

Protegendo o "Banco de OTT"



Introdução

A pirataria de vídeo não é um problema novo. Desde o início da produção profissional de filmes, há pessoas dispostas a ganhar dinheiro rápido explorando “a propriedade privada na forma de violação de direitos autorais”. Durante o período do cinema mudo, era comum que os rolos de filme exibidos em um cinema fossem levados e exibidos ilegalmente em outras salas. Essa prática se tornou tão popular que Hollywood mandava agentes para pegar donos de cinemas inescrupulosos no ato. Mas o “compartilhamento” pela Internet tornou a distribuição digital, de longe, a maneira mais fácil e eficaz de distribuir milhares de cópias de vídeo piratas para milhões de espectadores instantaneamente.

Os piratas de hoje usam agora uma gama de vetores de ataque para recuperar e distribuir conteúdo. As táticas comuns incluem credential stuffing (para capturar detalhes do visualizador e sequestrar contas legítimas) ou re-streaming de canais lineares com uma experiência indistinguível da TV. As empresas piratas até oferecem uma fácil experiência de usuário (UX), atendimento ao cliente e uma variedade de modelos flexíveis de negócios.

Com esse cenário em mente, exploraremos o desafio da pirataria e veremos como podemos combatê-la por meio de uma estrutura estratégica.

Estima-se que 13,7 milhões de pessoas em todos os países da UE acessem regularmente serviços ilegais piratas (de acordo com o EUIPO 2019), sendo que Reino Unido (2,4 mi) e França (2,3 mi) representam as maiores populações infratoras. As receitas anuais geradas por piratas na UE são estimadas em 1 bilhão de euros (EUIPO 2019). Na América do Norte, estima-se que mais de 12,5 milhões de residências dos EUA acessem vídeos piratas (Parks Associates 2019), mas na região Ásia-Pacífico, o problema pode ser muito mais predominante. Em Hong Kong, por exemplo, um estudo da AVIA de 2019 mostrou que 24% dos consumidores usam dispositivos de streaming da Internet para acessar canais pirateados. Esse valor aumentou para 28% dos consumidores nas Filipinas, 34% em Taiwan e 45% na Tailândia. Portanto, apesar dos esforços de todo o setor, podemos ver que a pirataria de vídeo ainda é um problema sério em todo o mundo. O impacto pode ser sentido em todo o setor, causando perdas financeiras e perda de postos de trabalho e, além disso, estamos começando a ver sinais de que isso afeta o licenciamento.

Os valores absolutos são difíceis de estabelecer devido à complexidade do assunto, mas num relatório encomendado pela Câmara de comércio dos EUA, estima-se que as perdas financeiras se situem entre 40 e 97,1 bilhões de dólares para a indústria cinematográfica e entre 39,3 e 95,4 bilhões de dólares para a indústria televisiva (NERA Consulting 2019). Isso exclui a perda de receita para os governos por meio da tributação.

As indústrias de TV e cinema sustentam milhões de empregos, de cenógrafos, maquiadores e músicos a produtores e diretores, e a pirataria está colocando esses empregos em risco. Em seu relatório de 2019 sobre o impacto da pirataria digital na economia dos EUA, Blackburn, Eisenach e Harrison estimaram que entre 230.000 e 560.000 empregos foram perdidos nos Estados Unidos naquele ano como resultado direto da atividade de pirataria.

Protegendo o “Banco de OTT”

**US\$ 40 -
US\$ 97,1 bilhões**

Perdas estimadas da indústria cinematográfica devido a vídeos pirateados

**US\$ 39,3 -
US\$ 95,4 bilhões**

Perdas estimadas da indústria da TV devido a vídeos pirateados

Além disso, começaram a surgir sinais de que a pirataria está afetando o licenciamento, que é a força vital da indústria criativa e, possivelmente, um problema estratégico ainda mais delicado. Simplificando, por que distribuidores em potencial pagariam quantias significativas de dinheiro por direitos quando o conteúdo é facilmente encontrado de graça em websites piratas? Yousef Al-Obaidly, presidente-executivo da beIN, um dos maiores compradores de direitos esportivos do mundo, afirmou que “a bolha dos direitos esportivos está prestes a estourar por causa da pirataria global e o modelo de negócios terá que ser revisado”. Ele estava sinalizando que o valor dos direitos para sua organização será baseado no nível de exclusividade. O produtor Jason Blum, indicado ao Oscar e ganhador do Emmy, também descreveu como a pirataria está tendo um impacto direto nos investimentos disponibilizados para filmes inovadores de vanguarda. Ele sugere que, em algum momento em um futuro não muito distante, os números se tornarão insustentáveis e os estúdios precisarão reduzir suas fichas.

