WHITE PAPER

Protezione dei dati OTT

Introduzione

La pirateria video non è un problema nuovo. Fin dagli albori della produzione cinematografica professionale, c'è sempre stato chi ha cercato di fare soldi facili sfruttando "la proprietà privata attraverso la violazione del copyright". Ai tempi del cinema muto, il concetto di "proiezione prolungata" (protrazione della proiezione dei film nei cinema) divenne così diffuso che Hollywood dovette inviare dei "controllori" per cogliere sul fatto i proprietari dei cinema senza scrupoli. Ma la "condivisione" tramite Internet ha reso la distribuzione digitale il metodo di gran lunga più semplice ed efficace per la distribuzione immediata di migliaia di copie di video contraffatti a diversi milioni di spettatori.

Oggi utilizzano una serie di vettori di attacco per ottenere e distribuire i contenuti. Le comuni tattiche includono il credential stuffing (per acquisire i dati degli spettatori e violare account legittimi) o il ristreaming di canali lineari con un'experience assolutamente identica a quella televisiva. Le società dedite alla pirateria offrono ai propri clienti persino user experience semplificate, un servizio di assistenza e una gamma di modelli aziendali flessibili.

In tale contesto, andremo ad esaminare la sfide poste dalla pirateria, considerando i modi con cui è possibile difendersi tramite un sistema strategico.

Si stima che, nei vari paesi europei, 13,7 milioni di persone accedono regolarmente a servizi pirata illegali (dati dell'EUIPO 2019), con le popolazioni del Regno Unito (2,4 milioni) e della Francia (2,3 milioni) che violano maggiormente le regole. La stima dei ricavi annuali generati dai pirati informatici nell'Unione europea è pari a 1 miliardo di euro (EUIPO 2019). In Nord America, si stima che più di 12,5 milioni di famiglie statunitensi accedono da casa a video illegali (Parks Associates 2019), mentre nell'area Asia-Pacifico il problema è molto più diffuso. A Hong Kong, ad esempio, uno studio AVIA 2019 ha rivelato che il 24% dei consumatori utilizza dispositivi di streaming Internet per accedere a canali contraffatti. Tale cifra è salita al 28% dei consumatori nelle Filippine, al 34% in Taiwan e al 45% in Thailandia. Pertanto, nonostante gli sforzi compiuti all'interno del settore, si può notare come la pirateria video rappresenti ancora un problema serio a livello globale. L'impatto viene percepito in tutto il settore, comportando perdite finanziarie, licenziamenti e, ora, stiamo iniziando a notare un impatto anche sulle licenze.

40,0 - 97,1 miliardi di dollari

Perdite stimate per il settore cinematografico a causa dei video pirata

39,3 - 95,4 miliardi di dollari

Perdite stimate per il settore televisivo a causa dei video pirata

È difficile stabilire cifre assolute, data la complessità della materia, ma in un rapporto commissionato dalla Camera di Commercio degli Stati Uniti, le perdite finanziarie sono stimate tra i 40 e i 97,1 miliardi di dollari per il settore cinematografico e tra i 39,3 e i 95,4 miliardi di dollari per il settore televisivo (NERA Consulting 2019), escludendo da tutto ciò la perdita di ricavi per i governi attraverso le tasse.

I settori televisivo e cinematografico occupano milioni di posti di lavoro, da scenografi, truccatori e musicisti a produttori e registi, che la pirateria sta mettendo a rischio. Nel loro rapporto 2019 sull'impatto della pirateria digitale sull'economia degli Stati Uniti, Blackburn, Eisenach e Harrison hanno stimato che negli Stati Uniti si sono persi tra i 230.000 e i 560.000 posti di lavoro come conseguenza diretta della pirateria.

