SCTE·ISBE CABLE-TEC EXPO 2018 ATLANTA, GA OCTOBER 22-25

2018 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Analyzing the Modern OTT Piracy Video Ecosystem

A Technical Paper Prepared for SCTE•ISBE by

Don Jones
Senior Manager
Comcast Cable Communications Management, LLC
4100 East Dry Creek Rd, Centennial CO 80122
303-712-3588
Don_Jones@comcast.com

Kei Foo
Senior Manager
Charter Communications
8560 Upland Drive, Suite B, Englewood, CO 80112
720-518-2343
Kei.Foo@charter.com

Table of Contents

Introduction

This paper outlines contemporary so-called "pirate" video content ecosystems and enabling technologies. It describes the methods used to acquire, package and distribute this content that largely consists of works that infringe copyright by being used without the permission of the copyright owner in the underlying video content. The primary intent of this paper is to clearly define the sources, distribution mechanisms and sales channels that allow the use of this content to grow.

Infringing video content is now being directly advertised, marketed and targeted to the average consumer looking to "cut the cord," often under the false pretense that this content is completely legal. In many cases, the marketing tactic is to sell inexpensive, Android-based devices preloaded with the Kodi media player preconfigured with add-ons that deliver infringing content. Kodi, formerly known as Xbox Media Center (XBMC), is a legitimate open source media player that can run on almost any operating system or device. The software is written in Python, which allows even the most basic programmers to quickly create an add-on that can link to any content available. It allows the author to enter links to content found across the Internet and allows playback of video files as well as the ability to view live streams and offer the Kodi user a graphically-rich environment with electronic program guide, poster art, movie information, closed captioning and allows for conditional access. In addition to Android-based devices, Kodi can also be "sideloaded" onto the Amazon Fire TV family of devices, and is often marketed on this hardware platform through eBay, Amazon, Craigslist, and others. While this is referred to as a hardware sales model, several additional business models are being employed, which will be covered by this paper for perspective. According to a 2017 report by Sandvine[i], over six percent of U.S. households currently utilize Kodi to watch infringing content. The Sandvine report indicated that 8.8% of households have an active Kodi installation, however their product has determined that 68.6% of households with Kodi devices also have unofficial add-ons configured to access unlicensed content.

Other standalone, Android-based piracy enabling applications, such as Terrarium TV and Mobdro, have also emerged, most of which utilize Android's Software Development Kit's built-in ad-insertion software. This is known as the "freemium option." Some of these ad-supported applications include an additional "premium option," which removes the ads from the application, similar to Pandora or Spotify. These applications are referred to as an "ad sales model." Versions that have the ads removed are classified as a subscription service as they require a payment.

People contribute to the pirated-content ecosystem either by directly creating unauthorized copies, uploading and sharing their content directly, or by "seeding" content through BitTorrents (downloading a movie, then seeding or sharing it into a torrent peer-to-peer sharing network.) "**BitTorrent**"("**BT"**) is a communication protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet."[ii] BT "protocols move as much as 40% of the world's traffic on a daily basis."[iii] Because content is relatively easy to distribute, it is not possible to completely eradicate infringing video content. This paper will help to better identify the sources, distribution mechanisms, and marketing of infringing video content.

A Brief History of the Pirated-Content Ecosystem

In the early 1980s, as personal computers started to evolve, the need to interconnect them became an imperative. By today's standards, computer speeds were very slow, and lacking in terms of computing power, network connectivity, and storage.

Nearly as soon as people started connecting computers together, file sharing became extremely popular, but only among the few people who were pioneering the Internet.

Initially, content such as video games, software and pornography were shared illegally through Usenet Newsgroups[iv] and local Bulletin Board Services (BBSs)[v]. This was before Mosaic came along to put a stylish user interface and a new protocol (Hyper Text Markup Language) on top of what was considered the Internet. Mosaic, one of the first widely accepted HTML browsers, gave way to what we now know as the click-navigable World Wide Web.

During the 1990s, the Internet and World Wide Web ("WWW") started gaining users, connections speeds increased, and the file sharing system continued to grow with it. Usenet Newsgroups remained a source for content sharing, but faded into the background. Similarly, BBSs mostly disappeared, as new technologies became available. Internet Relay Chat[vi] was born and was also used to share unauthorized content, but has similarly faded in usage. The term "warez" (pronounced "ware" with a "z" at the end) became synonymous with illegally downloaded content.

1992 marked the start of the exponential growth of the Internet, as the number of online websites surpassed one million[vii]. As the Internet and the WWW grew, so did the scale of the illegal downloading of copyrighted material. In June of 1999, the average Internet user was learning about file sharing, most specifically with music, which coincided with the start of a service called Napster. This service allowed anyone on a PC to download the application and immediately start downloading and sharing their music collections. Napster was shut down due to the aggressive prosecution of the Recording Industry Association of America (RIAA) in 2001. However, in 2000, the Limewire Service was born (as well as Kazaa and a few others), which expanded the scope of music sharing to include software, video games and movies. Limewire continued to grow until 2010, when it, too, was finally shut down.

After learning that a central distribution topology made the pirate ecosystem vulnerable to fast take downs (as in the case of Napster), the BitTorrent (peer-to-peer sharing) was created in 2001 to disperse the content and multiply the sources of downloads, making the content availability much more resilient. BitTorrents (or torrents) became popular around 2006, and are still used today to fuel the Video-on-Demand (file-based) portion of the pirate ecosystem. A torrent works by sharing small parts of files from many users, which increases the speed of the download as well as the availability of the file. Torrent files also contain a tracking URL, which makes IPs addresses easier to identify on the network. Torrents are currently giving way to "magnet links." Magnet links work similarly; however, they lack the tracking URL information, which helps keep the user's identity anonymous.

