Answers

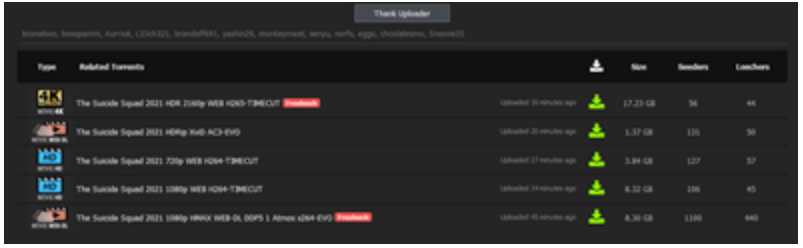
We Have A Porblem.

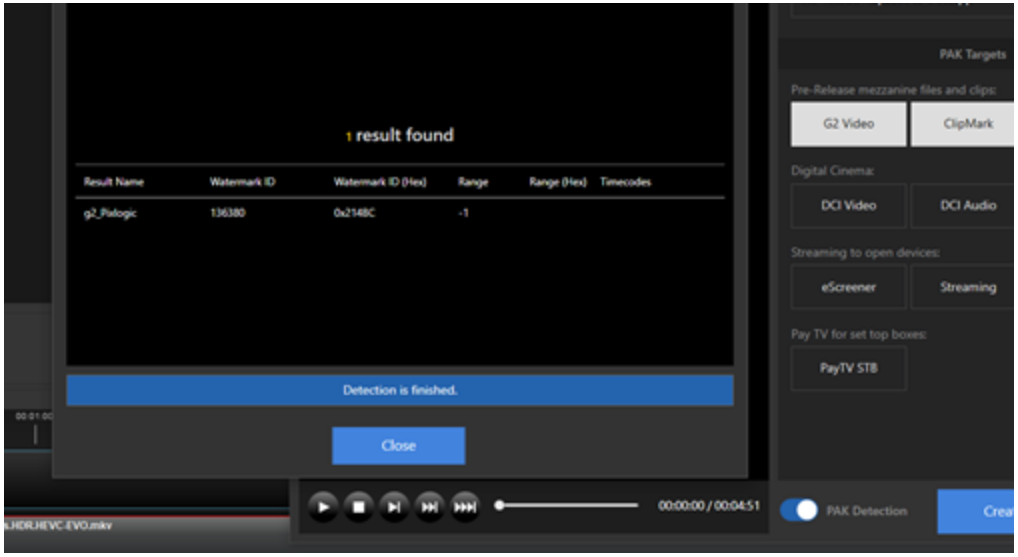


Pirate Party Popcorn Party

Joint Piracy Operational Tooling

- Pulls of CDN and DRM Logs
- Custom Built Torrent Scraping Tooling
- Industry Watermark Detection Software
- Good Old Internet Sleuthing
- Highly Calibrated Mark 1 Eyeball





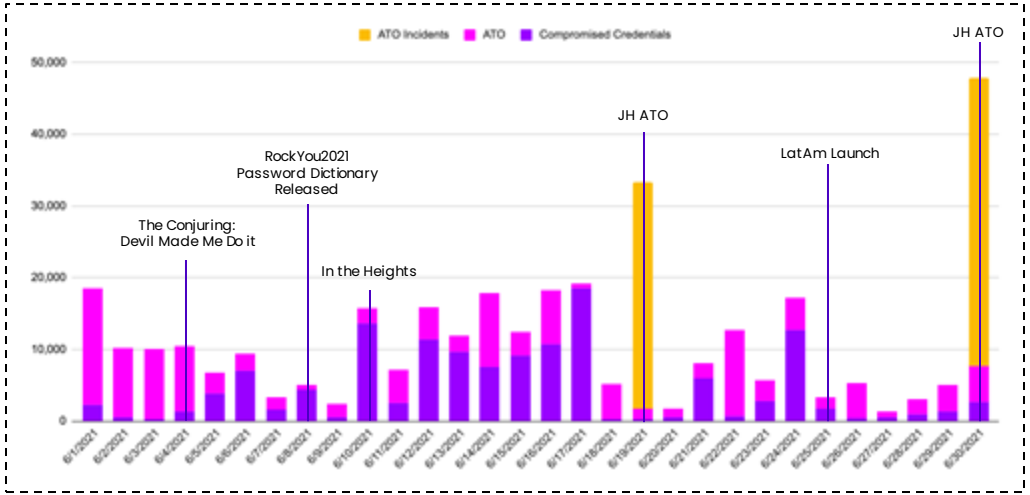
Joint Piracy Operational Goals

- Confirmation of high quality (4K/UHD) content theft with accurate timestamps and tooling familiarization for possible expansion of operations
- Independent verification of vendor reporting for content theft
- DRM functionality research and piracy operation intelligence
- Accurate timestamps of pirated release to narrow CDN and DRM log reviews
- Cool Eyepatches and Team Parrot *(budget pending on*

Account Integrity

Why can't we just drop user-based session based watermarks on our clients and be done with it?

Account Takeover and Compromised Accounts



June 2021 ATO and Compromise Activity

- High level of Compromised Credential and Account Takeover activity increases the likelihood that the source account of an asset was stolen or used against the account holder's knowledge
- This makes targeted legal actions accounts difficult at best, however identifying source accounts would provide valuable and specific logging as well as a pathway to increase friction on specific accounts

June KPIs

Recovered Accounts

Number of customer accounts which have been repaired including password resets and email rollbacks.

344.7 k

May: **68.2 k**

Trending: ⇧

Email Notifications Sent

Emails sent to active customers only to alert them for password resets.

