WHITEPAPER

SANDVINE

Video and Television Piracy

Ecosystem and Impact

EXECUTIVE SUMMARY

Due to the rise in popularity and prevalence of video and television piracy, a significant percentage of internet users are accessing content in a manner that violates content licensing agreements.

The risk to communications service providers (CSPs) is enormous: continued adoption of unlicensed video and TV streaming services could lead to increased cord-cutting and create 'cord-nevers', significantly impacting top-line revenue and overall profitability and - by extension - undermining the very business models that keep CSPs operating.

The modern reality is that CSPs are spending large sums to license, produce, and/or distribute exclusive content, but it's easier than ever before for subscribers to get this content at a lower cost than the licensed alternatives.

A rich piracy ecosystem containing several different participants and revenue streams has emerged to deliver video on demand, catch-up, and live video use cases. In North America alone, we estimate that this ecosystem generates revenues in excess of one billion dollars ($1 billion USD). For CSPs to make informed decisions about business strategy, it's important to investigate and to quantify video and television piracy.

Aided by an accurate understanding, CSPs can monitor the threat, support law enforcement and regulatory efforts aimed at preventing the proliferation of these services, incorporate insight into churn prediction models, and help educate other stakeholders.

This whitepaper shines a light on the shadow market of the video and television piracy ecosystem and explains how CSPs can begin to quantify the impact on their own networks and, ultimately, to their business.

INTRODUCTION TO VIDEO AND TELEVISION PIRACY

By producing or licensing TV, film, sports, and other premium content, CSPs aim to create exclusive libraries that increase the appeal of bundled offers (e.g., triple and quad play services), stand out from the competition, and provide exclusive value to their subscribers, all of which contribute to top-line revenue. For some CSPs, the video strategy is to deliver TV and video-on-demand (VOD) services exclusively via an app.

However, due to the rise in popularity and prevalence of video and TV piracy, a significant percentage - up to 8% in some North American markets we examined - of internet users are accessing content in a manner that violates content licensing agreements. Left unchecked, we expect this trend to grow due to the ease and relative low cost of accessing unlicensed content and due to the facilities available on the internet for pirates to leverage.

Evolution of Video and Television Piracy

Today's pirate streaming services are only the latest in a long line of television- and video-related fraud, as there have always been those who want to acquire content for less than the market price. Decades ago, cable piracy was a major threat: either a consumer would buy a basic package and slip the technician some cash for full access, or a consumer would splice from another cable connection[1]. The adoption of digital cable, which includes authentication, has made this type of piracy/fraud more difficult.

As satellite television became more popular, card programmers made it possible to decode signals that hadn't been paid for; in response, satellite providers would frequently 'flash' the cards to disable them. During major events, like a FIFA World Cup, it wasn't uncommon to see line-ups out the door of the local 'satellite card guy'.

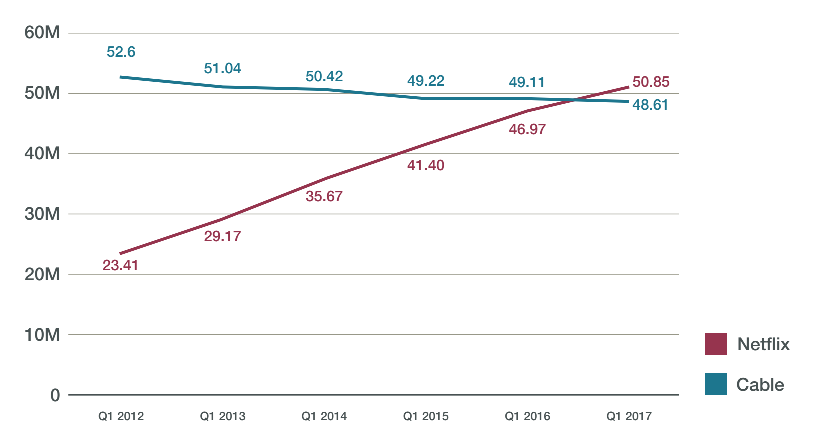
For a number of years, roughly between 2006 and 2010, peer-to-peer (P2P) filesharing applications took up the cause of content piracy, first with music, but then with television programs and movies. Applications like Napster, KaZaA, BitTorrent (and its clients), Gnutella, and eDonkey took advantage of the increase in broadband speeds and explosion in broadband availability to make it relatively straightforward to exchange very large files over the internet. In this environment, live television was considered an important differentiator of licensed television plans: for viewers who absolutely had to see something live (e.g., a major news event, professional sports, etc.), P2P filesharing wasn't a substitute. However, around the same time, the prevalence of live television fraud increased as new, user-friendly (i.e., non-technical) applications emerged.