Inoltre, stiamo iniziando a vedere i primi segnali dell'impatto della pirateria sulle licenze, che sono la linfa vitale del settore creativo e, probabilmente, un problema strategicamente più dannoso. In poche parole, perché i potenziali distributori dovrebbero pagare ingenti somme di denaro per i diritti quando il contenuto è facilmente reperibile gratuitamente attraverso siti pirata? Yousef Al-Obaidly, amministratore delegato di beIN, uno dei maggiori acquirenti di diritti sportivi al mondo, ha affermato che "la bolla dei diritti sportivi sta per scoppiare a causa della pirateria globale e che il modello di business dovrà essere aggiornato". Ha segnalato che il valore dei diritti della propria organizzazione sarà basato sul livello di esclusività. Il produttore vincitore del premio Emmy, candidato all'Oscar, Jason Blum ha descritto come la pirateria stia influendo direttamente sui fondi messi a disposizione per film innovativi e ad alto rischio, suggerendo che, ad un certo punto in un futuro non troppo lontano, le cifre diventeranno insostenibili e le case cinematografiche dovranno effettuare tagli sulle proprie selezioni.

Come funziona il settore della pirateria?

Come in ogni battaglia, è importante capire i propri avversari per poter calcolare le loro motivazioni, le tattiche, i punti di forza e le debolezze. Anche se le informazioni sono comprensibilmente difficili da reperire, sappiamo che esiste una serie complessa di gruppi e sottogruppi, ciascuno con propri fattori trainanti e livelli di sofisticazione, come abbiamo riassunto qui di seguito.

I gruppi di distribuzione

I membri si considerano rivoluzionari impegnati nella lotta contro le grandi corporazioni. Solo chi è meritevole e fidato può diventare un membro dei siti in cui vengono caricati i contenuti. Diversi gruppi e individui si specializzano in determinati generi e competono per acquisire nuovi materiali, quindi vengono poi premiati con il meritato riconoscimento. FACT li descrive come "gruppi in stile hacker complessi, sofisticati e ben organizzati, sospettati di essere coinvolti in altri tipi di crimini informatici".

Esiste una serie complessa di gruppi e sottogruppi di pirati, ciascuno con propri fattori trainanti e livelli di sofisticazione.

I gestori di siti

Gestiscono siti di video pirata, compresi i siti di torrent, come Pirate Bay, o siti di streaming, come TeaTV. Non è noto se i gruppi di distribuzione e i gestori di siti siano le stesse persone, ma molti studi hanno dimostrato che esiste una significativa sovrapposizione tra i due. I gestori sicuramente acquisiscono proventi dall'intero processo e spesso gestiscono diversi siti "mirror" in modo che, se uno viene rimosso dalle autorità, possono comunque rimanere online e continuare a guadagnare.

I grossisti di dispositivi di streaming Internet

La crescita di questi dispositivi, in particolare Kodi, fornisce un flusso di entrate relativamente costante e prevedibile per i criminali opportunisti. I grossisti importano le unità attraverso canali del tutto legali o reti criminali e le modificano con software illegali, per poi venderle online.

I pirati sui social

Utilizzando spesso i social media per distribuire i contenuti, le persone in questo gruppo sono meno consapevoli o ambivalenti riguardo al fatto di considerare la pirateria come illegale e rispondono al costo di determinati generi di contenuti o alla saturazione di abbonamenti.

In che modo i pirati acquisiscono i contenuti?

Esistono molti metodi usati dai pirati per sottrarre contenuti, per via di una serie di punti deboli lungo la catena di valore che è possibile sfruttare. Possiamo raggruppare i metodi più importanti in base al caso di utilizzo.

Simulcast di canali TV ed eventi live

Una delle forme di pirateria a più rapida crescita riguarda l'acquisizione e la ridistribuzione di canali TV o eventi live. Questo obiettivo può essere raggiunto con:

- Manomissione del software di riproduzione video o del sistema operativo Android
- Schermate di registrazione durante la riproduzione tramite un dispositivo mobile
- Intercettazione di video decrittografati utilizzando stripper HDCP collegati a set-top box
- Attacchi di credential stuffing per accedere e utilizzare i dettagli dello spettatore legittimo
- Trasporto di video al di fuori di un determinato mercato utilizzando una VPN

Contenuti on-demand

I gruppi di distribuzione premiano programmi TV e film in anteprima. La struttura del settore dei media presenta una gamma di opportunità, con un numero talmente elevato di diverse organizzazioni e persone coinvolte nel processo di produzione. I metodi comunemente utilizzati dai pirati per acquisire video includono:

- Violazioni del data center, che provocano il furto di credenziali utente o contenuti video
- Furto di ID utente, per fornire l'accesso a contenuti video tramite vari sistemi di produzione
- Registrazione di risorse fisiche (ora meno diffuse) per la condivisione e la distribuzione
- Attacchi al sistema contro vari sistemi di produzione che forniscono l'accesso diretto ai video
- Estrazione di contenuti da fonti legittime, ad esempio iTunes
- Sistemi di ripresa cinematografica
- Furto diretto tramite attacchi MITM (Man-In-The-Middle)

In che modo vengono distribuiti i contenuti?

