WHITE PAPER

Protección del banco de OTT

Akamai

Introducción

La piratería de vídeo no es un problema nuevo. Desde los inicios de la producción cinematográfica profesional, ha habido personas dispuestas a ganar dinero fácil aprovechándose de la "propiedad privada, pero infringiendo los derechos de autor". Durante la época del cine mudo, el concepto de "prolongación" (proyección prolongada de películas en los cines) se volvió tan popular que Hollywood enviaba "revisores" para pillar a los propietarios de cines sin principios con las manos en la masa. Sin embargo, "compartir" a través de Internet hizo que la distribución digital fuera con diferencia la forma más fácil y eficaz de distribuir miles de copias de vídeo pirateadas a millones de espectadores al instante.

Las piratas de hoy en día utilizan una amplia variedad de vectores de ataque para recuperar y distribuir contenido. Las tácticas comunes incluyen el Credential Stuffing (para capturar los detalles del espectador y secuestrar cuentas legítimas) o el restreaming de canales lineales con una experiencia que no se diferencia del televisor. Los negocios piratas incluso ofrecen a sus clientes una experiencia sencilla, servicio al cliente y una variedad de modelos de negocio flexibles.

Teniendo en cuenta este telón de fondo, exploraremos el desafío de la piratería y observaremos las maneras en que podemos combatirlo mediante un marco estratégico.

Se estima que 13,7 millones de personas en los países de la Unión Europea acceden regularmente a servicios piratas ilegales (según la EUIPO de 2019), con el Reino Unido (2,4 millones) y Francia (2,3 millones) a la cabeza en población infractora. Los ingresos anuales generados por la piratería en la Unión Europea se estiman en 1000 millones de euros (EUIPO 2019). Se calcula que en Norteamérica más de 12,5 millones de hogares estadounidenses acceden a vídeos piratas (Parks Associates, 2019), pero en la región de Asia Pacífico la prevalencia del problema puede ser mucho mayor. Por ejemplo, en Hong Kong, un estudio de AVIA de 2019 halló que el 24 % de los consumidores utiliza dispositivos de streaming por Internet para acceder a canales pirateados. Esto aumentó a un 28 % de los consumidores en Filipinas, un 34 % en Taiwán y un 45 % en Tailandia. Así que, a pesar de los esfuerzos de todo el sector, podemos ver que la piratería de vídeo sigue siendo un problema grave en todo el mundo. El impacto se advierte en toda la industria, con pérdidas financieras, pérdidas de empleo y, de hecho, empezamos a ver señales de que afecta a las licencias.

40 000 - 97 100 millones de dólares

Pérdidas estimadas de la industria cinematográfica por la piratería de vídeo

39 300 - 95 400 millones de dólares

Pérdidas estimadas de la industria televisiva por la piratería de vídeo

Es difícil determinar unas cifras absolutas debido a la complejidad del asunto, sin embargo, en un informe solicitado por la Cámara de Comercio de EE. UU., se estimaban unas pérdidas financieras de entre 40 000 millones y 97 100 millones de dólares para la industria cinematográfica, así como entre 39 300 millones y 95 400 millones de dólares para la televisión (NERA Consulting, 2019). Se excluye la pérdida de ingresos para los gobiernos a través de los impuestos.

Las industrias del cine y la televisión sustentan millones de puestos de trabajo, desde escenógrafos, maquilladores y músicos hasta productores y directores, y la piratería los pone en riesgo. En su informe de 2019 sobre la repercusión de la piratería digital en la economía de EE. UU., Blackburn, Eisenach y Harrison estimaron que se perdieron entre 230 000 y 560 000 empleos en Estados Unidos ese año como resultado directo de la actividad pirata.

