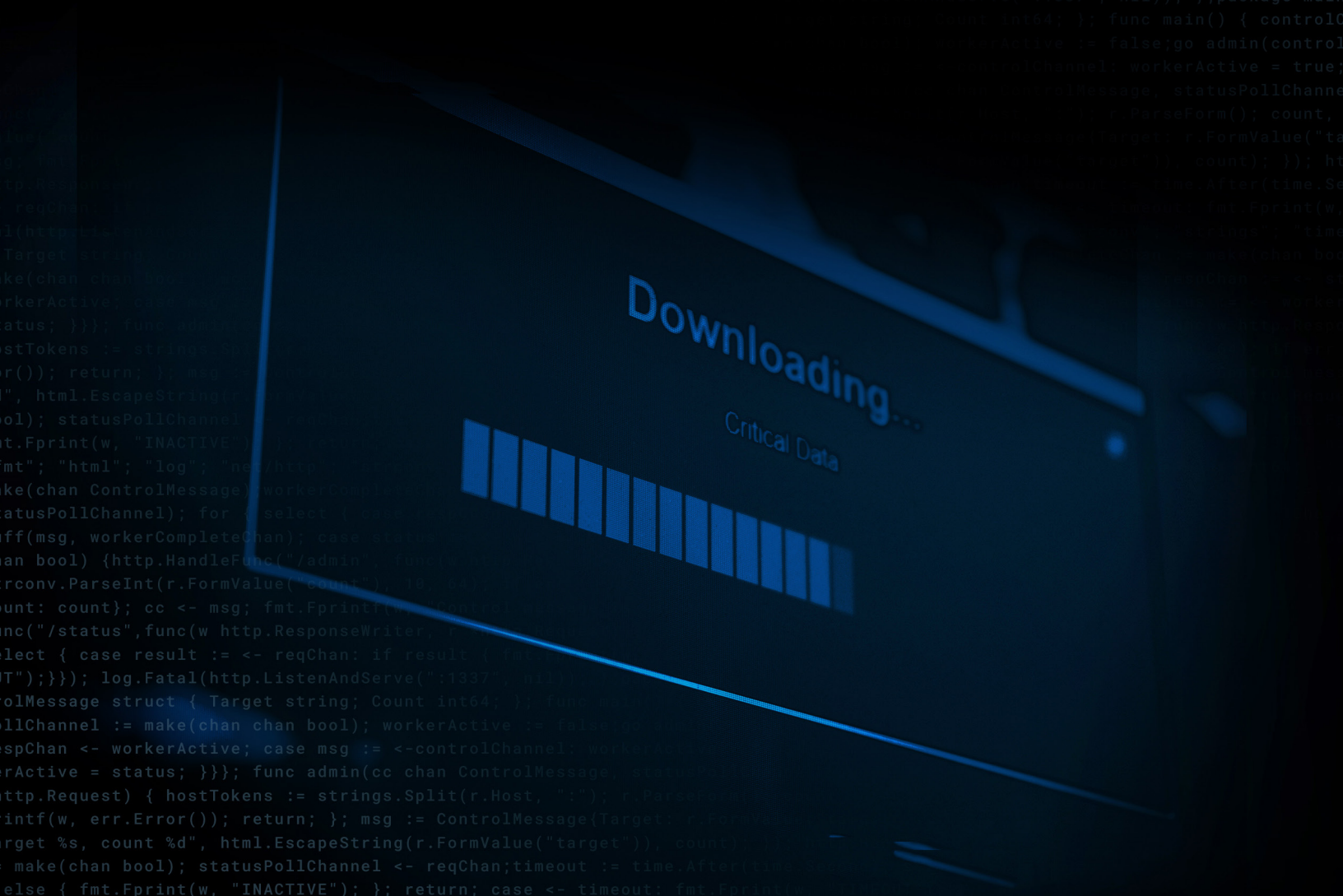
LIVRE BLANC

Immersion dans le monde des pirates vidéo

Comment les arrêter ?



Akamai

Table des matières

L'histoire du piratage vidéo

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. Ensuite, un nouveau type d'escrocs est apparu, utilisant des bobines positives pour créer de nouveaux négatifs, et ainsi des copies des films. Au fur et à mesure des avancées technologiques, les versions pirates « CAM » (enregistrements illégaux directement dans les salles de cinéma) se sont popularisées dans la pratique du vol du droit d'auteur dans les années 60, le secteur les qualifiant de « vidéo d'origine indéterminée ». Toutefois, il a fallu attendre les années 80, avec l'avènement de la VHS, pour que le piratage devienne une activité lucrative qui puisse prendre de l'ampleur. Ceux qui ont grandi aux États-Unis à cette époque se souviennent surement du camion du glacier ou de la supérette du coin, d'où ils repartaient souvent un esquimau à la main et les derniers films sortis sous le bras (bien qu'en qualité médiocre).

Dans les années 80 et 90, en plus de la présence de formats physiques de contenu piraté comme les DVD, qui nécessitaient relativement peu d'expertise technique, le piratage a commencé à se compliquer. Tout d'abord, l'amélioration de la connectivité Internet a permis aux pirates de passer en ligne. La scène « warez », ou « The Scene », une communauté de partage illégal de contenu protégé par le droit d'auteur, à l'origine dédiée aux jeux vidéo, mais qui s'est transformée en d'autres formes de piratage, a développé ce qui a été décrit comme la première véritable sous-culture de l'Internet. Bien que suggérer que les groupes warez sont en grande partie responsables de la croissance du piratage n'ait rien d'original, ils ont joué (et jouent toujours) un rôle important dans la création et la distribution du contenu.

L'augmentation de l'offre de chaînes de télévision payantes dans les années 80 et 90 a également conduit à de nouvelles formes de piratage, comme l'accès illégal à des transmissions chiffrées. Cela a encouragé le développement rapide de technologies d'accès conditionnel. Cependant, en raison des gains commerciaux potentiels et de la complexité technique, les pirates ont eux aussi commencé à devenir plus sophistiqués, organisés et axés sur le potentiel commercial.

Pendant cette période, le « partage » sur Internet a également été facilité par de nouveaux acteurs qui ont encouragé le transfert non autorisé de fichiers, un concept créé par Napster. Malgré sa disparition en 2001, les sites de partage de fichiers P2P (peer-to-peer, ou pair-à-pair) ont commencé à apparaître sur Internet, faisant de la distribution digitale le moyen le plus simple et le plus efficace de partager instantanément des milliers de copies de vidéos piratées avec des millions de spectateurs. La nouvelle génération de plateformes de partage était plus perfectionnée sur le plan technique et les protocoles comme Morpheus, Gnutella, LimeWire, eMule et BitTorrent se sont multipliés. Les plateformes et les protocoles ne stockaient généralement pas de contenu protégé par droit d'auteur sur un serveur central, mais facilitaient les échanges P2P directs entre les utilisateurs (pairs) pour éviter toute responsabilité et vulnérabilité.

La scène warez, ou « The Scene », a été décrite comme la première vraie sous-culture de l'Internet.

La technologie de vidéo digitale légale s'est développée pour fournir de meilleures expériences aux spectateurs sur Internet, et les pirates ont fait de même. Les pirates d'aujourd'hui utilisent toute une gamme de vecteurs d'attaque pour récupérer et distribuer du contenu. La rediffusion de chaînes linéaires est capable de fournir une expérience en tout point semblable à la télévision. Les sites d'hébergement de fichiers, comme Megaupload (remplacé par Mega), utilisent le stockage dans le cloud hébergé dans des endroits où l'application du droit d'auteur est difficile à appliquer. Les méthodes de distribution, variées et solides, comptent notamment les sites Web et les terminaux de streaming. Les entreprises pirates offrent à leurs clients une expérience utilisateur simple, un service client et une gamme de modèles commerciaux flexibles. Une personne interrogée pour ce livre blanc a même laissé entendre que les entreprises de streaming vidéo légitimes auraient beaucoup à apprendre des pirates.

Dans ce contexte, ce livre explorera le « défi du piratage de la propriété intellectuelle » et posera la question suivante : pourra-t-on l'arrêter un jour ?

Faut-il résoudre le problème du piratage vidéo sur Internet ?