I pirati utilizzano ogni canale possibile e ogni innovazione tecnica a loro disposizione per distribuire i propri contenuti, tra cui:

- Set-top box IP personalizzati che accedono a flussi televisivi pre-programmati
- Software in esecuzione su dispositivi di streaming e PC che consentono la distribuzione pirata, ad esempio Kodi
- App che vengono caricate lateralmente su dispositivi di streaming al dettaglio popolari
- Siti web e servizi di social media che ospitano contenuti creati dagli utenti, come YouTube
- Siti web che trasmettono contenuti pirata tramite collegamenti che possono essere scoperti tramite ricerche o sui social media
- I siti di download, hosting di file, cyberlocker e torrent sempre presenti

Sebbene le strategie di diffusione dei vari pirati siano meno note, si può osservare che i gruppi di distribuzione potrebbero favorire modelli di condivisione delle risorse (ad es. i cyberlocker e siti torrent), a causa della loro ubiquità e del loro altruismo. Al contrario, i gestori dei siti motivati finanziariamente favorirebbero la strategia di ISD/streaming per emulare servizi legittimi e la possibilità di questi ultimi di incoraggiare più modelli di reddito.

La domanda

Esistono molti motivi per i quali le persone cercano siti pirata, tra cui la motivazione economica, l'ignoranza di un maggior impatto e la capacità di base di accedere ai contenuti senza limitazioni di windowing. Sono molti i pirati descritti da VFT Solutions Inc. nel suo rapporto 2019 relativo agli spettatori pirata, come abbiamo riassunto qui di seguito:

- **L'"anarchico dei contenuti"** crede nell'accesso comunitario e libero ai contenuti online. Qualsiasi addebito richiesto per i contenuti è sempre troppo e non crede che la pirateria sia immorale o illegale.
- **Il "Robin Hood dei contenuti"** ha un'opinione meno estrema ed è aperto a considerare proposte alternative. Questo tipo di pirata non è un utente di servizi di streaming live, ma si dedica alla diffusione di file torrent condivisi.
- **L'"utilitarista"** giustifica le proprie azioni sostenendo che l'ampio consumo di contenuti supera i danni subiti dai detentori di diritti, poiché la maggior parte dei contenuti ha un valore effimero.
- **Il "pirata pigro"** è spesso inconsapevole o millanta di non sapere che la pirateria sia illegale. Si fa influenzare dai risparmi sui costi e dall'ampia disponibilità, nonché dall'accesso semplificato.

VFT stima che il pirata pigro e l'utilitarista rappresentino fino al 70% della comunità totale e gli sforzi per educare, convertire o sanzionare tali gruppi avranno un maggior impatto sulla pirateria.

Possiamo fermare questi pirati?

Purtroppo, la risposta in breve è: non completamente. La storia ci insegna che ci saranno sempre pirati che cercano di sfruttare i contenuti, sia per ragioni altruistiche o commerciali. Tuttavia, non tutto è perduto. Se il problema viene affrontato in modo strategico lungo la catena di valore, è possibile ridurlo al minimo. In termini pratici, una migliore cooperazione all'interno del settore, nelle aree strategiche identificate qui di seguito, avrà un impatto duraturo.

Dati

Un requisito chiaramente evidente è una metodologia standard per misurare la portata e l'impatto della pirateria a livello globale. Diverse metodologie e tecniche non consentono un'analisi continua o contestuale e creano confusione quando si assegnano priorità alle attività o si stabilisce il ritorno sulle iniziative contro la pirateria. Tale problema potrebbe essere risolto attraverso l'assunzione di un ruolo di leadership nella raccolta dei dati da parte di organismi di settore, come l'Alleanza per la Creatività e l'Intrattenimento (ACE).

