WHITE PAPER

Protecting the Bank of OTT

Akamai

Introduction

Video piracy is not a new issue. Since the dawn of professional movie production, there have been people willing to make a fast buck by exploiting "private property in the form of copyright infringement". During the silent movie period, the concept of "bicycling" (extended screening of movies in theatres) became so popular, Hollywood would send out "checkers" to catch unscrupulous theatre owners in the act. But "sharing" over the internet made digital distribution by far the easiest and most effective way of distributing thousands of pirated video copies to many millions of viewers instantly.

The pirates of today now use a range of attack vectors to retrieve and distribute content. Commonplace tactics include credential stuffing (to capture viewer details and hijack legitimate accounts) or re-streaming linear channels with an experience indistinguishable from TV. Pirate businesses even offer their customers easy UX, customer service, and a range of flexible business models.

With this backdrop in mind, we will explore the piracy challenge and look at ways we can fight back through a strategic framework.

It is estimated that 13.7 million people across E.U. countries are regularly accessing illegal pirate services (per EUIPO 2019), with the United Kingdom (2.4 mil) and France (2.3 mil) having the largest single offending populations. Annual revenues generated by pirates in the E.U. are estimated at €1 billion (EUIPO 2019). In North America, it is estimated that more than 12.5 million U.S. households access pirate video (Parks Associates 2019), but in Asia Pacific the problem can be much more prevalent. In Hong Kong, for example, a 2019 AVIA study showed that 24% of consumers use internet streaming devices to access pirated channels. This increased to 28% of consumers in the Philippines, 34% in Taiwan, and 45% in Thailand. So despite efforts from across the industry, we can see that video piracy is still a serious issue globally. The impact can be felt across the industry, causing financial losses, job losses, and indeed we are starting to see signs that it impacts licensing.

$40.0 – $97.1 Billion

Estimated losses to film industry from pirated video

$39.3 – $95.4 Billion

Estimated losses to TV industry from pirated video

Absolute figures are hard to establish due to the complexity of the subject, but in a report commissioned by the U.S. Chamber of Commerce, financial losses are estimated to be between $40.0 billion and $97.1 billion for the film industry and $39.3 billion and $95.4 billion for the TV industry (NERA Consulting 2019). This excludes loss of revenue to governments through taxation.

The TV and film industries support millions of jobs, from set designers, makeup artists, and musicians through to producers and directors – and piracy is putting these at risk. In their 2019 report on the impact of digital piracy on the U.S. economy, Blackburn, Eisenach, and Harrison estimated that between 230,000 and 560,000 jobs were lost in the United States that year as a direct result of pirating activity.

Moreover, we're beginning to see signs that piracy is impacting licensing, which is the lifeblood of the creative industry and arguably a more damaging strategic issue. Put simply, why would potential distributors pay significant sums of money for rights when content is readily found for free through pirate sites? Yousef Al-Obaidly – chief executive of beIN, one of the largest sports rights buyers in the world – stated that "The sports rights bubble is about to burst because of global piracy, and the business model will have to be overhauled". He was signaling that the value of rights to his organisation will be based on the level of exclusivity. Oscar-nominated, Emmy award–winning producer Jason Blum also described how piracy is having a direct impact on the funds being made available for innovative, risky movies. He suggests that at some point in the not-too-distant future, the numbers will become unsustainable and the studios will need to cut back their slates.

How does the piracy industry work?

As in any battle, it's important to understand your adversaries so you can work out their motivations, tactics, strengths, and weaknesses. Whilst insight is understandably difficult to come by, we do know that there is a complex array of groups and subgroups, each with their own drivers and levels of sophistication, as summarised below.

The release groups

Members see themselves as revolutionaries in a struggle against big corporations. Membership to upload sites is earned by those who are worthy and trusted. Different groups and individuals specialise in certain genres and compete to acquire new material that is then rewarded with recognition. FACT describes the structure as "complex, sophisticated, and well-organised hacker-style groups suspected of being involved in other kinds of cybercrime".

There's a complex array of pirate groups and subgroups, each with their own drivers and levels of sophistication.

The site operators

They manage pirate video sites, including torrenting sites like Pirate Bay or streaming-style sites such as TeaTV. It's not known if the release groups and site operators are the same individuals, but many studies have made the case that there is a significant overlap between the two. The operators certainly make money out of the process and often run several "mirror" sites so that if one is taken down by the authorities, they can still stay online and make money.