167.1 k

May: **47.3 k**

Trending: ⇧

Login Success Rate

Indicates the percentage of traffic that legitimate *(Credential stuffing activity lowers this rate)*

7.81%

May: **9.17%**

Trending: ⇩

Pirates and “popcorn” releases

Sent: Tuesday, December 8, 2020 2:39 PM
To: [redacted] (HBO) <[redacted]@hbo.com>; [redacted] (HBO) <[redacted]@warnermedia.com>; [redacted] (HBO) <[redacted]@hbo.com>
Cc: [redacted] (HBO) <[redacted]@hbo.com>; [redacted] <[redacted]@warnerbros.com>
Subject: RE: HBO Max rip

CONFIDENTIAL

Online chatter:

Online chatter in early December before we’d put out any Ultra HD content

“Wonder Woman 1984 will be ripped”

We heard chatter that:

- WEBDL encoders will produce WEBDL content from HBO MAX platform using L3 CDM keys.
- Rippers are outside the U.S. and would need to use VPN
- These three groups have access to L1 keys compatible with HBO MAX: [redacted], [redacted] and [redacted] They claim that they will try to get WW1984 pre-release date and all pre-release requires L1 keys.
- They claim they will leak WW1984 in a 1080p English-language WEBDL
- Custom modified Bluray drives are currently used to dump scene Blurays. This Bluray drive purportedly has a custom modified laser and firmware to facilitate the bypass of content protection.

We have been investigating the release groups and local law enforcement is now handling[redacted]

Let us know if you have questions

Thank you

[redacted]

Pirates and “popcorn” releases

- *Wonder Woman 1984* on 2020-12-25
  - 45 min. to Full HD rip from HBO Max
- *The Little Things* on 2021-01-29
  - 3 min. to Full HD rip from HBO Max

NOW-TYPICAL PATTERN

FHD and UHD rips up to private torrent network within 10 minutes of HBO Max release (usually 5 minutes … sometimes 2 minutes)

Sent: Friday, January 29, 2021 10:12 AM
To: Subject: The Little Things Content Protection Summary - January 29, 2020

Dear All,

Two digital sources for The Little Things are online and are high quality with English audio and English subtitles. Updated/new source information is highlighted in yellow.

The online dates are summarized below.

Pirate Date	Quality	Payload	Source
January 29, 2021 12:04 AM PT	HD	59715 DETE	HBOMax
January 29, 2021 12:13 AM PT	UHD	91689 Pixelogic	HBOMax

Audio online	Date
January 29, 2021	English

Pirates and “popcorn” releases

JULY 2020 →

ASSESSMENT REPORT

TURNER BROADCASTING SYSTEM, INC.

HBO MAX CONTENT SECURITY ASSESSMENT 2020

JULY 8, 2020

EXECUTIVE REPORT

Project Overview

Turner Broadcasting System, Inc. engaged [redacted] to assess the security of the HBO Max applications. The following report details the findings identified during the course of the engagement, which started on June 8, 2020.

Goals

- Identify any implementation flaws in the digital rights management (DRM)
- Test and document HBO Max's adherence to the content security requirements set forth by studios
- Test and recreate attacks from streaming piracy software
- Attempt to copy DRM-protected content from CDNs
- Verify region locking is in place to prevent content from being accessed in restricted countries

FINDING COUNTS
1 Low
5 Informational

6 Total findings

SCOPE
HBO Max DRM

DATES
06/08/2020
Kickoff

06/08/2020 – 06/26/2020
Active testing

07/08/2020
Report delivery

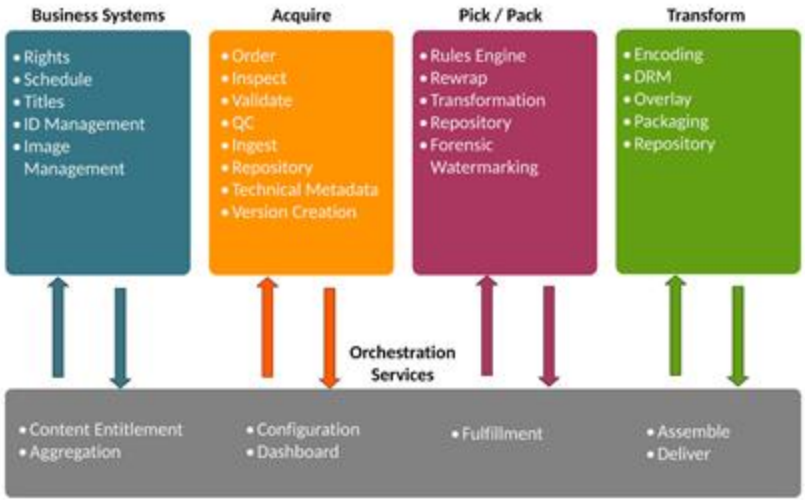
Summary of Findings

The HBO Max mobile applications for iOS and Android were found to follow modern best practices for DRM implementations, and the use of FairPlay and Widevine DRM preemptively thwarted common attacks such as key interception and forced DRM downgrades for both online streaming and offline viewing. At no point in the assessment were content encryption keys exposed, and no methods were identified by which an attacker could rapidly download and decrypt protected content. Well-known screen