Como funciona a indústria da pirataria?

Como em qualquer batalha, é importante entender seus adversários, para que você possa compreender suas motivações, táticas, pontos fortes e fracos. Naturalmente, é difícil enxergar o que está acontecendo, mas já sabemos que há uma rede complexa de grupos e subgrupos, cada um com seus próprios motivos e níveis de sofisticação, conforme resumido abaixo.



Os grupos de lançamento

Os membros se veem como revolucionários na luta contra as grandes corporações. A associação a websites de upload é conquistada por aqueles que são dignos e confiáveis. Diferentes grupos e indivíduos se especializam em determinados gêneros e competem para adquirir um novo material, que é então recompensado com reconhecimento. A FACT descreve a estrutura como “grupos complexos, sofisticados e bem organizados do tipo hacker, suspeitos de estarem envolvidos em outros tipos de cibercrime”.



Há uma rede complexa de grupos e subgrupos piratas, cada um com seus próprios motivos e níveis de sofisticação.



Os operadores do website

Eles gerenciam websites de vídeo pirata, incluindo websites de torrent, como o Pirate Bay, ou de streaming, como o TeaTV. Não se sabe se os grupos de liberação e os operadores do website são os mesmos indivíduos, mas muitos estudos argumentaram que há uma sobreposição significativa entre os dois. Os operadores certamente lucram com o processo e muitas vezes executam vários websites “espelhos” de modo que, se um é derrubado pelas autoridades, eles ainda podem ficar on-line e ganhar dinheiro.



Os atacadistas de dispositivos de streaming da Internet

O crescimento desses dispositivos, em particular o Kodi, fornece um fluxo de receita relativamente estável e previsível para criminosos oportunistas. Os atacadistas importam as caixas através de canais inteiramente legais ou redes criminosas e as modificam com software ilegal, que pode a partir daí ser vendido on-line.



Os piratas sociais

Usando muitas vezes as redes sociais para distribuir conteúdo, as pessoas desse grupo são menos conscientes ou ambivalentes quanto ao fato de que a pirataria é ilegal e estão respondendo ao custo de certos gêneros de conteúdo ou à fadiga de assinaturas.

Como os piratas adquirem conteúdo?

Existem muitos métodos viáveis para piratas roubarem conteúdo devido à variedade de pontos fracos na cadeia de valor que podem ser explorados. Podemos agrupar os métodos mais predominantes com base no caso de uso.



Difusão simultânea de canais de TV e eventos ao vivo

Uma das formas de pirataria que mais cresce é a captação e redistribuição de canais de TV ou eventos ao vivo. Isso é obtido por meio de:

- Adulteração do software de reprodução de vídeo ou do sistema operacional Android
- Gravação de telas durante a reprodução usando um dispositivo móvel
- Interceptação de vídeo descryptografado usando strippers HDCP conectados a decodificadores
- Ataques de credential stuffing para acessar e usar detalhes legítimos do espectador
- Transporte de vídeo para fora de um determinado mercado usando uma VPN



Conteúdo sob demanda

Pré-lançamento de programas de TV e filmes para grupos de lançamento. A estrutura do setor de mídia apresenta uma variedade de oportunidades com muitas organizações e indivíduos diferentes envolvidos no processo de produção. Os métodos comuns usados para adquirir vídeo incluem:

- Violações de data center, que resultam no roubo de credenciais do usuário, chaves criptográficas ou conteúdo de vídeo
- Roubo de ID de usuário, fornecendo acesso ao conteúdo de vídeo por meio de vários sistemas de produção
- Gravação de conteúdo físico (menos predominante agora) para compartilhamento e distribuição
- Hackers de sistema contra vários sistemas de produção, fornecendo acesso direto aos vídeos
- Extração de conteúdo de fontes legítimas, por exemplo, iTunes
- Sistemas de filmagem de cinema
- Roubo direto usando ataques man-in-the-middle

Como eles distribuem conteúdo?

