LIVRE BLANC

Protéger la Banque de l'OTT

Akamai

Introduction

Le problème du piratage vidéo n'a rien de nouveau. Dès la création des premières œuvres cinématographiques professionnelles, des personnes ont voulu gagner de l'argent facilement en exploitant « la propriété privée par le biais de la violation du droit d'auteur ». À l'époque du cinéma muet, l'allongement de la durée de projection des films dans les cinémas s'est tellement répandu qu'Hollywood envoyait des « contrôleurs » pour prendre sur le fait les gérants de cinéma peu scrupuleux. Mais le « partage » sur Internet a fait de la distribution digitale de loin le moyen le plus simple et le plus efficace de distribuer instantanément des milliers de copies de vidéos piratées à des millions de téléspectateurs.

Les pirates d'aujourd'hui utilisent toute une gamme de vecteurs d'attaque pour récupérer et distribuer du contenu. Les tactiques courantes incluent le « credential stuffing » (pour récupérer les informations du spectateur et détourner des comptes légitimes) ou la rediffusion de chaînes linéaires avec une expérience qui ne se distingue pas de la télévision. Les entreprises pirates offrent même à leurs clients une expérience utilisateur simple, un service client et une gamme de modèles commerciaux flexibles.

Dans ce contexte, nous explorerons le défi du piratage et nous verrons comment nous pouvons nous défendre grâce à un cadre stratégique.

On estime que 13,7 millions de personnes dans les pays de l'UE accèdent régulièrement à des services de piratage illégaux (selon l'EUIPO 2019), le Royaume-Uni (2,4 millions) et la France (2,3 millions) ayant la plus grande population incriminée. Le chiffre d'affaires annuel généré par les pirates de l'UE est estimé à 1 milliard d'euros (EUIPO 2019). En Amérique du Nord, on estime que plus de 12,5 millions de ménages américains ont accès des vidéos pirates (Parks Associates, 2019), mais en Asie-Pacifique, le problème peut être beaucoup plus répandu. À Hong Kong, par exemple, une étude AVIA de 2019 a montré que 24 % des consommateurs utilisent des terminaux de streaming sur Internet pour accéder à des chaînes piratées. Cette proportion atteint 28 % aux Philippines, 34 % à Taïwan et 45 % en Thaïlande. Ainsi, malgré les efforts de l'ensemble du secteur, nous pouvons constater que le piratage vidéo reste un problème grave dans le monde entier. L'impact peut se faire sentir dans l'ensemble du secteur, entraînant des pertes financières, des pertes d'emplois, et nous commençons à voir des signes d'impact sur les licences.

40 à 97,1 milliards de dollars

Estimation des pertes pour l'industrie cinématographique à cause du piratage vidéo

39,3 à 95,4 milliards de dollars

Estimation des pertes pour le secteur de la télévision à cause du piratage vidéo

Les chiffres absolus sont difficiles à établir en raison de la complexité du sujet, mais dans un rapport commandé par la Chambre de commerce des États-Unis, les pertes financières sont estimées entre 40,0 et 97,1 milliards de dollars pour l'industrie cinématographique et entre 39,3 et 95,4 milliards de dollars pour le secteur de la télévision (NERA Consulting, 2019). En est exclue la perte de revenu pour les gouvernements par le biais de la fiscalité.

Les industries cinématographique et de la télévision soutiennent des millions d'emplois - allant des décorateurs, maquilleurs ou musiciens aux producteurs et réalisateurs - que le piratage met en danger. Dans leur rapport de 2019 sur l'impact du piratage digital sur l'économie américaine, Blackburn, Eisenach et Harrison ont estimé que le piratage a directement causé la perte d'entre 230 000 et 560 000 emplois aux États-Unis cette année.

En outre, nous commençons à voir des signes indiquant que le piratage a une incidence sur les licences, qui sont la force vitale du secteur de la création, et que cela constitue sans aucun doute le problème stratégique le plus dommageable. En d'autres termes, pourquoi les distributeurs potentiels paieraient-ils des sommes d'argent colossales pour des droits alors que le contenu peut être facilement trouvé gratuitement par le biais de sites pirates ? Yousef Al-Obaidly, directeur général de beIN (l'un des plus grands acheteurs de droits de retransmission sportifs) a déclaré que « la bulle des droits sportifs est sur le point d'éclater à cause du piratage à l'échelle mondiale et le modèle commercial va devoir être revu ». Il a aussi signalé que la valeur des droits pour son entreprise sera basée sur le niveau d'exclusivité. Jason Blum, producteur nominé aux Oscars et récompensé aux Emmy Awards, a également décrit l'impact direct du piratage sur les fonds mis à disposition pour les films innovants et risqués. Il suggère qu'à un moment ou à un autre, dans un avenir pas si lointain, les chiffres ne pourront plus être atteints et que les studios devront revoir leurs ambitions à la baisse.