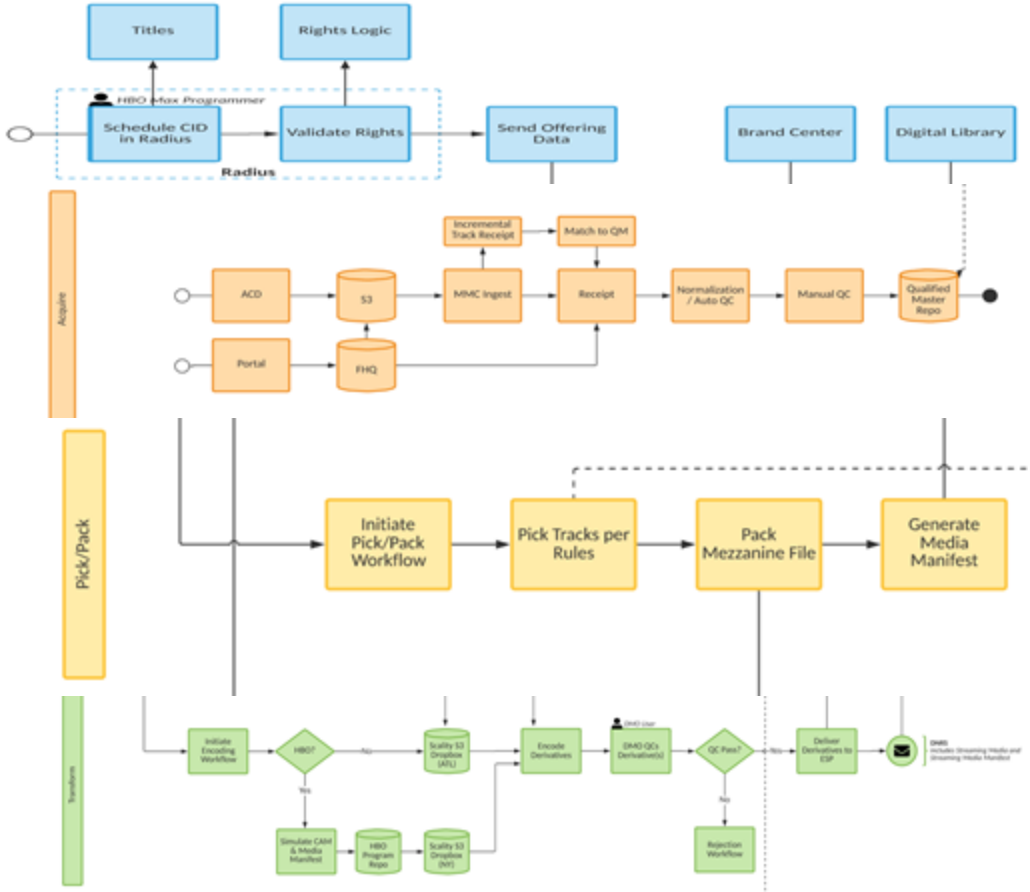
Content security assurance efforts to date

- **DTC Security goals for content security**
  - Stop faster-than-runtime Ultra HD content rips
  - Stop Ultra HD “screen recordings” <-> Stop faster-than-runtime Full HD content rips

Attack Surface : Content supply chain



- In order to effectively protect our content we must completely understand how content is delivered, from Distributor to Consumer.
- The DTC Security Team conducted a threat model across our known MSR.



Attack Surface : Vs. Industry Peers

- We do not have DRM in-house so rely on Google, Microsoft, and Apple's overall settings for how we license content to specific devices
    - Bringing Widevine in-house is on HBO Max roadmap and expected later this year

- All devices go through the same authentication pathway, limiting what security controls we can use there

- Our Media Delivery architecture uses 5 separate CDNs with dynamic switching and no access control
    - This is performant but sacrifices security
        - Inconsistent levels of logging
        - No explicit authN, authZ, or access control

- No user-based or session-based watermarking.

Attack Surface : DRM Introduction

Attack Surface : DRM Introduction

Attack Surface : DRM Widevine

Security Level	Device/Technical Differences	HBO Max Top Quality Provided	
L1	Video processing and decryption occurs all in trusted execution env. (TEE)	2160p , Dolby Atmos, etc.	
L2	Video processing occurs outside TEE, decryption occurs inside		
L3	Does not have a trusted execution area (TEE) so sensitive stuff hidden in usual device memory	1080p	• WEB BROWSER • OLDER PHONES • OLDER DEVICES