Avant de nous demander si le piratage peut être arrêté, nous devons d'abord comprendre si le problème mérite vraiment notre attention, ce qui peut sembler un peu paradoxal pour un livre blanc sur le piratage. Les secteurs de la télévision et du cinéma traversent une ère de bouleversements techniques et commerciaux. Les diffuseurs et les distributeurs de films ont de nombreux besoins concurrents en ce qui concerne les frais d'exploitation et les dépenses d'investissement, le but étant de prendre en charge la production, les nouveaux formats techniques et, souvent, les nouveaux modèles commerciaux. Ainsi, les fonds nécessaires à la lutte contre le piratage seront placés sur l'échelle de priorités de l'entreprise aux côtés de ces autres besoins. Nous devons donc être clairs quant à sa valeur relative et au retour sur investissement potentiel.

Par le passé, ce secteur investissait environ 1 % des coûts de licence dans des mesures de lutte contre le piratage, mais cela a diminué au fil des ans, à mesure que les technologies d'accès conditionnel se sont stabilisées et sont parvenues efficacement à prévenir la fraude à la télévision payante. Le piratage basé sur la propriété intellectuelle ne date pas d'hier, mais dans son article sur les risques du piratage, Parks Associates décrit le secteur des médias comme étant en phase d'adoption précoce. La firme suggère que la plupart des efforts à ce jour n'ont pas été axés sur la prévention du vol ou de la redistribution, mais davantage sur le credential stuffing. Alors que le marché de la vidéo est en marche vers un avenir « tout IP » et que les pirates sont en mesure d'exploiter de nouvelles formes de distribution, devons-nous réévaluer la situation ? Pour répondre à cette question, nous devons parfaitement cerner le problème. Quelle est la véritable ampleur du piratage à l'échelle mondiale et dans différentes régions ? Quel impact a-t-il sur l'entreprise ?

L'ampleur du problème

De nombreuses études remarquables ont été menées sur le piratage vidéo, mais il est encore difficile d'établir l'ampleur réelle du piratage à l'échelle mondiale, régionale et nationale. La raison à cela est simple : personne n'utilise la même méthode pour suivre le problème. C'est pourquoi tout dirigeant d'une entreprise de médias cherchant à établir des priorités serait complètement perdu face à la multitude d'informations.

Les ensembles de données fournis par les organisations commerciales sont utiles, mais peuvent souvent être contradictoires en fonction de la méthodologie utilisée. Les études non commerciales, bien qu'approfondies, sont généralement limitées à des pays ou groupes de pays spécifiques en raison des limites financières ou réglementaires. De même, la terminologie utilisée dans les rapports n'a pas été standardisée, ce qui ajoute encore à la confusion. Enfin, les chiffres absolus sont difficiles à définir, car de nombreux spectateurs de contenu piraté sont aussi de grands utilisateurs de services légaux.

L'une des personnes interrogées pour ce livre blanc compare le piratage à un jeu du chat et de la souris. Tout le monde comprend l'aspect général des vecteurs d'attaque et des formes de distribution, mais personne ne sait vraiment jauger leur ampleur individuelle, ni même identifier la nature du vol d'origine.

Plus récemment, cependant, plusieurs études ont commencé à utiliser des méthodes reproductibles pour quantifier l'ampleur du piratage. À titre d'exemple, l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) a mené une étude sur l'impact du piratage dans les États membres. Il a pu estimer que 13,7 millions d'habitants de pays européens accèdent à différents services de piratage illégaux. Il a également déterminé que les Pays-Bas, la Suède et l'Espagne ont les pourcentages les plus élevés de spectateurs contrevenants, avec respectivement 8,9 %, 8,5 % et 6,9 % de la population (la moyenne européenne est de 3,6 %). Le Royaume-Uni (2,4 millions), la France (2,3 millions) et l'Espagne (2,2 millions) comptent les populations les plus importantes utilisant régulièrement des services illégaux. (À noter que certaines recherches sur l'adoption du piratage viennent contredire ces résultats, notamment une étude récente de YouGov qui a rapporté la présence de 4,9 millions de boîtiers Kodi illégaux en fonctionnement au Royaume-Uni.) En Europe, contrairement à d'autres régions, le piratage a quelque peu baissé. Bien que les chiffres réels soient sujets à débat, cela est lié au durcissement des mesures de répression et des poursuites judiciaires visant les pirates, ainsi qu'à l'effort continu de certains gouvernements pour sensibiliser leur population aux conséquences néfastes du piratage.

13,7 millions

Estimation du nombre de personnes ayant accès à des vidéos piratées au sein de l'Union européenne.

En Amérique du Nord, la situation est moins claire. Sandvine a analysé l'utilisation de plusieurs réseaux fixes de « niveau 1 » et a estimé que 6,5 % des ménages interagissaient régulièrement avec des sites pirates. En revanche, selon un rapport de Park Associates, plus de 14,1 millions de ménages américains ont accédé à des vidéos piratées en 2019, ce qui équivaut à environ 16 % du marché total de la télévision payante. Bien qu'il s'agisse de chiffres comparatifs avec l'Union européenne, les différences de méthodologie peuvent sous-estimer l'ampleur du problème dans cette région.

La situation en Asie-Pacifique est beaucoup plus complexe. En effet, dans une région diversifiée sans organisme de réglementation centralisé, la plupart des études sont menées dans des pays spécifiques et, généralement, par le biais d'organisations commerciales ou sectorielles. Les recherches disponibles montrent toutefois que le nombre d'adeptes de contenu piraté est parmi les plus élevé dans ce territoire.

L'étude de 2017 de l'Université d'Amsterdam a identifié les habitudes de piratage à Hong Kong, en Indonésie, au Japon et en Thaïlande. Les résultats indiquent que les populations indonésiennes et thaïlandaises montrent une très forte propension à consommer du contenu piraté, l'étude estimant respectivement la proportion autour de 65 % et 54 % des internautes. Une proportion de 27 % des internautes a été enregistrée pour Hong Kong, contre à peine 12 % pour le Japon (11 % de la population totale).

Un rapport d'étude indépendant auprès des internautes commandé par l'Asia Video Industry Association en 2019 corroborait ces résultats et constatait qu'à Hong Kong, 24 % des internautes utilisaient des terminaux de streaming en ligne pour accéder à des chaînes piratées. Cette proportion atteint 28 % aux Philippines, 34 % à Taïwan et 45 % en Thaïlande.

Ces chiffres montrent clairement que le piratage vidéo, et en particulier le piratage télévisuel, reste un problème grave à l'échelle mondiale. Cela dit, nous devons encore évaluer l'impact de ce piratage pour déterminer la nécessité d'investir plus de temps et de ressources dans la lutte contre ce problème.

Quel est l'impact du piratage ?

L'impact du piratage vidéo sur la viabilité à long terme du modèle commercial des médias a fait l'objet de nombreuses recherches détaillées. La plupart des personnes interrogées s'accordent sur les défis stratégiques, mais on constate des écarts considérables sur les chiffres absolus. Ce facteur prend de l'importance lorsque l'on considère la valeur relative d'un investissement dans des initiatives de lutte contre le piratage par rapport à d'autres demandes commerciales. De nombreux facteurs peuvent être pris en compte lors de l'examen de l'impact du piratage, notamment la propagation de logiciels malveillants et d'autres cybermenaces. Toutefois, aux fins du présent document, nous nous sommes concentrés sur trois aspects clés de cet impact : le domaine financier, les emplois et les licences.

L'impact financier du piratage

L'impact financier négatif dû au piratage vidéo est généralement reconnu par la plupart des personnes interrogées. Des études ont estimé les pertes pour ce secteur à 52 milliards de dollars d'ici 2022 à l'échelle mondiale (Digital TV Research 2017), avec des estimations de pertes de PIB dues à une réduction des impôts atteignant des niveaux encore plus élevés. Rien qu'aux États-Unis, l'estimation des pertes de PIB dues au piratage représente entre 47 et 115 milliards de dollars (Blackburn et al, 2019).

Malgré ces chiffres désolants, de nombreux distributeurs voient encore la prévention du piratage comme un coût pour leur entreprise plutôt que comme un facteur d'augmentation potentielle de leurs revenus. Les raisons qui motivent cette vision sont complexes, mais sensées. Premièrement, il est difficile de prouver que la prévention du piratage entraînerait une hausse des revenus. En effet, les recherches ont montré que le piratage améliore parfois les revenus tirés des abonnements (Sanchez, 2012), car il fournit de la publicité gratuite pour des services légaux. La méthode de l'« essai gratuit » a également été décrite comme un moyen de faire connaitre aux spectateurs de nouveaux acteurs ou genres, ce qui, dans un modèle commercial payant, serait impossible (cela est bien sûr nuancé par le genre et la disponibilité d'alternatives légales). Des études ont montré que les personnes qui consomment du contenu provenant de sources illégales sont également les plus gros clients du secteur de la vidéo, c'est-à-dire que les adeptes de films ou de séries télévisées ont tendance à consommer davantage, via n'importe quel canal disponible. À ce titre, il est impossible de comparer la consommation légale et illégale des individus et d'établir un lien causal avec une perte financière.