Además, estamos comenzando a ver señales de que la piratería está afectando a las licencias, lo que es el alma de la industria creativa y posiblemente un problema estratégico más dañino. En otras palabras, ¿por qué los posibles distribuidores pagarían grandes sumas de dinero por derechos cuando se puede obtener contenido de manera gratuita en sitios piratas? Yousef Al-Obaidly, el director ejecutivo de beIN, uno de los mayores compradores de derechos deportivos del mundo, afirmó "la burbuja de los derechos deportivos está a punto de estallar debido a la piratería global y el modelo de negocio tendrá que revisarse". Señaló que el valor de los derechos para su organización se basará en el nivel de exclusividad. El productor Jason Blum, nominado al Oscar y ganador del premio Emmy, también describió cómo la piratería tiene un impacto directo en los fondos que se ponen a disposición para películas innovadoras y arriesgadas. Sugiere que en algún momento del futuro no muy lejano las cifras serán insostenibles y los estudios tendrán que reducir sus películas.

¿Cómo funciona el sector de la piratería?

Como en cualquier batalla, es importante conocer a sus adversarios, para que pueda comprender sus motivaciones, tácticas, fortalezas y debilidades. Aunque, comprensiblemente, resulta complicado obtener una perspectiva, lo que sí sabemos es que existe un conjunto complejo de grupos y subgrupos, cada uno con sus propios factores, niveles de sofisticación y dependencias entre grupos.

Los grupos de difusión

Los miembros se ver como revolucionarios en una lucha contra grandes corporaciones. Solo los usuarios dignos y fiables consiguen pertenecer a sitios donde se carga contenido. Los diferentes grupos e individuos se especializan en determinados géneros y compiten por adquirir material nuevo, que luego se recompensa con el reconocimiento. FACT describe la estructura como "grupos de hackers complejos, sofisticados y bien organizados que se sospecha que están involucrados en otros tipos de delitos cibernéticos".

Existe un conjunto complejo de grupos y subgrupos de piratería, cada uno con sus propios factores y niveles de sofisticación.

Los operadores de sitios

Gestionan sitios de vídeo piratas, como páginas de torrents, por ejemplo, Pirate Bay o sitios de streaming como TeaTV. No se sabe si los grupos de difusión y los operadores de sitios son las mismas personas, pero muchos estudios abogan por que hay una superposición importante entre ambos. Los operadores ciertamente ganan dinero del proceso y suelen operar varias "réplicas" de modo que, si las autoridades los cierran, pueden permanecer en Internet y ganar dinero.

Los mayoristas de dispositivos de streaming por Internet

El crecimiento de estos dispositivos, en particular Kodi, ofrece un flujo de ingresos relativamente constante y predecible para los delincuentes oportunistas. Los mayoristas importan los decodificadores a través de canales totalmente legales o redes criminales y los modifican con un software ilegal, que luego se pueden vender online.

Los piratas sociales

Las personas de este grupo, que suelen distribuir contenido a través de las redes sociales, son menos conscientes o ambivalentes con respecto al hecho de que la piratería es ilegal, y lo hacen debido al coste de determinados géneros de contenido y la pereza que suponen las suscripciones.

¿Cómo adquieren contenido los piratas?

Existen muchos métodos viables para que los piratas roben contenido debido a la serie de debilidades de toda la cadena de valor que se pueden aprovechar. Podemos agrupar los métodos más frecuentes según el caso de uso.

Transmisión simultánea de canales de televisión y eventos en directo

Una de las formas de piratería de más rápido crecimiento es la captura y redistribución de canales de televisión o eventos en directo. Esto se logra a través de los siguientes métodos:

- Manipulación del software de reproducción de vídeo o del sistema operativo Android.
- Grabación de pantallas durante la reproducción con un dispositivo móvil.
- Interceptación de vídeo descifrado mediante los separadores HDCP conectados a decodificadores.
- Ataques de Credential Stuffing para acceder y utilizar información de espectadores legítimos.
- Transporte de vídeo fuera de un mercado determinado mediante una VPN.