Attack Surface : DRM Widevine L3

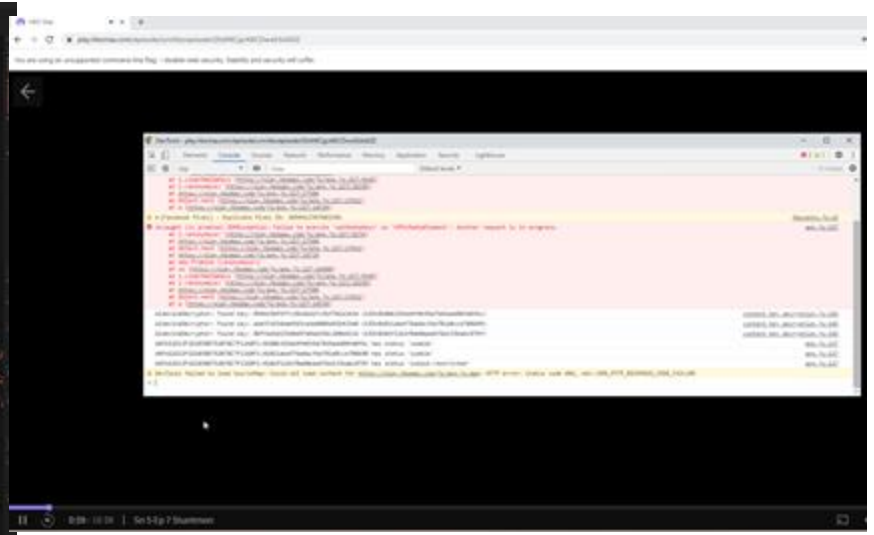
NOVEMBER 2020

Attack Surface : DRM Widevine L3

content_key_decryption.js > ...

```
/*      Tomer, 4 months ago • Initial commit
This is where the magic happens
*/


var WidevineCrypto = {};

(function() {

// The public 2048-bit RSA key Widevine uses for Chrome devices in L3, on Windows
WidevineCrypto.chromeRSAPublicKey =
`-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtdHcRBiDWWxdJyKDLTPO9OTapumVnW+9g6k3RSflM0CESFEufZUJG
aOibJklLBkd7Yfn1OndVrenMKTE1F4/6jgSrmwyv4qFQ1u8M/ThZUrAgb8pTmKfb9vrv1V8AApwVzcQg3s48eESnKjBU99Vk8
YrOzlde+V3UOb5FVzPcrOmaERfyujV3h4sHGRbTCsqYVwMalO7hmNmtemwt0x8uf5Juia7t1scuJypQ8lI1iEsB+JZVo3Uovf
CQIDAQAB
-----END PUBLIC KEY-----`;

// The private 2048-bit RSA key Widevine uses for authenticating Chrome devices in L3, on Windows
// Extracted by applying some mathematical tricks to Arxan's white-box algorithm
WidevineCrypto.chromeRSAPrivateKey =
`-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC10dxEGINZbF0nIoMtM8705Nqm6ZWdb72D
dYHRc7Fo6JsmSUsGR3th+fU6d1Wt6cwpMTUXj/qODmubDK/ioVDW7wz90FlSsCBvylOYp9v2+u/VXwACnBXN
ozB+02xis7OV175XdQSvkVXM9ys6ZoRF/K6NXeHiwcZFtMKyphXAxqU7uGY2a16bC3TEG5/km6Jru3Wxy4nK
YCKtYe8JAgMBAAECggEAGOPDJvFCHd43PFG9qlTyylR/2CSWzigLRfhGsClfd24oDaxLVHav+YcIZRqpVkr1
Hf91+KVFk+fGdEG+3CPgKKQt34Y0uByTPCpy2i10b7F3Xnq0Sicq1vG33DhYT9A/DRIjYr8Y0AVovq0VDjWq
0GVk17YpBiB/iTpw4zBUIcaneQX3eaIfSCDHK0SCD6IRF7kl+uORzvWqiWlGzpdG2B96uyP4hd3WoPcZntM7
HqDPduIm4hEAZf6sQLd8Fe6ywM4p9KOEVx7YPaFxQHFSgIiWXswildPJl8Cg5cM2EyMU1tdn5xaR4VIDk8e2
IhlLdcYp5KxiJ3mwINSSO94ShwKBgQDavJvF+c8AINfCaMocUX0knXz+xCwdP430GoPQCHa1rUj5bZ3qn3XM
Zo4OF7IUedFBS5B508yAq7RiPhN2VOC8LRdDh5oqnFufjafFB2y9d+/czCrVIG43D+KO2j4F7wKBgDg/HZWFi
jVilOcZAvXOMTA5LMnQ13ExeE2m0MdxaRJyeiUOKnrmisFYHuvNXM9qhQPtKIgABmA2QOG728SX5LHd/RRJq
```

Tomer, 4 months ago Ln 1, Col 1 Spaces: 4 UTF-8

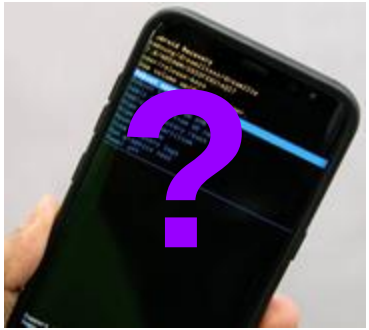


```
WidevineDecryptor: Found key: 8994158f5f7c381dbd27c5bf7022163d (KID=0100b325be9f4639a79d5add80fa8f6c)
WidevineDecryptor: Found key: ede37d324da4363cedd6009a592433e8 (KID=01011abdf76a4acfbb781a8cce708698)
WidevineDecryptor: Found key: 88ffad2d235b0d97e4ee254c288b4116 (KID=0102f1161f8a40eab676d133ba6c879f)
A4FA21D13F1D10388752078C7F1168F1:0100b325be9f4639a79d5add80fa8f6c has status 'usable'
A4FA21D13F1D10388752078C7F1168F1:01011abdf76a4acfbb781a8cce708698 has status 'usable'
A4FA21D13F1D10388752078C7F1168F1:0102f1161f8a40eab676d133ba6c879f has status 'output-restricted'
DevTools failed to load SourceMap: Could not load content for https://play.hbomax.com/js/app.js.map: HTT
>
```

Attack Surface : DRM Widevine L1

- **DTC Security goals for content security**
  - Stop faster-than-runtime Ultra HD content rips
  - Stop Ultra HD “screen recordings” <-> Stop faster-than-runtime Full HD content rips

Determine compromised decryption keys (device system ID) so Widevine* can revoke

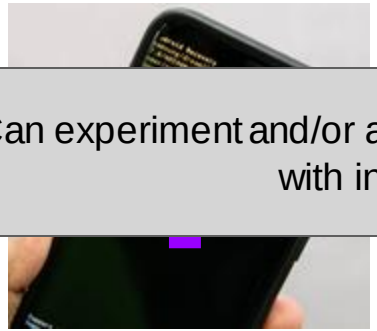


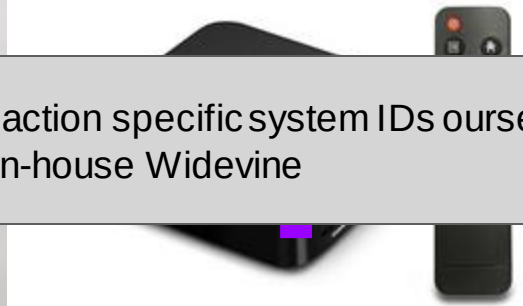
** Once we have Widevine DRM in-house, we could downgrade or otherwise handle more granularly than full key revocation*