Dans le même ordre d'idées, le partage d'informations d'identification, bien que considéré comme une forme de piratage, est souvent négligé par les services de vidéo à la demande par abonnement (SVOD), car il fournit lui aussi des avantages marketing. Comme l'indique un CTO : « Nous avons conscience de ce phénomène, mais nous savons également qu'ils finiront par revenir. Donc, à l'heure actuelle, cela ne compte pas parmi nos priorités. »

L'autre facteur à prendre en compte lors de l'examen des pertes financières est l'utilisation fréquente de l'« effet multiplicateur » par les chercheurs, qui peut à son tour surestimer à tort l'impact financier sur le secteur. Par exemple, la Motion Picture Association of America (MPAA) a admis que les pertes financières dues au piratage communiquées dans l'un de leurs rapports ont largement surévalué le problème (Greenburg, 2015 ; Sanchez, 2012).

Les impacts financiers du piratage vidéo sont donc fortement nuancés au niveau régional, national et selon les entreprises. Une étude réalisée en 2017 par l'Université d'Amsterdam a identifié la complexité de la compréhension de l'impact financier du piratage au niveau mondial. Les résultats ont montré que les attitudes nationales individuelles continuent d'avoir un impact prépondérant sur l'adoption du piratage, montrant des exemples à la fois dans les pays développés et dans les pays en développement où la législation sur le droit d'auteur est présente. Cette confusion est déroutante pour les dirigeants des chaînes de télévision et des studios, surtout lorsqu'il s'agit d'établir des priorités budgétaires.

Entre 79,3 et 192,5 milliards de dollars

Estimation du coût du piratage mondial pour les secteurs du cinéma et de la télévision.

Cela dit, l'effet de substitution (c'est-à-dire lorsqu'un spectateur n'achète pas ou ne regarde pas légalement un contenu spécifique après l'avoir acquis ou consommé par le biais d'une source illégale, ou après avoir remplacé la consommation légale par un autre loisir) est considéré comme un défi de taille pour le secteur. Une étude commandée par la Chambre de commerce des États-Unis et publiée en 2019 a estimé que, en 2017, les pertes totales de recettes mondiales dues au piratage de vidéos digitales liées à la substitution et d'autres facteurs se situaient entre 40 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. Aux États-Unis, ces chiffres ont été évalués à 2,5 milliards de dollars (cinéma) et à 3,6 milliards de dollars (télévision), ce qui montre que le piratage touche en fait le monde entier.

Quel que soit le point de vue sur les pertes financières liées à la substitution, les gains financiers réalisés par les pirates sont plus clairs. Au sein de l'Union européenne, on estime que les pirates génèrent plus de 941,7 millions d'euros de revenus annuels grâce à des abonnements payants et à la publicité. Le Royaume-Uni, la France, l'Allemagne, les Pays-Bas et l'Espagne génèrent près de 76 % de ces revenus (EUIPO, 2019). Aux États-Unis, Sandvine a estimé que l'écosystème du piratage génère des chiffres similaires, avec des revenus de plus de 1 milliard de dollars. Aucune étude viable n'a été réalisée dans les régions de l'Asie-Pacifique ou de l'Amérique du Sud pour fournir des chiffres comparatifs.

L'impact du piratage vidéo sur les emplois

La plupart des documents concernant l'impact du piratage se concentrent sur la perte de revenus, mais les secteurs de la télévision et du cinéma soutiennent également des millions d'emplois, des scénographes, des maquilleurs et des musiciens aux producteurs et aux réalisateurs, et le piratage met ces derniers en danger. Jusqu'à récemment, la relation entre piratage vidéo et pertes d'emplois était relayée par plusieurs annonces très médiatisées de réduction du personnel ou de fermeture de services. Par exemple, beIN a annoncé 300 suppressions de postes comme conséquence directe du piratage et RTL International a annoncé la clôture de ses chaînes de télévision payante internationales.

Un autre exemple notable est l'annulation du thriller d'horreur psychologique *Hannibal* en raison de « mauvaises notes ». La série s'est pourtant classée au cinquième rang des séries les plus téléchargées illégalement en 2013. Martha de Laurentiis, la productrice de la série, a déclaré « les fans déçus de la série ne peuvent en vouloir qu'à eux-mêmes et à leurs pairs », ajoutant que « le piratage a joué un grand rôle dans l'annulation d'Hannibal ».

Avec l'arrivée d'études mieux renseignées, nous commençons maintenant à appréhender l'impact plus large de cette pratique. Dans leur rapport 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 en 2017. Des pertes d'emploi ont été observées dans tous les domaines de ce secteur, y compris les rôles directs et indirects, créatifs et non créatifs.

L'impact sur les pertes d'emplois à l'extérieur des États-Unis a été moins souvent étudié en raison de la répartition inégale des rôles entre les différents pays, contrairement aux États-Unis qui sont un marché homogène. En Italie, des recherches de la Fédération pour la protection du contenu audiovisuel et multimédia (FAPAV) ont toutefois estimé que les pertes d'emplois directement liées au piratage s'élevaient à près de 6 000. Encore une fois, cela était basé sur l'impact plus large sur les rôles associés à la production et à la distribution de médias. En examinant les méthodologies utilisées par la FAPAV, il est clair que les pertes d'emplois dans les autres États membres de l'UE pourraient être proches de celles observées en Italie. En outre, dans les pays producteurs/exportateurs de contenu plus importants, comme le Royaume-Uni, l'Espagne et l'Allemagne, ces taux pourraient être encore plus élevés.

Il convient de noter que l'importance de l'impact du piratage sur l'emploi a été réfutée par un certain nombre de chercheurs. Plusieurs experts ont remis en question la validité de « l'effet de substitution », ou l'impact réel du piratage sur les revenus dérivés du secteur, qui à leur tour ont des répercussions sur l'emploi. Plusieurs chercheurs ont suggéré que la mesure de la substitution « d'opportunité » pourrait être un indicateur plus précis lors de l'analyse des pertes d'emplois. Cela est dû au fait que la production dépend des professionnels de la création indépendants, qui peuvent ne pas être employés à temps plein si le piratage a un impact sur les investissements de programmation. Il a aussi été mis en évidence que la dynamique actuelle dans le secteur de la production, en partie favorisée par les investissements réalisés par les services de SVOD, réduit les perspectives d'emploi négatives dues au piratage.

Malgré le débat en cours sur les niveaux de l'effet de substitution du piratage, il est clair que la violation du droit d'auteur a un effet inhibiteur sur l'emploi, ou en tout cas sur les possibilités d'emploi. Tout secteur qui subit des vols de produits à des niveaux aussi monumentaux aurait du mal à assurer le plein emploi. L'impact sera probablement plus marqué dans les pays ou les entreprises qui sont fortement impliqués dans la production ou qui gèrent des chaînes internationales.

L'impact du piratage vidéo sur les licences

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 un problème stratégique plus dommageable que les autres. En d'autres termes, pourquoi les distributeurs potentiels paieraient-ils des sommes d'argent colossales pour des droits lorsque le contenu est facilement trouvable gratuitement par le biais de sites pirates ? À l'inverse, pourquoi les titulaires de droits les vendraient-ils à des distributeurs responsables de fuites de contenu et qui pourraient nuire à leurs ventes internationales ?

Le sport en tant que genre est évidemment sensible à ce phénomène, ce que confirment des communiqués de presse récents. Yousef Al-Obaidly, le 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 international ». Il a aussi signalé que la valeur des droits pour son entreprise sera basée sur le niveau d'exclusivité. Si le contenu acquis n'est pas exclusif en raison du piratage, sa valeur diminuera considérablement.

Dans un autre article, Jason Blum, producteur nominé aux Oscars et récompensé aux Emmy Awards, a décrit l'impact direct du piratage sur les fonds mis à disposition pour les films innovants et risqués qui font la part belle au storytelling. 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. « Ils ne toucheront pas à leurs franchises (qui leur rapportent gros) ni à leurs films d'horreur à petit budget : les coupes viseront les films d'auteur, qui sont risqués et rarement rentables. Bientôt, des films comme *The Big Short : Le casse du siècle* ne pourront plus être piratés, car ils n'existeront plus ».