Comment fonctionne l'industrie du piratage ?

Comme dans tout combat, il est important de comprendre ses adversaires, afin d'évaluer leurs motivations, leurs tactiques, leurs forces et leurs faiblesses. Malgré la difficulté, logique, pour obtenir des informations, nous savons qu'il existe un éventail complexe de groupes et de sous-groupes, chacun ayant ses propres motivations et niveaux de complexité, comme le résume l'exposé ci-dessous.

Les groupes d'acquisition

Les membres se considèrent souvent comme des révolutionnaires engagés dans une lutte contre les grandes entreprises. Pour devenir membres des sites de téléchargement, ils doivent prouver qu'ils sont méritants et dignes de confiance. Différents groupes et individus se spécialisent dans certains genres, rivalisent pour acquérir de nouveaux contenus et gagnent ensuite de la reconnaissance. LES FAITS décrivent la structure comme « des groupes de pirates complexes, sophistiqués et bien organisés, soupçonnés d'être impliqués dans d'autres types de cybercriminalité ».

Il existe une gamme complexe de groupes et de sous-groupes de pirates, chacun avec leurs propres motivations et niveaux de sophistication.

Les opérateurs de sites

Ils gèrent des sites vidéo pirates, notamment des sites de torrents comme Pirate Bay ou des sites de type streaming comme TeaTV.
On ne sait pas si les groupes d'acquisition et les opérateurs de sites sont les mêmes individus, mais de nombreuses études ont démontré qu'il existe un recoupement important entre les deux. Les opérateurs gagnent certainement de l'argent grâce à ce processus et gèrent souvent plusieurs sites « miroirs » de sorte que si l'un est fermé par les autorités, ils peuvent toujours rester en ligne et gagner de l'argent.

Les grossistes de terminaux de streaming Internet

La croissance de ces appareils, en particulier Kodi, fournit un flux de revenus relativement stable et prévisible pour les criminels opportunistes. Les grossistes importent les boîtes par le biais de canaux entièrement légaux ou de réseaux criminels et les modifient avec des logiciels illégaux, qui peuvent ensuite être vendus en ligne.

Les pirates sociaux

Utilisant souvent les réseaux sociaux pour distribuer du contenu, les personnes de ce groupe sont moins conscientes ou ambivalentes quant à l'illégalité du piratage et répondent soit au coût de certains genres de contenu soit à la lassitude des abonnements.

Comment les pirates obtiennent-ils le contenu ?

Il existe de nombreuses méthodes permettant aux pirates de voler du contenu en raison des multiples faiblesses qui peuvent être exploitées sur toute la chaîne de valeur. Nous pouvons regrouper les méthodes les plus répandues en fonction des cas d'utilisation.

La diffusion simultanée de chaînes de télévision et d'événements live

L'une des formes de piratage dont la croissance est la plus rapide est l'enregistrement et la redistribution de chaînes de télévision et d'événements live. Voici le moyen d'y parvenir :

- en modifiant le logiciel de lecture vidéo ou du système d'exploitation Android
- en enregistrant des écrans pendant la lecture à l'aide d'un appareil mobile
- en interceptant des vidéos déchiffrées à l'aide de suppresseurs de HDCP connectés à des décodeurs
- en utilisant des attaques par « credential stuffing » pour accéder aux informations d'un utilisateur légitime
- en transférant les vidéos hors d'un marché donné à l'aide d'un VPN

Le contenu à la demande

Les groupes d'acquisition préfèrent diffuser à l'avance des séries TV et des films. La structure de l'industrie des médias présente une gamme de possibilités avec d'innombrables organisations et personnes différentes impliquées dans le processus de production. Les méthodes courantes utilisées pour acquérir de la vidéo sont les suivantes :

- les violations de centres de données, qui conduisent au vol des identifiants des utilisateurs ou du contenu vidéo
- le vol des identifiants des utilisateurs, qui permet d'accéder au contenu vidéo par l'intermédiaire de divers systèmes de production
- les enregistrements de ressources physiques (moins répandus aujourd'hui) pour le partage et la distribution
- le piratage de différents systèmes de production offrant un accès direct aux vidéos
- l'extraction de contenu à partir de sources légitimes, comme iTunes
- les systèmes de prise de vue cinématographique
- le vol direct à l'aide d'attaques de type « Man-in-the-Middle » (MitM)

Comment distribuent-ils le contenu ?