To acquire live television streams, internet users started using a set of applications that leveraged the efficiencies of the P2P distribution model, but specialized in streaming. These 'peercasting' applications, including PPStream and PPLive, gained widespread adoption and came to account for a significant amount of global internet traffic[2]. Around 2010, the ability of broadband internet to deliver high-quality video streams was established; just a short time later, Netflix dominated North America's broadband networks, and started to compete with traditional television services for viewership (Figure 1).

Figure 1

Netflix vs. Cable Pay-TV subscribers in the US

In the US, Netflix now has more subscribers than Cable TV providers[3]



[1] Here's a wonderful example of a counter-piracy effort from 1993

[2] In Sandvine's 1H 2013 Global Internet Phenomena Report, peercasting accounted for over 10% of fixed network traffic in the Asia-Pacific region

[3] Data from Leichtman Research Group, chart from Statista

Today's Piracy Economy

Today, despite the continued growth in licensed services, including Netflix, Hulu, Sling TV, HBO NOW, BBC iPlayer (and many, many more), there are still consumers committing content fraud through piracy service that cater to these market demands. Some consumers knowingly commit fraud, others do so without fully understanding that their activities are illegal; some are motivated purely or predominantly by money[4].

As before, today's video and television piracy comes in a few forms.

Perhaps the simplest is password-sharing: a user with a legitimate account with a streaming service (e.g., HBO NOW, MLB TV, a streaming service associated with a cable package, etc.) shares the account credentials with someone else. In this model, the traditional parties involved in content production and distribution still receive revenue, but not as much revenue as they would if each person using the service paid for a subscription.

Executives from both HBO[5] and Netflix[6] have openly acknowledged that the password sharing phenomenon exists with their services, but up until this point their position is that it contributes positively to the growth of their services.

Video and Television Piracy Use Cases

The larger threat to legitimate (i.e., not fraudulent) business models comes from a comprehensive piracy economy that addresses/enables three consumer 'use cases':

Video on Demand	Catch-Up	Live Video
- An extensive content library of select television shows and movies available for playback at any time - Example: all past episodes of **Game of Thrones**	- A sliding window of on-demand content, acting like a DVR in the cloud - Example: all programs that aired on a channel in the last seven days are available on-demand	- Video streams that are available as something is aired/broadcast/transmitted - Example: Sunday night's new episode of **Game of Thrones**; professional sports

The modern reality is that CSPs are spending large sums to license, produce, and/or distribute exclusive content, but it's easier than ever before for subscribers to get this content at a lower cost than licensed alternatives.