Attack Surface : DRM Widevine L1

- **DTC Security goals for content security**
  - Stop faster-than-runtime Ultra HD content rips
  - Stop Ultra HD “screen recordings” <-> Stop faster-than-runtime Full HD content rips

Determine compromised decryption keys (device system ID) ~~so Widevine* can revoke~~

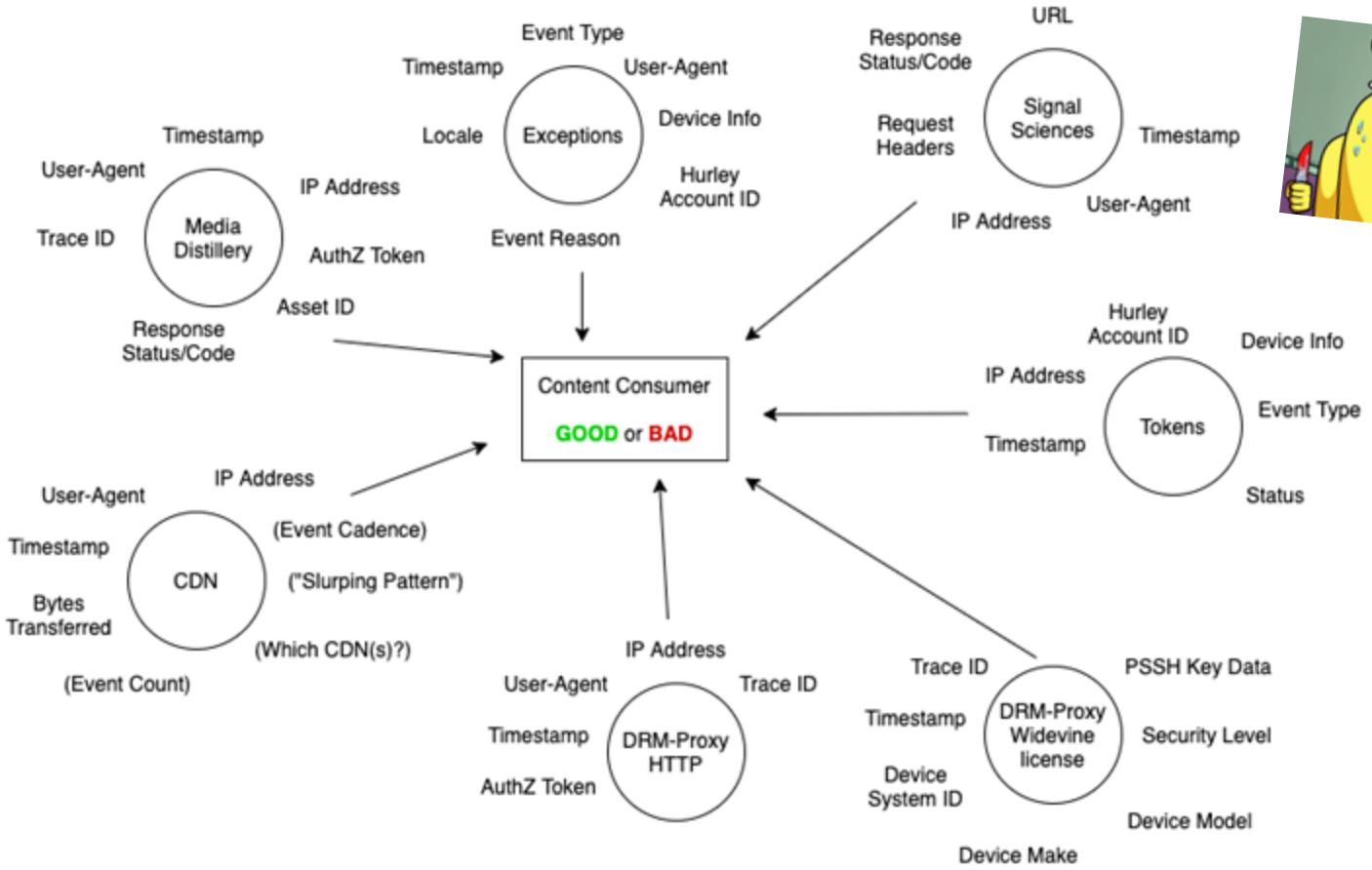




Can experiment and/or action specific system IDs ourselves with in-house Widevine

** Once we have Widevine DRM in-house, we could downgrade or otherwise handle more granularly than full key revocation*

Attack Surface : Logging and data around content consumption



Smart device client

Billions of daily requests

fastly

comet.api.hbo.com
gateway.api.hbo.com
(*N* variations …)