The WWW provides an online storefront for business to promote their product and services directly to consumers. It also paves ways for pirates to offer their pirate devices and services directly to the public. The advances in website development have made it very easy for anyone to build a brand new website within minutes, just by signing up for a website design service and using a web design template. These professional-looking websites can also make it challenging for an average consumer to distinguish between legitimate and illegitimate services. While these advances in website development do promote e-commerce, they also make it easy for pirates to re-brand themselves when enforcement happens. Web hosting companies for the online storefronts do not proactively look for web sites that infringe others' content rights. They rely on content owner to report abuse and infringement through online reporting. Because it is so easy to register a new domain and create a new online storefront, pirates can easily rebrand themselves by building a new website. Today, pirates will use social media to notify the public that their site has been "moved" to a new website, and re-direct potential customers to visit there. This is an important part of the piracy ecosystem, because it provides the public compelling, authentic-seeming entrances to consume pirated content.

Pirates, aggregators, distributors, and consumers are financially incentivized to continue their ways. The availability of online payment systems (or e-payment system) that were originally designed to serve legitimate small businesses to collect payments, also make it easier for pirate content distributors to collect revenue. For the distributors and aggregators, the revenue streams include direct cash for ads and content sales/subscriptions. For consumers of pirated content, they benefit from reduced entertainment costs and an increased scope of titles, including "in theaters now" content. This also provides the pirate consumer with a higher availability of content. They are not as easily dissuaded from using unauthorized content, and have become accustomed to seeking other ways to find the content they desire. As technology continues to evolve, new sharing techniques will be developed, with better obfuscation. New countermeasures will need to keep pace.

The Financial Impact of Piracy

A 2010 Government Accountability Office report cast doubts regarding the accuracy of a 2006 MPAA study which found that pirated video content costs the entertainment business more than $6 billion in annual losses as well as other studies, including one in 2008 from the Business Software Alliance on software piracy (claiming over $9 billion in annual losses). The GAO study concluded that, while piracy is bad for the U.S. economy, it's extremely difficult to quantify just how bad. As such, there remains a dire need for quantitatively-sound studies that inspire broad confidence. Many studies have detailed the financial impact of online piracy.

In 2017, Sandvine published a report[viii] finding that 6.5% of North American Households are accessing known piracy services for subscription television. They estimated that the financial impact to U.S. cable service providers alone is $4.2 billion dollars a year.

Monitoring pirated content is also complicated by the number of web users employing VPN is on the rise, which obfuscates the current monitoring of pirate traffic. The rise in VPN usage could very well signal that more pirates are "going dark" rather than stopping illegal activity.

Beyond the overall financial impact, here are two examples of the impact piracy has had on movie franchise as well as one pay-per-view (PPV) event:

Movie Theater Return Impact:

Piracy can damage the likeliness of a sequel. For example, the Kick-Ass movies came to an end due to lack of funding from piracy. According to Chloë Grace Moretz who stars as "Hit-Girl" in the series, Kick-Ass 2 was one of the most pirated films of 2013 despite having an extremely low Box Office Revenue…" [ix] . "Kick-Ass 2' was one of the number one pirated movies of the year, but that doesn't help us because we need box office figures. We need to prove to the distributors that we can make money from a third and a fourth movie - but because it didn't do so well, we can't make another one.

If you want more than one movie, everyone has to go and see movies at the cinema. It's all about the numbers in the theater."[x]

PPV Event Impact:

The most anticipated fight in 2017 was Mayweather vs. McGregor. The suggested retail price to order the PPV event was $89.95 and an additional $10 for HD version of the event. According to an article from Yahoo!Sport, "two screenshots from Facebook Live showed 472,000 viewers watching a pirated stream, while the other had 234,000 viewers. Just the viewership from those two streams could cost the event

more than $70.6 million"[v]. The cost could potentially be higher, as Irdeto, a digital platform security company, discovered 239 streams that reached 2,930,598 viewers."[v]

Business Models of the Pirate Offerings to Consumers

The most pervasive sales model is the hardware sales model. This is the easiest model to sell, as it requires very little support or maintenance. The hardware sales model is simple: Someone acquires an Android-based STB (less than $50 in most cases) or Amazon Fire TV device, loads Kodi, then loads a handful of pirate-content-enabled add-ons. These add-ons are free to download, install and use. The add-ons are preconfigured to automatically update from their respective repositories, each time the Kodi application is launched. New content and configurations (i.e. pointers to new movies or streaming locations) are updated on the device. From the retailer's viewpoint, unless a device is malfunctioning, the customers of that device will not need to contact them again. The resale of these devices ranges from $99-$399 and come with hardware warranties. The hardware sales model usually includes Kodi and some pirate add-ons, and is often augmented with ad-supported Android piracy applications, since they are also free to download and use.

The next most common sales model is the subscription sales model. This model has several derivatives. The first is a monthly/annual charge for access to content delivered by one add-on. These Kodi add-ons are usually maintained, to ensure most assets are available, and usually charge a monthly fee of about $10-$25 for access to their playlist. The add-ons can be installed in any Android type device, PC/MAC, Linux or simply a smartphone.

The second involves using a STB device known as a MAG (MAG250, MAG 254, Infomir). These devices are different than the Android/Kodi-based devices in that they do not store the streaming information on the device, as Kodi add-ons do, but securely login to a web portal (known as a "stalker portal") for command and control, downloading the latest M3U playlist file from the portal every time the device is turned on. These devices mimic a cable STB experience more closely in that they download a "channel map" which the user can navigate, just like a cable STB, to create favorite channel lists, etc. Some subscription services also include PPV events like UFC fights. The subscription sales model usually is accompanied by a customer support phone number; in some cases, 24x7 customer support is available.

The latest product to emerge in delivering pirated video content is referred to as the ad-supported model. Android based ad-supported applications greatly increased in number in 2017, and are expected to continue to grow. The reason is that such applications can essentially run on any device that can support an Android emulator, without the need for the user to obtain any new hardware. The Android Development SDK (software development kit) allows any programmer the quick and easy ability to integrate ad insertion capabilities into any Android application. This gives the author of the application the sole ability to monetize their platform for themselves, as opposed to Kodi add-on authors who would have to create custom advertisement insertions. iOS ad-supported applications have been developed but are fewer than Android based applications it is a bit more technical to allow iOS devices to bypass their own security and use unverified 3rd party applications. In the Android space, this is accomplished with a simple change in the settings.