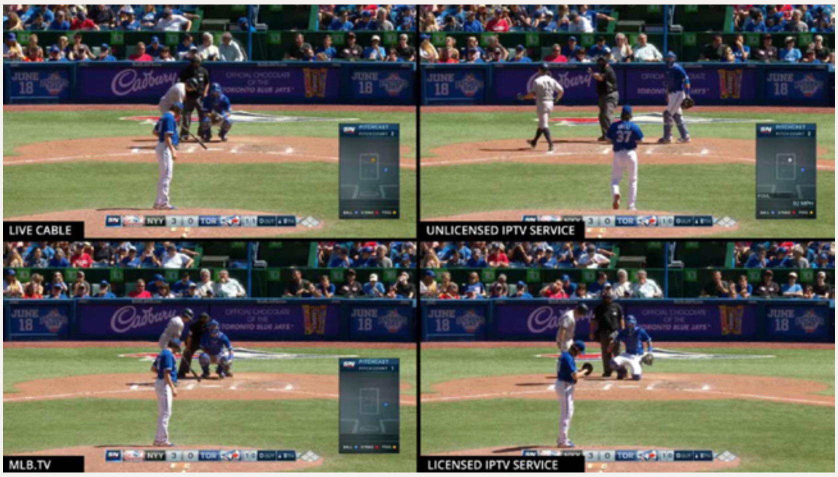
[4] Nevertheless, the availability of reasonably priced legal options has led to a marked decline in relative levels of P2P filesharing: in 2017, P2P file-sharing accounted for only 4% of internet traffic in North America

[5] HBO's CEO, Richard Plepler, referred to password sharing as a "terrific marketing vehicle for the next generation of viewers."

[6] Netflix's CEO Reed Hastings said that consumers sharing Netflix account information was "a positive thing."

Figure 2

Snapshot of four live television services showing the same baseball game



As an example, Figure 2 (on previous page) shows a live video snapshot of four IPTV services showing a Major League Baseball game. Three are licensed services, and one is unlicensed:

- Live cable (top-left): this feed is delivered over the traditional cable network
- MLB.TV (bottom-left): this feed is from the MLB.TV service; in this test, it played 22 seconds behind the live cable feed
- Licensed IPTV service (bottom-right): this feed is from a licensed provider; in this test, it played 28 seconds behind the live cable feed
- Unlicensed IPT service (top-right): this feed is from an unlicensed provider; in this test, it played 13 seconds behind the live cable feed – significantly ahead of the legal streaming alternatives

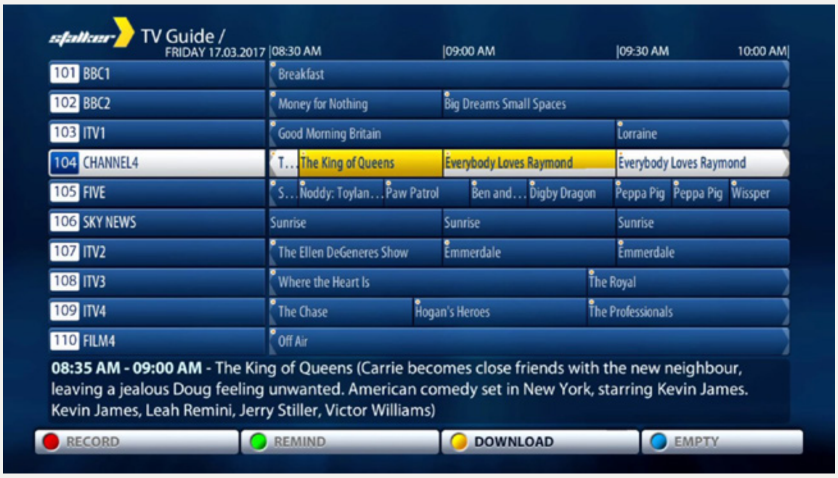
Aside from the variation in timing, all four streaming services played HD video, and any differences in quality of experience were indistinguishable.

Video and Television Piracy Use Cases

To access or use unlicensed video streams, a consumer needs a video service and a device to/on which to stream that service. The most popular approach is to use a set-top box (STB) pre-configured with media software; an STB easily connects to a television and replicates the familiar TV experience (see Figure 3). These set-top boxes, like many browsers and media players, rely on M3U8 playlists[7] to power their content.