Les pirates utilisent tous les canaux possibles et innovations techniques disponibles pour distribuer leur contenu, notamment :

- des décodeurs IP personnalisés permettant d'accéder aux diffusions TV préprogrammées
- des logiciels exécutés sur des PC et des terminaux de streaming qui permettent la distribution de contenu piraté, par exemple, Kodi
- des applications qui sont installées sur les terminaux de diffusion courants disponibles dans le commerce
- des sites Web et services de réseaux sociaux qui hébergent du contenu créé par les utilisateurs, comme YouTube
- des sites Web qui diffusent du contenu piraté par le biais de liens que l'on trouve par le biais de recherches ou de réseaux sociaux
- des sites de téléchargement, d'hébergement de fichiers et de torrent omniprésents

Bien que les stratégies de distribution des différents groupes de pirates soient moins comprises, il est probable que les groupes d'acquisition favorisent des modèles de partage de ressources, comme les sites d'hébergement de fichiers et les sites de torrent, en raison de leur soutien inhérent de la démocratisation du contenu et de l'altruisme. En revanche, les opérateurs de sites ayant des motivations financières préfèreraient la stratégie du streaming/du terminal de streaming illégal pour imiter les services légaux et encourager de multiples modèles de revenus.

La demande

Il y a beaucoup de raisons pour lesquelles les gens cherchent des sites pirates. Ces raisons comprennent l'argument financier, l'ignorance de leur impact à plus grande échelle et la possibilité d'accéder au contenu sans restriction de date ou de durée de diffusion. De nombreuses personnes différentes sont décrites par VFT Solutions Inc. dans son rapport de 2019 sur les spectateurs pirates. En voici un résumé :

- **L'« anarchiste du contenu »** croit en un accès communautaire et sans entrave au contenu en ligne. Les frais liés aux contenus sont trop élevés et ils ne croient pas que le piratage est immoral ou illégal.
- **Le « Robin des Bois du contenu »** est moins extrême dans ses opinions et n'exclut pas d'envisager des propositions alternatives. Cette personne n'est pas un utilisateur de services de diffusion live, mais il est investi dans la diffusion de fichiers torrent partagés.
- **L'« utilitariste »** justifie ses actions en affirmant que la consommation généralisée de contenu l'emporte sur les dommages ou les préjudices subis par les détenteurs de droits, la plupart des contenus ayant une valeur éphémère.
- **Le « pirate fainéant »** ignore souvent ou professe l'ignorance du fait que la piraterie est illégale. Ils sont influencés par les économies de coûts et la disponibilité généralisée, ainsi que par la facilité d'accès.

VFT suggère que les pirates fainéants et les utilitaristes représentent jusqu'à 70 % du total de la communauté et que les efforts visant à éduquer, convertir ou pénaliser ces groupes auront le plus grand impact sur le piratage.

Pouvons-nous les arrêter ?

Malheureusement, la réponse est, en bref : pas totalement. L'histoire nous a appris qu'il y aura toujours des pirates cherchant à exploiter du contenu, que ce soit pour des raisons altruistes ou commerciales. Cependant, tout n'est pas perdu. Si le problème est abordé de manière stratégique dans l'ensemble de la chaîne de valeur, il peut être minimisé. En pratique, une meilleure coopération à l'échelle du secteur (dans les domaines stratégiques identifiés ci-dessous) aura un impact durable.

Données

Une exigence évidente est une méthodologie standard pour mesurer l'ampleur et l'impact du piratage à l'échelle mondiale. L'utilisation de méthodologies et techniques différentes ne permet pas une analyse continue ou contextuelle et introduit une confusion lors de la hiérarchisation de l'activité ou de la compréhension du retour des initiatives de lutte contre le piratage. Ce problème pourrait être résolu par des organismes du secteur tels que Alliance for Creativity and Entertainment (ACE) jouant un rôle de leaders dans la collecte de données.