Contenido a la carta

Los grupos de difusión valoran los programas y películas de TV antes de su estreno. La estructura de la industria de los medios de comunicación presenta una variedad de oportunidades con numerosas organizaciones y personas diferentes involucradas en el proceso de producción. Los métodos comunes que se utilizan para adquirir vídeos incluyen:

- Las filtraciones del centro de datos, que dan lugar al robo de credenciales de usuarios o contenido de vídeo.
- Robo de las identificaciones de usuario para acceder al vídeo desde varios sistemas de producción.
- Registros de activos físicos (con menor prevalencia en este momento) para compartir y distribuir.
- Ataques a diversos sistemas de producción para tener acceso directo a los vídeos.
- Copia de contenido de fuentes legítimas, por ejemplo, iTunes.
- Sistemas de filmación en cines.
- Robo directo mediante ataques de tipo intermediario.

¿Cómo distribuyen el contenido?

Los piratas utilizan todos los canales e innovaciones técnicas posibles y disponibles para distribuir su contenido, por ejemplo:

- Decodificadores de IP personalizados que acceden a retransmisiones de TV preprogramadas.
- Software que se ejecuta en los PC y dispositivos de streaming que permiten la distribución pirata, por ejemplo, Kodi.
- Aplicaciones en dispositivos de streaming de retail populares.
- Sitios web y servicios de redes sociales que alojan contenido creado por el usuario, como YouTube.
- Sitios web que transmiten contenido pirata con enlaces que encuentran mediante búsquedas o en las redes sociales.
- La descarga siempre disponible, el alojamiento de archivos, cyberlocker y los sitios de torrents.

Aunque las estrategias de distribución de las diversas personalidades de piratas se conocen menos, podemos ver que los grupos de difusión prefieren los modelos de uso compartido de activos (como los cyberlockers y los sitios de torrents), debido a la omnipresencia y el altruismo, características inherentes de dichos modelos. En contraste, los operadores de sitios con motivaciones económicas prefieren la estrategia de streaming/ISD para emular servicios legítimos y su capacidad de alentar múltiples modelos de ingresos.

La demanda

Hay muchas razones por las que la gente busca sitios piratas. Entre las razones se incluye la justificación económica, la ignorancia del impacto general y la capacidad básica de acceder al contenido sin restricciones de visualización. VFT Solutions Inc. señala numerosas personalidades diferentes en su informe de 2019 sobre espectadores de contenido pirateado, que se resumen aquí:

- **El "anarquista de contenido"** cree en el acceso comunitario y sin restricciones al contenido online. Cobrar una tarifa por cualquier contenido es excesivo y no considera que la piratería sea inmoral o ilegal.
- **El "Robin Hood de contenido"** es menos extremo en sus puntos de vista y está abierto a considerar propuestas legítimas alternativas. Esta personalidad no es usuaria de servicios de streaming en directo, pero sí difunde archivos torrent.
- **El "utilitario"** justifica sus acciones con el argumento de que el consumo generalizado de contenido supera el daño o el perjuicio a los titulares de derechos, ya que la mayoría del contenido tiene un valor fugaz.
- **El "pirata perezoso"** a menudo desconocen o declara su ignorancia al hecho de que la piratería sea ilegal. Se ven influenciados por el ahorro de costes y la disponibilidad generalizada, junto con la facilidad de acceso.

VFT estima que las personalidades del "perezoso" y "utilitario" representan hasta el 70 % del total de la comunidad y las iniciativas por educar, convertir o penalizar a esos grupos serán las que tengan el mayor impacto en la piratería.

¿Podemos detenerlos?

Lamentablemente, la respuesta es que no del todo. La historia nos dice que siempre habrá piratas que deseen sacar partido del contenido, ya sea por motivos altruistas o comerciales. Sin embargo, no todo está perdido. Si el problema se aborda estratégicamente a través de la cadena de valor, podrá minimizarse. En términos prácticos, una mayor cooperación en todo el sector, en las áreas estratégicas que se señalan a continuación, tendrá una repercusión duradera.

Datos

Un requisito obvio es el establecimiento de una metodología estándar para medir el alcance y el impacto de la piratería a nivel global. Las diferentes metodologías y técnicas no permiten un análisis continuo o contextual y presentan confusión a la hora de priorizar la actividad o entender los resultados de las iniciativas antipiratería. Esto podría corregirse a través de organismos de la industria, como la Alliance for Creativity and Entertainment (ACE), que ejerzan el liderazgo en la recopilación de los datos.