> *« La bulle des droits sportifs est sur le point d'éclater à cause du piratage international ».*
>
> *– Yousef Al-Obaidly, PDG, beIN*

Et donc, pour répondre à la question, faut-il résoudre le problème du piratage vidéo sur Internet ? De prime abord, les retombées de la mise en œuvre de stratégies de lutte contre le piratage pour la plupart des distributeurs semblent claires : protection des revenus de base, des droits exclusifs et des emplois. Le piratage est répandu dans toutes les régions et, malgré un certain succès limité dans l'Union européenne, il devrait croître au cours des prochaines années. Il est clair que le piratage a un impact préjudiciable sur les finances des producteurs, des titulaires de droits et des distributeurs. Ce qui l'est moins, en revanche, c'est l'ampleur de cet impact au niveau des entreprises, ce qui rend notoirement difficile pour n'importe quel conseil d'administration de justifier des investissements antipiratage.

Il s'agit d'un sujet très nuancé qui dépend de la réponse à différentes questions, notamment : la télévision payante est-elle la forme dominante de visionnage au sein d'une nation ou est-ce la télévision gratuite ? L'entreprise est-elle une exportatrice nette de droits ou une importatrice de droits exclusifs ? L'entreprise a-t-elle un avantage concurrentiel dans un genre particulier, comme les séries télévisées ou les films ? Une fois ces facteurs compris, il devient possible de créer une analyse claire des risques financiers au niveau de l'entreprise, qui peut à son tour contribuer à établir une stratégie appropriée.

Le point commun entre toutes les sociétés de médias, quel que soit leur modèle commercial, ce sont les défis plus stratégiques créés par le piratage, à savoir l'impact sur les possibilités d'emploi et les licences. Ces facteurs sont tous deux essentiels à la santé et à la viabilité à long terme de ce secteur, en particulier parce que le déficit budgétaire pour la production est désormais courant. À l'avenir, les titulaires de droits, organismes sectoriels et même les régulateurs vont vraisemblablement inciter les entreprises de tout l'écosystème à mettre en œuvre des stratégies plus complètes pour résoudre ce problème. Nous explorerons ces stratégies dans la dernière section de ce document.

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. Contrairement à de nombreux autres aspects du piratage vidéo, il existe très peu d'études fiables dans ce domaine, probablement pour des raisons évidentes.

Qui sont les pirates ?

Les études décrivent souvent les pirates vidéo comme un groupe homogène infâme avec un but commun : gagner de l'argent. Une simple recherche sur Internet fera apparaître de nombreux articles décrivant comment la police a démantelé un certain « gang de pirates » qui a gagné des millions de dollars de revenus avec son site.

Les pirates y sont représentés comme des criminels organisés et opportunistes à l'origine d'entreprises complexes et sophistiquées, ce qui est certainement vrai dans de nombreux cas. Comme tant d'aspects du Web, cependant, le piratage digital est par nature international et anonyme. Il est difficile d'identifier avec certitude la provenance d'un film ou d'une émission de télé piraté, ou l'auteur du piratage. Ce que nous savons, cependant, c'est qu'il existe un éventail complexe de groupes et de sous-groupes, chacun avec ses propres motivations, niveaux de sophistication et dépendances inter-groupes.

Les groupes d'acquisition

Plusieurs études sur les pirates décrivent des personnages altruistes, qui rappellent la scène warez originale. Les membres se considèrent souvent comme des révolutionnaires « idéalistes » engagés dans une lutte contre les grandes entreprises. Ceux qui sont arrêtés et poursuivis sont souvent acclamés comme des héros. Après avoir purgé une peine de 10 mois d'emprisonnement, Fredrik Neij, cofondateur de Pirate Bay, a déclaré : « Vu l'importance du site pour les gens, un séjour en prison en valait largement la peine. »

Dans ce groupe, les pirates sont liés par un sentiment d'appartenance, malgré un faux sentiment d'altruisme, mais ils ne sont pas forcément motivés par les gains financiers. Pour devenir membres des sites sur lesquels le contenu est mis en ligne, 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. Le contenu de mauvaise qualité ou infecté par des virus est « détruit » et la personne qui l'a fourni perd toute crédibilité aux yeux de la communauté. Dans son article sur le développement des torrents pour *Vanity Fair*, Steve Daly a décrit les membres du groupe d'acquisition comme des stéréotypes classiques du geek passionné d'informatique : mal à l'aise en société, de nature obsessionnelle et chez qui voler du contenu induit un sentiment d'appartenance. FACT a décrit cette structure très différemment : « Il s'agit de groupes de pirates complexes, sophistiqués et bien organisés, soupçonnés d'être impliqués dans d'autres types de cybercriminalité, comme la diffusion de ransomware ou le vol de données bancaires qu'ils revendent sur le Dark Web ». Quelle que soit leur motivation, et comme dans la scène warez, les groupes ont une hiérarchie et une structure claires qui s'accompagnent de nombreuses lois écrites et de solides relations de confiance.

Les opérateurs de sites

Les sites accessibles au public, comme les sites d'hébergement de fichiers ou les sites de streaming, sont gérés par un autre groupe distinct : les opérateurs de sites. 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 et une dépendance importants entre les deux. Quoi qu'il en soit, les opérateurs de sites se remplissent les poches avec ces activités. Les opérateurs de sites utilisent souvent plusieurs « miroirs », des sites qui se dupliquent les uns les autres de sorte que si l'un d'eux est fermé par les autorités, les autres restent actifs et continuent de rapporter de l'argent. Comme pour toute opération de vente au détail sophistiquée, ces activités impliquent également des grossistes de sites (par exemple, Streamango et Openload) qui, à eux seuls, ont alimenté plus de 50 des principaux sites illégaux de liens et de streaming vidéo. Le plus effronté de tous doit certainement être la marque beoutQ qui, malgré la restriction de ses flux illégaux sur Arabsat, continue à distribuer du contenu sur Internet via ce qui a été décrit comme du piratage à l'échelle industrielle. Bien que l'on puisse aisément comprendre pourquoi les groupes d'acquisition ne sont pas nécessairement motivés par l'appât du gain, il est clair que les opérateurs de site le sont. Dans certains cas, il s'agit à la base de couvrir les frais du site (comme l'ont suggéré les créateurs de Pirate Bay). Pour d'autres, les bénéfices potentiels sont trop lucratifs, ce qui a conduit des opérateurs de sites à se développer pour devenir des entreprises mondiales très sophistiquées.

Les grossistes de terminaux de streaming Internet

Parmi les différents types de pirates vidéo, on trouve également les grossistes de terminaux de streaming Internet. La multiplication de ce type de terminaux, en particulier ceux qui utilisent Kodi, fournit un flux de revenus relativement stable et prévisible pour les criminels opportunistes, capables de générer des centaines de milliers de dollars par an. Les grossistes importent souvent les boîtiers par le biais de canaux entièrement légaux, puis les modifient chez eux avec des logiciels illégaux. D'autres collaborent avec des réseaux criminels sophistiqués pour importer des boîtiers, puis les vendre en ligne, en parvenant parfois à vendre des centaines ou des milliers de boîtiers avant d'être arrêtés. La disponibilité de modules complémentaires illégaux pour le boîtier Kodi a permis aux gangs organisés de toucher une audience plus large. Bien que le Kodi lui-même soit légal, les modules complémentaires ne le sont pas. Ils n'ont aucune fonction de contrôle parental ni norme de sécurité et soumettent les utilisateurs à de nombreux risques, qu'il s'agisse de contenu pour adulte ou inapproprié.

Le pirate amateur

Plus récemment, et en plus des améliorations apportées à la diffusion live sur les plateformes de réseaux sociaux, un nouveau personnage a émergé : le pirate amateur. Contrairement aux opérateurs de sites, aux grossistes de terminaux de streaming illégaux et aux groupes d'acquisition qui sont motivés par le profit ou l'altruisme organisé, les membres de ce groupe sont moins conscients ou plus mitigés vis-à-vis du fait que le piratage est illégal, et agissent en réponse au coût de certains genres de contenu, à la lassitude vis-à-vis des abonnements ou à l'omniprésence des réseaux sociaux. À titre d'exemple, pour le match de boxe Mayweather contre McGregor, on a dénombré 132 millions de vues piratées provenant de plus de 6 977 diffusions illégales. Ces diffusions étaient principalement émises par des personnes qui tenaient simplement leur téléphone devant leurs écrans de télévision et utilisaient des plateformes de réseaux sociaux pour diffuser le contenu.