Os piratas usam todos os canais possíveis e inovações técnicas disponíveis para distribuir seu conteúdo, incluindo:

- Decodificadores de IP personalizados que acessam streams de TV pré-programados
- Software executado em dispositivos de streaming e PCs que permitem a distribuição pirata, como o Kodi
- Apps que são carregados em dispositivos populares de streaming de varejo
- Websites e serviços de redes sociais que hospedam conteúdo criado pelo usuário, como o YouTube
- Websites que transmitem conteúdo pirata por meio de links encontrados através de pesquisa ou mídia social
- Os sempre presentes websites de download, hospedagem de arquivos, cyberlocker e torrent

Embora as estratégias de distribuição dos vários tipos de piratas sejam menos compreendidas, podemos ver que os grupos de lançamento possivelmente favorecem os modelos de compartilhamento de conteúdo (ex.: ciberlockers e websites de torrent), devido ao suporte inerente à ubiquidade e ao altruísmo. Em contraste, os operadores de websites têm motivação financeira para realizar uma estratégia de DSL/streaming que emule serviços legítimos e sua capacidade de incentivar vários modelos de receita.

A demanda

Há muitas razões que levam as pessoas a procurar websites piratas. Elas incluem justificativas financeiras, ignorância em relação ao impacto mais amplo causado e a capacidade básica de acessar conteúdo sem restrições de janelas. Há vários tipos diferentes de pessoas descritos pela VFT Solutions Inc. em seu relatório de 2019 sobre espectadores piratas, que são resumidos aqui:

- O **“anarquista de conteúdo”** acredita no acesso comunitário e irrestrito ao conteúdo on-line. Qualquer encargo por conteúdo é demais e eles não acreditam que a pirataria seja imoral ou ilegal.
- O **“Robin Hood de conteúdo”** é menos extremo em seus pontos de vista e aberto para considerar propostas alternativas. Esse tipo não é um usuário de serviços de transmissão ao vivo, mas está incumbido em disseminar arquivos de torrent compartilhados.
- O **“utilitário”** justifica suas ações argumentando que o consumo generalizado de conteúdo ultrapassa os danos ou prejuízos aos titulares dos direitos, uma vez que a maior parte do conteúdo é de valor fugaz.
- O **“pirata preguiçoso”** muitas vezes não tem consciência ou professa a ignorância ao fato de que a pirataria é ilegal. Eles são influenciados pela economia de custos e pela ampla disponibilidade, juntamente com a facilidade de acesso.

A VFT estimou que os tipos de piratas preguiçoso e utilitário representam até 70% da comunidade total, e os esforços para educar, converter ou penalizar esses grupos terão maior impacto sobre a pirataria.

É possível deter a pirataria?

Infelizmente, a resposta imediata é: não integralmente. A história nos diz que sempre haverá piratas procurando explorar o conteúdo, seja por razões altruístas ou comerciais. No entanto, nem tudo está perdido. Se o problema for abordado estrategicamente em toda a cadeia de valor, ele poderá ser minimizado. Em termos práticos, a melhoria da cooperação em todo o setor, nas áreas estratégicas identificadas abaixo, terá um impacto duradouro.

Dados

Um requisito evidente é uma metodologia padrão para medir a extensão e o impacto da pirataria globalmente. Metodologias e técnicas diferentes não permitem análises contínuas ou contextuais e se confundem ao priorizar atividades ou ao tentar entender o retorno de iniciativas antipirataria. Isso pode ser corrigido por meio dos órgãos do setor, como a Alliance for Creativity and Entertainment (ACE), ao assumirem um papel de liderança na coleta de dados.

Educação

A pirataria para a população em geral se tornou algo que “todo mundo” faz e, portanto, não parece mais ilegal porque o comportamento é normalizado. Os esforços para educar o público devem continuar para alertar as pessoas de que a pirataria é um crime e tem um impacto real sobre os meios de subsistência.

Jurídico e regulamentar

Existem várias iniciativas excelentes lideradas por órgãos do setor ou iniciativas governamentais, como as da FAPAV, na Itália, que processa judicialmente os piratas de vídeo e reduz as lacunas legislativas em todo o mundo. Esses esforços exigem coordenação e acesso a dados relevantes.

Técnico e operacional

Acabou o tempo em que se deixava conteúdo desprotegido. Na prática, significa uma análise estratégica das operações para detectar elos frágeis na cadeia técnica de valores, da produção à distribuição, e a aplicação das medidas cabíveis. Descrevemos isso como uma postura de 360 graus.