Formazione

Per una vasta parte della popolazione, la pirateria è diventata qualcosa che fanno "tutti" e, quindi, non è più considerata illegale perché il comportamento è stato normalizzato. Bisognerebbe sforzarsi di continuare a ricordare a tutti che la pirateria è un crimine e ha un impatto reale sulle fonti di reddito.

Aspetto legale e normativo

Esistono diverse eccellenti iniziative promosse da organismi di settore o governativi, come la FAPAV in Italia, che perseguono i video pirata e riducono le scappatoie legislative in tutto il mondo. Questi sforzi richiedono coordinamento e accesso ai dati pertinenti.

Aspetto tecnico e operativo

L'era in cui si consentivano contenuti non protetti è finita da tempo. In pratica, tuttavia, significa adottare un'analisi strategica delle operazioni e identificare gli anelli deboli nella catena di valore tecnico, dalla produzione alla distribuzione, applicando misure appropriate. Questo viene definito un approccio a 360°.

Se il problema viene affrontato in modo strategico lungo la catena di valore, è possibile ridurlo al minimo.

L'approccio a 360°

Dopo aver esaminato i mezzi con cui i gruppi di pirati acquisiscono e distribuiscono video, abbiamo strutturato un sistema basato su tre principi chiave: protezione, rilevamento e applicazione. Tramite questo sistema, le organizzazioni possono esaminare strategicamente il panorama delle minacce in base al proprio ruolo nel settore e implementare iniziative operative e tecniche pertinenti atte a ridurre al minimo l'impatto.

Protezione

Protezione contro il credential stuffing

Come descritto in precedenza, il credential stuffing è un popolare vettore di attacco utilizzato dai pirati per acquisire i dati dello spettatore, in genere attraverso bot automatizzati. Ecco i nostri principali consigli:

- Pagine di accesso con codice/API con OWASP. Scrittura di codici sicuri secondo le best practice OWASP ed esecuzione regolare di test di penetrazione sugli endpoint di accesso.
- Uso della protezione contro gli attacchi DDoS. Questo può aiutarvi a impedire che botnet volumetriche raggiungano la vostra infrastruttura e sovraccarichino le vostre risorse.
- Uso di una soluzione per la gestione dei bot, come Bot Manager Premier di Akamai, che può aiutarvi a prevenire sofisticati attacchi di abuso di credenziali verificando il comportamento degli utenti e la telemetria dei dispositivi.

Protezione contro il furto nei sistemi

Il furto nei sistemi di produzione interni, storage digitale o cloud pubblico è un'importante fonte di contenuti contraffatti. In generale, osserviamo diverse forme di furto di risorse video:

- Attacchi diretti o MITM (Man-In-The-Middle) da parte di pirati.
- Acquisizione di ID di sistema univoci, ad esempio, le password.
- Furto da parte di dipendenti o liberi professionisti.

Esistono diverse tecnologie utilizzabili dalle aziende per ridurre al minimo il rischio, che, in sostanza, ruotano intorno al concetto di Zero Trust, un sistema utilizzato dalle aziende per trasformare l'accesso alla tecnologia. I componenti principali del sistema includono: protezione dell'accesso alle risorse, indipendentemente dalla posizione o dal modello di hosting; applicazione di una strategia di controllo degli accessi, basata sul principio del privilegio minimo; ispezione e registrazione di tutto il traffico per rilevare eventuali attività sospette. Il sistema prevede che solo gli utenti e i dispositivi autenticati possano accedere alle applicazioni e ai dati. Inoltre, protegge le applicazioni e gli utenti dalle avanzate minacce su Internet.

Esistono diversi componenti che le aziende possono utilizzare per implementare un sistema Zero Trust, tuttavia la protezione dell'accesso dei dipendenti/collaboratori ai principali sistemi di produzione e archiviazione è un aspetto chiave. Con una forza lavoro transitoria, le società del settore dei media devono affrontare sfide uniche nell'implementazione e nella revoca dell'accesso ai sistemi, a volte quotidianamente. Utilizzando servizi come Enterprise Application Access di Akamai, è possibile concedere rapidamente le autorizzazioni ad applicazioni specifiche in base all'identità e al contesto di sicurezza dell'utente e del dispositivo, senza consentire agli utenti di accedere alla rete aziendale, laddove possono verificarsi esfiltrazioni di video.