Figure 3

The user interface of a popular STB used for video and television piracy



TV Guide /

FRIDAY 17.03.2017	08:30 AM	09:00 AM	09:30 AM	10:00 AM
101 BBC1	Breakfast			
102 BBC2	Money for Nothing	Big Dreams Small Spaces		
103 ITV1	Good Morning Britain		Lorraine	
104 CHANNEL4	T… The King of Queens	Everybody Loves Raymond	Everybody Loves Raymond	
105 FIVE	S… Noddy: Toylan… Paw Patrol	Ben and… Digby Dragon	Peppa Pig Peppa Pig Wissper	
106 SKY NEWS	Sunrise	Sunrise	Sunrise	
107 ITV2	The Ellen DeGeneres Show	Emmerdale	Emmerdale	
108 ITV3	Where the Heart Is		The Royal	
109 ITV4	The Chase	Hogan's Heroes	The Professionals	
110 FILM4	Off Air			

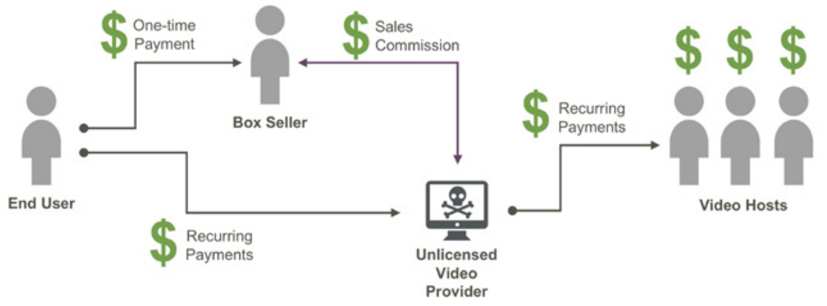
08:35 AM - 09:00 AM - The King of Queens (Carrie becomes close friends with the new neighbour, leaving a jealous Doug feeling unwanted. American comedy set in New York, starring Kevin James. Kevin James, Leah Remini, Jerry Stiller, Victor Williams)

Nowadays, a rich piracy ecosystem (Figure 4 on following page) containing several different participants and revenue streams has emerged to deliver the video on demand, catch-up, and live video use cases. In North America alone, we estimate that this ecosystem generates revenues in excess of one billion dollars ($1 billion USD).

[7] M3U8 is a popular format for multimedia playlists; more information is available at https://en.wikipedia.org/wiki/M3U#M3U8

Figure 4

Today's television and video piracy ecosystem.
Note the complete absence of the content developer and content licensee from the revenue streams



End User (Consumer)	• Pays a subscription fee to an unlicensed video provider for access to content • May make a one-time payment to purchase a dedicated set top box (STB) that comes fully loaded with media software; alternatively, may install media player software on another device (e.g., tablet, laptop, smartphone) • May believe that the services are legitimate, may know that they aren't, or may not want to know either way
Box Seller	• Sells a 'fully loaded' STB configured with media player software to access video streams; many of these boxes are produced by vendors who also sell STBs to CSPs • May or may not also act as an unlicensed video provider; may receive a sales commission for recommending/selling particular unlicensed video provider services
Unlicensed Video Provider	• Sells access to unlicensed video streams • Acquires content from licensed digital streams and from over-the-air (OTA) broadcasts; could be as simple as an individual at home capturing content from a CSP's television service, then re-encoding and distributing it • Might provide a single channel, or might aggregate many into a more comprehensive service
Video Hosts	• The cloud providers whose services are used to host live and on-demand video content • Unlicensed video providers pay the video hosts for the use of their servers

The ubiquitous availability of STBs and streaming services, coupled with their ease-of-use and the reality that money changes hands might be creating an air of legitimacy around the piracy ecosystem. It is not a stretch to think that an average (i.e., not tech-savvy) consumer who buys an STB from an electronics or computer store (see Figure 5) and then pays money to subscribe to a service could conclude that the actions are legitimate, rather than contributing to an ecosystem of fraud and piracy.

Nevertheless, the reality is different.

Figure 5

This billboard from a local computer store is around the corner from Sandvine's Waterloo office

MEASURING VIDEO AND TELEVISION PIRACY

For CSPs to make informed decisions about business strategy, it's important to investigate and to quantify video and television piracy.

Aided by an accurate understanding, CSPs can monitor the threat, support law enforcement and regulatory efforts aimed at preventing the proliferation of these services, incorporate insight into churn prediction models, and help to educate other stakeholders.