Enseignement

Pour la population générale, le piratage est devenu quelque chose que « tout le monde » fait et ne semble donc plus illégal, car le comportement s'est normalisé. Les efforts visant à éduquer le public devraient continuer de rappeler aux personnes que le piratage est un crime et a un impact réel sur les moyens de subsistance.

Aspect juridique et réglementaire

Il existe plusieurs initiatives excellentes lancées par des organismes du secteur ou des initiatives gouvernementales comme le FAPAV en Italie qui poursuivent des pirates vidéo et comblent les failles législatives dans le monde entier. Ces efforts exigent une coordination et un accès aux données pertinentes.

Aspect technique et opérationnel

L'ère du contenu non protégé est révolue depuis longtemps. Ce que cela signifie dans la pratique, cependant, c'est de procéder à un examen stratégique des opérations et d'identifier les maillons faibles de la chaîne de valeur technique, de la production à la distribution, et d'appliquer les mesures appropriées. Nous décrivons cela comme une posture à 360°.

Si le problème est abordé de manière stratégique dans l'ensemble de la chaîne de valeur, il peut être minimisé.

La posture à 360°

Après avoir passé en revue les moyens par lesquels les groupes de pirates acquièrent et distribuent des vidéos, nous avons structuré un cadre basé sur trois principes fondamentaux : protéger, détecter et appliquer. À l'aide de ce cadre, les organisations peuvent examiner de manière stratégique l'écosystème des menaces en fonction de leur rôle dans l'industrie et mettre en œuvre des initiatives opérationnelles et techniques pertinentes afin de minimiser l'impact.

Protéger

Se protéger contre le « credential stuffing »

Comme décrit précédemment, le « credential stuffing » est un vecteur d'attaque populaire utilisé par les pirates pour acquérir des informations de spectateur, généralement par le biais de robots automatisés. Voici nos principales recommandations :

- Codez les pages de connexion/API avec OWASP. Écrivez un code sécurisé en suivant les meilleures pratiques OWASP et effectuez des tests de pénétration réguliers sur vos points de terminaison de connexion.
- Utilisez une protection contre les attaques DDoS. Cela peut vous aider à empêcher les botnets volumétriques d'atteindre votre infrastructure et de submerger vos ressources.
- Utilisez une solution de gestion de bot, telle que Bot Manager Premier d'Akamai, qui peut vous aider à prévenir les attaques sophistiquées de vol d'identifiants en vérifiant le comportement des utilisateurs et la télémétrie des terminaux.

Se protéger contre le vol depuis des systèmes

Le vol qui s'attaque aux systèmes de production internes, au stockage digital ou au cloud public est une source importante de matériel piraté. De manière générale, nous observons plusieurs formes de vol de ressources vidéo :

- Le piratage direct ou les attaques de type MitM par des pirates
- L'enregistrement d'un ID système unique comme des mots de passe
- Le vol par des employés ou des travailleurs indépendants

Il existe plusieurs technologies que les entreprises peuvent utiliser pour minimiser les risques ; elles tournent essentiellement autour du concept de Zero Trust, un cadre que les entreprises utilisent pour transformer l'accès à la technologie. Les principaux composants de la structure incluent : la sécurisation de l'accès à toutes les ressources, quel que soit l'emplacement ou le modèle d'hébergement, l'application d'une stratégie de contrôle d'accès fondée sur le principe du moindre privilège, ainsi que l'inspection et la journalisation de tout le trafic pour y rechercher des activités suspectes. Le cadre impose que seuls les utilisateurs et les terminaux authentifiés puissent accéder aux applications et aux données. Il protège également les applications et les utilisateurs contre les menaces avancées sur Internet.

Plusieurs composants peuvent être utilisés par les entreprises pour mettre en œuvre un cadre Zero Trust. Cependant, la sécurisation de l'accès des employés/travailleurs indépendants aux systèmes de production et de stockage de base est un aspect essentiel. Avec une main-d'œuvre transitoire, les sociétés de médias sont confrontées à des défis uniques en ce qui concerne la mise en œuvre et la révocation de l'accès aux systèmes, et ce parfois quotidiennement. Grâce à des services tels que Enterprise Application Access d'Akamai, les autorisations sur des applications spécifiques peuvent être accordées rapidement en fonction de l'identité et du contexte de sécurité de l'utilisateur et du terminal, sans accorder aux utilisateurs l'accès au réseau d'entreprise où l'exfiltration vidéo peut avoir lieu.