Educación

La piratería para muchas personas se ha convertido en algo que "todo el mundo" hace, por lo tanto, ya no parece ilegal porque el comportamiento se normaliza. Entre las labores para educar al público debe mantenerse seguir recordando a la gente que la piratería es un delito y tiene un impacto real en el medio de vida de las personas.

Aspectos legales y normativos

A través de organismos de la industria u organismos gubernamentales se han presentado iniciativas excelentes, como la FAPAV en Italia, que procesa a los piratas de vídeo y refuerza los vacíos legislativos en todo el mundo. Estos esfuerzos requieren coordinación y acceso a los datos relevantes.

Aspectos técnicos y operativos

La época en la que se permitía que el contenido estuviera desprotegido pasó hace mucho tiempo. Sin embargo, en la práctica esto supone una revisión estratégica de las operaciones y la identificación de los eslabones más débiles en la cadena de valor técnico, desde la producción hasta la distribución, para aplicar las medidas adecuadas. Lo describimos como una estrategia de 360°.

Si el problema se aborda estratégicamente a través de la cadena de valor, podrá minimizarse.

La estrategia de 360°

Después de revisar los medios por los que los grupos dedicados a la piratería adquieren y distribuyen los vídeos, estructuramos un marco basado en tres principios fundamentales: Proteger, detectar y aplicar. Con este marco, las organizaciones pueden revisar estratégicamente el panorama de amenazas según su función en la industria e implementar iniciativas operativas y técnicas pertinentes para minimizar el impacto.

Proteger

Protección frente al Credential Stuffing

Como se ha descrito anteriormente, el Credential Stuffing es un vector de ataque popular utilizado por piratas para adquirir los datos de los espectadores a través de bots automatizados. Estas son nuestras principales recomendaciones:

- Codificación de API/páginas de inicio de sesión con OWASP. Escriba código seguro de acuerdo con las prácticas recomendadas de OWASP y realice una prueba de penetración en sus terminales de inicio de sesión.
- Uso de protección contra DDoS. Esto puede ayudarle a evitar que los botnets volumétricos lleguen a su infraestructura y saturen sus activos.
- Utilice una solución de gestión de bots como Bot Manager Premier de Akamai, que puede ayudar a prevenir ataques sofisticados de abuso de credenciales mediante la verificación del comportamiento de los usuarios y la telemetría de dispositivos.

Protección contra el robo de sistemas

El robo de los sistemas de producción internos, el almacenamiento digital o la nube pública es una importante fuente de material pirateado. En términos generales, vemos varias formas de robo de activos de vídeo:

- Ataques de tipo intermediario o piratería directa por parte de los piratas.
- Captura de ID exclusivos de sistemas, como contraseñas.
- Robo por parte de empleados o trabajadores independientes.

Las empresas pueden emplear diversas tecnologías para minimizar el riesgo; básicamente, giran en torno al concepto Zero Trust, un marco que las empresas utilizan para transformar el acceso a la tecnología. Entre los componentes básicos de Zero Trust se incluyen: acceso seguro a todos los recursos, independientemente de la ubicación o el modelo de alojamiento, aplicación de una estrategia de control de acceso basada en los privilegios mínimos, e inspección y registro de todo el tráfico en busca de actividad sospechosa. Este marco de seguridad impone que solo los usuarios y dispositivos autenticados puedan acceder a las aplicaciones y a los datos. También protege las aplicaciones y a los usuarios de las amenazas avanzadas de Internet.

Hay varios componentes que las empresas pueden utilizar para implementar un marco Zero Trust, pero proteger el acceso de los empleados/trabajadores independientes a los sistemas básicos de almacenamiento y producción es un aspecto clave. Con una plantilla de empleados muy transitoria, las compañías de medios de comunicación se enfrentan a desafíos únicos a la hora de implementar y revocar el acceso a los sistemas, a veces a diario. Con el uso de servicios como Enterprise Application Access de Akamai, se pueden otorgar permisos rápidamente para aplicaciones específicas según el contexto de identidad y seguridad del usuario y el dispositivo, sin otorgar nunca acceso a la red corporativa completa donde puede tener lugar la filtración de vídeo.