Un altro aspetto fondamentale del sistema Zero Trust è l'implementazione di sistemi che identificano e bloccano in modo proattivo minacce mirate come malware, ransomware e phishing, strumenti utilizzati dai pirati nei propri attacchi MITM (Man-In-The-Middle). Enterprise Threat Protector di Akamai, ad esempio, è un gateway web sicuro che utilizza l'intelligence sulla sicurezza in tempo reale per identificare e bloccare in modo proattivo minacce mirate come malware, ransomware, phishing ed esfiltrazione di dati basata su DNS.

Con una forza lavoro transitoria, le società del settore dei media devono affrontare sfide uniche nell'implementazione e nella revoca dell'accesso ai sistemi, a volte quotidianamente.

Protezione contro le violazioni dei diritti geografici e IP. I pirati spesso utilizzano la tecnologia VPN per mascherare il proprio paese di origine e l'indirizzo IP, acquisendo, di conseguenza, i dati degli utenti legittimi per ritrasmettere i contenuti. Una tecnologia di rilevamento proxy come Enhanced Proxy Detection di Akamai blocca in modo intelligente le richieste sull'edge associate a proxy anonimi o servizi VPN, impedendo tali casi di utilizzo.

Protezione contro le violazioni della riproduzione. Questa è di gran lunga la tattica più comune nella lotta contro la pirateria e si ottiene attraverso una serie di mezzi diversi, di cui il più diffuso è rappresentato dalla gestione dei diritti digitali (DRM). Il DRM si riferisce agli strumenti, agli standard e ai sistemi utilizzati per limitare i contenuti protetti da copyright e impedire la distribuzione non autorizzata. Non si tratta di una singola tecnologia.

A seconda della criticità delle risorse protette, alcuni distributori preferiscono la crittografia semplice (ovvero scrivere il contenuto in un codice che può essere letto solo da dispositivi o software con la chiave per sbloccare il codice), che richiede comunque una chiave per essere resa disponibile, il che fornisce, così, una protezione rapida, di sicuro contro i pirati casuali. Tuttavia, le chiavi vengono generalmente fornite dai server HTTP e possono essere copiate e condivise, quindi spesso non sono sufficienti per proteggere i contenuti più importanti.

Per migliorare la crittografia, le tecnologie DRM più avanzate gestiscono le comunicazioni principali tramite un modulo di decrittografia dei contenuti utilizzando un sistema di verifica/risposta. Queste comunicazioni sono crittografate in modo che la chiave di decrittografia non venga mai esposta e non corra quindi il rischio di essere violata. Le tecnologie DRM avanzate offrono anche regole aziendali che definiscono quando e come utilizzare le chiavi su diversi dispositivi, ad esempio regole basate sulla posizione o sul tempo.

Per i distributori che desiderano implementare la tecnologia DRM durante il processo di creazione dei pacchetti, è spesso utile collaborare con i provider cloud in grado di gestire la complessità. Akamai, ad esempio, ha integrato lo storage di origine per i contenuti on-demand con le capacità di elaborazione di diversi provider, come Bitmovin ed Encoding.com, che sono in grado di implementare la crittografia quasi in tempo reale.

Rilevamento

Come per qualsiasi forma di furto, la protezione non garantisce sempre un esito positivo e, di conseguenza, il rilevamento di eventuali violazioni è essenziale. Esistono diversi metodi per rilevare l'attività di pirateria quasi in tempo reale:

Fingerprinting

Questo metodo fornisce la capacità di identificare i contenuti video senza modificare i media originali. Gli strumenti vengono utilizzati per identificare, estrarre e quindi rappresentare gli attributi appartenenti a un file video, in modo che un qualunque video possa essere identificato dalla propria "impronta digitale" univoca, ad esempio sulle reti di condivisione di file. I media originali non devono essere modificati in alcun modo, il che è un vantaggio, tuttavia, un'impronta digitale non consente di distinguere tra diverse copie dello stesso titolo, ovvero, quale sia la prima copia di un video che è stata diffusa.