Se o problema for abordado estrategicamente em toda a cadeia de valor, ele poderá ser minimizado.

A postura de 360 graus

Após analisar os meios pelos quais os grupos piratas adquirem e distribuem vídeos, criamos uma estrutura baseada em três princípios fundamentais: Proteger, Detectar e Aplicar. Usando essa estrutura, as organizações podem analisar estrategicamente o cenário de ameaças com base em sua função no setor e implementar iniciativas operacionais e técnicas relevantes para minimizar o impacto.

Proteger



Proteger-se contra credential stuffing

Como descrito anteriormente, credential stuffing é um vetor de ataque popular usado por piratas para adquirir detalhes do visualizador, geralmente por meio de bots automatizados. Aqui estão nossas principais recomendações:

- Codifique páginas de login/API com OWASP. Escreva um código seguro de acordo com as práticas recomendadas do OWASP e faça testes regulares de penetração nos seus pontos de extremidade de login.
- Use proteção anti-DDoS. Isso pode ajudar a evitar que botnets volumétricos atinjam sua infraestrutura e sobrecarregem seus ativos.
- Utilize uma solução de gerenciamento de bots, como o Bot Manager Premier da Akamai, que pode ajudá-lo a evitar ataques sofisticados de abuso de credenciais, verificando o comportamento do usuário e a telemetria do dispositivo.



Proteger-se contra roubo de sistemas

O roubo de sistemas internos de produção, armazenamento digital ou nuvem pública é uma fonte importante de material pirateado. Em termos gerais, vemos várias formas de roubo de ativos de vídeo:

- Hacking direto ou ataques man-in-the-middle por piratas.
- Captura de identidades exclusivas do sistema, como senhas.
- Roubo por funcionários ou freelancers.

Existem várias tecnologias que as empresas podem empregar para minimizar o risco; essencialmente, elas giram em torno do conceito de Zero Trust, uma estrutura que as empresas usam para transformar o acesso à tecnologia. Os componentes centrais da estrutura incluem: acesso seguro aos recursos, independentemente da localização ou do modelo de hospedagem, aplicando uma estratégia de controle de acesso baseada em privilégios mínimos, e inspecionando e registrando todo o tráfego de atividades suspeitas. A estrutura estabelece que somente usuários e dispositivos autenticados podem acessar aplicações e dados. Ela também protege aplicativos e usuários contra ameaças avançadas na Internet.

Há vários componentes que as empresas podem usar para implementar uma estrutura Zero Trust, mas restringir o acesso de funcionários/freelancer a sistemas essenciais de produção e armazenamento é uma faceta importante. Com uma equipe de trabalho transitória, as empresas de mídia enfrentam desafios únicos na implementação e revogação do acesso aos sistemas, às vezes diariamente. Usando serviços como o Enterprise Application Access da Akamai, as permissões para aplicações específicas podem ser concedidas rapidamente com base na identidade e no contexto de segurança do usuário e do dispositivo, sem conceder aos usuários acesso à rede corporativa onde a exfiltração de vídeo pode ocorrer.

Outra faceta importante do Zero Trust é a implementação de sistemas que identificam e bloqueiam proativamente ameaças direcionadas, como malware, ransomware e phishing, que são ferramentas usadas por piratas em seus ataques man-in-the-middle. O Enterprise Threat Protector da Akamai, por exemplo, é um gateway seguro da Web que usa inteligência de segurança em tempo real para identificar e bloquear proativamente ameaças direcionadas, como malware, ransomware, phishing e exfiltração de dados baseada em DNS.


Proteja-se contra violações geográficas e de direitos de IP. Os piratas costumam usar a tecnologia VPN para mascarar seu país de origem e endereço IP após a aquisição bem-sucedida dos detalhes de um assinante legítimo para retransmitir conteúdo. A tecnologia de detecção de proxy, como a Enhanced Proxy Detection da Akamai, bloqueia de forma inteligente as solicitações em edge associadas a serviços anônimos de proxy ou VPN, impedindo tais casos de uso.

Proteja-se contra violações de reprodução. Esta é, de longe, a tática mais popular na luta contra a pirataria e pode ser obtida através de uma variedade de meios diferentes, sendo o mais prevalente a gestão dos direitos digitais (Digital Rights Management, DRM). A DRM refere-se às ferramentas, padrões e sistemas usados para restringir materiais protegidos por direitos autorais e impedir a distribuição não autorizada. Não se trata de uma tecnologia única.