Il est important de bien comprendre ce qui différencie les groupes de pirates. Comme pour toute activité criminelle organisée, les gangs qui veulent gagner de l'argent cherchent des cibles faciles pour maximiser leurs rendements. Les obstacles, même rudimentaires, qu'ils rencontrent peuvent les empêcher d'agir. Les pirates plus idéalistes ont d'autres motivations, c'est pourquoi il est beaucoup plus difficile de contrer leurs activités.

Ce qui est vrai dans presque tous les cas, cependant, c'est la présence d'un écosystème de participants organisés composés d'auteurs d'infractions principaux (les fournisseurs de contenu non autorisé), d'une série d'intermédiaires passifs et actifs, de facilitateurs qui, par exemple, aident les internautes à exploiter des middlewares et, enfin, les spectateurs de matériel piraté eux-mêmes. Nous aborderons ces derniers dans la section « Qui regarde du contenu piraté ? ».

Les obstacles peuvent décourager certaines activités, mais les pirates plus idéalistes ont d'autres motivations et il est beaucoup plus difficile de les empêcher d'agir.

Comment les pirates obtiennent-ils le contenu ?

En raison de l'omniprésence des flux de travail digitaux, de nombreuses méthodes viables sont désormais à disposition des pirates pour voler du contenu, mais pour des raisons évidentes, il existe très peu d'analyses fiables indiquant lesquelles de ces méthodes sont favorisées ou plus répandues chez les différents sous-groupes. Cependant, les informations disponibles montrent plusieurs faiblesses qui peuvent être exploitées dans toute la chaîne de valeur. Pour donner un exemple clair, nous pouvons regrouper les vecteurs d'attaque 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. En effet, dans le rapport 2019 sur le secteur de la vidéo en Asie, la Coalition Against Piracy a déterminé que de nombreux téléspectateurs qui avaient opté pour un terminal de streaming illégal s'étaient également désabonnés de services légaux, faisant de leur terminal leur principal service de télévision. Par exemple, à Hong Kong, près d'un ménage sur quatre utilise un terminal de streaming illégal, et 10 % d'entre eux ont annulé leur abonnement à des services légaux. En outre, la généralisation des smartphones, associée aux améliorations de la diffusion live sur les plateformes de réseaux sociaux, permet désormais à n'importe qui de simplement diriger un terminal vers un écran de télévision et de diffuser du contenu. Les pirates utilisent donc différentes méthodes pour enregistrer des canaux live, notamment :

- en modifiant le logiciel de lecture vidéo ou du système d'exploitation Android ;
- en enregistrant l'écran pendant la lecture ou en capturant le contenu pendant une session en écran partagé ;
- 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 modifiant la vidéo pour supprimer le tatouage numérique, par exemple, le rééchantillonnage ;
- en transférant les vidéos hors d'un marché donné à l'aide d'un VPN.

Le contenu à la demande. Il s'agit sans doute de la forme de piratage la plus prolifique au monde. Les groupes d'acquisition, en particulier, raffolent des nouveaux supports vidéo et cherchent à enregistrer des émissions et des films avant même leur première diffusion au public. Fait intéressant, dans ce scénario, la structure du secteur de la création elle-même offre un éventail d'opportunités aux pirates. Le fait que tant d'entreprises et de travailleurs indépendants différents soient impliqués dans les processus de production et de postproduction donne aux pirates de nombreuses occasions d'identifier et d'exploiter les vulnérabilités. En effet, un individu interrogé pour ce livre blanc illustre ce point en décrivant comment les pirates ont ciblé les outils de montage connectés à Internet et les plateformes de stockage associées pour accéder à de nouvelles séries avant qu'elles n'atteignent la phase de diffusion. Pour acquérir des ressources vidéo, les pirates utilisent également les méthodes suivantes :

- Les violations de centres de données, qui conduisent au vol des identifiants des utilisateurs, des clés cryptographiques ou du contenu vidéo
- Le vol d'identifiants de travailleurs indépendants et du personnel à temps plein fournissant l'accès aux vidéos via différents systèmes
- 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 ressources vidéo
- 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)

Le contenu à la demande est sans doute la forme de piratage la plus prolifique au monde.

Comment les pirates distribuent-ils le contenu ?

Contrairement aux méthodes d'acquisition de contenu, ce domaine du modèle commercial pirate est bien documenté et, comme c'est le cas avec le streaming légal, les pirates utilisent tous les canaux possibles et les innovations techniques disponibles, y compris :

- 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, le 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 aux utilisateurs avec des liens trouvables par une simple recherche sur Internet ou mis en avant sur les 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 clair que les groupes d'acquisition favoriseraient probablement 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. En revanche, les pirates 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. Il convient de noter que la relation entre les groupes pirates est moins claire. Les propriétaires de sites s'appuient-ils sur les groupes d'acquisition pour les ressources à la demande ? Les propriétaires de sites sont-ils autonomes ou emploient-ils des groupes plus compétents sur le plan technique pour contourner les technologies de lutte contre le piratage ?

Un aspect commun dans la plupart des cas, cependant, est la nécessité de générer des revenus, au moins pour prendre en charge les coûts d'infrastructure de base. La plupart des sites ont des modèles de revenus basés sur la publicité, mais les sites qui prennent en charge le streaming en diffusion simultanée ont certainement adopté une approche multidimensionnelle, y compris des modèles d'abonnement ou hybrides.

TechCrunch (2008) a signalé que Pirate Bay générait plus de 4 millions de dollars de revenus publicitaires par an grâce à ses 2,5 millions d'abonnés. FACT a également indiqué dans son rapport de 2017 que même les sites plus petits pourraient générer des revenus publicitaires équivalents à 100 000 dollars par an. Bien que ces chiffres soient faibles par rapport aux entreprises légales, les marges bénéficiaires des pirates sont estimées à 80-94 % (FACT, 2017). Sachant qu'une entreprise légale bénéficie de marges de 7 à 20 %, l'attrait pour le piratage est facile à comprendre.

Les publicités sont généralement des bannières publicitaires ou des fenêtres contextuelles pour des casinos, des sites de rencontres, de la pornographie et des services de téléchargement. Cependant, certains sites présentent des publicités qui ont été placées à l'aide d'une technologie programmatique, ce qui signifie que les marques légitimes ne savent souvent pas exactement où leurs publicités atterrissent, mais peuvent donner un air respectable au site. Dans les modèles basés sur l'abonnement, les pirates encouragent les utilisateurs à souscrire un compte « premium », qui offre une meilleure expérience de visionnage et supprime les publicités, en échange d'un paiement mensuel. Les prix varient d'un site à l'autre et la plupart offrent plusieurs forfaits avec des options et des prix variés. Mais, en général, les abonnements coûtent entre 6 et 60 dollars par mois.

Il y a cependant une face plus sombre. Les individus qui envoient du contenu sur les sites de torrent ne gagnent que peu ou pas d'argent et, comme la concurrence s'intensifie entre les pirates, de nombreux sites de streaming se sont tournés vers des logiciels malveillants, des virus, des logiciels publicitaires et de courrier indésirable. Les logiciels malveillants sont souvent conçus pour promouvoir le piratage, l'usurpation d'identité, l'exploitation forcée de cryptomonnaies et le contenu en ligne illégal, comme la pornographie. Les individus qui distribuent des logiciels malveillants sont parfois très bien rémunérés pour leur peine. Une étude menée aux États-Unis a révélé qu'un site pirate sur trois a exposé ses utilisateurs à des logiciels malveillants, et les gangs criminels ont enregistré au moins 70 millions de dollars de recette par an en payant des pirates informatiques pour l'intégration de logiciels malveillants (Digital Citizens Alliance, 2017).

Plus récemment, les pirates ont exploré de nouvelles façons de gagner de l'argent, y compris des tentatives de « rançon contre contenu ». Dans ce scénario, les pirates volent (ou prétendent avoir volé) des épisodes de séries ou des films et demandent ensuite le paiement de rançons à l'organisme demandeur du contenu en question. Plusieurs incidents de ce type ont été rapportés dans les médias, notamment en 2017, pour les vols de la série *Orange Is the New Black* et du film *Pirates des Caraïbes : La Vengeance de Salazar*. HBO a été victime d'une cyberattaque au cours de laquelle 1,5 téraoctet de données aurait été volé, des pirates menaçant de distribuer les épisodes et les scripts de *Game of Thrones* (Sulleyman, 2017).

La diffusion live d'événements ou rencontres sportives majeurs a été particulièrement ciblée par les pirates en raison des coûts dont les fans doivent s'acquitter pour accéder à des diffusions légales et de l'attrait émotionnel de ces événements. Dans certaines circonstances, par exemple lors de matchs de football de grande envergure, les études montrent un nombre plus élevé de diffusions piratées que légales (Forbes, 2015).