Une autre facette essentielle du cadre Zero Trust est la mise en œuvre de systèmes qui identifient et bloquent de manière proactive les menaces ciblées comme les logiciels malveillants, les ransomware et l'hameçonnage, qui sont des outils utilisés par les pirates dans leurs attaques de type MitM. Enterprise Threat Protector d'Akamai, par exemple, est une passerelle Web sécurisée qui utilise des informations de sécurité en temps réel pour identifier et bloquer de manière proactive les menaces ciblées comme les logiciels malveillants, les ransomware, l'hameçonnage et le vol de données DNS.

Avec une main-d'œuvre transitoire, les sociétés de médias sont confrontées à des défis uniques en ce qui concerne la mise en œuvre et la révocation de l'accès aux systèmes, et ce parfois quotidiennement.

Se protéger contre les violations liées à la zone géographique et aux droits de propriété intellectuelle. Les pirates utilisent souvent la technologie VPN pour masquer leur pays d'origine et leur adresse IP après l'acquisition réussie des informations d'un abonné légitime pour rediffuser du contenu. La technologie de détection de proxy, telle que la détection de proxy améliorée d'Akamai, bloque intelligemment les requêtes à la périphérie associées aux services de proxy ou VPN anonymes, ce qui empêche de tels cas d'utilisation.

Se protéger contre les violations liées à la lecture. C'est de loin la tactique la plus populaire de lutte contre le piratage. Elle peut être réalisée de diverses manières, la plus répandue étant la gestion numérique des droits (GND). La GND fait référence aux outils, normes et systèmes utilisés pour restreindre l'accès aux contenus protégés par le droit d'auteur et empêcher toute distribution non autorisée. Il ne s'agit pas d'une seule technologie en soi.

Selon l'importance des ressources protégées, certains distributeurs se contentent d'un chiffrement simple (c'est-à-dire, en écrivant le contenu à l'aide d'un code qui peut être lu par des terminaux ou des logiciels uniquement avec la clé permettant de déverrouiller le code), car cela nécessite une clé, ce qui offre une protection superficielle pouvant probablement servir contre les pirates occasionnels. Mais les clés sont généralement fournies par des serveurs HTTP et peuvent être copiées et partagées. Par conséquent, elles ne sont parfois pas suffisantes pour protéger le contenu à plus haute valeur ajoutée.

Pour renforcer le chiffrement, des technologies de GND plus avancées gèrent les communications clés via un module de déchiffrement de contenu à l'aide d'un système de défi/réponse. Ces communications sont chiffrées, de sorte que la clé de déchiffrement n'est jamais exposée aux tentatives de piratage. Les technologies de GND avancées utilisent également des règles métier qui définissent quand et comment les clés peuvent être utilisées sur différents terminaux, notamment l'emplacement ou les règles temporelles.

Pour les distributeurs qui cherchent à mettre en œuvre la technologie de GND pendant le processus de mise en package, il est souvent utile de faire appel à des fournisseurs de cloud capables de gérer cette complexité. Akamai, par exemple, a intégré son stockage d'origine pour le contenu à la demande aux capacités de traitement de plusieurs fournisseurs, comme Bitmovin et Encoding.com, capables de mettre en œuvre le chiffrement en temps quasi réel.

Détecter

Comme pour toute forme de vol, la protection ne garantit pas toujours la réussite et, à ce titre, la détection des infractions est essentielle. Il existe plusieurs méthodes de détection des activités de piratage en temps quasi réel :

L'empreinte

Cette méthode permet d'identifier le contenu vidéo sans modifier le support d'origine. Les outils sont utilisés pour identifier, extraire et représenter les attributs appartenant à un fichier vidéo. Toute vidéo peut ainsi être identifiée par son « empreinte » unique, par exemple sur les réseaux de partage de fichiers. Le support d'origine n'a pas besoin d'être modifié d'aucune façon, ce qui est un avantage, mais une empreinte digitale ne peut pas distinguer différentes copies du même titre, c'est-à-dire quelle copie d'une vidéo a été divulguée en premier lieu.

