MANUALE

Protezione per il settore dei video, dalle aziende ai contenuti agli spettatori

Akamai

> *Sono dentro. All'interno del perimetro. Sono qui. Sono dentro. Sono dentro!"*
>
> *- Bill Paxton nel ruolo di Private Hudson in "Aliens" (1986)*

Punto 1: aziende sotto attacco

La produzione di video è un atto intrinsecamente collaborativo e, dal momento che il nostro settore si è spostato verso workflow basati sui file, il numero di "endpoint" che possono accedere o toccare una risorsa è incrementato. Ciò significa che anche il numero di potenziali crepe nella struttura di sicurezza è aumentato.

Prendiamo, ad esempio, i freelancer e le case di post-produzione. In genere, non si considerano degli obiettivi e potrebbero non disporre dell'esperienza o delle risorse necessarie per mettere in atto adeguate procedure in termini di sicurezza, se anche se lo facessero. Ciò li rende dei bersagli ideali.

Ad esempio, il famoso attacco di *Orange Is the New Black* del 2018 derivava dalla capacità, da parte di criminali motivati finanziariamente, di compromettere una casa di post-produzione che stava lavorando alla nuova stagione di un famoso show di Netflix. I criminali rubano i file mezzanine e chiedono un riscatto.[1]

Durante una recente conferenza sulla *cybersicurezza per le emittenti* rivolta a più di due dozzine di aziende negli Stati Uniti, tra le maggiori richieste figuravano la protezione dell'accesso remoto e la sicurezza dei fornitori.

Qui troverete due strumenti che possono aiutare:

1. Applicazione della strategia del privilegio minimo tramite lo strumento Zero Trust Network Access per dipendenti e collaboratori che devono accedere a risorse chiave
2. Rilevamento e blocco del traffico dannoso originato all'interno della rete tramite un SWG (Secure Web Gateway)

Questi approcci Zero Trust ridurranno la probabilità che i criminali possano arrivare all'interno dell'azienda e, nel caso ci riescano, limiteranno la loro capacità di sottrarre i dati.

> *Mio padre era un ladro insignificante. Lui diceva: "Tutti rubano. Ecco come funziona. Io rubo, figlio mio. Ma non mi prendono."*
>
> *- Christian Slater nel ruolo di Mr. Robot, "Mr. Robot" (2015)*

Punto 2: video sotto attacco

Nel 2013, la serie TV horror-thriller psicologica "Hannibal" è stata cancellata a causa dei bassi indici di ascolto. La serie, tuttavia, è stata il quinto show più scaricato illegalmente dell'anno. La sua produttrice, Martha De Laurentiis, ha dichiarato che la cancellazione di "Hannibal" aveva molto a che vedere con la pirateria.[2]

Nel giugno 2019, l'emittente del Qatar BeIN Media Group ha annunciato che stava per licenziare 300 dipendenti per la perdita di fatturato. La causa? BeIN sostiene che il servizio rivale beoutQ abbia contraffatto i suoi contenuti sportivi ultra-premium.[3]

La pirateria dei contenuti multimediali ha fatto parte del nostro panorama fin dall'epoca dei film muti. Il passaggio allo streaming e la globalizzazione della distribuzione l'hanno resa semplicemente più facile e redditizia per i criminali. Gli studi sull'impatto della pirateria variano in modo significativo, ma gli analisti concordano sul fatto che la pirateria video sia arrivata a generare almeno 1 miliardo di dollari l'anno negli Stati Uniti[4] e un altro miliardo di Euro in Europa.[5]

La pirateria è anche un ecosistema multisfaccettato, con appassionati che mandano programmi in diretta streaming per gli amici sui social media, "anarchici dell'informazione" che rubano e condividono contenuti in prima visione tramite i gruppi di rilascio, criminali motivati finanziariamente che mandano in onda sofisticati servizi video e persino governi che usano la pirateria come parte della loro campagna sulla guerra dell'informazione.