Lors de matchs de football de grande envergure, les records montrent un nombre plus élevé de diffusions piratées que légales.

Qui regarde du contenu piraté ?

De nombreuses études ont été menées sur les raisons pour lesquelles des personnes qui respectent normalement la loi regardent des vidéos piratées. Ces raisons comprennent l'argument financier, l'ignorance et la possibilité d'accéder au contenu sans restriction de date ou de durée de diffusion. Cependant, il va sans dire que quiconque disposant d'un accès à Internet peut visiter un site pirate ou utiliser un terminal parfaitement légal et diffuser toutes sortes de contenus de haute qualité à l'aide de modèles commerciaux conviviaux. En effet, la diffusion de contenu piraté via les boîtiers Kodi a été décrite comme le déploiement digital le plus réussi de l'histoire de la télévision britannique ! Les motivations diffèrent considérablement selon la population de spectateurs et, encore une fois, il est utile de comprendre ces motivations pour lutter contre le problème.

Dans son étude sur la consommation de contenu piraté, VFT a identifié différents types de personnages et leurs motivations, qui sont résumés ci-dessous.

a) L'« anarchiste du contenu » croit en un accès communautaire et sans entrave au contenu en ligne, et que les frais, quels qu'ils soient, sont inacceptables. Au fond, l'anarchiste du contenu ne croit pas que le piratage est illégal.

b) Le « Robin des Bois du contenu » est moins extrême dans ses opinions et n'exclut pas d'envisager des propositions alternatives légales. Les membres de ce groupe sont fidèles aux principes du partage de contenu et, à ce titre, sont investis dans le remplissage et la diffusion de fichiers.

c) L'« utilitariste » justifie ses actes par la croyance selon laquelle le contenu est de faible valeur. Il achète uniquement du contenu qui a une valeur durable et qui peut être regardé à plusieurs reprises. Il comprend que le piratage est illégal, mais continue tout de même.

d) Le spectateur « fainéant » est principalement influencé par les économies financières et la disponibilité des films et séries, et ignore souvent que le piratage est illégal. Dans son étude, VFT suggère que les pirates fainéants et utilitaires représentent jusqu'à 70 % de la communauté totale des spectateurs et, par conséquent, les efforts visant à éduquer, convertir ou pénaliser ces groupes auront le plus grand impact sur le piratage.

Pouvons-nous arrêter les pirates ?

Malheureusement, la réponse à cette question est, en bref : pas totalement. L'histoire du piratage montre que tant que du contenu sera créé, des pirates chercheront toujours à exploiter la relation entre l'offre et la demande. Cependant, tout n'est pas perdu. Les diverses initiatives relatives au piratage à travers le monde montrent clairement que si le problème est abordé de manière stratégique, il peut certainement être réduit. Chaque entreprise impliquée dans la chaîne de valeur, de la production à la distribution, en passant par les législateurs et les organismes de réglementation, a un rôle à jouer.

Les initiatives du côté de la demande

Fournir l'accès au contenu. Les données montrent que, de manière constante, les spectateurs de contenu piraté sont souvent les plus gros acheteurs de contenu légal. Ainsi, le fait d'offrir aux spectateurs du contenu qu'ils veulent regarder (avec une bonne expérience de streaming à un prix raisonnable) et la réduction du piratage sont fortement liés. Une nouvelle étude réalisée par le groupe Vocus en Nouvelle-Zélande a révélé que si 11 % des spectateurs obtenaient du contenu protégé par le droit d'auteur via des diffusions illégales, 55 % d'entre eux obtiendraient le même contenu via des services de streaming légaux s'ils étaient disponibles. Autre exemple : malgré l'adoption de lois strictes contre le piratage, la Suède n'a observé aucun changement. Le taux de piratage télévisuel a en fait augmenté après l'entrée en vigueur de la loi et n'a diminué que des années plus tard, après l'arrivée de Netflix sur le marché.

Malheureusement, les méandres juridiques et les coûts associés aux droits internationaux sont des sujets compliqués. Autant dire que l'accès universel au contenu n'est pas pour demain. Cela étant dit, jusqu'à relativement récemment, de nombreux services OTT (Over-The-Top) fournis par les diffuseurs ou les studios servaient de mécanismes de défense et n'étaient pas nécessairement considérés comme des générateurs de valeur significatifs. Ainsi, les ressources vidéo étaient soit cachées derrière des paywalls OTT coûteux, soit totalement indisponibles. Les temps ont changé et, avec le succès des acteurs internationaux de la SVOD, de nombreux titulaires de droits principaux investissent maintenant massivement dans leurs services en ligne. Le piratage devrait diminuer au fur et à mesure que ces services se déploient à l'échelle mondiale.

La sensibilisation. Pour ceux qui travaillent dans ce secteur, il est évident que le piratage est une activité criminelle, comme n'importe quel autre type de vol. Pour les personnes extérieures, ce n'est pas si simple à comprendre. 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. Malheureusement, l'impact de la sensibilisation du grand public au sujet du piratage a été limité jusqu'à présent, mais les efforts doivent se poursuivre pour rappeler à tous que le piratage est un crime et a un impact réel sur les revenus des professionnels du secteur. De même, la sensibilisation des annonceurs vis-à-vis de l'association des marques avec des sites pirates doit continuer.

L'aspect juridique. De nombreuses personnes interrogées ont souligné l'inefficacité des poursuites judiciaires comme moyen de réduire la demande. Outre les défis logistiques liés aux poursuites contre des milliers, voire des millions d'individus, des obstacles techniques considérables empêchent l'association des adresses IP, en particulier avec l'augmentation du nombre de sites d'hébergement de fichiers. De plus, avec des lois de protection des données de plus en plus établies, le précédent juridique refuse l'établissement d'un lien entre les adresses IP et les identités individuelles (le précédent juridique a refusé le lien entre les adresses IP et les auteurs d'infractions au droit d'auteur dans les États américains de Washington, de Floride et de Californie, et récemment à la cour d'appel du neuvième circuit des États-Unis). Plusieurs affaires novatrices sont en cours et pourraient fournir des mesures alternatives pour poursuivre les spectateurs qui consomment du contenu piraté de manière répétée, mais il serait peut-être plus judicieux de diriger les activités juridiques contre les acquéreurs et les propriétaires des sites pirates.

Les initiatives du côté de l'offre

Les données. Une exigence évidente est la nécessité d'établir une méthodologie standard pour mesurer l'ampleur et l'impact du piratage sur les marchés internationaux. Au cours du processus de recherche pour ce livre blanc, il est clairement apparu qu'une part importante de la confusion entourant le piratage réside dans la pléthore d'études disponibles. Cela ne permet aucune forme d'analyse continue ou contextuelle et crée de la confusion chez les gouvernements et les distributeurs lors de la hiérarchisation des activités. Cette situation pourrait facilement être corrigée par des organismes industriels, comme l'Alliance for Creativity and Entertainment (ACE), la MPAA ou des organismes régionaux comme l'EUIPO, qui joueraient un rôle de leader.

Aspect juridique et réglementaire. Contrairement au côté de la demande, d'excellentes initiatives sont prises dans ce domaine, tant au niveau national qu'international. Au niveau stratégique, divers organismes industriels comme l'ACE, ou des initiatives gouvernementales comme la FAPAV en Italie commencent à observer un effort commun visant à identifier et poursuivre les pirates vidéo et combler les failles législatives dans le monde entier. Ces efforts exigent une coordination et un accès aux données pertinentes.

Aspect technique et opérationnel. De la même manière que nous voulons faciliter l'accès des spectateurs à d'excellents divertissements par le biais de canaux légaux, nous voulons compliquer le travail des pirates. En pratique, dans le monde digital actuel, cela signifie que les entreprises examinent les opérations, identifient les faiblesses de leur flux de travail, de la production à la distribution, et appliquent les mesures appropriées. De nombreux titulaires de droits (au moins pour les droits liés au cinéma et aux retransmissions sportives payantes) prévoient déjà des normes opérationnelles minimales acceptables pour les tiers. Ces droits sont parfois associés à des obligations contractuelles. Toutefois, en raison des coûts et de la complexité en jeu, les titulaires de droits ne peuvent stipuler que le strict minimum en matière de protection. À titre d'exemple, les directives sur les meilleures pratiques de la MPAA pour la manipulation de contenu de valeur sont complètes, mais appliquées sur la base du volontariat. Aucune organisation ne peut résoudre à elle seule le problème du piratage et si la chaîne comprend des maillons faibles, le problème ne sera jamais résolu. L'adoption d'une approche à 360° en matière de piratage et la mise en œuvre des procédures pertinentes basées sur les rôles au sein du flux de travail contribueront grandement à la résolution du problème.