Le tatouage numérique

Bien qu'il ne puisse pas empêcher le piratage, il permet aux fournisseurs de services de le détecter, d'identifier ceux qui en sont responsables, puis de prendre des mesures en conséquence. Le tatouage numérique de vidéo consiste à ajouter un motif de « bits » imperceptibles et inamovibles dans un fichier vidéo. Lier ces données à l'identité du spectateur signifie qu'il est possible de retrouver un pirate qui copie le contenu après l'avoir déchiffré et le distribue illégalement. Trois méthodes principales de tatouage numérique de vidéo sont actuellement utilisées :

- **Modification Bitstream.** Elle implique la modification de zones sélectionnées d'une image qui conserve la qualité vidéo, mais rend identifiables le spectateur et la session. Il s'agit d'une méthodologie fiable, mais qui nécessite un temps de traitement important et augmente la latence du système, ce qui la rend inadaptée au contenu live.

- **Tatouage numérique côté client.** Il fonctionne bien pour l'extraction rapide de tatouage numérique et permet de le déployer sur des plates-formes existantes telles que les boîtiers décodeurs. Une superposition graphique est composée sur le flux vidéo du terminal client et peut être rendue visible ou invisible. Le tatouage numérique n'étant pas appliqué tant qu'il n'a pas atteint le terminal client, le flux vidéo nécessite une protection supplémentaire. La technologie côté client nécessite également le déploiement de SDK, qui peut être complexe dans les environnements OTT.

- **Tatouage numérique de variante A/B.** Destinées au secteur OTT, deux diffusions vidéo identiques sont créées, marquées par un tatouage numérique, puis combinées ou entrelacées ensemble côté client ou via le traitement en périphérie du CDN, ce qui fournit un identifiant unique. Il s'agit d'une méthode solide et économique. Cependant, comme la séquence d'identification peut être assez longue, elle n'est pas privilégiée dans les situations qui nécessitent une extraction rapide des tatouages numériques.

Pour toute stratégie de tatouage numérique, une surveillance adaptée est capitale pour que des techniques d'application adéquates puissent être appliquées aux pirates. Des services de surveillance gérés sont disponibles ou vous pouvez demander conseil pour développer des capacités internes. Akamai collabore avec tous les fournisseurs de tatouages numériques pour garantir la disponibilité et l'intégration d'une solution viable dans une stratégie globale relative au piratage vidéo.

L'identification du journal de diffusion

Une autre forme de détection consiste à examiner en temps réel les journaux de diffusion. Dans ce cas, l'inspection approfondie des journaux fournit une image en temps réel de l'activité illégale fondée sur les adresses IP autorisées et non autorisées. L'avantage de ces solutions, telles que Stream Protector d'Akamai, est la possibilité d'activer et de désactiver la fonctionnalité selon la situation, ce qui est idéal pour protéger des droits limités dans le temps, tels que le sport.

Appliquer

Lorsque des activités de piratage ont été détectées, il est important de pouvoir agir de manière appropriée. Selon votre stratégie, cela peut aller dans un certain nombre de directions différentes.

- **La révocation de l'accès.** Si vos contenus vidéo sont temporaires, comme c'est le cas des événements sportifs, vous devrez révoquer l'accès de l'auteur de la diffusion illégale immédiatement. Il existe différents moyens d'y parvenir. Une méthodologie commune consiste à travailler avec votre fournisseur de services de distribution, à échanger les informations pertinentes et à stopper l'activité de streaming provenant de l'adresse IP incriminée. Cela peut toutefois prendre du temps. Akamai fournit un service qui permet la révocation des diffusions en temps réel et sans intervention inutile. Cela est particulièrement efficace lorsque la surveillance du piratage se fait à l'aide de tatouages numériques ou de l'identification d'un journal de diffusion.
- **La modification de la diffusion.** Dans des situations moins urgentes, les distributeurs peuvent décider de modifier la diffusion piratée en la remplaçant par un contenu alternatif (« Big Buck Bunny » est souvent utilisé) ou en réduisant la qualité de la diffusion. Cette approche a l'avantage de dissimuler la détection pour que le pirate ne se doute de rien et d'empêcher ce dernier de passer à une source de diffusion différente.
- **La messagerie en temps réel.** Comme décrit dans la section sur les types de pirates, les fainéants se sentent en sécurité grâce à l'anonymat offert par Internet. Les organisations comme VFT sont en mesure d'identifier les spectateurs de diffusions piratées sur les plateformes de réseaux sociaux et envoient directement des messages à l'auteur de l'infraction. Grâce à cette forme d'application, les distributeurs peuvent adapter leur réponse, par exemple en offrant l'accès à des diffusions légitimes et, si l'infraction continue, en envoyant des avis juridiques.