Dependendo da criticidade dos ativos protegidos, alguns distribuidores se sentem confortáveis com a criptografia simples (ou seja, gravando o conteúdo em um código que só pode ser lido por dispositivos ou software com a chave para desbloquear o código), pois isso ainda requer que uma chave esteja disponível fornecendo, portanto, proteção superficial, certamente contra piratas casuais. No entanto, as chaves são normalmente entregues por servidores HTTP e podem ser copiadas e compartilhadas, portanto, com frequência, isso não é suficiente para proteger conteúdo de valor mais alto.

Para reforçar a criptografia, as tecnologias DRM mais avançadas lidam com a comunicação principal por meio de um módulo de decodificação de conteúdo usando um sistema de desafio/resposta. Essas comunicações são criptografadas para que a chave de decodificação nunca esteja aberta onde possa ser hackeada. As tecnologias DRM avançadas também usam regras de negócios que definem quando e como as chaves podem ser usadas em diferentes dispositivos, como local ou regras baseadas em tempo.

Para os distribuidores que desejam implementar o DRM durante o processo de empacotamento, muitas vezes é útil se envolver com provedores na nuvem capazes de gerenciar a complexidade. A Akamai, por exemplo, integrou seu armazenamento de origem para conteúdo sob demanda com os recursos de processamento de vários provedores, como Bitmovin e Encoding.com, que podem implementar DRM quase em tempo real.



Com uma equipe de trabalho transitória, as empresas de mídia enfrentam desafios únicos na implementação e revogação do acesso aos sistemas, às vezes diariamente.

Protegendo o “Banco de OTT”

Detectar

Como em qualquer forma de roubo, a proteção nem sempre garante o sucesso e, como tal, a detecção de quaisquer violações é essencial. Existem vários métodos de detecção de atividade de pirataria quase em tempo real:



Impressão digital

Este método fornece a capacidade de identificar conteúdo de vídeo sem modificar a mídia original. As ferramentas são usadas para identificar, extrair e, em seguida, representar atributos pertencentes a um arquivo de vídeo, de modo que qualquer vídeo específico possa ser identificado por sua “impressão digital” exclusiva, por exemplo, em redes de compartilhamento de arquivos. A mídia original não precisa ser modificada de nenhuma forma, o que é uma vantagem, mas uma impressão digital não pode distinguir entre cópias diferentes do mesmo título; ou seja, qual cópia de um vídeo foi divulgada na primeira instância.



Marca d'água

Ela não pode impedir a pirataria, mas permite que os provedores de serviços detectem a pirataria, identifiquem aqueles que a praticam e façam algo a respeito. A marca d'água de vídeo consiste em adicionar um padrão de “bits” imperceptíveis e não removíveis em um arquivo de vídeo. Vincular esses dados à identidade do espectador significa que é possível rastrear um pirata que copia conteúdo depois que ele é descryptografado e o distribui ilegalmente. Existem três métodos principais de marca d'água em vídeo atualmente em uso:

- **Modificação de bitstream.** Ela envolve a modificação de áreas selecionadas de uma imagem de forma a manter a qualidade do vídeo, de forma que o espectador e a sessão sejam identificáveis. Como metodologia, ela é robusta, mas requer uma sobrecarga de computação significativa e adiciona latência ao sistema, tornando-o inadequado para conteúdo ao vivo.
- **Marca d'água do cliente.** Ela funciona bem para extração rápida de marca d'água e tem a capacidade de implantar em plataformas legadas, como decodificadores. Uma sobreposição gráfica é composta no stream de vídeo no dispositivo cliente, que pode ficar visível ou invisível. Como a marca d'água não é aplicada até atingir o dispositivo cliente, o fluxo de vídeo requer proteção extra. A tecnologia do cliente também requer a implantação de SDK, que pode ser complexa em ambientes OTT.
- **Marca d'água de variante A/B.** Voltado para o setor OTT, dois streams de vídeo idênticos são criados, com marca d'água e, subsequentemente, costurados ou entrelaçados juntos no lado do cliente ou através do processamento de edge de CDN para fornecer um identificador exclusivo. É um método robusto e econômico, mas, como a sequência de identificação pode ser longa, não é favorecido em situações que exigem extração rápida de marca d'água.