Aucune organisation ne peut résoudre à elle seule le problème du piratage et si la chaîne comprend des maillons faibles, le problème ne sera jamais résolu.

La coopération. Il est clair qu'une meilleure coopération est nécessaire pour fournir aux titulaires de droits, aux distributeurs et aux législateurs les connaissances et la coordination opérationnelle nécessaires pour lutter contre l'activité des pirates. Les écosystèmes de la télévision et du cinéma sont habitués à être en concurrence, mais l'impact potentiel du piratage est trop important pour qu'aucune coopération ne se mette en place. Cela doit avoir lieu à tous les niveaux du secteur et à toutes les étapes du processus, de la production à la sécurité du contenu sur site, jusqu'à la transmission. Plus le nombre d'entreprises et d'organisations impliquées sera important, plus la solution globale sera efficace. Malheureusement, l'inverse est également vrai. S'il y a des points faibles, ceux-ci peuvent être exploités.

Une approche à 360°

Après avoir passé en revue les moyens par lesquels les différents groupes de pirates acquièrent et distribuent les vidéos, nous avons mis en place un cadre permettant aux clients d'examiner de manière stratégique leur écosystème des menaces et d'évaluer les solutions techniques pertinentes. Chez Akamai, nous développons des services pour former une stratégie antipiratage englobant trois aspects essentiels : protéger, détecter et appliquer. Ces mesures peuvent à leur tour être combinées à d'autres activités pour former un cadre efficace de lutte contre le piratage.

Protéger

1. Se protéger contre le credential stuffing. Comme décrit précédemment dans ce document, le credential stuffing est un vecteur d'attaque populaire utilisé par les pirates pour acquérir des informations sur le spectateur. Le principal moyen pour les pirates d'exécuter une attaque de credential stuffing est d'utiliser des bots automatisés sur les pages de connexion. Akamai a travaillé avec des sociétés de médias, petites et grandes, pour relever ce défi, et ce travail a donné lieu à de nombreuses meilleures pratiques. Voici nos principales recommandations :

a) Codez les pages de connexion/API avec OWASP. Écrivez un code sécurisé en suivant les meilleures pratiques OWASP et effectuez un test de pénétration sur vos points de terminaison de connexion.

b) 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.

c) Utilisez une solution de gestion des bots. Cela peut vous aider à prévenir les attaques sophistiquées de vol d'identifiant en vérifiant le comportement de l'utilisateur et la télémétrie du terminal.

2. Se protéger contre le vol depuis des systèmes. Le vol depuis des systèmes de production internes, du stockage digital ou du cloud public est rarement rapporté par le secteur, mais, comme nous l'avons identifié, il s'agit d'une source importante de contenu piraté. De manière générale, nous observons plusieurs formes de vol de ressources vidéo :

a) Le piratage direct ou les attaques de type MitM par des pirates

b) Le vol par des employés ou des travailleurs indépendants

c) L'enregistrement d'un ID système unique comme des mots de passe

Les entreprises impliquées dans le flux de production et de prédistribution peuvent utiliser différentes technologies pour minimiser les risques, mais elles tournent essentiellement autour du concept de Zero Trust. Dans un secteur qui fonctionne depuis longtemps avec des niveaux de confiance élevés au sein de son écosystème, cela peut sembler draconien. La réalité, cependant, est que dans un monde digital, les normes et les sanctions qui soudaient la communauté des médias n'existent plus.

Zero Trust est un cadre que les entreprises utilisent pour transformer leurs systèmes informatiques et de production multimédia de base et remplacer les systèmes de sécurité basés sur le périmètre plus traditionnels. Il est construit autour de l'idée que plus rien ni personne n'est digne de confiance sur aucun réseau interne. Les principaux composants de la structure Zero Trust 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 strict basée 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 et autorisés puissent accéder aux applications et aux données. En même temps, il protège ces applications et ces utilisateurs contre les menaces avancées sur Internet.

Plusieurs composants peuvent être utilisés par les entreprises pour mettre en œuvre un cadre Zero Trust, mais la sécurisation de l'accès des employés/travailleurs indépendants aux applications de production et aux systèmes de stockage multimédia de base est un aspect essentiel. Avec une telle 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 l'utilisation de services comme Enterprise Application Access d'Akamai, les autorisations utilisateur peuvent être accordées facilement et rapidement pour des applications spécifiques en fonction de l'identité et du contexte de sécurité de l'utilisateur, ainsi que du terminal, sans jamais accorder aux utilisateurs l'accès à l'ensemble du réseau de l'entreprise.

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.

Se protéger contre les violations liées à la zone géographique et aux droits de propriété intellectuelle. Un autre moyen pour les pirates d'acquérir du contenu est l'utilisation de la technologie VPN pour masquer leur pays d'origine et leur adresse IP. Cette méthode est généralement utilisée après l'acquisition réussie des informations d'un abonné légitime. Une fois les informations acquises, les pirates brouillent ensuite leur emplacement géographique et leurs adresses IP afin de diffuser du contenu vers plusieurs emplacements, un processus appelé re-streaming. L'omniprésence des services VPN signifie également que les pirates de type fainéant peuvent facilement s'inscrire et accéder à du contenu restreint sur le plan géographique, par exemple, des spectateurs à l'étranger qui cherchent à accéder à des épisodes de séries particuliers. Les mécanismes qui peuvent être utilisés pour se protéger contre cette activité incluent la technologie de détection de proxy. La détection de proxy améliorée d'Akamai bloque intelligemment les requêtes à la périphérie associées à des services proxy ou VPN anonymes.

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 sécurisation de l'accès des employés/ travailleurs indépendants aux applications de production et aux systèmes de stockage multimédia de base est un élément clé.

En résumé, la GND fait référence aux outils, normes et systèmes utilisés pour restreindre l'accès aux contenus digitaux 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, empêcher les spectateurs de faire des copies de vidéos 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 encore une « clé » offrant une protection superficielle. Cependant, les clés sont généralement fournies par des serveurs HTTP et peuvent être copiées et partagées. Par conséquent, le chiffrement n'est parfois pas suffisant pour protéger le contenu à plus haute valeur ajoutée. 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 offrent également la possibilité d'ajouter des règles métier qui définissent quand et comment les clés peuvent être utilisées sur différents terminaux, notamment l'emplacement, l'enregistrement des terminaux et les règles temporelles. Comme toutes les technologies, cependant, la technologie GND s'accompagne de défis.

a) Le premier est la complexité. Sans donner trop de détails, les entreprises qui souhaitent mettre en œuvre une stratégie de GND complète doivent prendre en charge plusieurs technologies, notamment Apple FairPlay, Google Widevine et Microsoft PlayReady. Cela permet de couvrir correctement les navigateurs, terminaux et systèmes d'exploitation potentiels disponibles sur le marché. Cela ajoute des frais et de la complexité au flux de travail. Notez que, grâce à une spécification appelée format CMAF (Common Media Application Format), le marché de la GND s'oriente vers un ensemble unique de fichiers chiffrés pouvant prendre en charge les trois technologies, mais à ce jour, il ne prend pas en charge les anciens terminaux.

b) Le deuxième défi est la dépendance à l'égard de systèmes tiers pour que la GND fonctionne. Si ces systèmes sont piratés ou victimes d'une attaque DoS, l'expérience du spectateur est compromise.

c) Le dernier point souvent cité par les opposants à la GND est la faillibilité de la technologie. La GND est incapable de protéger le contenu une fois qu'il a été déchiffré, par exemple, lors de l'enregistrement d'un écran. Certains spécialistes ont même décrypté diverses technologies GND pour en repérer les faiblesses. Lorsque vous rivalisez avec des pirates acharnés et plus que compétents sur le plan technique, cela n'a rien d'étonnant, mais ce n'est pas une raison pour exclure la GND de votre stratégie.

Beaucoup de titulaires de droits, surtout liés aux événements sportifs et aux films de grande valeur, exigent des distributeurs qu'ils mettent en œuvre une certaine forme de protection par GND. Les spécifications peuvent aller de simples directives générales à de très strictes exigences. 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 la technologie de GND en temps quasi réel. Les entreprises commencent également à étudier les avantages de l'association du chiffrement et du tatouage numérique comme alternative à la GND. Cette méthodologie offre des avantages considérables en ce qui concerne les coûts de traitement et l'expérience du spectateur, mais fournit néanmoins une solide protection liée à la lecture.