The internet streaming device wholesalers

The growth of these devices, in particular Kodi, provides a relatively steady and predictable revenue stream for opportunist criminals. Wholesalers import the boxes through entirely legal channels or criminal networks and modify them with illegal software, which can then be sold online.

The social pirates

Often using social media to distribute content, people in this group are less aware or ambivalent to the fact that piracy is illegal and are responding either to the cost of certain content genres or subscription fatigue.

How do the pirates acquire content?

There are many viable methods for pirates to steal content because of the range of weaknesses across the value chain that can be exploited. We can group the most prevalent methods based on use case.

Simulcast of TV channels and live events

One of the fastest growing forms of piracy is the capture and redistribution of TV channels or live events. This is achieved through:

- Tampering with video playback software or Android OS
- Recording screens during playback using a mobile device
- Intercepting decrypted video using HDCP strippers connected to set-top boxes
- Credential stuffing attacks to access and use legitimate viewer details
- Transportation of video out of a given market using a VPN

On-demand content

Release groups prize pre-release TV shows and movies. The structure of the media industry presents a range of opportunities with so many different organisations and individuals involved in the production process. Common methods used to acquire video include:

- Data-centre breaches, which result in the theft of user credentials or video content
- User ID theft, providing access to video content through various production systems
- Recording of physical assets (less prevalent now) for sharing and distribution
- System hacks against various production systems, providing direct access to video
- Ripping content from legitimate sources, e.g., iTunes
- Cinema filming systems
- Direct theft using man-in-the-middle attacks

How do they distribute content?

Pirates use every possible channel and technical innovation available to distribute their content, including:

- Custom-built IP set-top boxes that access pre-programmed TV streams
- Software running on streaming devices and PCs that enable pirate distribution, e.g., Kodi
- Apps that are side-loaded onto popular retail streaming devices
- Websites and social media services that host user-created content, such as YouTube
- Websites that stream pirate content through links that are found via search or social media
- Ever-present download, file hosting, cyberlocker, and torrent sites

Whilst the distribution strategies of the various pirate personas are less understood, we can see that release groups would possibly favour asset-sharing models (e.g., cyberlocker and torrent sites) because of the inherent support for ubiquity and altruism. As a contrast, the financially motivated site operators would favour the ISD/streaming strategy to emulate legitimate services and their ability to encourage multiple revenue models.

The demand

There are many reasons why people seek out pirate sites. These include financial justification, ignorance of the wider impact, and the basic ability to access content without windowing restrictions. There are many different personas outlined by VFT Solutions Inc. in its 2019 report on pirate viewers, which are summarised here:

- **The "Content Anarchist"** believes in communal and unfettered access to online content. Any charge for content is too much and they do not believe that piracy is immoral or illegal.
- **The "Content Robin Hood"** is less extreme in their views and open to consider alternative propositions. The persona is not a user of livestreaming services but vested in disseminating shared torrent files.
- **The "Utilitarian"** justifies their actions by arguing that the widespread consumption of content outweighs the damage or harm to rights holders, as most content is of fleeting value.
- **The "Lazy Pirate"** is often either unaware or professes ignorance to the fact that piracy is illegal. They are influenced by cost savings and widespread availability, coupled with ease of access.

VFT estimated that the Lazy Pirate and Utilitarian personas represent up to 70% of the total community – and efforts to educate, convert, or penalize those groups will have the greatest impact on piracy.

Can we stop them?

The unfortunate short answer is: not entirely. History tells us that there will always be pirates looking to exploit content whether for altruistic or commercial reasons. All is not lost, however. If the problem is tackled strategically across the value chain, then it can be minimised. In practical terms, improved cooperation across the industry – in the strategic areas identified below – will have a lasting impact.

Data

One glaringly obvious requirement is a standard methodology to measure the extent and impact of piracy globally. Different methodologies and techniques do not allow for continual or contextual analysis, and introduce confusion when prioritizing activity or understanding the return for anti-piracy initiatives. This could be remedied through industry bodies such as the Alliance for Creativity and Entertainment (ACE) taking a leadership role in data gathering.

Education

Piracy to the wider population has become something that "everyone" does and therefore no longer appears illegal because the behavior is normalised. Efforts to educate the public should continue to remind people that piracy is a crime and has a real impact on livelihoods.

Legal and Regulatory

There are several excellent initiatives through industry bodies or governmental initiatives such as FAPAV in Italy that are prosecuting video pirates and tightening the legislative loopholes around the world. These efforts require coordination and access to relevant data.