Um elemento-chave para qualquer estratégia de marca d'água é o monitoramento adequado para que as técnicas de fiscalização possam ser aplicadas aos piratas. Há serviços de monitoramento gerenciados disponíveis, ou pode-se buscar orientação para desenvolver recursos internos. A Akamai trabalha com todos os principais provedores de marca d'água para garantir que uma solução viável possa ser disponibilizada e integrada a uma estratégia geral de pirataria de vídeo.

Identificação do registro de stream

Outra forma de detecção é através de um exame em tempo real dos registros de entrega. Neste cenário, a inspeção de registros detalhados fornece uma imagem em tempo real da atividade de violação com base em endereços IP autorizados e não autorizados. A vantagem dessas soluções, como o Stream Protector da Akamai, é a capacidade de ativar e desativar a capacidade, dependendo da situação, o que é ideal para proteger direitos limitados pelo tempo, como esportes.

Aplicar

Quando a atividade de pirataria for detectada, é importante poder agir de maneira adequada. Dependendo da sua estratégia, isso pode levar a diversas ações.

- **Revogar acesso.** Se os seus recursos de vídeo forem sensíveis ao tempo, como ocorre com eventos esportivos, você desejará revogar o acesso ao originador da transmissão ilegal imediatamente. Existem diferentes formas de conseguir isso. Uma metodologia comum é trabalhar com seu provedor de serviços de distribuição, trocar detalhes relevantes e interromper a atividade de streaming de um endereço IP malicioso. No entanto, isso pode levar algum tempo. A Akamai fornece um serviço que permite a revogação de stream em tempo real e sem intervenção desnecessária. Isso se mostrou particularmente eficaz quando o monitoramento da pirataria está ocorrendo com marca d'água ou com identificação de registro de stream.
- **Modificação do stream.** Em situações menos urgentes, os distribuidores podem decidir modificar o stream pirateado substituindo-o por conteúdo alternativo (Big Buck Bunny é popular) ou reduzindo a qualidade do stream. Essa abordagem tem o benefício de ocultar a detecção pelos piratas, impedindo que saltem para uma fonte de stream diferente.
- **Mensagem em tempo real.** Conforme descrito na seção de tipos de pessoas, os piratas do tipo preguiçoso se sentem seguros com o anonimato da Internet. Organizações como a VFT podem identificar espectadores de transmissões pirateadas em plataformas de mídia social e enviar mensagens diretamente ao infrator. Usando essa forma de imposição, os distribuidores podem modificar o tipo de intervenção. Por exemplo, podem oferecer acesso a streams legítimos e, se a violação continuar, emitir advertências jurídicas.

Conclusão

A pirataria de vídeo via IP é um assunto complexo e com nuances, mas que tem o potencial de ameaçar a viabilidade a longo prazo do setor de mídia, como sabemos. Há evidências esmagadoras que apontam para danos financeiros significativos, mas o mais importante é que a pirataria tem o potencial de minar ou impactar fundamentalmente os modelos de licenciamento global.

Até o momento, a resposta do setor foi um silêncio relativo. Conforme descrito por um analista, "estamos no estágio de adoção inicial com muito trabalho à frente". Um número crescente de distribuidores despertou para a ameaça, e a maioria dos produtores e operadores de vídeo de "nível 1" já estabeleceu equipes dedicadas para entender melhor a pirataria, avaliar sua própria situação e implementar estratégias antipirataria relevantes.

Há vários requisitos imediatos identificados neste documento que são necessários para ajudar o setor a lutar nessa batalha. Isso inclui pontos de dados de pirataria consistentes, educação aprimorada e continuada do público em geral, melhor cooperação em todo o setor e, finalmente, liderança de proprietários de direitos em todos os gêneros para impulsionar a onipresença em todo o setor ao lidar com direitos e distribuí-los.

A boa notícia é que o setor está começando a se mobilizar. As pesquisas sobre esse assunto estão se tornando mais reconhecidas, leis mais rigorosas já começam a surgir e os fornecedores estão unindo suas capacidades para multiplicar seu potencial. Por exemplo, além de oferecer sua experiência em segurança cibernética, a Akamai está trabalhando com todas as empresas líderes de marcas d'água para garantir que, uma vez que os piratas sejam detectados, suas atividades possam ser encerradas imediatamente. Finalmente, já aparecem sinais de que os titulares dos direitos autorais estão reivindicando padrões mínimos de proteção ao conteúdo produzido ao longo da cadeia técnica. Por enquanto, são casos pontuais ou "sugestões" (como no caso da MPAA), mas, futuramente, essa função poderá se tornar imprescindível para se atuar no mercado.