Otro aspecto fundamental de Zero Trust es la implementación de sistemas que identifican y bloquean de manera proactiva amenazas específicas como malware, ransomware y phishing, que son herramientas utilizadas por piratas en sus ataques de tipo intermediario. Por ejemplo, Enterprise Threat Protector de Akamai es una puerta de enlace web segura que utiliza inteligencia de seguridad en tiempo real para identificar y bloquear de forma proactiva amenazas específicas como malware, ransomware, phishing y filtraciones de datos basadas en DNS.

Con una plantilla de empleados muy transitoria, las compañías de medios de comunicación se enfrentan a desafíos únicos a la hora de implementar y revocar el acceso a los sistemas, a veces a diario.

Protección contra las infracciones geográficas y de derechos de propiedad intelectual. Los piratas suelen utilizar tecnología VPN para enmascarar su país de origen y la dirección IP tras conseguir los datos de los suscriptores legítimos para volver a transmitir el contenido. La detección de proxy mejorada de Akamai bloquea de manera inteligente las solicitudes en el borde de Internet asociadas a un proxy anónimo o con servicios de VPN, lo que evita tales casos de uso.

Protección contra las infracciones de reproducción. Esta es con diferencia la táctica más popular en la lucha contra la piratería y se puede lograr a través de diferentes medios entre los que destaca la gestión de derechos digitales (DRM). DRM hace referencia a las herramientas, los estándares y los sistemas utilizados para restringir los materiales protegidos por derechos de autor y evitar su distribución no autorizada. No es una sola tecnología por sí sola.

Según la importancia de los activos que se protegen, algunos distribuidores se sienten cómodos con el cifrado simple (es decir, escribiendo el contenido en un código que solo pueda leerse con dispositivos o software con la clave para desbloquear el código), ya que esto requiere una "clave" para acceder al contenido, lo que ofrece protección rápida, sin duda útil para los piratas informales. Sin embargo, las claves generalmente las proporcionan los servidores HTTP, y se pueden copiar y compartir, por lo que a veces no es suficiente para proteger el contenido de mayor valor.

Para reforzar el cifrado, las tecnologías DRM más avanzadas gestionan la comunicación de claves a través de un módulo de descifrado de contenido mediante un sistema de desafío/respuesta. Estas comunicaciones se cifran, de modo que nunca se puede acceder a la clave de descifrado para piratearla. Las tecnologías DRM avanzadas también emplean reglas empresariales que definen cuándo y cómo se pueden utilizar las claves en diferentes dispositivos, como la ubicación, el registro de dispositivo y las reglas basadas en el tiempo.

En el caso de los distribuidores que buscan implementar la DRM durante el proceso de empaquetado, suele ser útil colaborar con proveedores de nube que puedan ayudarles con la complejidad. Akamai, por ejemplo, ha integrado su almacenamiento de origen para el contenido a la carta con las capacidades de procesamiento de varios proveedores, como Bitmovin y Encoding.com, que pueden implementar el cifrado casi en tiempo real.

Detectar

Como en cualquier tipo de robo, la protección no siempre garantiza el éxito y, por tanto, la detección de las infracciones es esencial. Hay varios métodos para detectar la piratería casi en tiempo real:

Huellas digitales

Este método permite identificar el contenido de vídeo sin modificar el medio original. Las herramientas se utilizan para identificar, extraer y luego representar los atributos de un archivo de vídeo, de modo que cualquier vídeo determinado se puede identificar por su "huella digital" única, por ejemplo, en redes de uso compartido de archivos. No es necesario modificar los medios originales de ninguna forma, lo que supone una ventaja, pero una huella digital no puede distinguir entre copias diferentes del mismo título; es decir, qué copia de un vídeo se filtró en primer lugar.

