INFORMA-
CIÓN BÁSICA

Protección de empresas de vídeo desde la empresa hasta el espectador, pasando por el contenido

Akamai

> *Están dentro. Dentro del perímetro. Están aquí dentro. Están dentro. ¡Están dentro!"*
>
> *Bill Paxton, soldado Hudson en "Aliens: El regreso" (1986)*

Nudo de la trama 1: El ataque a la empresa

La producción de vídeo es un acto inherentemente colaborativo y, a medida que nuestro sector se ha trasladado a flujos de trabajo basados en archivos, ha aumentado el número de "terminales" que pueden acceder o tener contacto con un activo. Esto significa que también ha crecido el número de posibles grietas en su armadura de seguridad.

Tomemos, por ejemplo, a los trabajadores autónomos y las empresas de posproducción. Por lo general, no se consideran a sí mismos objetivos de ataque y es posible que, aunque lo hicieran, no dispongan de los recursos o la experiencia necesarios para practicar una higiene de seguridad adecuada. Eso los convierte en blancos perfectos.

Por ejemplo, el famoso hackeo de *Orange Is the New Black* en 2018 fue la consecuencia de la capacidad de unos atacantes con motivaciones financieras para vulnerar una empresa de posproducción que trabajaba en la nueva temporada de la exitosa serie de Netflix. Robaron los archivos con calidad mezzanine y pidieron un rescate por ellos.[1]

En un reciente retiro a puerta cerrada de *Ciberseguridad para cadenas de televisión* en Estados Unidos para más de dos docenas de empresas, entre las principales peticiones estaban la protección del acceso remoto y la seguridad de los proveedores.

Estas son dos herramientas que pueden ayudar:

1. Implementar una estrategia según el principio de mínimo privilegio mediante el uso de una herramienta de acceso a la red Zero Trust para los empleados y contratistas que traten de acceder a recursos clave
2. Detectar y bloquear tráfico malicioso que se origine dentro de la red mediante una puerta de enlace web segura (SWG)

Estos enfoques Zero Trust reducirán la probabilidad de que el ladrón pueda acceder a la "cámara acorazada" y, si lo hace, limita su capacidad para llevarse el botín.

> *Mi padre era un ladrón. Muy bueno. Me dijo «Todos robamos. Así es como funciona. Yo robo, hijo. Pero no me han cogido».*
>
> *Christian Slater, Mr. Robot en "Mr Robot" (2015)*

Nudo de la trama 2: El ataque al vídeo

En 2013, la serie de televisión "Hannibal", un thriller de terror psicológico, se canceló por sus "malas valoraciones". Sin embargo, la serie fue la quinta más descargada ilegalmente de ese año. Su productora, Martha De Laurentiis, ha declarado que la cancelación de "Hannibal" tuvo mucho que ver con la piratería.[2]

En junio de 2019, el grupo de televisión catarí BeIN Media Group anunció que iba a despedir a 300 empleados debido a la disminución de sus ingresos. ¿El motivo? BeIN afirma que el servicio de la competencia beoutQ piratea su contenido deportivo ultrapremium.[3]

La piratería de los medios forma parte de nuestro paisaje desde la época del cine mudo. El paso al streaming y la globalización de la distribución no han hecho sino ponérselo más fácil y rentable a los malos. Los estudios sobre el impacto de la piratería varían considerablemente, pero los analistas coinciden de forma sistemática en que la piratería de vídeo genera al menos 1000 millones de dólares al año para los piratas en los Estados Unidos[4] y otros 1000 millones de euros en Europa.[5]

La piratería también es un ecosistema multifacético, en el que los aficionados emiten en streaming para sus amigos en las redes sociales, los "anarquistas de la información" copian y comparten contenido recién estrenado a través de grupos de difusión, los atacantes con motivación financiera dirigen sofisticados servicios de vídeo y, sí, los países usan la piratería en sus campañas para la guerra de información.