Adotadas essas iniciativas, podemos minimizar o problema para reduzir o prejuízo, proteger empregos e manter o sucesso do licenciamento no mercado global.

REFERÊNCIAS

- Asia Video Industry Association. The Asia Video Industry Report. 2019.
- Bevir. Cost of online piracy to hit \$52bn. 2017. Retirado de <https://www.abc.org/publish/cost-of-online-piracy-to-hit52bn/2509.article>
- Blackburn et al. Impacts of Digital Video Piracy on the U.S. Economy. 2019.
- Coberly. Streaming services are 'killing' piracy. Retirado de <https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>
- CustosTech. The Economics of Digital Piracy. 2014.
- Daly. The pirates of the multiplex. Retirado de <https://www.vanityfair.com/news/2007/03/piratebay200703>
- Decary, Morselli, Langlois. A study of Social Organisation and Recognition Among Warez Hackers. 2012.
- Digital Citizens Alliance. Fishing in the piracy stream. Retirado de https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf
- EnigmaX. Interview with a Warez Scene Releaser. 2007. Retirado de <https://torrentfreak.com/interview-with-a-warez-scene-releaser/>
- European Commission. Estimating displacement rates of copyrighted content in the EU. MAIO DE 2015.
- Escritório de propriedade intelectual da União Europeia. Trends in Digital Copyright Infringement in the European Union. 2018.
- Escritório de propriedade intelectual da União Europeia. Illegal IPTV in the European Union. 2019.
- FACT. Cracking down on digital piracy. 2017.

Feldman. Quase cinco milhões de britânicos usam serviços de transmissão de TV pirateados. 2017. Retirado de <https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami>

FriendsMTS. Comparando tecnologias de marca d'água de assinantes para conteúdo premium de TV paga. 2019.

Frontier Economics. The economic impacts of counterfeiting and piracy. Relatório preparado para BASCAP e INTA. 2017.

Granados. Relatório: Millions Illegally Live-Streamed El Clásico. 2015. Retirado 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. 2015. <https://pitjournal.unc.edu/article/economics-video-piracy>

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

Escritório de Propriedade Intelectual. Online Copyright Infringement Tracker. 2018.

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

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

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

Kan. Pirating 'Game of Thrones'? Esse arquivo provavelmente é um malware. 2019. Retirado de <https://mashable.com/article/pirating-game-of-thrones-malware/?europa>

Lee, T. Texas-size sophistry. 2006. Retirado de <http://techliberation.com/2006/10/01/texas-size-sophistry/>

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners", uma versão resumida de "Internet piracy: the estimated impact on sales" em Handbook on the Digital Creative Economy, editado por Ruth Towse e Christian Handke, Edward Elgar. 2013.

Mick, J. Nearly half of Americans pirate casually, but pirates purchase more legal content. 21 de janeiro de 2013. Retirado 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. Novembro de 2018.

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

MUSO. Measuring ROI in content protection. 2020.

Nordic Content Protection Group. Relatório anual 2020.

Parks Associates. Pirataria de vídeo: Ecosystem, Risks, and Impact. 2019.

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

Sanchez, J., 03 de janeiro de 2012. How copyright industries con congress. Retirado de <http://www.cato.org/blog/how-copyright-industries-con-congress>

Sandvine. Video and Television Piracy. 2019.

Schonfeld. Pirate Bay makes \$4m a year. 2008. Retirado 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. 2017. Retirado de <https://www.independant.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html>



A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A Akamai Intelligent Edge Platform engloba tudo, desde a empresa até a nuvem, para que os clientes e suas empresas possam ser rápidos, inteligentes e estar protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a obter vantagem competitiva por meio de soluções ágeis que estendem o poder de suas arquiteturas multinuvm. A Akamai mantém as decisões, as aplicações e as experiências mais próximas dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções Edge Security, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeos da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante o ano todo. Para saber por que as principais marcas do mundo confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou [@Akamai](https://twitter.com/Akamai) no Twitter. Nossas informações de contato globais podem ser encontradas em www.akamai.com/locations. Publicado em 20/07.