Technical and Operational

The era of allowing content to be unprotected is long gone. What that means in practice, however, is taking a strategic review of operations and identifying weak links in the technical value chain from production to distribution and applying appropriate measures. We describe this as a 360° posture.

If the problem is tackled strategically across the value chain, then it can be minimised.

The 360° posture

After reviewing the means by which pirate groups acquire and distribute video, we have structured a framework based on three core principles: Protect, Detect, and Enforce. Using this framework, organisations can strategically review the threat landscape based on their role in the industry and implement relevant operational and technical initiatives to minimise the impact.

Protect

Protect against credential stuffing

As described previously, credential stuffing is a popular attack vector used by pirates to acquire viewer details, usually through automated bots. Here are our top recommendations:

- Code login pages/APIs with OWASP. Write secure code according to the OWASP best practices and perform regular penetration tests on your login endpoints.
- Use anti-DDoS protection. This can help you prevent volumetric botnets from reaching your infrastructure and overwhelming your assets.
- Utilise a bot management solution such as Akamai's Bot Manager Premier, which can help you prevent sophisticated credential abuse attacks by verifying user behavior and device telemetry.

Protect against theft from systems

Theft from internal production systems, digital storage, or the public cloud is an important source of pirated material. Broadly speaking, we see several forms of video asset theft:

- Direct hacking or man-in-the-middle attacks by pirates.
- Capture of unique system ID, such as passwords.
- Theft by employees or freelancers.

There are several technologies that companies can employ to minimize the risk; essentially, they revolve around the concept of Zero Trust, a framework that companies use to transform access to technology. Core components of the framework include: securing access to resources, regardless of location or hosting model; enforcing a strategy of access control based on least privilege; and inspecting and logging all traffic for suspicious activity. The framework dictates that only authenticated users and devices can access applications and data. It also protects applications and users from advanced threats on the internet.

There are several components that companies can use to implement a Zero Trust framework; however, securing employee/freelancer access to core production and storage systems is a key facet. With a transitory workforce, media companies face unique challenges in implementing and revoking access to systems, sometimes on a daily basis. Using services such as Akamai's Enterprise Application Access, permissions to specific applications can be granted quickly based on the identity and security context of the user and device, without granting users access to the corporate network where video exfiltration can take place.

Another core facet of Zero Trust is implementing systems that proactively identify and block targeted threats such as malware, ransomware, and phishing, which are tools used by pirates in their man-in-the-middle attacks. Akamai's Enterprise Threat Protector, for example, is a secure web gateway that uses real-time security intelligence to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration.

With a transitory workforce, media companies face unique challenges in implementing and revoking access to systems, sometimes on a daily basis.

Protect against geo and IP rights infringements. Pirates often use VPN technology to mask their country of origin and IP address following the successful acquisition of a legitimate subscriber's details to re-stream content. Proxy detection technology such as Akamai's Enhanced Proxy Detection intelligently blocks requests at the edge associated with anonymous proxy or VPN services, preventing such use cases.

Protect against playback infringements. This is by far the most popular tactic in the fight against anti-piracy and can be achieved through a variety of different means, the most prevalent being digital rights management (DRM). DRM refers to the tools, standards, and systems used to restrict copyrighted materials and prevent unauthorised distribution. It is not a single technology per se.

Depending on the criticality of the assets being protected, some distributors are comfortable with simple encryption (i.e., writing the content in a code that can only be read by devices or software with the key to unlock the code), as this still requires a key to be made available, therefore providing cursory protection – certainly against casual pirates. But keys are typically delivered by HTTP servers and can be copied and shared, so it's often not sufficient to protect higher value content.

To bolster encryption, more advanced DRM technologies handle key communication via a content decryption module using a challenge/response system. These communications are encrypted so the decryption key is never in the open where it can be hacked. Advanced DRM technologies also use business rules that define when and how keys can be used on different devices, such as location or time-based rules.

For distributors looking to implement DRM during the packaging process, it's often useful to engage with cloud providers who are able to manage the complexity. Akamai, as an example, has integrated its origin storage for on-demand content with the processing capabilities of several providers, such as Bitmovin and Encoding.com, which are able to implement encryption in near real time.

Detect

As with any form of theft, protection does not always guarantee success and, as such, detection of any infringements is essential. There are several methods of detecting piracy activity in almost real time:

Fingerprinting

This method provides the ability to identify video content without modifying the original media. Tools are used to identify, extract, and then represent attributes belonging to a video file, so that any given video can be identified by its unique "fingerprint"; for example, on file-sharing networks. The original media does not need to be modified in any way, which is an advantage — but a fingerprint cannot distinguish between different copies of the same title; that is, which copy of a video was leaked in the first instance.

