Protection des sociétés de vidéo, de l'entreprise au contenu en passant par les téléspectateurs

Akamai

> *Ils sont à l'intérieur. À l'intérieur du périmètre. Ils sont ici. Ils sont à l'intérieur. Ils sont à l'intérieur ! »*
>
> *– Bill Paxton dans le rôle du soldat Hudson, « Aliens » (1986)*

Stade n° 1 de l'intrigue : Attaque de l'entreprise

La production vidéo est un acte collaboratif par nature. À mesure que notre secteur est passé aux flux de travail basés sur des fichiers, le nombre de « points de terminaison » pouvant accéder à une ressource ou rentrer en contact avec l'une d'elle a augmenté. Cela signifie que le nombre de brèches potentielles dans votre bouclier de sécurité a également augmenté.

Prenez les travailleurs indépendants et les sociétés de post-production par exemple. En général, ils ne se considèrent pas comme des cibles et peuvent ne pas avoir les ressources ou l'expertise nécessaires pour adopter une stratégie de sécurité adéquate. Cela en fait des cibles idéales.

Ainsi, le célèbre piratage d'*Orange is the New Black* en 2018 est le travail de hackers financièrement intéressés, capables de compromettre une société de post-production travaillant sur la nouvelle saison de la série à succès de Netflix. Ils ont volé les fichiers mezzanine et ont ensuite exigé une rançon.[1]

Lors du récent séminaire *CyberSecurity for Broadcasters* qui s'est tenu à huis clos aux États-Unis et a réuni plus d'une vingtaine d'entreprises, la sécurisation de l'accès à distance et la sécurité des prestataires ont figuré parmi les principales demandes.

Voici deux outils qui peuvent être utiles :

1. Appliquez la stratégie du moindre privilège en utilisant un outil d'accès réseau Zero Trust pour les employés et les sous-traitants qui cherchent à accéder aux ressources clés.
2. Détectez et bloquez le trafic malveillant provenant du réseau à l'aide d'une passerelle Web sécurisée (SWG).

Ces approches Zero Trust réduiront la probabilité qu'un hacker réussisse à pénétrer dans la chambre forte, et s'il y parvient, limiteront sa capacité à s'évader.

> *Mon père était un petit voleur. Il disait : "Tout le monde vole. C'est comme ça que ça marche. Je vole, fiston. Mais je ne me fais pas prendre." »*
>
> *– Christian Slater dans le rôle de Mr. Robot, « Mr. Robot » (2015)*

Stade n° 2 de l'intrigue : Attaque de la vidéo

En 2013, la série thriller psychologique d'horreur « Hannibal » a été annulée en raison de « mauvaises critiques ». Elle s'est pourtant classée au cinquième rang des séries les plus téléchargées illégalement de l'année. Sa productrice, Martha De Laurentiis, a déclaré que l'annulation de « Hannibal » avait beaucoup à voir avec le piratage.[2]

En juin 2019, le diffuseur qatarien BeIN Media Group a annoncé devoir licencier 300 employés en raison d'une baisse de chiffre d'affaires. La cause ? BeIN affirme que le service concurrent beoutQ pirate son contenu sportif ultra-haut de gamme.[3]

Le piratage des médias fait partie de notre environnement depuis l'ère du film muet. Le passage au streaming et la mondialisation de la distribution le rendent tout simplement plus facile et plus rentable pour les personnes malveillantes. Les études sur l'impact du piratage varient considérablement, mais les analystes s'accordent sur le fait que le piratage vidéo génère au moins 1 milliard de dollars par an pour les hackers aux États-Unis[4] et un autre milliard d'euros en Europe.[5]

Le piratage est également un écosystème à plusieurs facettes, avec des amateurs qui diffusent en live des contenus sur les réseaux sociaux à leurs amis, des « anarchistes de l'information » qui détournent et partagent du contenu inédit via des groupes de diffusion, des hackers financièrement intéressés qui réalisent des services vidéo sophistiqués, et aussi des nations qui utilisent le piratage dans le cadre de leur campagne de guerre de l'information.