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. 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. Une empreinte ne permet pas de distinguer différentes copies du même titre, c'est-à-dire quelle copie d'une vidéo a été divulguée en premier lieu. Ainsi, la technologie est généralement utilisée par des services comme l'outil Content ID de YouTube, pour aider à déterminer le moment où du contenu protégé par le droit d'auteur est mis en ligne par des comptes qui ne disposent pas des droits pour le redistribuer. Les empreintes sont également utilisées pour aider les organisations à comprendre la fréquence du piratage de leur propre contenu, avant qu'une stratégie plus robuste ne soit mise en place.

Le tatouage numérique. Il s'agit aujourd'hui de l'une des formes les plus répandues de détection de piratage. Bien que le tatouage numérique ne puisse pas directement arrêter le piratage, il permet aux fournisseurs de services de le détecter, d'identifier ceux qui en sont responsables et de prendre des mesures en conséquence. Fondamentalement, le tatouage numérique de vidéo consiste à ajouter un motif de « bits » invisible à l'œil nu et impossible à supprimer, dans un fichier vidéo que vous souhaitez authentifier. Lier ces données à l'identité du spectateur signifie qu'il est possible de retrouver un pirate qui copie le contenu après qu'il a été déchiffré et distribué illégalement.

Trois méthodes principales de tatouage numérique de vidéo sont utilisées à l'heure actuelle : la modification « Bitstream », la variante A/B et le tatouage numérique côté client.

> ***La modification Bitstream*** 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.
>
> ***Le tatouage numérique de la variante A/B*** est destiné au secteur OTT. Deux diffusions vidéo identiques sont créées, marquées par un tatouage numérique, puis 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, mais 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.

Le tatouage numérique côté client est privilégié pour son extraction rapide des tatouages numériques et sa capacité à se déployer sur les anciennes plateformes comme les décodeurs. Une superposition graphique est composée sur le flux vidéo du terminal client et peut être rendue invisible. Le tatouage numérique n'est pas appliqué avant qu'il n'arrive dans les mains du client. Par conséquent, le contenu doit être protégé séparément lors de la livraison. De plus, les distributeurs doivent envisager de déployer des kits de développement logiciel (SDK) pour les terminaux OTT, ce qui peut ajouter des frais de fonctionnement.

De nombreuses formes de tatouages numériques sont disponibles en fonction des cas d'utilisation. Cependant, pour toute stratégie de tatouage numérique, il est capital de s'assurer que la surveillance adaptée est mise en place afin que des techniques d'application adéquates puissent être appliquées aux pirates. De nombreux fournisseurs de technologies de lutte contre le piratage fournissent des services de surveillance gérés. Il est aussi possible de demander conseil à des consultants en lutte contre le piratage comme Cartesian afin de développer des capacités internes plus facilement.

Akamai collabore avec les principaux 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 les journaux des partenaires de distribution, comme les CDN en temps réel, qui peuvent identifier les activités de piratage pour les diffusions live. Dans ce cas, l'inspection approfondie des journaux fournit une image en temps réel de l'activité illégale basée sur les adresses IP autorisées et non autorisées. L'avantage de ce type de solutions, comme Stream Protector d'Akamai, réside dans la capacité à activer la fonctionnalité rapidement en fonction de la situation et à appliquer des règles spécifiques. Par exemple, un diffuseur peut avoir acquis de précieux droits sportifs pendant une période limitée, mais ne veut pas investir dans la technologie du tatouage numérique. Ainsi, il peut utiliser l'identification du journal de diffusion pour fournir un niveau de détection similaire sans le flux de travail initial ou les coûts technologiques. L'inconvénient de cette technologie est qu'elle ne peut être utilisée qu'avec un seul partenaire de distribution, ce qui pose problème dans un environnement multi-CDN.

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.

S'assurer que la surveillance est adéquate afin que des techniques d'application appropriées puissent être mises en œuvre à l'encontre des pirates.

La révocation de l'accès. Si vos contenus vidéo sont temporaires, comme c'est le cas des événements sportifs et d'autres événements live, vous devrez révoquer l'accès de l'auteur de la diffusion illégale immédiatement ou dès que possible. 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. Si des procédures opérationnelles claires sont mises en place, cela peut se produire dans un délai raisonnable. Toutefois, il existe de nombreuses situations dans lesquelles le temps est essentiel, comme les événements sportifs de grande valeur, ou lorsque la distribution de contenu piraté peut devenir virale. 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 remplaçant les diffusions légales 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 live piratées sur les plateformes de réseaux sociaux et peuvent envoyer directement des messages à l'auteur de l'infraction. Grâce à cette forme d'application, les distributeurs peuvent graduer leur réponse, par exemple en commençant par offrir l'accès à des diffusions légitimes et, si l'infraction continue, en envoyant des avis juridiques.

Pour faciliter l'éducation générale sur le sujet, des plateformes de messagerie en temps réel de plus en plus sophistiquées pouvant cibler les contrevenants voient le jour. Avec les services de lutte contre le piratage appropriés, les opérateurs peuvent identifier les spectateurs qui regardent les diffusions illégales et les inciter, par des contre-mesures souples et strictes, à passer à des services légaux. Les actions peuvent inclure d'expliquer l'impact de leurs actions et de proposer des incitations commerciales pour accéder à des diffusions légales, ou des contre-mesures plus dures impliquant l'intervention des forces de l'ordre. Ici, la clé est de supprimer l'anonymat du processus et d'éduquer activement le spectateur.

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 profondément ébranler ou influencer les modèles de licence du monde entier.

Jusqu'à présent, la réponse du secteur de médias était relativement discrète, le fardeau de la lutte contre les pirates étant fragmenté entre différents diffuseurs, opérateurs de chaînes de télévision payantes et organismes de l'industrie. 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. Comme décrit dans le présent document, cependant, sans une forme d'omniprésence opérationnelle et de coordination dans l'ensemble du secteur, associée à un soutien des gouvernements, des régulateurs et des législateurs, le combat sera difficile. Comme pour n'importe quel combat, un maillon faible suffit pour réduire à néant les efforts de tout un groupe.

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 qui permettront d'aider les cadres et l'ensemble du secteur à comprendre la menace, de l'éducation continue du grand public sur l'impact plus large du piratage sur l'emploi et sur la menace pour les industries nationales, de la coopération entre les fournisseurs de services de lutte contre le piratage pour garantir l'intégration efficace des solutions techniques et, enfin, du leadership des titulaires de droits de tous les genres pour favoriser l'omniprésence dans l'industrie lors de la gestion et de la distribution des droits.

La bonne nouvelle, c'est qu'une grande partie de ces éléments commence à être mis en place. L'EUIPO, par exemple, fournit des points de données clairs sur l'étendue et l'impact du piratage dans l'Union européenne, en utilisant une méthodologie qui pourrait être adoptée par d'autres régions. Les gouvernements nationaux doivent encore prendre conscience du problème, mais grâce aux informations plus claires disponibles sur l'impact du piratage, nous pouvons espérer voir la mise en œuvre d'une législation plus stricte. Les fournisseurs étudient les avantages de la mutualisation de leurs capacités. Par exemple, Akamai, en plus de mettre à profit son expertise en matière de cybersécurité, 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 relatifs à des contenus de valeur 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 souvent des cas isolés ou des « suggestions » (comme c'est le cas avec la MPAA), mais nous pensons qu'à l'avenir, cela sera 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 opportunités d'emploi et à garantir la prospérité des licences sur le marché mondial.

Akamai collabore avec toutes les principales sociétés de tatouage numérique afin de s'assurer qu'une fois les pirates détectés, leurs activités peuvent être stoppées immédiatement.

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-hit-52bn/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. Article on the use of streaming services (Article sur l'utilisation des services de streaming). 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

Techspot. Streaming services are killing piracy (Les services de streaming tuent le piratage). Analyse de la recherche du groupe Vocus. 2019. Extrait de https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html

TorrentFreak. Making Money from Movie Streaming Sites, an Insiders Story (Gagner de l'argent avec les sites de streaming de films, une histoire d'initiés). 2013. Extrait de https://torrentfreak.com/making-money-from-movie-streaming-sites-an-insiders-story-131019/

VFT. Pirate Persona Whitepaper (Livre blanc sur les types de pirates). 2014.

Walters, B. Interview with Helen Mirren (Entretien avec Helen Mirren). Time Out London. Extrait de http://www.timeout.com/london/film/interview-with-helen-mirren