Una bella gatta da pelare. Noi di Akamai lavoriamo con molti dei maggiori produttori e distributori di contenuti multimediali video al mondo e stiamo collaborando su un approccio basato sulle fasi di protezione, rilevamento e applicazione. Riepilogando:

Protezione: fermate il furto di contenuti e credenziali

- Proteggetevi dal furto di produzioni video e sistemi di storage
- Proteggetevi dal furto delle informazioni sugli spettatori per prevenire il ristreaming
- Proteggetevi dalle violazioni geografiche e dei diritti
- Proteggetevi dalle violazioni di riproduzione

Rilevamento: scoprite chi sta usando i file una volta che sono stati rubati

- Un'ispezione approfondita dei registri può fornirvi un quadro in tempo reale dell'attività di violazione
- Il rilevamento del proxy può individuare gli utenti di servizi VPN
- L'applicazione di una filigrana può identificare e tracciare i file rubati

Applicazione: sbaragliate i pirati informatici che usano la vostra proprietà intellettuale

- La revoca dell'accesso ai token può impedire lo streaming degli indirizzi IP dannosi.
- La modifica dei flussi può sostituire i flussi contraffatti con un contenuto alternativo
- Il blocco dei proxy può impedire all'utente individuato di usare l'IP di quel proxy

> *Il nostro mondo intero si poggia su un computer. I vostri registri della motorizzazione. La vostra sicurezza sociale. Le vostre carte di credito. Le vostre cartelle mediche. È tutto lì e sta implorando che qualcuno lo porti via. E sai una cosa? L'hanno fatto a me e sai una cosa? Lo faranno a te."*
>
> *- Sandra Bullock nel ruolo di Angela, "Intrappolata nella rete" (1995)*

Il crescendo: spettatori sotto attacco

Nel 2019, negli Stati Uniti è stato lanciato un nuovo importante servizio di abbonamento che ha riscontrato un enorme successo. Tuttavia, nel giro di 24 ore, alcuni dei nuovi clienti hanno acceso i social media lamentandosi del fatto che i loro account erano stati bloccati. In questo caso, non si era trattato di una violazione di dati, ma di un attacco di credential stuffing.

Quando i servizi OTT (Over-The-Top) scoprono che l'account di uno spettatore è stato compromesso, molti rispondono chiedendo al cliente che ha sottoscritto l'abbonamento di effettuare un ripristino dell'account per prevenire ulteriori furti. Ciò salvaguarda la proprietà intellettuale dell'azienda, ma comporta una pessima experience per gli utenti.

Molti di questi attacchi assumono la forma di "account stuffing" automatizzato e una difesa che può ridurre la necessità di bloccare e ripristinare l'account consiste nell'utilizzo di uno strumento di gestione dei bot. I bot "buoni" riescono a identificare in maniera proattiva l'accesso di una persona reale e possono bloccare i bot che assumono l'identità fittizia di questa persona.

Poiché l'identità è uno degli elementi base fondamentali della rivoluzione OTT, garantire un'eccellente experience per gli spettatori e modelli di business più redditizi basati sugli abbonamenti e sulle pubblicità è un fattore imprescindibile per proteggere queste identità.

La conclusione: il ritorno degli eroi

Mentre produttori e distributori di video completano il passaggio verso un ecosistema più sicuro, sanno benissimo che i criminali si stanno semplicemente leccando le ferite, preparandosi al prossimo attacco.

Partner chiave per la delivery di video e soluzioni per la sicurezza nel cloud, Akamai può aiutarvi egregiamente. Ecco come possiamo proteggere la vostra azienda, le vostre app e le vostre API, aiutarvi ad affrontare e combattere le sfide poste dalla pirateria e ridurre l'attacco dei cloni tramite le nostre soluzioni di gestione dei bot.

Ci vediamo nel sequel.

RIFERIMENTI

1) Netflix sotto attacco: divulgati 10 nuovi episodi di Orange Is the New Black
2) I pirati hanno ucciso "Hannibal"? | The Hill
3) BeIN licenzia il personale additando la pirateria come causa della perdita di profitti
4) White paper Sandvine - La pirateria video e televisiva: ecosistema e impatto
5) Rapporti EUIPO: circa 1 miliardo di Euro in streaming "IPTV" illegale nel 2018; pirateria complessiva in leggero calo

---

Akamai Experience the Edge

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: 06/20.