Signal Sciences

WAF

Tokens service

reCAPTCHA Enterprise

User table

Android & iOS

Mobile client

reCAPTCHA Enterprise

play.hbomax.com

www.hbomax.com

Web browsers

reCAPTCHA Enterprise

Millions of daily requests

fastly

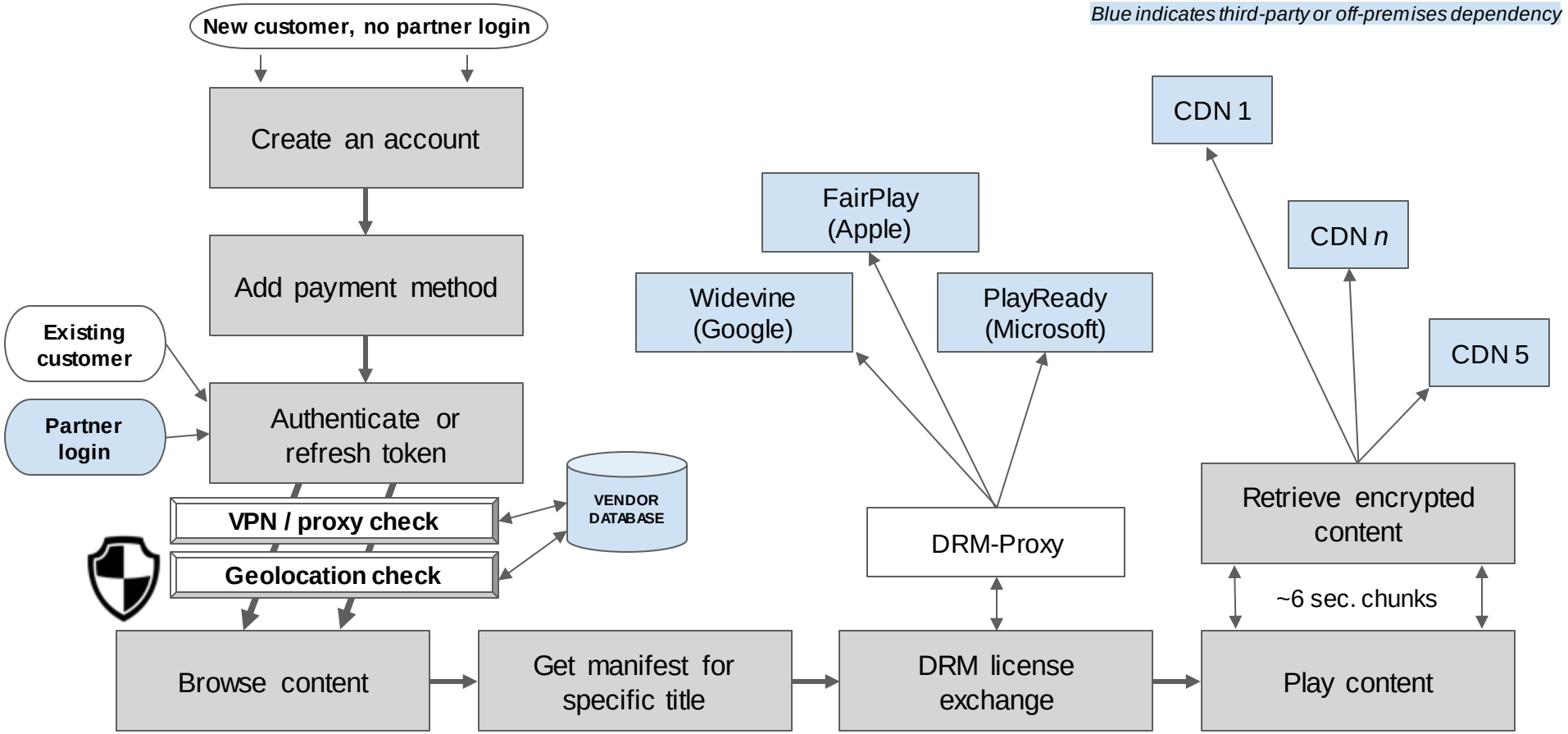
commerce-experience.api.hbo.com

AWS WAF

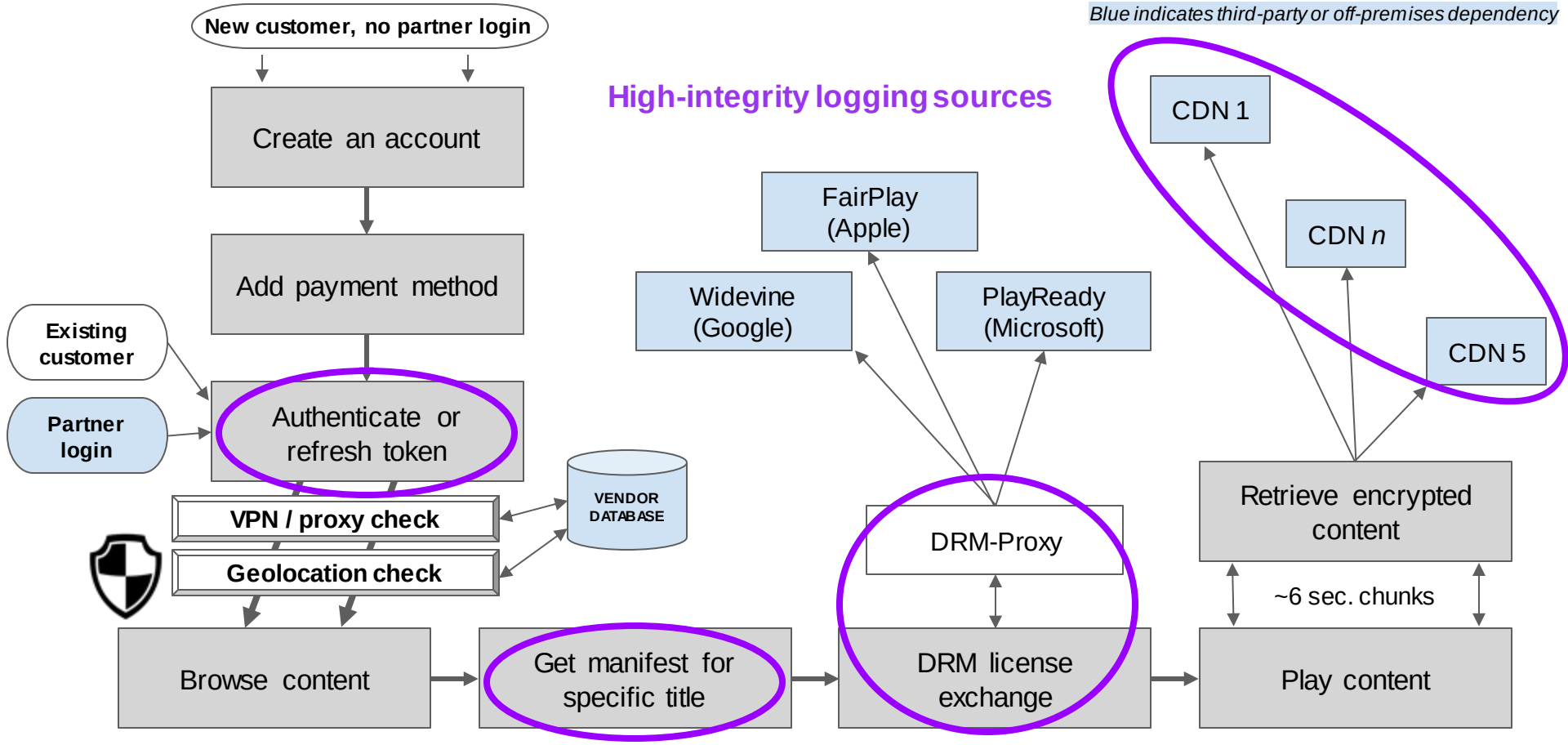
Buy flow login service

reCAPTCHA Enterprise

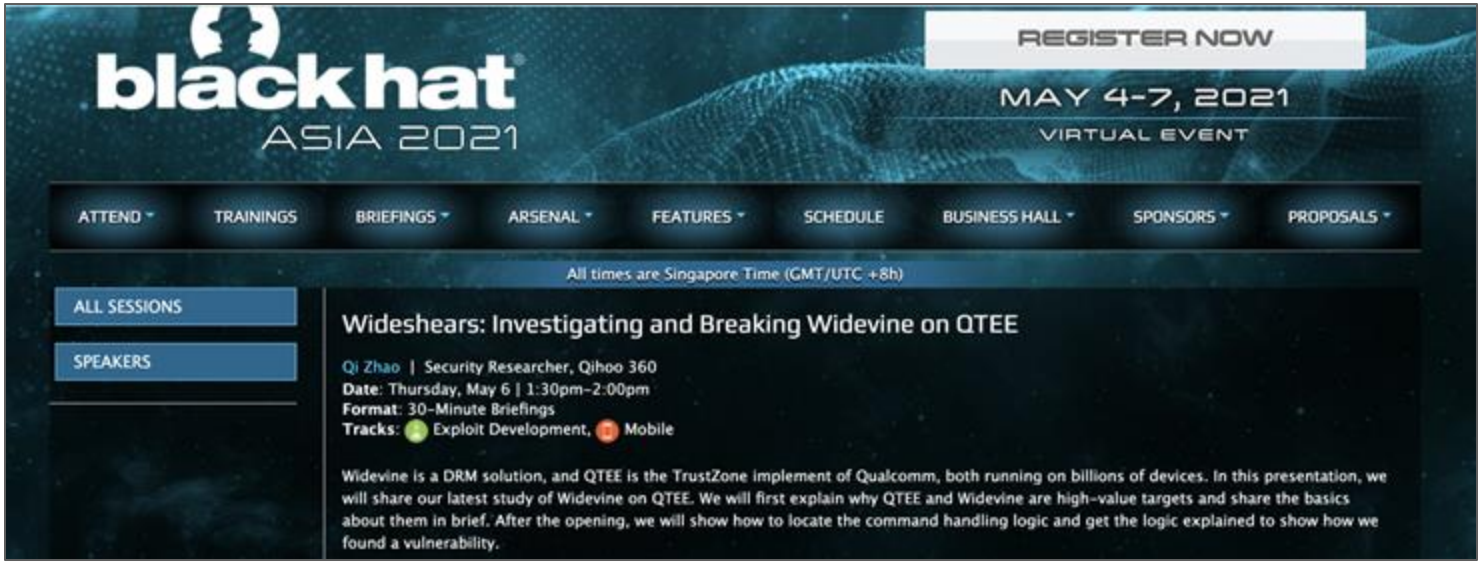
Attack Surface : Logging and data around content consumption



Attack Surface : Logging and data around content consumption



Black Hat Asia 2021 exploit



- **blackhat.com page**
- **Slides link (PDF)**
- **Whitepaper link (PDF)**

Steps forward

- **Widevine DRM in-house**
  - Act on specific device IDs, i.e. limit quality of Qualcomm exploit-affected devices
    - Anything suspicious in the future