C'est un véritable casse-tête. Chez Akamai, nous travaillons avec la plupart des plus grands producteurs et distributeurs de médias vidéo au monde, et avons élaboré avec eux une approche appelée « Protection, Détection et Mise en œuvre ». Pour résumer :

Protection : Empêcher le vol de contenu et d'informations d'identification

- Protéger contre le vol de systèmes de production et de stockage vidéo
- Protéger contre le vol d'informations des téléspectateurs pour éviter le restreaming
- Protéger contre les violations liées à la zone géographique et aux droits
- Protéger contre les violations liées à la lecture

Détection : Découvrir qui utilise les fichiers une fois qu'ils ont été volés

- L'inspection approfondie des journaux peut vous donner un aperçu en temps réel de l'activité illicite
- La détection de proxy peut trouver les utilisateurs de services VPN
- Le filigrane permet d'identifier et de suivre les fichiers volés

Mise en œuvre : Stopper les hackers qui utilisent votre propriété intellectuelle

- La révocation de l'accès à jeton peut empêcher des adresses IP délictueuses de diffuser en streaming
- La modification du streaming peut remplacer la diffusion piratée par un contenu alternatif
- Le blocage de proxy peut empêcher l'utilisateur détecté d'utiliser cette adresse IP de proxy

> *Tout est stocké sur des machines. De votre permis de conduire à votre numéro de sécurité sociale. Vos cartes de crédit. Vos dossiers médicaux. Tout est là, il ne nous reste plus qu'à attendre que quelqu'un vienne nous entuber. Et vous savez quoi ? C'est ce qui m'est arrivé. Et vous savez quoi ? C'est ce qui va vous arriver. »*
>
> *– Sandra Bullock dans le rôle d'Angela, « Traque sur Internet » (1995)*

Intensification dramatique : Attaque des téléspectateurs

En 2019, un nouveau service d'abonnement a été lancé aux États-Unis et a remporté un succès considérable. Cependant, après 24 heures, certains nouveaux clients ont déferlé sur les réseaux sociaux pour se plaindre que leurs comptes avaient été verrouillés. Dans ce cas précis, ce n'était pas dû à une violation de données mais à une attaque de type « credential stuffing ».

Lorsque les services OTT ont découvert que le compte d'un téléspectateur avait été compromis, beaucoup ont réagi en exigeant que l'abonné réinitialise son compte pour éviter tout nouveau vol. Cela a permis de protéger la propriété intellectuelle de l'entreprise, mais a dégradé l'expérience client.

Ces attaques se présentent souvent sous la forme de « remplissage de compte » automatisé. L'utilisation d'un outil de gestion des bots peut limiter la nécessité de bloquer et réinitialiser les comptes. Les meilleurs outils peuvent déterminer de manière proactive quand une vraie personne se connecte et bloquer les bots prétendant être cette personne.

De plus, l'identité étant l'un des éléments fondamentaux de la révolution OTT, assurant une expérience de visionnage exceptionnelle ainsi qu'une meilleure rentabilité des modèles commerciaux basés sur un système d'abonnement et financés par la publicité, il est essentiel d'en assurer la protection.

Dénouement : Le retour du héros

Alors que les producteurs et les distributeurs de vidéos achèvent leur migration vers un écosystème plus sécurisé, ils savent bien que les hackers se préparent déjà à la prochaine attaque.

En tant que partenaire stratégique pour la diffusion vidéo et la sécurité dans le cloud, Akamai va vite devenir votre fidèle compagnon. Découvrez comment nous pouvons vous aider à protéger votre entreprise, vos applications et vos API, à évaluer l'ampleur du problème du piratage et à lutter contre ce fléau, mais également comment nos solutions de gestion des bots peuvent réduire l'attaque des clones.

Rendez-vous au prochain épisode.

RÉFÉRENCES

1) Netflix piraté, 10 nouveaux épisodes d'Orange is the New Black divulgués
2) Les hackers ont-ils tué « Hannibal » ? | The Hill
3) BeIN réduit drastiquement ses effectifs et accuse le piratage pour la chute de son chiffre d'affaires
4) Livre blanc de Sandvine – Piratage vidéo et télévisuel : écosystème et impact
5) Rapports de l'EUIPO : près de 1 milliard d'euros de streaming « IPTV » illégal en 2018 ; le piratage global en légère baisse

---

Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multi-clouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et mobiles, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques mondiales font confiance à Akamai, rendez-vous sur les pages www.akamai.com et blogs.akamai.com ou suivez @Akamai sur Twitter. Nos coordonnées dans le monde entier sont disponibles à l'adresse www.akamai.com/locations. Publication : 06/20.