Watermarking

Aunque no puede evitar directamente la piratería, permite a los proveedores de servicios detectarla, identificar a las personas que participan y hacer algo al respecto. Las marcas de agua en los vídeos consisten en agregar un patrón de "bits" que son imperceptibles y no se pueden quitar en un archivo de vídeo. Vincular estos datos con la identidad del usuario significa que es posible rastrear un pirata que copia contenido después de descifrarlo y distribuirlo ilegalmente. Existen tres métodos principales de introducir marcas de agua en vídeos:

- **Modificación del flujo de bits.** Implica modificar las áreas seleccionadas de una imagen de manera que se mantenga la calidad del vídeo, pero que se pueda identificar al espectador y la sesión. Como metodología, es sólida, pero requiere una sobrecarga informática significativa y agrega latencia al sistema, por lo que es inadecuada para el contenido en directo.
- **Marcas de agua para el cliente.** Funciona bien por lo rápido que se quitan y por su capacidad de implementarse en plataformas heredadas, como decodificadores. Se coloca una superposición gráfica en la retransmisión de vídeo en el dispositivo del cliente, que puede ser visible o invisible. Como la marca de agua no se aplica hasta que llega al dispositivo del cliente, el streaming de vídeo requiere protección adicional. La tecnología del lado del cliente también requiere la implementación de SDK, que puede ser compleja en entornos OTT.
- **Marcas de agua con variante A/B.** Dirigidas al sector de OTT, se crean dos retransmisiones de vídeo idénticas, con marcas de agua, y posteriormente se entrelazan en el lado del cliente o a través del procesamiento del borde de la CDN, lo que proporciona un identificador único. Es un método robusto y rentable; sin embargo, dado que la secuencia de identificación puede ser larga, es poco práctica en situaciones que requieren una extracción rápida de las marcas de agua.

Un elemento clave de cualquier estrategia de marcas de agua es el control adecuado para que se puedan aplicar técnicas de cumplimiento válidas para luchar contra los piratas. Hay servicios de control gestionados disponibles o se puede solicitar asesoramiento para desarrollar capacidades internas. Akamai trabaja con todos los importantes proveedores de marcas de agua para garantizar que se pueda poner a disposición una solución viable e integrarla dentro de una estrategia general contra la piratería de vídeo.

Identificación del registro de retransmisiones

Otra forma de detección es mediante el examen en tiempo real de los registros de entrega. En este escenario, la inspección exhaustiva de registros proporciona una imagen en tiempo real de la actividad en función de direcciones IP autorizadas y no autorizadas. La ventaja de estas soluciones, como Stream Protector de Akamai, es la posibilidad de poner en marcha la capacidad rápidamente según la situación, lo que resulta idea para proteger derechos de tiempo limitado, como en el caso de los deportes.

Aplicar

Cuando se detecta actividad de piratería, es importante poder actuar de manera adecuada. Dependiendo de su estrategia, esto puede tomar varias direcciones.

- **Revocar acceso.** Si sus activos de vídeo se retransmiten en tiempo real, como eventos deportivos o en directo, entonces querrá revocar de inmediato el acceso al creador de la retransmisión ilegal. Existen diferentes maneras de lograrlo. Una metodología común es trabajar con su proveedor de servicios de distribución, intercambiar detalles relevantes y detener la actividad de streaming desde una dirección IP infractora. Sin embargo, esto puede llevar tiempo. Akamai ofrece un servicio que permite la revocación de la retransmisión en tiempo real y sin intervención innecesaria. Esto ha demostrado ser particularmente eficaz cuando se lleva a cabo el control de la piratería mediante las marcas de agua o la identificación del registro de retransmisiones.
- **Modificación de la retransmisión.** En situaciones en las que el tiempo no es esencial, los distribuidores pueden decidir modificar la retransmisión pirateada sustituyéndola por contenido alternativo (Big Buck Bunny es popular) o reduciendo la calidad de la retransmisión. Este enfoque tiene la ventaja de que oculta la detección del pirata y evita que salte a una fuente de transmisión diferente.
- **Mensajes en tiempo real.** Como se describe en la sección de tipos de personalidades de piratas, los piratas "perezosos" se sienten seguros con el anonimato en Internet. Las organizaciones como VFT son capaces de identificar a los espectadores de retransmisiones pirateadas en plataformas de redes sociales y pueden enviar un mensaje directamente al infractor. Con esta forma de aplicación, los distribuidores pueden modificar el cumplimiento, como ofrecer acceso a flujos legítimos; y si la infracción continúa, enviar avisos legales.