Watermarking

Questo metodo non può fermare direttamente la pirateria, ma consente ai provider di servizi di rilevarla, identificare chi la pratica e poi agire al riguardo. Il watermarking video consiste nell'aggiungere un modello di "bit" non evidenti e non rimovibili in un file video. Collegando questi dati all'identità dello spettatore è possibile tracciare il pirata che copia il contenuto dopo che è stato decrittografato e lo distribuisce illegalmente. Esistono tre metodi principali di watermarking video attualmente in uso:

- **Modifica di bitstream.** Prevede la modifica di alcune aree di un'immagine in modo da mantenere la qualità del video e permettere allo spettatore e alla sessione di essere identificabili. Si tratta di una metodologia solida, che, tuttavia, richiede un significativo sovraccarico di elaborazione e aggiunge latenza al sistema, risultando quindi inadatta per i contenuti live.
- **Watermarking lato client.** Questo metodo funziona bene per l'estrazione rapida della filigrana e ha la capacità di implementazione sulle piattaforme legacy e sulle set-top box. Sul flusso video nel dispositivo client viene implementata una sovrapposizione grafica, che può essere resa visibile o invisibile. Poiché la filigrana non viene applicata fino a quando non raggiunge il dispositivo client, lo streaming video necessita di una protezione aggiuntiva. La tecnologia del lato client richiede anche un'implementazione SDK, che può essere complessa in ambienti OTT.
- **Watermarking con variante A/B.** Destinati al settore OTT, vengono creati due flussi video identici, con filigrana, successivamente uniti o interlacciati sul lato client oppure tramite elaborazione edge CDN, per fornire un identificatore univoco. È un metodo affidabile e conveniente, tuttavia, poiché la sequenza di identificazione può essere lunga, non è l'ideale in situazioni che richiedono l'estrazione rapida della filigrana.

Un elemento chiave di qualsiasi strategia di watermarking è un monitoraggio adeguato, che consenta di applicare le tecniche appropriate nei confronti dei pirati. Sono disponibili servizi di monitoraggio gestiti oppure è possibile richiedere assistenza per sviluppare funzionalità interne. Akamai collabora con tutti i principali fornitori di servizi di watermarking per garantire la disponibilità e l'integrazione di una soluzione attuabile all'interno di una strategia globale di pirateria video.

Identificazione dei registri dei flussi

Un'altra forma di rilevamento avviene tramite l'esame in tempo reale dei registri di delivery. In questo scenario, l'ispezione approfondita dei registri fornisce un'immagine in tempo reale dell'attività di violazione basata su indirizzi IP autorizzati e non autorizzati. Il vantaggio di queste soluzioni, come Stream Protector di Akamai, è la capacità di attivare e disattivare la funzionalità a seconda della situazione, il che è l'ideale per proteggere i diritti di eventi a tempo limitato, come quelli sportivi.

Applicazione

Quando viene rilevata un'attività di pirateria, è importante essere in grado di agire in modo appropriato. A seconda della strategia, ciò può avvenire in diverse direzioni.

- **Revoca dell'accesso.** Se le risorse video sono sensibili al tempo, come gli eventi sportivi, sarà necessario revocare immediatamente l'accesso all'autore dello streaming illegale. Questo può essere ottenuto in due modi. Una metodologia comune consiste nel collaborare con il provider di servizi di distribuzione, scambiare dettagli rilevanti e interrompere l'attività di streaming da un indirizzo IP dannoso. Tale operazione, tuttavia, può richiedere tempo. Akamai fornisce un servizio che consente la revoca del flusso in tempo reale e senza interventi inutili. Ciò si è rivelato particolarmente efficace quando il monitoraggio della pirateria viene effettuato utilizzando il watermarking o l'identificazione dei registri dei flussi.
- **Modifica del flusso.** In situazioni meno sensibili al fattore tempo, i distributori possono decidere di modificare il flusso contraffatto sostituendolo con contenuti alternativi (Big Buck Bunny è popolare) o riducendo la qualità del flusso. Questo approccio ha il vantaggio di nascondere il rilevamento al pirata e impedirgli di passare a un'origine flusso diversa.
- **Messaggistica in tempo reale.** Come descritto nella sezione sulle tipologie di pirati, i pirati pigri si sentono protetti dall'anonimato di Internet. Organizzazioni come VFT sono in grado di identificare gli spettatori di flussi pirata su piattaforme di social media e inviare messaggi direttamente al trasgressore. Utilizzando questa forma di applicazione, i distributori sono in grado di modificare l'applicazione, ad esempio offrendo l'accesso a flussi legittimi e, se la violazione continua, inviando avvisi legali.