Watermarking

This cannot prevent piracy, but it enables service providers to detect piracy, identify those who engage in it, and then do something about it. Video watermarking consists of adding a pattern of unnoticeable and nonremovable "bits" into a video file. Linking this data to the identity of the viewer means it is possible to trace a pirate who copies content after it is decrypted and illegally distributes it. There are three main methods of video watermarking currently in use:

- **Bitstream modification.** This involves modifying selected areas of a picture in a way that maintains video quality so that the viewer and session are identifiable. As a methodology, it is robust but requires significant compute overhead and adds latency into the system, making it unsuitable for live content.
- **Client-side watermarking.** This works well for rapid watermark extraction and has the ability to deploy on legacy platforms such as set-top boxes. A graphical overlay is composited onto the video stream in the client device, which can be made visible or invisible. As the watermark is not applied until it reaches the client device, the video stream requires extra protection. Client-side technology also requires SDK deployment, which can be complex in OTT environments.
- **A/B variant watermarking.** Aimed at the OTT sector, two identical video streams are created, watermarked, and subsequently stitched or interlaced together either client-side or through CDN edge processing to provide a unique identifier. It is a robust cost-effective method; however, as the identifying sequence can be long, it is not favored in situations that require quick watermark extraction.

A key element to any watermarking strategy is adequate monitoring so that enforcement techniques can be applied to pirates. There are managed monitoring services available, or advice can be sought to develop in-house capabilities. Akamai works with all major watermarking providers to ensure a viable solution can be made available and integrated within an overall video piracy strategy.

Stream log identification

Another form of detection is through real-time examination of delivery logs. In this scenario, deep log inspection provides a real-time picture of infringing activity based on authorised and unauthorised IP addresses. The advantage of these solutions, such as Akamai's Stream Protector, is the ability to turn the capability on and off depending on the situation, which is ideal for protecting time-limited rights such as sports.

Enforce

When piracy activity has been detected, it's important to then be able to act in an appropriate manner. Depending on your strategy, this can take a number of different directions.

- **Revoke access.** If your video assets are time sensitive, such as sports events, then you will want to revoke access to the originator of the illegal stream immediately. There are different ways of achieving this. A common methodology is to work with your distribution service provider, exchange relevant details, and stop streaming activity from an offending IP address. This can take time, however. Akamai provides a service that allows stream revocation in real time and without unnecessary intervention. This has proved particularly effective where piracy monitoring is taking place using either watermarking or stream log identification.

- **Stream modification.** In less time-sensitive situations, distributors can decide to modify the pirated stream by replacing it with alternative content (Big Buck Bunny is popular) or reducing the stream quality. This approach has the benefit of hiding detection from the pirate, stopping them from jumping to a different stream source.

- **Real-time messaging.** As described in the pirate persona section, Lazy Pirates feel safe with the anonymity of the internet. Organisations such as VFT are able to identify viewers of pirated streams on social media platforms and message the infringer directly. Using this form of enforcement, distributors are able to modify the enforcement, such as by offering access to legitimate streams and, if infringement continues, sending legal notices.

Conclusion

Video piracy over IP is a complex, nuanced subject, but one that has the potential to threaten the long-term viability of the media industry as we know it. There is overwhelming evidence that points towards significant financial damage, but, more important, that piracy has the potential to fundamentally undermine or impact global licensing models.

To date, the response from the industry has been relatively muted. As described by one analyst, "We are at the early adopter stage with much work ahead". An increasing number of distributors have woken up to the threat, and most "tier 1" video producers and operators have now established dedicated teams to better understand piracy, evaluate their own situation, and implement relevant anti-piracy strategies.

There are several immediate requirements identified in this paper that are required to help the industry fight the battle. These include consistent piracy data points, improved and continued education of the general public, better cooperation across the industry, and finally, leadership from rights owners across all genres to drive ubiquity across the industry when handling and distributing rights.

The good news is that much of this is starting to mobilise. Research into the subject is becoming more considered, tougher legislation is starting to appear, and vendors are combining capabilities to maximise potential. As an example, in addition to bringing its cybersecurity expertise to bear, Akamai is working with all leading watermarking companies to ensure that once pirates have been detected, their activities can be terminated immediately. Finally, we are seeing signs that rights owners are insisting on minimum standards of content protection across the technical workflow. Today, these are isolated instances or "suggestions" (as is the case with the MPAA) – but moving forward, we see these becoming a necessary function of doing business.