Conclusion

Le piratage de vidéos soumises à la propriété intellectuelle est un sujet complexe, nuancé, mais qui peut potentiellement menacer la viabilité à long terme du secteur des médias telle que nous la connaissons. De très nombreuses preuves font ressortir des dommages financiers importants, mais pire encore, que le piratage pourrait porter fondamentalement préjudice ou influencer les modèles de licence du monde entier.

À ce jour, la réponse de l'industrie a été relativement discrète. Comme l'a décrit un analyste, « nous en sommes au stade de l'adoption précoce, il nous reste beaucoup de travail ». Un nombre croissant de distributeurs se sont réveillés face à cette menace et la plupart des producteurs et opérateurs vidéo de « niveau 1 » ont mis en place des équipes dédiées pour mieux comprendre le piratage, évaluer leur propre situation et mettre en œuvre des stratégies de lutte contre le piratage pertinentes.

Plusieurs exigences immédiates identifiées dans ce livre blanc sont nécessaires pour aider le secteur dans cette lutte. Il s'agit notamment de points de données cohérents sur le piratage, d'une éducation plus efficace et continue du grand public, d'une meilleure coopération à l'échelle du secteur, et enfin, d'un leadership de la part des propriétaires de droits de tous les genres pour favoriser l'omniprésence dans l'industrie lors de l'octroi et de la distribution des droits.

La bonne nouvelle, c'est qu'une grande partie de ces éléments commence à être mis en place. La recherche sur le sujet est de plus en plus prise en compte, une législation plus stricte commence à apparaître et des fournisseurs combinent les capacités pour maximiser le potentiel. Par exemple, en plus de mettre à profit son expertise en matière de cybersécurité, Akamai travaille avec toutes les grandes sociétés de tatouage numérique pour s'assurer qu'une fois que les pirates ont été détectés, leurs activités peuvent être interrompues immédiatement. Enfin, nous observons des signes indiquant que les titulaires de droits insistent sur la mise en place de normes minimales de protection du contenu dans tout le flux de travail technique. À l'heure actuelle, ce sont des cas isolés ou des « suggestions » (comme c'est le cas avec la MPAA), mais nous pensons qu'à l'avenir, cela deviendra indispensable à la conclusion des contrats.

Une fois ces initiatives en place, nous pourrons réduire le problème de façon à limiter les pertes financières, à préserver les emplois et à garantir l'avenir des licences sur le marché mondial.

RÉFÉRENCES

Asia Video Industry Association. The Asia Video Industry Report (Rapport sur le secteur de la vidéo en Asie). 2019.

Bevir. Cost of online piracy to hit $52bn (Le coût du piratage en ligne atteint 52 milliards de dollars). 2017. Extrait de 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 (Impacts du piratage vidéo digital sur l'économie américaine). 2019.

Coberly. Streaming services are 'killing' piracy (Les services de streaming « tuent » le piratage). Extrait de https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html

CustosTech. The Economics of Digital Piracy (L'économie du piratage digital). 2014.

Daly. The pirates of the multiplex (Les pirates du multiplex). Extrait de https://www.vanityfair.com/news/2007/03/piratebay200703

Decary, Morselli, Langlois. A study of Social Organisation and Recognition Among Warez Hackers (Une étude de l'organisation sociale et de la reconnaissance chez les pirates de la scène warez). 2012.

Digital Citizens Alliance. Fishing in the piracy stream (La menace pirate). Extrait de https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

Enigmax. Interview with a Warez Scene Releaser (Entretien avec un acquéreur de contenu de la scène warez). 2007. Extrait de https://torrentfreak.com/interview-with-a-warez-scene-releaser/

Commission européenne. Estimating displacement rates of copyrighted content in the EU (Estimation des taux de remplacement du contenu protégé par le droit d'auteur dans l'UE). Mai 2015.

Office de l'Union européenne pour la propriété intellectuelle. Trends in Digital Copyright Infringement in the European Union (Tendances en matière d'atteinte au droit d'auteur digital dans l'Union européenne). 2018.