Another pirate marketing and delivery strategy requires no device at all and enables the owners of Smart TVs to directly view pirated video. This is referred to as the Smart TV-based model. Most manufacturers of Smart TVs have "Application Stores" that provide the consumer with a number of free and paid IPTV player applications (such as SS-IPTV, OTT Player, and Perfect Player). These applications are, configured with the consumer's credentials and the web address of the pirate server (portal) that allows the TV to download a playlist from their IPTV provider. Once the playlist is loaded, all the services the IPTV provider supplies become available to the consumer. This platform not only provides the command and control (conditional access) but also allows for ad insertion, closed caption data, Electronic Program Guide, poster art, channel logos and VOD playback. The platform does require a small amount of technical ability, in that the consumer would have to download and install the application, go to a website presented by the application and enter the MAC address of the television.

Two Types of Content Delivery

There are two general types of unauthorized content being delivered today: Live streaming and Video on Demand (file-based playback of a recording).

Live streaming usually involves some sort of playlist (M3U, XML, etc.) that points the media player to a streaming source, then joins a live broadcast stream (such as an RTMP, MMS, ACESTREAM, HLS or other stream format.) These playlists and media players are capable of conditional access, EPG, poster art, channel logos and ad insertion.

Video on Demand or file-based playback can also be included in these playlists. The Kodi add-ons also provide access to video libraries stored on websites or CDNs (content delivery networks), without having to go through the website navigation. It blocks pop-up ads and Captcha/Recaptcha challenges (designed as a DDoS attack prevention method) that are inserted by "indexing" websites. Indexed web sites do not store the content, but rather serve links to CDN servers.

Live Streaming Content Acquisition

While streaming sources of unauthorized live content vary, the majority of such sources are coming from satellite content. Several satellite hacking mechanisms exist that fuel a great majority of the live video content. The first and most predominant method of satellite content acquisition is based on the "CCcam Cardsharing" system (also known as control word sharing). Card sharing is a method that allows multiple client devices (receivers) to access subscription services based on an aggregation of authorizations of valid subscription Smart Cards. The primary flaw in these types of Smart Cards lies in the decrypted control word being sent from the Smart Card to the host box. The decrypted control word is then captured by a network intercept and commences the forwarding of the decrypted control word (64 bit, very small) from one card to a CCcam Server. All other devices that join this CCcam server can now have access to the conditional access keys stored on the CCcam server, and view all the content that the first Smart Card was authorized to receive. As more clients join the pool, each of their authorization levels are added to the pool of authorizations and made available to all clients in that CCcam server. Once all channels have combined authorizations, everyone who joins the CCcam server is now authorized for every service on the satellite. One of the most predominant receivers in this category is called the DreamBox, however, there are a good deal of Linux-based satellite receivers (Enigma, Enigma 2 etc.) that can also be modified to use the CCcam server system. All satellite providers using DVB-CSA scrambling have the potential of being impacted by card sharing.

Another method of illegal satellite acquisition is the publishing of satellite locations and their associated BISS keys. BISS (Basic Interoperable Scrambling System) is a satellite scrambling system developed by the European Broadcasting Union and a collection of hardware manufacturers. The BISS-E key (E for encrypted) is a 16-digit hexadecimal value that, when entered into the decoder, can decrypt all the ECM's for that satellite. BISS is just one of many types of security keys systems used in satellite communications that have been compromised. Hacking websites often post discovered satellite keys for BISS, Viaccess, Viaccess 2, Nagravision 1 & 2 (partially broken), Cryptoworks, Conax, Mediaguard (seca) and NDS Videoguard, as well.

All of these mechanisms can be used by pirates to provide access to hundreds or thousands of services, illegally. Satellite receiver PCIe (Peripheral Component Interconnect Express) cards, such as Shenzhen Turbosight Technology's TBS6908 DVB-S2 Quad Tuner, can capture up to four transponders simultaneously per card; two can be used in one computer. Off-the-shelf systems also exist, ranging in price from $99-499 (MOI-V price unknown) and capacity (dual tuner, two transponders through 48 tuners/transponders (MOI-V.) Examples of Linux-based appliances running a few IPTV applications, including TV Headend, include the MOI DVB-S2 Streaming Box, MOI Pro, Moi Pro – AMD, Moi+ and Moi-V. These retail devices come ready to accommodate the TBS-series of cards mentioned above, and are marketed as "IPTV Streamers." From a service volume perspective, each transponder on a satellite carries about 12-32 channels. Each satellite can have from 12 to 96 (though standard C Band is usually 12) transponders. There are over 100 commercial video satellites in geosynchronous orbit, with content availability in almost any language. Both of these acquisition methods are predominantly occurring in European countries because of regulations surrounding set-top interoperability, which accounts for the high availability of European content.

North American cable video operators currently employ video delivery technologies that make bulk acquisition difficult. However, that does not stop authorized users from sharing their content, if the proper security measures are not implemented. Unauthorized redistribution of authorized content ranges from sharing a single "stream" via social media to HDMI streamers capable of taking up to 24 HDMI ports and convert them to IP streams.

Ceton offers its infiniTV6 PCIe card for the computer, which houses six tuners and a CableCARD interface. This device can be used to record or stream up to six simultaneous channels of HD content. Two of these cards can work in one computer to provide capture/streaming capability for a maximum of 12 HD channels. Additionally, the SiliconDust HDHomeRun Prime includes three tuners and a CableCARD interface. Other CableCARD-enabled devices exist in the market that offer varying levels of capture/streaming capability. The CableCARD, allows the capability of using these devices to receive encrypted content. The Hauppauge WinTV-quadHD PCIe card, for instance, includes four 4 QAM tuners, capable of capturing four channels. This device does not have an embedded DRM solution and is only used to capture clear QAM content. Some cable video operators still operate with some channels in the clear; however, these poor protection practices can lead to wide scale leakage of content.

Online IPTV providers such as Filmon (www.filmon.com) offer several hundred FTA (Free to Air) channels but also offer premium live TV and Hollywood movies on demand. As this content is already delivered by IP, acquisition and redistribution can be done in mass, limited only by network speed.