Conclusión

La piratería de vídeo en el ámbito de la propiedad intelectual es un tema complejo con matices, pero tiene el potencial de amenazar la viabilidad a largo plazo de la industria de los medios de comunicación tal como la conocemos. Hay pruebas abrumadoras que apuntan a daños económicos importantes, pero lo que es más importante es que la piratería tiene el potencial de debilitar o afectar fundamentalmente los modelos de licencias globales.

Hasta la fecha, la respuesta de la industria ha sido relativamente tenue. Como describió un analista: "Estamos en una etapa temprana de adopción con mucho trabajo adelante". Cada vez son más los distribuidores que son conscientes de la amenaza, y la mayoría de los productores y operadores de vídeo de "nivel 1" han establecido equipos dedicados para comprender mejor la piratería, evaluar su propia situación e implementar estrategias antipiratería.

Existen varios requisitos inmediatos identificados en este documento que son necesarios para ayudar a la industria a luchar contra la batalla. Estos incluyen puntos de datos consistentes sobre la piratería, educación continua y mejorada del público en general, mejor cooperación en todo el sector y, finalmente, el liderazgo de propietarios de derechos de todos los géneros para impulsar la omnipresencia en toda la industria a la hora de gestionar y distribuir derechos.

La buena noticia es que gran parte de esto se está comenzando a poner en marcha. Las investigaciones sobre el tema se están volviendo más exhaustivas, empieza a aparecer una legislación más estricta y los proveedores combinan capacidades para maximizar el potencial. Por ejemplo, además de aportar su experiencia en ciberseguridad, Akamai está trabajando con las principales empresas dedicadas a las marcas de agua para garantizar que una vez que se detectan piratas, se pueda poner fin a sus actividades inmediatamente. Por último, estamos observando que los titulares de derechos insisten en estándares mínimos de protección de contenido en todo el flujo de trabajo técnico. En la actualidad, son instancias aisladas o "sugerencias" (tal como sucede con la MPAA), pero consideramos que en el futuro se convertirán en algo necesario para hacer negocios.

Con estas iniciativas en marcha, podemos minimizar el problema para que las pérdidas financieras se reduzcan, se protejan las oportunidades laborales y las licencias puedan seguir prosperando en un mercado global.

REFERENCIAS

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

Bevir. Cost of online piracy to hit $52bn. 2017. Fuente: 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. Fuente: 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. Fuente: 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. Fuente: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

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

Comisión Europea. Estimating displacement rates of copyrighted content in the EU. Mayo de 2015.

Oficina de Propiedad Intelectual de la Unión Europea. Trends in Digital Copyright Infringement in the European Union. 2018.

Oficina de Propiedad Intelectual de la Unión Europea. 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. Fuente: 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. Informe: Millions Illegally Live-Streamed El Clasico. 2015. Fuente: 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. y 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. Julio de 2018.

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

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

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners", una versión abreviada de "Internet piracy: the estimated impact on sales" en Handbook on the Digital Creative Economy, editado por Ruth Towse y Christian Handke, Edward Elgar. 2013.

Mick, J. Nearly half of Americans pirate casually, but pirates purchase more legal content. 21 de enero de 2013. Fuente: 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. Noviembre de 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. 15 de abril de 2014. "Game of Thrones" sets piracy world record, but does HBO care? Fuente: http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care

Sanchez, J. 3 de enero de 2012. How copyright industries con congress. Fuente: http://www.cato.org/blog/how-copyright-industries-con-congress

Sandvine. Video and Television Piracy. 2019.

Schonfeld. Pirate Bay makes $4m a year. 2008. Fuente: 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. Fuente: https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html

---

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com o blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en julio de 2020.