Conclusione

La pirateria video tramite IP è un argomento complesso e ricco di sfumature, ma che, come sappiamo, ha il potenziale per minacciare la redditività a lungo termine del settore dei media. Esistono prove schiaccianti che dimostrano significativi danni finanziari, ma soprattutto che la pirateria ha il potenziale per minare alla base o compromettere i modelli di licenza globali.

Ad oggi, la risposta del settore è stata relativamente pacata. Come descritto da un analista, "Siamo nella fase iniziale e abbiamo molto lavoro da fare". Un numero crescente di distributori si è reso conto della minaccia e la maggior parte dei produttori e operatori di video di "livello 1" ha ora istituito team dedicati per comprendere meglio la pirateria, valutare la propria situazione e implementare strategie antipirateria pertinenti.

In questo documento, sono stati identificati diversi requisiti immediati necessari per aiutare il settore a combattere questa battaglia. Questi includono punti di dati coerenti sulla pirateria, educazione migliore e continua del pubblico in generale, migliore cooperazione all'interno del settore e, infine, la leadership dei titolari di diritti in tutti i generi per promuovere la capillarità nel settore durante la gestione e la distribuzione dei diritti.

La buona notizia è che molto sta già iniziando a mobilitarsi. La ricerca sull'argomento sta diventando sempre più attenta, con legislazioni più rigorose e fornitori che riuniscono le funzionalità per massimizzare il potenziale. Ad esempio, oltre a mettere a frutto la propria esperienza in materia di cybersicurezza, Akamai sta collaborando con tutte le principali società di watermarking per garantire che, una volta rilevati i pirati, sia possibile interromperne immediatamente le attività. Infine, stiamo notando che i titolari dei diritti stanno iniziando a insistere su standard minimi di protezione dei contenuti in tutto il workflow tecnico. Oggi si tratta di casi isolati o "suggerimenti" (come nel caso della MPAA), ma osserviamo che stanno diventando una funzione sempre più necessaria per le attività commerciali.

Con queste iniziative in atto, possiamo ridurre al minimo il problema in modo da diminuire le perdite finanziarie, proteggere l'occupazione e garantire la prosperità delle licenze in un mercato globale.

RIFERIMENTI

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

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

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

Coberly. Streaming services are 'killing' piracy. Estratto da 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. Estratto da 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. Estratto da https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

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

Commissione europea. Estimating displacement rates of copyrighted content in the EU. Maggio 2015.

Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO). Trends in Digital Copyright Infringement in the European Union. 2018.

Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO). Illegal IPTV in the European Union. 2019.

FACT. Cracking down on digital piracy. 2017.

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

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

Frontier Economics. The economic impacts of counterfeiting and piracy. Rapporto preparato per BASCAP e INTA. 2017.

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

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

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

Intellectual Property Office. Online Copyright Infringement Tracker. 2018.

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

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

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

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

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

Liebowitz S. "The impact of internet piracy on sales and revenues of copyright owners", una versione abbreviata di "Internet piracy: the estimated impact on sales" in Handbook on the Digital Creative Economy A cura di Ruth Towse e Christian Handke, Edward Elgar. 2013.

Mick, J. Nearly half of Americans pirate casually, but pirates purchase more legal content. 21 gennaio 2013. Estratto da 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. Novembre 2018.

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

MUSO. Measuring ROI in content protection. 2020.

Nordic Content Protection Group. Annual Report, 2020.

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

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

Sanchez, J. 3 gennaio 2012. How copyright industries con congress. Estratto da http://www.cato.org/blog/how-copyright-industries-con-congress

Sandvine. Video and Television Piracy. 2019.

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

---

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 07/20.