Office de l'Union européenne pour la propriété intellectuelle. Illegal IPTV in the European Union (La télévision sur IP illégale dans l'Union européenne). 2019.

FACT. Cracking down on digital piracy (La répression du piratage digital). 2017.

Feldman. Près de 5 millions de Britanniques utilisent des services de diffusion de télévision piratés. 2017. Extrait de 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 (Comparaison des technologies de tatouage numérique des abonnés pour le contenu des chaînes de télévision payantes premium). 2019.

Frontier Economics. The economic impacts of counterfeiting and piracy. Report prepared for BASCAP and INTA (Les impacts économiques de la contrefaçon et du piratage. Rapport préparé pour la BASCAP et l'INTA). 2017.

Granados. Rapport : Millions Illegally Live-Streamed El Clasico (Des millions de personnes ont accédé à une diffusion live illégale d'El Clasico). 2015. Extrait de 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 (L'économie du piratage vidéo). 2015. https://pitjournal.unc.edu/article/economics-video-piracy

Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S. et Tysony G. Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers (Le film Pirates des Caraïbes : exploration des sites d'hébergement de fichiers de streaming illégaux). 2018.

Intellectual Property Office. Online Copyright Infringement Tracker (Outil de suivi des violations du droit d'auteur en ligne). 2018.

Jarnikov et al. A Watermarking System for Adaptive Streaming (Un système de tatouage numérique pour le streaming adaptatif). 2014.

Jones, Foo. Analyzing the Modern OTT Piracy Video Ecosystem (Analyse de l'écosystème vidéo du piratage OTT actuel). SCTE•ISBE. 2018

Joost Poort et al. Global Online Piracy Study, University of Amsterdam Institute for Information Law (Étude mondiale sur le piratage en ligne, Institut du droit de l'information de l'Université d'Amsterdam). Juillet 2018.

Kan. Pirating 'Game of Thrones'? That file is probably malware (Vous piratez « Game of Thrones » ? Ce fichier est probablement un logiciel malveillant). 2019. Extrait de https://mashable.com/article/pirating-game-of-thrones-malware/?europe

Lee, T., Texas-size sophistry (Un sophisme aussi grand que le Texas). 2006. Extrait de http://techliberation.com/2006/10/01/texas-size-sophistry/

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners" (« L'impact du piratage sur les ventes et les revenus des titulaires de droits d'auteur »), une version abrégée de "Internet piracy: the estimated impact on sales" (« Piratage sur Internet : l'impact estimé sur les ventes ») dans Handbook on the Digital Creative Economy (Manuel sur l'économie créative digitale), publié sous la direction de Ruth Towse et Christian Handke, Edward Elgar. 2013.

Mick, J. Nearly half of Americans pirate casually, but pirates purchase more legal content (Près de la moitié des Américains piratent à la légère, mais les pirates achètent plus de contenu légal). 21 janvier 2013. Extrait de 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 (La contribution économique du secteur du cinéma et de la télévision aux États-Unis). Novembre 2018.

MPA Content Security Program. Content Security Best Practices Common Guidelines (Programme de sécurité du contenu de la MPA. Directives communes relatives aux meilleures pratiques en matière de sécurité du contenu). Motion Picture Association. 2019.

MUSO. Measuring ROI in content protection (Mesure du retour sur investissement dans la protection du contenu). 2020.

Nordic Content Protection Group. Rapport annuel, 2020.

Parks Associates. Video Piracy: Ecosystem, Risks, and Impact (Le piratage vidéo : écosystème, risques et impact). 2019.

Tassi, P. 15 avril 2014. "Game of Thrones" sets piracy world record, but does HBO care? (« Game of Thrones » établit le record du monde du piratage, mais cela affecte-t-il HBO ?). Extrait de http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care

Sanchez, J. 3 janvier 2012. How copyright industries con congress (Comment les secteurs du droit d'auteur arnaquent le Congrès). Extrait de http://www.cato.org/blog/how-copyright-industries-con-congress

Sandvine. Video and Television Piracy (Piratage vidéo et télévisuel). 2019.

Schonfeld. Pirate Bay makes $4m a year (Pirate Bay empoche 4 millions de dollars par an). 2008. Extrait de 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 (Le trésor des pirates : comment les criminels gagnent des millions avec des diffusions illégales). 2017. Extrait de https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html

---

Akamai *Experience the Edge*

Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations. Publication : 07/20.