El panorama es un hueso duro de roer. En Akamai trabajamos con muchos de los mayores productores y distribuidores de vídeo del mundo, y estamos colaborando en un enfoque que denominamos protección, detección y aplicación. En resumen:

Protección: Detener el robo de contenido y credenciales

- Proteger contra el robo de sistemas de almacenamiento y producción de vídeo
- Proteger contra el robo de los datos de espectadores para evitar el restreaming
- Proteger contra las infracciones geográficas y de derechos
- Proteger contra las infracciones de reproducción

Detección: Descubrir quién está usando los archivos una vez que han sido robados

- Una inspección en profundidad de los registros puede ofrecer una imagen en tiempo real de la actividad infractora
- La detección de proxy puede revelar usuarios de servicios de VPN
- Las marcas de agua pueden identificar y rastrear archivos robados

Aplicación: Aislar a los piratas que utilizan su propiedad intelectual

- La revocación de acceso mediante token puede impedir que las IP infractoras transmitan en streaming
- La modificación del streaming puede reemplazar la transmisión pirata por otro contenido
- El bloqueo de proxy puede impedir que el usuario detectado utilice esa IP de proxy

> *Todo nuestro mundo dentro de un ordenador. Tu ficha de tráfico. Tu seguridad social. Tus tarjetas de crédito. Tu historial médico. Todo está metido ahí. [Una pequeña sombra]... pidiendo que alguien la manipule. Y ¿sabe qué? Lo han hecho conmigo y van a hacerlo con usted".*
>
> *Sandra Bullock, Angela en La red (1995)*

In crescendo: El ataque a los espectadores

En el 2019, se lanzó un nuevo servicio de suscripción en Estados Unidos que tuvo un éxito masivo. Sin embargo, en un plazo de 24 horas, algunos nuevos clientes encendieron las redes sociales quejándose de que sus cuentas se habían bloqueado. En este caso, la causa no era una filtración de datos, sino un ataque de Credential Stuffing.

Cuando los servicios de libre transmisión (OTT) descubren que la cuenta de un espectador se ha vulnerado, muchos responden solicitando al cliente de pago que realice un restablecimiento de su cuenta para evitar nuevos robos. Eso protege la propiedad intelectual de la empresa, pero afecta negativamente a la experiencia del cliente.

Muchos de estos ataques adoptan la forma de "Account Stuffing" automatizada. Con una herramienta de gestión de bots, es posible reducir la necesidad de bloquear y restablecer las cuentas. Las buenas herramientas pueden identificar proactivamente si una persona real inicia sesión y bloquear a los bots que simulan ser esa misma persona.

Y dado que la identidad es uno de los elementos fundamentales de la revolución de OTT, que permite una fantástica experiencia para los espectadores, así como modelos empresariales más rentables basados en suscripciones y con anuncios, es fundamental proteger esas identidades.

El desenlace: El retorno del héroe

A medida que los productores y distribuidores de vídeo culminan su viaje hacia un ecosistema más seguro, no cabe duda de que saben que los atacantes solo se están lamiendo las heridas y preparando el siguiente ataque.

Como partner clave para la distribución de vídeo y la seguridad en la nube, Akamai se encuentra en una buena posición para ser su compañero de aventuras. Compruebe cómo podemos ayudar a proteger su empresa, así como sus aplicaciones y API, cómo podemos ayudar a determinar y combatir el desafío de la piratería y cómo nuestras soluciones de gestión de bots permiten reducir el ataque de los clones.

Nos vemos en la secuela.

REFERENCIAS

1) Netflix hacked, 10 new Orange Is the New Black episodes leaked
2) Did pirates kill 'Hannibal'? | The Hill
3) BeIN axes staff claiming profits hit by piracy
4) Sandvine White Paper – Video and Television Piracy: Ecosystem and Impact
5) EUIPO Reports: Nearly €1B in illegal 'IPTV' streaming in 2018; overall piracy down slightly

---

Akamai Experience the Edge

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com y blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado el 20 de junio.