Traditional cable set-tops are also subject to unauthorized redistribution of high quality content. Devices that are designed to split HDMI and remove the HDCP content protection, for instance, have become readily available. HDMI splitters and switches can be purchased for between $10 and $100 from many different sources. New, commercial-grade HDMI streamers have recently surfaced on eBay and Alibaba that offer from eight to 24 HDMI input ports, while simultaneously creating an IPTV output stream for

each input. These devices remove HDCP as well. The latest functionality of these devices allows the operator to use two different input sources, meaning the device can compare the two streams and detect any hashcodes detected in the stream. Hashcodes are used in video for watermarking and logo insertion. The hashcode removal process consists of video comparison and an intentional blurring of any area of the screen that differs from one stream to another.

This comprises the bulk of the "home brew" streaming sources; however, other sources exist and are often streamed through legitimate online streaming services such as Google, Wowza, Amazon Web Services, Akamai, YouTube Live, Facebook Live, Twitter, Periscope, and so on.

During the 2016 Olympics, unauthorized live streams were sometimes seen to have the "Activate Windows" logo on the lower right corner of the screen, indicating that the content was being received into a computer that, in turn, was using screen sharing to redistribute the live video. Evidently, the pirates didn't like to pay for the Microsoft license, either. In a few other cases, viewers could see a black screen with a satellite video barker that the Smart Card had lost authorization (including its ID number.) In other cases, a slate would appear to tell the viewer "we are in a commercial break", tacitly indicating the video was intercepted pre-production before it reached the local broadcast destination.

Live Streaming Content Distribution

In the case of satellite acquisition, the problem of the relative ease of acquiring encrypted video content is accelerated by a protocol called SAT>IP (or SAT-IP). The SAT>IP protocol allows satellite-delivered (DVB-S/S2 RF signals) to be demodulated and converted to IP right at the point of reception in a SAT>IP server. Such a conversion may happen already in the satellite antenna itself (IP-LNB), close to the antenna (SAT>IP multiswitch or converter) or in a master STB. Effectively SAT>IP servers remove the DVB-S/S2 layer and replace it with an IP transport layer. Several open source products have been created, such as TV Headend (the most predominantly used), which is used as a software video multiplexing streaming server and recorder. TV Headend runs on Linux, FreeBSD and Android, and is lightweight enough to even run on a Raspberry Pi. TV Headend has many functions: It can take in video from almost any source, such as DVB-S/DVB-S2 (satellite), DVB-C (cable), DVB-T (terrestrial), ATSC (over the air), ISDB-T (over the air, Japan & South America), IPTV (any IP source), SAT>IP, local or network reachable file libraries and HDHomeRun. It then outputs IP multiplexes, assigning EPGs to streams as well as scheduled recordings. It can transcode the video into any profile (resolution, bitrate, compression etc.), assign stream limits (to avoid over subscription/tiling) and assign password protection.

The limitation to programs like TV Headend is incurred at the network level, in the number of connections that can be made to the server. For this reason, many infringing IPTV providers are "re-streaming" from several different sources, through an online hosting service with substantial network bandwidth. The TV Headend program outputs a playlist in the M3U format. These playlists can be consumed by almost any media player and are used for the Infomir-based (MAG250, MAG254, etc.) devices as well as Kodi directly, VLC (on a computer MAC/Windows/Linux/Android) and any of the pirate add-ons. In many cases, these playlists are published online for add-on authors to update their links and for others to download and use. In the subscription sales model, these playlists are assigned to a specific customer. SAT>IP is only useful in satellite transmissions (DVB-S/S2).

The average playlist size range is 100-300 channels, coinciding with the number of services on four transponders (the input of the PCIe receiver card). There are cases in which there are 3,000-11,000 services in one playlist. Those generally tend to be sourced from Filmon and other IPTV providers as well

as sourcing Video on Demand (or access to a file, which, in an M3U media playlist, plays as a stream) content. "Re-streamers" represent a group of people who subscribe to different IPTV services and combine the content of multiple playlists to output a single, larger playlist. They then offer IPTV services which boast much larger linear channel line ups. The duration of the stream lifecycle is difficult to measure in the case of the freely published playlists. Some streaming locations will stay up for months, while others just a few days.

There are many reasons for the variation in the availability of the streaming sources. Examples include changes in their satellite or key access, someone running their own Stalker Portal feeding subscriber-based Infomir devices, changed channel lineups or changed satellite providers. It could even represent boredom on the part of the person gaining satellite access, what with so many satellite providers from which to choose. Some sites publish these lists very frequently, although the trend seems to be once a day for larger lists. There are hundreds of websites that provide access to CCcam servers and IPTV Playlists, often on the same sites, although some specialize in one side or another. Again, these playlists can be used on any media player device, PC, Android STB, Amazon Fire TV Stick or on most Smart TVs -- but are most often included into the Kodi pirate add-ons.

Video on Demand Acquisition

The Video on Demand content acquisition points are far more distributed than the live video streams. One of the largest sources of infringing video is the BitTorrent peer-to-peer file sharing system. In 2016, the correlation between asset file names used in the Kodi add-ons, and the naming of the torrent file, was very clear to see, and substantiated torrents as the primary source of most VOD assets in the pirate video ecosystem. Since then, most Kodi add-on authors have begun obfuscating the links, in an attempt to reduce that level of visibility. The P2P sharing system can source 70% to 80% of a digital locker's inventory. One source into the P2P ecosystem for pirated video content is Oscar screeners (movies that are provided to movie critics and industry professionals, whose role it is to evaluate new movies before their theatrical release), which are often leaked into the P2P sharing system and represent very high video quality copies of the assets. Another source for the P2P ecosystem are individuals who share their personally purchased DVDs, Blu-Ray disks and movie digital copies. Still another source is "cam" versions, or video recording of a theatre screen presentation of a movie. This keeps the already massively large library of infringing video content updated with the latest content. Copy protection from this media has already been breached and can easily be removed by open source applications that strip copy protection mechanisms. The P2P system creates a living "library" of video content that can be regularly ingested into the online storage lockers through a VPN -- making the traffic very difficult to detect, let alone measure. While the P2P ecosystem offers this content to aggregators, it is primarily the online digital lockers provide access to illegal movies, for use by Kodi pirate add-ons, as well as the online "indexers", or, websites that aggregate links to the content sources and present them to web users. "On average, around 27 million P2P users have downloaded and shared files in peer-to-peer networks per day. Considering that file sharers are active on more than just one day, the number of daily file sharers in 2017 adds up to almost 10 billion!"[xi] The number of active file sharers who download at least one file of the following content types per day distributes as follows:

- 48.6% for identified movies titles
- 26.9% for identified TV show titles
- 19.7% for identified game titles
- 10.9% for songs of identified music artists"[xii]

Video on Demand Content Distribution

While pirated content has been on the Internet since the Internet began, the problem has become more mainstream and socially acceptable. The Kodi application and its add-ons have become a primary delivery mechanism. Quite often, the devices that are pre-loaded with piracy functions enabled/configured are marketed to the public, either through online ads on Amazon, eBay, Aliexpress, or Craigslist or at local mall kiosks and county fairs. Some of these devices have commercial grade packaging, with a look and feel that creates a sense of legitimacy. Again, most marketing campaigns for these items advise the potential customers that watching pirated movies is not illegal because they are not "downloading" the content, and that distributing pirated movies is not illegal because they are "just streaming" the content and/or they are "just providing streaming links." Additionally, verbose signage and legitimate marketing locales further give the impression that the sellers of these devices are legitimate.

While the Kodi application and the pirate add-ons are the primary source for mainstream pirate video content consumption, ad-supported apps are also gaining in popularity. Subscription-based devices (especially the MAG devices) are also very prevalent on marketing websites and are visible on ISP (Internet Service Provider) networks. Sandvine produced a report in 2017 which measured U.S. piracy usage, concluding that over six percent of U.S. households currently utilize Kodi to watch pirated content. The Sandvine report indicated that 8.8% of households have an active Kodi installation, however their product has determined that 68.6% of households with Kodi devices also have unofficial add-ons configured to access unlicensed content. More broadly, Irdeto reports that in 2017 the amount of people who view pirated video content from any platform is 32% of the U.S. population and 45% of Europe watch pirated video content.[xiii]

The next largest "actors" in pirate video distribution are the web site "indexers" that provide links to view illegal content. Kodi's pirate add-ons are configured to scrape these indexing websites for new titles and links to content (stored on CDNs or digital storage lockers), presenting the choices to the Kodi user. While Kodi is the most prevalent use, the availability of content through these indexers can also be viewed directly from the indexing website, and has crept into the mainstream through search engines. For instance, when using Google Search, quite often illegal sources of the content will appear before legitimate sources for the content. When searching for "watch House of Cards online" through Google, for instance, the first few results returned were from www.watchseries.ac and www.watchfree.to (pirate indexers) -- before Netflix, which created and owns the series. This underscores the emergence of pirated content out of the underground and directly into the purview of the average, law-abiding consumer and web user.

Because the Kodi application is open source, pirate add-on authors have begun to create their own versions of Kodi with their own "skins," or graphics preloaded with either their own add-ons, or another author's add-ons. In nearly all cases, some type of pirate-enabled add-on is included with their version of Kodi. That is a clear indicator that the "skinned" version is specifically created with the intention of watching pirate content (as opposed to the Kodi application, which does not come prepackaged with pirate add-ons.) A prime example is the www.tvaddons.co pirate add-on website. This author of this website has created a Kodi-based application called "FreeTelly," which comes preconfigured with at least six pirate-enabled add-ons. Currently, most ported or skinned versions of Kodi are only PC-based, whereas the Kodi application has been created for all operating system platforms.

Again, playlists based on the M3U file format direct the media players to access online content. Playlists can be configured to directly join live streams or simply playback a file from any location. Most media

players, including some Kodi add-ons, can also stream Torrent or Magnet files directly. This gives the media player direct access not only to online storage and streaming, but also to content streamed directly from the BitTorrent network.

VOD File Naming:

Because the VOD files are mostly sourced from torrents, the naming convention is carried from the torrent file to the asset name (i.e. the torrent name), as seen below.

- The.LEGO.Batman.Movie.2017.720p.HDCAM.HQMIC.x264.AC3.HQ.Hive-CM8 [IPT].torrent is the same as the streamed file name, minus the extension: The.LEGO.Batman.Movie.2017.720p.HDCAM.HQMIC.x264.AC3.HQ.Hive-CM8.mkv)

New Deployment Delivery Options

As the piracy ecosystem adapts with technology, capacity and tooling, several areas that have started to emerge as the newest delivery options for video piracy. The new delivery mechanisms are a response to technology trends and law enforcements prosecution of suspected video piracy.

Kodi:

Kodi contains built-in OpenVPN capabilities, but they are not enabled by default. When this option is invoked, network detection of these devices and the streaming of illegal content becomes extremely difficult, or impossible.

Ad Supported APKs:

The Android SDK also allows a programmer to enable "Tor" sockets, which is effectively a free, no cost VPN connection. There are other Android applications that can be combined easily into an application that enables a full VPN solution.

Smart TVs:

Nearly all Smart TVs are capable of downloading a free IPTV application, available at any CE (Consumer Electronic) manufacturer's "Content Store." This application can give the Smart TV the same functionality as the Kodi application, with conditional access, EPG data, ad insertion etc. The input to the TV is a playlist file (M3U), which can point to both live video streams and file-based VOD content. 45% of U.S. households currently have at least 1 Smart TV[xiv].

VPN:

In addition to the Kodi application being packaged with OpenVPN, VPN pay services are available to not only mask communications to and from the Kodi application, but that mask can also be applied to the whole home network. This affects the visibility into all illegal activity, from streaming pirate video content to uploading via torrents, etc. The average consumer may not choose this path because of the higher technical knowledge requirements.

Web2Web:

Web2web is a web server technology that enables a server-less and domain-less website that lives as a torrent, and is updatable using blockchain technologies. This technology will allow any website to live inside the torrent swarm, making it nearly impossible to take down. A small piece of the "website" is actually "hosted" by all the seeders in a torrent swarm. This technology also allows the user to stream video or audio from torrents, directly into any browser. "Torrents-Time" is an example of such a service, which allows the streaming of a torrent or magnet file directly through a web browser and application. The Torrents Time client also employs a free VPN client to obscure traffic.

These new technologies will be the next step in the evolution of piracy -- and will be far more resilient.

What's Been Done?