Measuring video and television piracy on the network requires a traffic classification (e.g., PCEF, TDF) solution that can reliably identify many aspects of the ecosystem.

Users

The first question most CSPs want answered is straightforward: "How many of my internet subscribers are using pirate video services?"

To answer this question, a solution must be subscriber aware and must be able to identify when a pirate video service is being used (i.e., distinguish between pirate and legitimate streaming services).

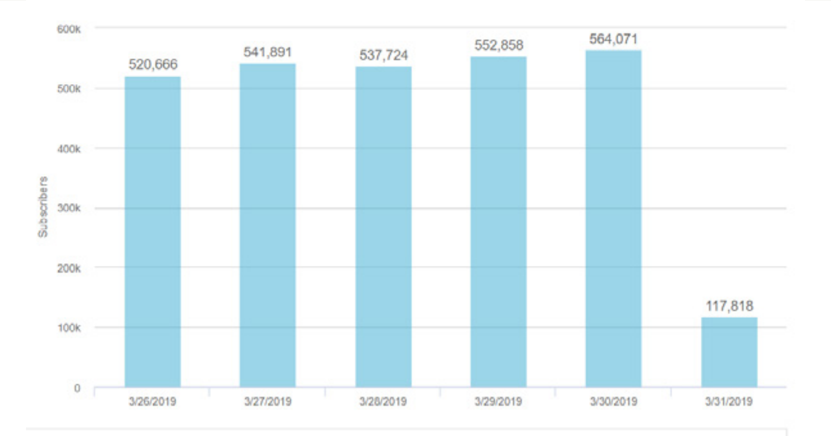
It's important to note that counting users and identifying users are different things: that is, a solution can count distinct users in a manner that preserves subscriber privacy and follows local regulatory restrictions on personally identifiable information (PII).

A recent Sandvine report from a single point-of-presence (POP) of a Canadian CSP's network revealed the number of unique subscribers accessing pirated video and television content from the operator's network (Figure 6 on the following page). This report shows two characteristics:

- the rise and fall of viewership throughout the day, with peak user numbers in the late evening
- the 'floor' of devices that are left powered-on overnight

Figure 6

Report showing the number of unique susbcribers accessing pirated video and television content



Usage

Identifying and counting users tells a CSP who is using pirated video and television streams; a logical follow-on question is, “How much of these services are my subscribers using?”

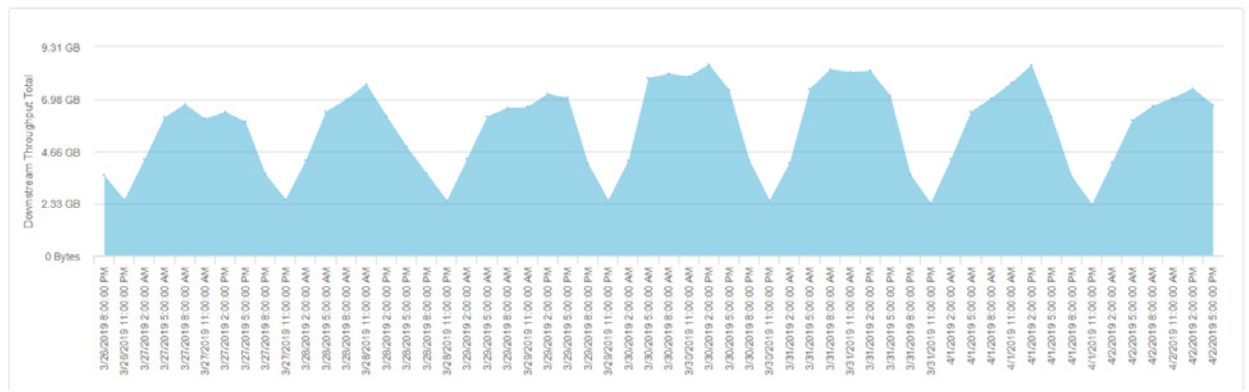
Again, to answer this question a solution must be subscriber aware and must be able to reliably identify pirate video services; going beyond identification, however, the solution must be able to count relevant volumetric data. For instance, it is instructive to know the absolute volume of pirated streaming content flowing on the network[8]; it is also useful to know the duration of viewing.