With these initiatives in place, we can minimise the issue so that financial losses are reduced, job opportunities are protected, and licensing can continue to thrive in a global marketplace.

REFERENCES

Asia Video Industry Association. The Asia Video Industry Report. 2019.

Bevir. Cost of online piracy to hit $52bn. 2017. Retrieved from https://www.ibc.org/publish/cost-of-online-piracy-to-hit52bn/2509.article

Blackburn et al. Impacts of Digital Video Piracy on the U.S. Economy. 2019.

Coberly. Streaming services are 'killing' piracy. Retrieved from https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html

CustosTech. The Economics of Digital Piracy. 2014.

Daly. The pirates of the multiplex. Retrieved from https://www.vanityfair.com/news/2007/03/piratebay200703

Decary, Morselli, Langlois. A study of Social Organisation and Recognition Among Warez Hackers. 2012.

Digital Citizens Alliance. Fishing in the piracy stream. Retrieved from https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

Enigmax. Interview with a Warez Scene Releaser. 2007. Retrieved from https://torrentfreak.com/interview-with-a-warez-scene-releaser/

European Commission. Estimating displacement rates of copyrighted content in the EU. May 2015.

European Union Intellectual Property Office. Trends in Digital Copyright Infringement in the European Union. 2018.

European Union Intellectual Property Office. Illegal IPTV in the European Union. 2019.

FACT. Cracking down on digital piracy. 2017.

Feldman. Almost 5 million Britons use pirated TV streaming services. 2017. Retrieved from https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami

FriendsMTS. Comparing subscriber watermarking technologies for premium pay TV content. 2019.

Frontier Economics. The economic impacts of counterfeiting and piracy. Report prepared for BASCAP and INTA. 2017.

Granados. Report: Millions Illegally Live-Streamed El Clasico. 2015. Retrieved from https://www.forbes.com/sites/nelsongranados/2016/12/05/sports-industry-alert-millions-illegally-live-streamed-biggest-spanish-soccer-rivalry/#3544c3f37147

Greenburg. Economics of video piracy. 2015. https://pitjournal.unc.edu/article/economics-video-piracy

Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S., and Tysony G. Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers. 2018.

Intellectual Property Office. Online Copyright Infringement Tracker. 2018.

Jarnikov et al. A Watermarking System for Adaptive Streaming. 2014.

Jones, Foo. Analyzing the Modern OTT Piracy Video Ecosystem. SCTE•ISBE. 2018

Joost Poort et al. Global Online Piracy Study, University of Amsterdam Institute for Information Law. July 2018.

Kan. Pirating 'Game of Thrones'? That file is probably malware. 2019. Retrieved from https://mashable.com/article/pirating-game-of-thrones-malware/?europe

Lee, T. Texas-size sophistry. 2006. Retrieved from http://techliberation.com/2006/10/01/texas-size-sophistry/

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners", an abridged version of "Internet piracy: the estimated impact on sales" in Handbook on the Digital Creative Economy Edited by Ruth Towse and Christian Handke, Edward Elgar. 2013.

Mick, J. Nearly half of Americans pirate casually, but pirates purchase more legal content. January 21, 2013. Retrieved from http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm

Motion Picture Association of America. The Economic Contribution of the Motion Picture & Television Industry to the United States. November 2018.

MPA Content Security Program. Content Security Best Practices Common Guidelines. Motion Picture Association. 2019.

MUSO. Measuring ROI in content protection. 2020.

Nordic Content Protection Group. Annual Report, 2020.

Parks Associates. Video Piracy: Ecosystem, Risks, and Impact. 2019.

Tassi, P. April 15, 2014. "Game of Thrones" sets piracy world record, but does HBO care? Retrieved from http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care

Sanchez, J. January 3, 2012. How copyright industries con congress. Retrieved from http://www.cato.org/blog/how-copyright-industries-con-congress

Sandvine. Video and Television Piracy. 2019.

Schonfeld. Pirate Bay makes $4m a year. 2008. Retrieved from https://techcrunch.com/2008/01/31/the-pirate-bay-makes-4-million-a-year-on-illegal-p2p-file-sharing-says-prosecutor/

Sulleyman. Pirate Treasure: How Criminals Make Millions From Illegal Streaming. 2017. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 07/20.