The United States (as well as Canada and many other countries) have sometimes taken the approach of warning subscribers of detected sharing of copyright protected content to impact the sharing of infringing content. In the U.S., the U.S. Copyright Alert System was a program operated by the Center for Copyright Information which sent warnings to subscribers of participating ISP's (AT&T, CableVision, Time Warner Cable, Verizon, Charter, and Comcast) notifying them of alleged copyright infringement.. The system sent up to six "notices" to the user sharing the content, pointing out that they are infringing on copyrights. The system was designed to discourage consumers from sharing or seeding pirated material through P2P networks. That system was shut down in 2017. Steven Fabrizio, MPAA Executive Vice President and Global Counsel, said that the program "was simply not set up to deal with the hard-core repeat infringer problem."[xv] Canada initiated a similar system, which also targets the uploader or sharer of infringing content. While this approach may have some success in stopping some users from sharing the content, it can also drive the user to simply search the Internet for an alternate solution (VPN). From a service provider's aspect, it can also impact network service quality, tarnish the brand and leave a less than favorable impression on customers.

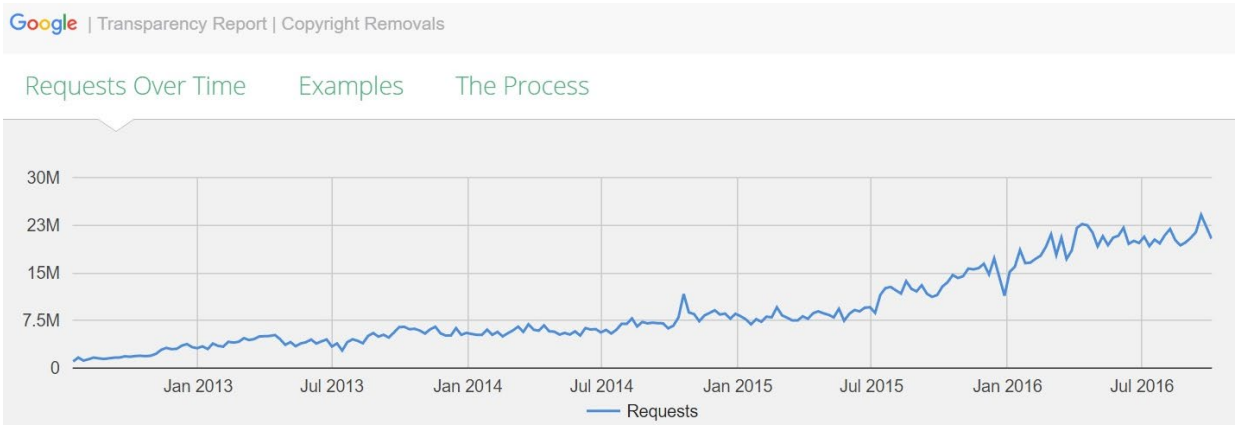
The CCcam/Card Sharing server infrastructure that fuels the live video stream portion of the pirate ecosystem is based on a weakness of the DVB-CSA protocol. Within this protocol, a Smart Card decrypts the ECM (Entitlement Control Message), which then provides the control word, allowing viewing of scrambled material. With Card Sharing, however, the Smart Card and its security features are bypassed: Software performs a network intercept of the decrypted control word and allows the user to share it across a computer network. This has not only grown in popularity but has also morphed into a commercial pay service for storage and access to these controls words. Several newer conditional access technologies are commercially available that have gained varying degrees of success when implemented. If employed more broadly, they could reduce the availability of pirated live video by well over 70%. This in and of itself would make it much more difficult for the add-on authors to provide live content, and will simultaneously drive more development of alternate bulk streaming methods. Addressing the fundamental issues involves the changing of laws (which this paper won't go into) and updating of conditional access systems.

Below are a few of the commercially available satellite encryption solutions that eliminate control word sharing. There are others, and this paper does not advocate a specific brand or technology -- only that the ability to share control words must be addressed, if the industry is to protect the value of the content. It's also noteworthy that most conditional access systems will be breached at some point, which drives the continual development of secure technologies.

Nagra's anyCast COMMAND and CONNECT resolves the control word sharing issue by securely passing video from Broadcom's SoC to NAGRA's secure component for decryption and descrambling. This eliminates the passing of the decrypted control word, as well as the ability to share it. In a press release describing the technology, NAGRA said this: "The unification of decryption and descrambling into a single piece of silicon not only exponentially increases the security of the CAS system, but also simplifies integration by reducing much of the STB testing and certification that was required when these two elements were separated."

Another single-silicon approach is NDS's VideoGuard. DirecTV has had great success in thwarting piracy through the latest (P4/P5) generation of the technology. While earlier versions were hacked, the latest versions have not yet been cracked with software. Some pirates are doing reverse engineering on them already, but that workaround involves removing a chip from one STB and putting it into another. Notably (and intentionally), VideoGuard chips will not update themselves unless they are in their original STB -- which requires reverse engineers to return the VideoGuard chip to its rightful place for several hours at a time, in order to update itself with the latest channels and services. That makes scaling this hack far too laborious for mass production.

The recent popularity of live streaming has also added an illegal component, through various screen sharing means. For example, someone buys an HDHomeRun, adds a CableCARD, plays HBO, and broadcasts the stream through YouTube (or Google, Yahoo, Bing, a torrent). Of course, more complex methods, as mentioned above, can also be employed to provide the content to an online streaming source. Shutting these streams down can be labor-intensive and can only be done by the copyright holder -- HBO, in this example, or by an agent on their behalf. YouTube has a "Content ID Tool" which, according to YouTube, enables "copyright holders to easily identify and manage their content on YouTube" through audio and video fingerprinting. Google employs a DMCA violation submission system as well, and posts its "Transparency Report" based on the submissions. Google's submissions, shown below, illustrate the scale of submitted copyright infringement notices. It is unclear if the rise of the copyright infringement notices indicates that they are ineffective (recipients ignore the notification), or actual infringement is on the rise, or copyright owners enforcement actions are succesful.