There’s also the concept of phantom bandwidth: bandwidth consumed by video content that isn’t actually viewed, for instance as the result of a user turning off the television but leaving the set-top box to stream away. A 4 Mbps stream going solid for 30 days consumes more than a Terabyte of data. Such consumption could easily threaten the oversubscription/shared-resource model that underlies consumer internet services.

Figure 7 shows a possible quantification for phantom bandwidth: on this POP, pirate content bandwidth has a ‘floor’ of around 400 Mbps. Combining these new measurements with the subscriber visibility allows CSPs to build detailed profiles of different piracy viewing behaviors. Of course, tracking these behaviors over time is also beneficial.

Figure 7

Report showing content piracy data volume



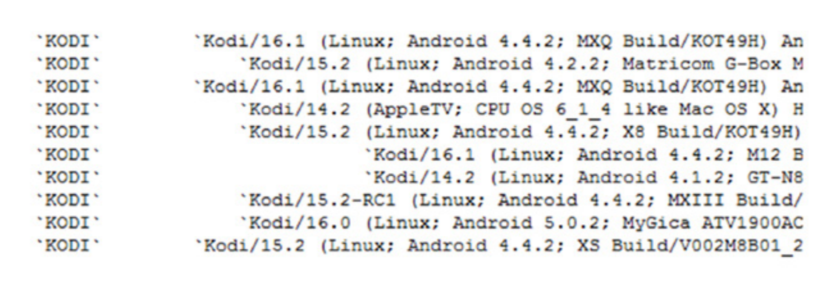
Devices and Software

Beyond the quantifications outlined above, many CSPs want to understand the devices (and software) that are participating in the piracy ecosystem.

One way to investigate this aspect is to inspect unencrypted HTTP user agents: for instance, Figure 8 shows the HTTP user agents of the Kodi software of 10 subscribers; note the wide variation in operating systems and devices.

Figure 8

A sample of Kodi user agents observed on a network



```
`KODI`        `Kodi/16.1 (Linux; Android 4.4.2; MXQ Build/KOT49H) An
`KODI`            `Kodi/15.2 (Linux; Android 4.2.2; Matricom G-Box M
`KODI`        `Kodi/16.1 (Linux; Android 4.4.2; MXQ Build/KOT49H) An
`KODI`            `Kodi/14.2 (AppleTV; CPU OS 6_1_4 like Mac OS X) H
`KODI`            `Kodi/15.2 (Linux; Android 4.4.2; X8 Build/KOT49H)
`KODI`                       `Kodi/16.1 (Linux; Android 4.4.2; M12 B
`KODI`                       `Kodi/14.2 (Linux; Android 4.1.2; GT-N8
`KODI`            `Kodi/15.2-RC1 (Linux; Android 4.4.2; MXIII Build/
`KODI`            `Kodi/16.0 (Linux; Android 5.0.2; MyGica ATV1900AC
`KODI`        `Kodi/15.2 (Linux; Android 4.4.2; XS Build/V002M8B01_2
```