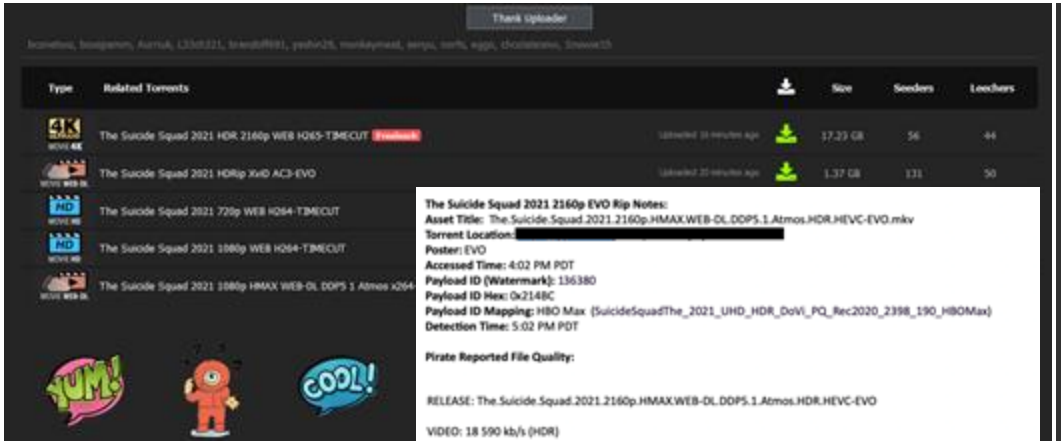
- **User Level based watermarking pilot**
  - Identify accounts that are the source of leaked content to perform targeted analytics on content thieves.
  - Allows for future action against repeat offenders and increased friction on accounts with weak security

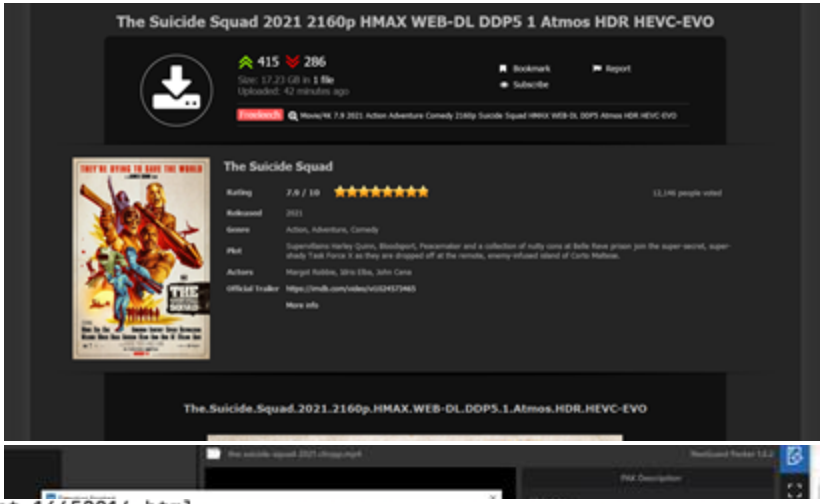
- **Continue other product security and fraud measures**
  - All connects together, i.e. login attacks degrade integrity of “who” an account is

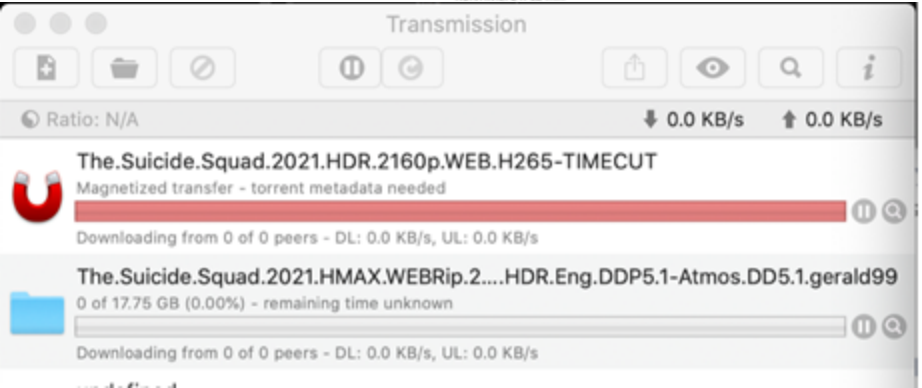
Questions?

(BACKUP)

Popcorn Release Joint Piracy Operations








```
IMECUT-torrent-16453214.html
[WARNING] config.execution.do_downloads is TRUE but no magnet link to download.
------------------------------------------------------------------------------
ID : 50559768
Time : Thu, 05 Aug 2021 23:46:03 GMT
Title : The.Suicide.Squad.2021.2160p.HMAX.WEB-DL.DDP5.1.Atmos.DV.MP4.x26
Provider : ThePirateBay
Seeds/Peers : 0/0
Magnet : magnet:?xt=urn:btih:540F9D134F8FE9B4005AB098D4E34CCC89F26314&dn=undefin
ed&tr=udp%3A%2F%2Ftracker.coppersurfer.tk%3A6969%2Fannounce&tr=udp%3A%2F%2F9.rar
bg.to%3A2920%2Fannounce&tr=udp%3A%2F%2Ftracker.opentrackr.org%3A1337&tr=udp%3A%2
F%2Ftracker.internetwarriors.net%3A1337%2Fannounce&tr=udp%3A%2F%2Ftracker.leeche
rs-paradise.org%3A6969%2Fannounce&tr=udp%3A%2F%2Ftracker.pirateparty.gr%3A6969%2
Fannounce&tr=udp%3A%2F%2Ftracker.cyberia.is%3A6969%2Fannounce
[INFO] Adding torrent to your Transmission torrent client...
------------------------------------------------------------------------------
```

Our Data Structure is a Tangled Web 🕷🕸

To make any sense of a specific user's behavior on our service using one of a series of key indicators, we have to perform a complex series of joins and backflips to get to actionable account information🕷🕸

[Something about systematizing account behavior detection goes here]