As such, it's less than optimal for each broadcaster or content provider to scour these streaming services looking for their content, file notices, and to physically validate the content. Commercial solutions are available from companies that specialize in DMCA take down notices, in addition to providing compliancy follow ups and monitoring streaming sources for specific content. These services also come into play with Video on Demand content, however, the burden of copyright ownership shifts to the production studios. DMCA take down notices are not always effective. However, a graduated response

system, along with clearly distinctive Acceptable Use Policies will set clear expectations for the consumer, while making enforcement more achievable.

The primary means to reduce the availability of pirate Video on Demand content takes a few different paths, but starts by addressing torrents.

Several techniques have been developed and implemented to date to "poison" torrents, with varying levels of success. Torrent poisoning is the intentional sharing of corrupt data, or data with misleading names, while using the BitTorrent protocol. Some of these techniques face legal challenges; some are too costly to implement on a large scale. Some of the methods developed are listed below.

Index Poisoning:

This method targets the index found in P2P file sharing systems. The intent of the index is to allow users to locate the IP addresses of desired content. Thus, this method of attack makes searching difficult for network users. To poison the index, the attacker inserts a large amount of invalid information into the index, thus preventing users from finding the correct resource.[3] Invalid information could include random content identifiers or fake IP addresses and port numbers.[5] When a user attempts to download the corrupted content, the server will fail to establish a connection, again because of the large volume of invalid information. Users will then waste time trying to establish a connection with bogus users, which increases the average time it takes to download the file.[3] The index poisoning attack requires less bandwidth and server resources than decoy insertion. Decoy insertion (or content pollution) is a method by which corrupted versions of a particular file are inserted into the network. This deters users from finding an uncorrupted version and also increases distribution of the corrupted file.[2] A malicious user pollutes the file by converting it into another format that is indistinguishable from uncorrupted files (e.g. it may have similar or same metadata). In order to entice users to download the decoys, malicious users may make the corrupted file available via high bandwidth connections.[3] This method consumes a large amount of computing resources since the malicious server must respond to a large quantity of requests.[4] As a result, queries return principally corrupted copies such as a blank file or executable files infected with a virus.[xvi] Furthermore, the attacker does not have to transfer files nor respond to requests. For this reason, index poisoning requires less effort than other methods of attack.[4]

Selective Content Poisoning:

Selective content poisoning (also known as proactive or discriminatory content poisoning) attempts to detect copyright violators, while allowing legitimate users to continue to enjoy the service provided by an open P2P network. The protocol identifies a peer by its endpoint address, while the file index format is changed to incorporate a digital signature. A peer authentication protocol can then establish the legitimacy of a peer when files are downloaded and uploaded. Using identity-based signatures, the system enables each peer to identify infringing users, without the need for communication with a central authority. The protocol then sends poisoned chunks to these detected users who request a copyright-protected file only. If all legitimate users simply deny download requests from known infringers, the latter can usually accumulate clean chunks from colluders (paid peers who share content with others without authorization.) However, this method of content poisoning forces illegitimate users to discard even clean chunks, prolonging their download time.[7]

Spoofing:

Some companies that disrupt P2P file sharing on behalf of content providers create their own software in order to launch attacks. MediaDefender has written their own program, which directs users to non-existent locations via bogus search results. As users typically select one of the top five search results only, this method requires users to persevere beyond their initial failed attempts to locate the desired file.[6] The idea is that many users will simply give up their search out of frustration.

Kodi pirate add-ons mostly pull the available Video on Demand content locations from website "indexers." Several hundred websites that act as indexers. These sites present web users with tens of thousands of movies, by genre, year etc., with poster art and descriptions. They provide links to secure digital lockers that actually host the video content. While there are hundreds of indexers, there is a commonality of only 50-70 actual digital lockers that host the majority of these movies. At the time of this writing (Spring 2018), those digital lockers are being cataloged with movie titles and copyright owners for distribution to the copyright owners. If higher-level legal action can be attained, site takedowns would be more effective than targeting individual DMCA violations. A very similar precedent has been set in the MegaUpload/Kim Dotcom case, although that case is still being disputed.

Some Helpful Strategies

Movie Studios & Production Companies:

As the copyright owner, studios and producers have the ability and a responsibility to legally address the distribution of their content. DMCA violations can only be filed by the copyright owner or their authorized agents. While it is not feasible for every studio or production company to employ resources to consistently monitor Kodi infringing add-ons, illegitimate applications and services on the Internet, and validate infringements, more services are available to outsource the work on their behalf. Retaining the value of the content is usually worth making the investment in protecting it. Requiring theatres to use anti-camera-recording technology (infrared spectrum projection, "Pirateeye" technology, etc.) in order to present their content would greatly reduce the recorded quality; some new and promising technologies can block recording completely. Requiring some form of content protection at the theater level can greatly reduce the amount of "in theaters now" content available from the pirate ecosystem.

Copyright owners can also drive the requirement, where feasible, that any pay service provider offers its content in watermarked form in order to be able to identify the source of the asset, as well as distribution points. The point of conditional access is the MAC address or Unit Address, Smart Card ID, account number or receiving IP that is authorized through conditional access authorization system, known as session watermarking. Distributer watermarking consists of information about who the content is being distributed through (Cable, Satellite, IPTV provider). Watermarking can allow quick and clear purchase point identification of the content found in the pirate libraries. Identifying the points of purchase for legally-obtained content that is then illegally shared is critical to stopping the flow of new content from service providers. Some digital watermarking technologies have already been defeated. The watermarking technologies employed should always be evaluated not just for resilience but from a return on investment standpoint as well.

Broadcasters and Broadcast Networks:

The role of the Broadcast Network is very similar to that of the movie studios, less the theater aspect. They are the voice of authority of the content they own and create, and as such have the ability/responsibility to protect it, as the copyright holder. Robust enforcement of these requirements will

ensure the efficacy of the entire effort here, too. Broadcaster Networks should work with service providers to identify content leaks. Using distributer watermarking can help in determining sources of leakage.

Service Providers:

Service providers such as cable companies, satellite operators, streaming services (Netflix, Hulu, etc.) may consider implementing digital fingerprinting in order to identify content leakage. Session watermarking employed at the service provider level will allow specific identification of the source of leakage, down to the authorized decrypting device that is re-distributing the content illegally. Again, watermarking can be effective but must be judiciously employed where it makes the most economical sense.