Devices and Hosts

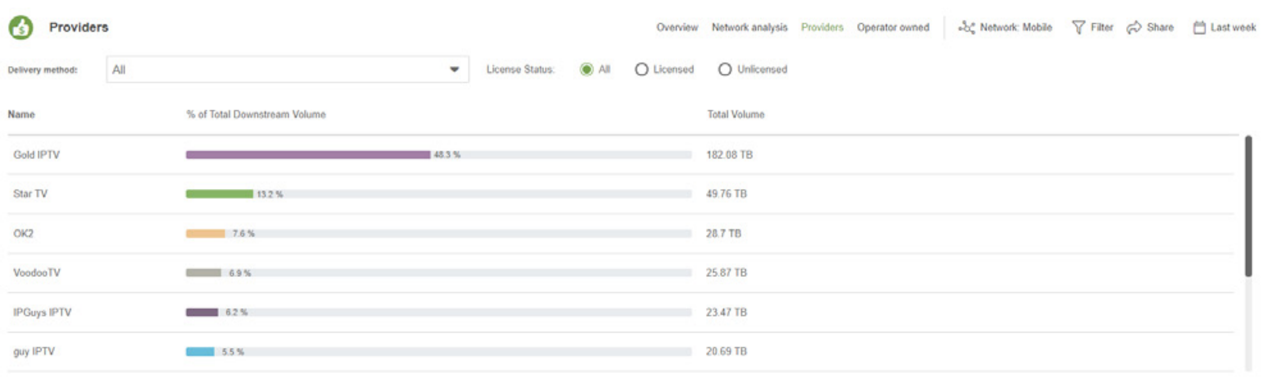
Fundamentally, none of the measurements and insights outlined above are possible unless a solution can reliably identify pirate video and television streams.

The primary challenge in achieving this result is distinguishing between legitimate streaming services and pirate services, because they have many things in common: the same users, the same devices, the same media software, etc.

Only advanced traffic classification solutions can reliably recognize pirate streams without succumbing to false positives and false negatives.

Figure 9

Report showing relative volume of different video and TV piracy services



Delivery method: All

License Status: ● All ○ Licensed ○ Unlicensed

Name	% of Total Downstream Volume	Total Volume
Gold IPTV	48.3 %	182.08 TB
Star TV	13.2 %	49.76 TB
OK2	7.6 %	28.7 TB
VoodooTV	6.9 %	25.87 TB
IPGuys IPTV	6.2 %	23.47 TB
guy IPTV	5.5 %	20.69 TB

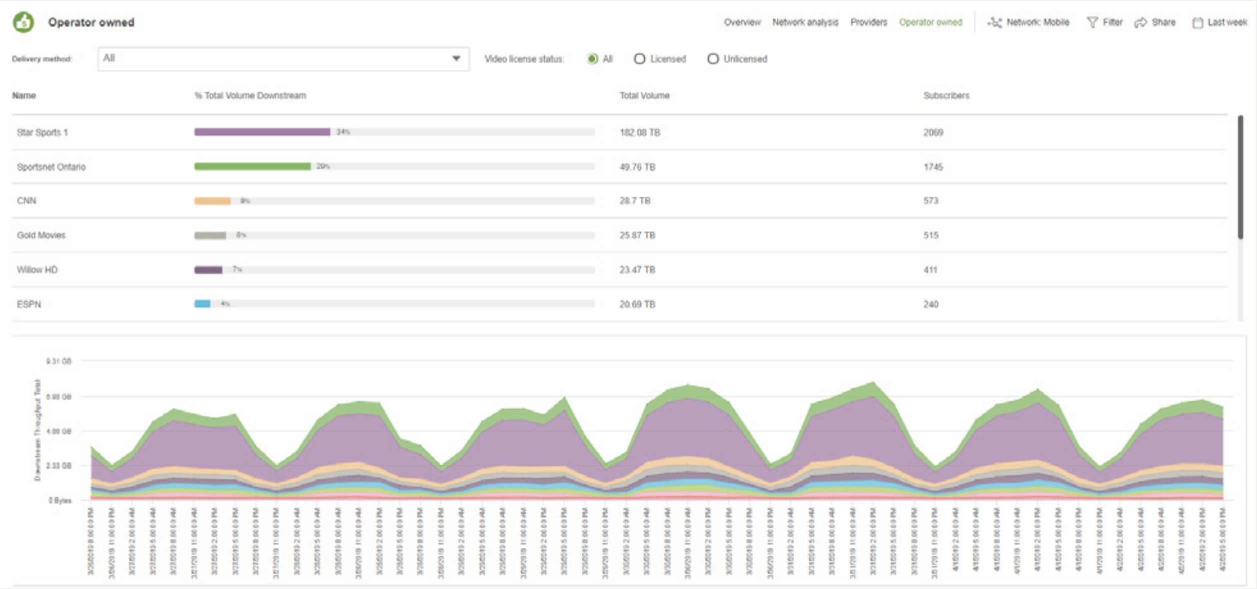
Channels

Because millions, and even billions, of dollars are invested by CSPs to produce, license, and distribute content, understanding which channels subscribers are watching can provide valuable insight.