Another important point is that as content delivery continues to move to IP, all service providers should use secure protocols whenever possible. Even though every security scheme may eventually be overcome, given enough time and resources by the pirates, any additional steps that service providers can add to make the content less convenient to obtain can help slow the growth of video piracy.

Satellite Service Providers:

In addition to the session and distributer watermarking, the encryption system used by a great many companies is far outdated. The ability for control word sharing has enabled the wide availability of illegal, high value live content. The "free" and easy availability of this content, combined with high-speed data connectivity, continues to devalue the entertainment industry's products and revenues

Social Media:

As social media providers embark on the journey to provide video streaming, they too have the responsibility to ensure that their platforms are not being used to stream infringing content. Social media is being proactive -- some are improving their platforms toward faster infringement detection and issue takedown. But until all the social media community participates in the improvement, pirates will continue to find "pirate friendly" systems and use those systems to promote their intentions.

Securing the Value of Content

Many industry alliances and trade organizations have defined best practices for security of video content. The Motion Picture Association of America (M.P.A.A.) published its "Content Security Best Practices Common Guidelines"[xvii] in November of 2017. The Alliance for Creativity and Entertainment (A.C.E.) is a "global coalition of leading content creators and on demand entertainment services committed to supporting the legal marketplace for video content and addressing the challenges of online piracy."[xviii] Its membership includes Amazon, Netflix, HBO, Hulu, Paramount and a host of others content rights holders. The International Broadcaster Coalition Against Piracy (I.B.C.A.P.) is another organization comprised of rights holders whose charter is to educate and prevent unauthorized streaming. Its membership includes Dish Network, MTV India, Sony, Zee TV and other content rights holders. NCTA - The Internet & Television Association is also focused on the video piracy issue. It initiated several working groups to explore different aspects of the video pirate ecosystem and its impact. Its membership includes cable providers and programmers. The NCTA also works with the U.S. government from a policy perspective.

Conclusion

When an agent or collective representative pursues legal action based on several rights owners' complaints, the infringing host can be held responsible, and legal action can be taken against the whole service, rather than individual streams of that service. The combined effort of the copyright owners can have an exponential effect in enforcement.

Card sharing contributes greatly to the vast availability of infringing live content. Card/keyword sharing is enabled by outdated conditional access systems. Conditional access system replacement is expensive. Service providers who utilize conditional access systems that are known to be compromised will need to be incentivized to replace the conditional access contractually by the broadcast networks. If a broadcast network delivers its content to a service provider with a compromised conditional access system, without requirements for the protection of that content, they not only degrade the value of their service but the value of all similar services.

Service providers should implement watermarking judiciously. Watermarking is expensive and is not always undefeatable. Further, not all devices are capable of supporting watermarks. Careful evaluation of the placement must be considered in order to arrive at a positive return on investment.

For consumers of infringing pirated video content, several factors must be considered. Education should be available about the effects and costs of piracy in their own communities: The threat of using some of the pirate applications have on their private information; the impact on future film releases; materials should be available so that consumers clearly understand the risks involved. Consumers often turn to the pirate ecosystem when they can't find the content they are looking for from their service provider. Careful analysis of the most consumed pirated content offers the service provider insight into content their customers want, and represents an opportunity to provide that content. Lastly, overall social acceptance must also be addressed. Most consumers are unaware of the impact that piracy has on the cost of content, the cost of jobs (even at the local theater level), and the future of new films or continuation of a film franchise. Better customer education is needed on the overall threat and impact of using these services. The creators of these applications often market them as completely legal and legitimate devices and services. There is very little information available to the contrary.

Abbreviations

ACESTREAM	Streaming Protocol Based on P2P (Peer-to-Peer), BitTorrent Protocol
DMCA	Digital Millennium Copyright Act
DDoS	Distributed Denial of Service
DRM	Digital Rights Management
EPG	Electronic Program Guide
HDCP	High-Bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HLS	HTTP Live Streaming
M3U	*MP3 URL*[1][2] or Moving Picture Experts Group Audio Layer 3 Uniform Resource Locator[3]
MMS	Microsoft Media Server
STB	Set Top Box
QAM	Quadrature Amplitude Modulation

VPN	Virtual Private Network
XML	Extensible Markup Language

References

[i] https://www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-kodi.pdf
[ii] https://en.wikipedia.org/wiki/BitTorrent
[iii] https://www.bittorrent.com/company/about
[iv] Giganews, 1979: Origins of Usenet; "A News", http://www.giganews.com/usenet-history/origins.html
[v] Wikipedia, Bulletin Board System, https://en.wikipedia.org/wiki/Bulletin_board_system
[vi] Daniel Stenberg, History of IRC (Internet Relay Chat), March 29, 2011, https://daniel.haxx.se/irchistory.html
[vii] Robert Hobbes Zakon, Hobbes' Internet Timeline V2.4a, http://www.educa.fmf.uni-lj.si/izodel/ponudba/matinfo/History/timlin24.htm
[v] https://www-yahoo-com.cdn.ampproject.org/c/s/www.yahoo.com/amphtml/sports/mayweather-mcgregor-pirated-upwards-100-million-viewers-205358627.html

[viii] https://www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-kodi.pdf
[ix] http://www.ndu.edu.ua/storage/2017/argumentative_essay.pdf
[x] https://screenrant.com/kick-ass-3-dead-chloe-moretz-piracy/
[xi] https://www.tecxipio.com/single-post/file-sharing-in-peer-to-peer-networks-2017
[xii] https://www.tecxipio.com/single-post/file-sharing-in-peer-to-peer-networks-2017
[xiii] https://resources.irdeto.com/irdeto-global-consumer-piracy-survey/irdeto-global-cusumer-piracy-survey-report
[xiv] https://www.soundandvision.com/content/survey-45-us-households-have-smart-tv
[xv] https://arstechnica.com/tech-policy/2017/01/rip-six-strikes-copyright-alert-system/
[xvi] https://en.wikipedia.org/wiki/Torrent_poisoning#Decoy_insertion
[xvii] https://www.mpaa.org/wp-content/uploads/2018/01/mpaa-best-practices-common-guidelines-v4.02.pdf
[xviii] https://www.alliance4creativity.com/