By inspecting unencrypted channels, CSPs gain a more complete perspective on how subscribers are viewing pirated content (see Figure 9); from a market research perspective, CSPs can also use this insight to identify channels that are in high demand but are not available via any licensed means in a CSP's region.

Figure 10

Report showing the top pirated channels along with traffic volume and superscribers



Delivery method: All

Video license status: ● All ○ Licensed ○ Unlicensed

Name	% Total Volume Downstream	Total Volume	Subscribers
Star Sports 1	34%	182.08 TB	2069
Sportsnet Ontario	29%	49.76 TB	1745
CNN	9%	28.7 TB	573
Gold Movies	8%	25.87 TB	515
Willow HD	7%	23.47 TB	411
ESPN	4%	20.69 TB	240

CONCLUSION

Today's pirate streaming services are only the latest in a long line of television- and video-related fraud, as there have always been people who want to acquire content for less than the market price.

The threat to legitimate (i.e., not fraudulent) business models comes from a comprehensive piracy economy that addresses/enables three consumer 'use cases': video on demand, catch-up, and live video. To access or use unlicensed video streams, a consumer needs a video service and a device to/on which to stream that service.

A rich piracy ecosystem containing several different participants and revenue streams has emerged to deliver the video on demand, catch-up, and live video use cases.

For CSPs to make informed decisions about business strategy, it's important to investigate and to quantify video and television piracy. Aided by an accurate understanding, CSPs can monitor the threat, support law enforcement and regulatory efforts aimed at preventing the proliferation of these services, incorporate insight into churn prediction models, and help educate other stakeholders.

Measuring video and television piracy on the network requires a traffic classification (e.g., PCEF, TDF) solution that can reliably identify many aspects of the ecosystem.

Users: "How many of my internet subscribers are using pirate video services?"
To answer this question, a solution must be subscriber aware and must be able to identify when a pirate video service is being used (i.e., distinguish between pirate and legitimate streaming services).

Usage: "How much of these services are my subscribers using?"
To answer this question a solution must be subscriber aware and must be able to reliably identify pirate video services; going beyond identification, however, the solution must also be able to count relevant volumetric data.

For instance, it is instructive to know the absolute volume of pirated streaming content flowing on the network; it is also useful to know the duration of viewing.

Devices and Software: "How are my subscribers viewing this pirated video content?"
Beyond satisfying curiosity about the device and software ecosystem, investigating the devices subscribers are using can help CSPs gain a more comprehensive understanding of security threats on the network. Many of these devices are purchased with 'fully loaded' software, and the software does not receive any subsequent updates – making them prime targets for attackers.

Services and Hosts: "What pirate services are my subscribers using, and from where is the content being delivered?"
The primary challenge in measuring pirate services and hosts is distinguishing between legitimate streaming services and pirate services, because they have many things in common: the same users, the same devices, the same media software, etc.

Only advanced traffic classification solutions can reliably recognize pirate streams without succumbing to false positives and false negatives.

ADDITIONAL RESOURCES

Thank you for taking the time to read this whitepaper. We hope that you found it useful, and that it contributed to a greater understanding of video and television piracy.

If you have any feedback,please get in touch with us at
info@sandvine.com.

ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
2055 Junction Avenue
Suite Number 105
San Jose,
CA, 95131
USA

EUROPE
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the Sandvine website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Sandvine Corporation and its affiliated companies ("Sandvine"), and Sandvine assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect Sandvine proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of Sandvine technology in generalized terms. Sandvine reserves the right to periodically change information that is contained in this documentation; however, Sandvine makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.