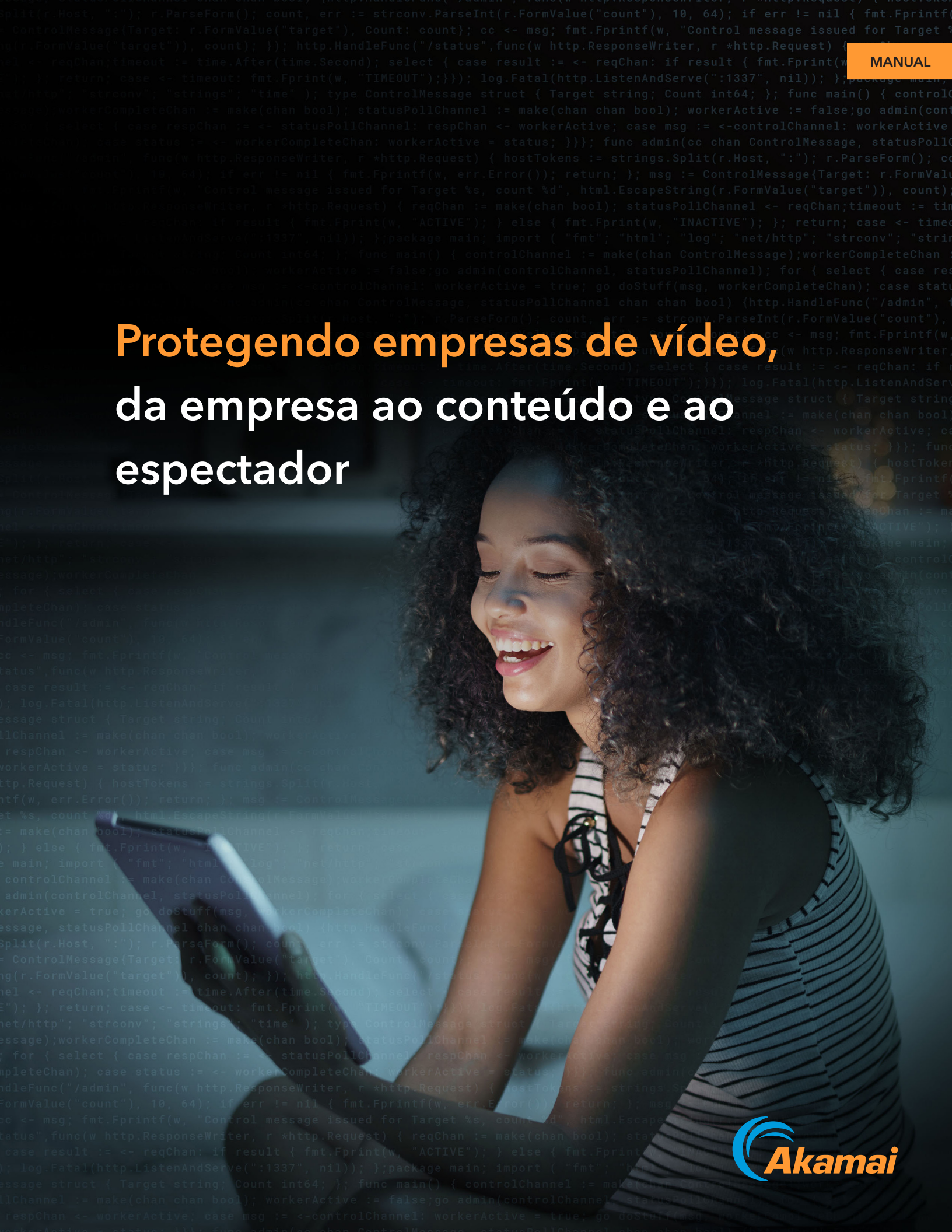
MANUAL

Protegendo empresas de vídeo, da empresa ao conteúdo e ao espectador



Akamai

> *Eles estão dentro. Dentro do perímetro. Eles estão aqui. Eles estão dentro. Eles estão dentro!"*
>
> *– Bill Paxton como soldado Hudson, "Aliens" (1986)*

Ponto 1 da trama: empresa sob ataque

A produção de vídeo é um ato inerentemente colaborativo e, à medida que nosso setor migrou para fluxos de trabalho baseados em arquivos, o número de "pontos de extremidade" que podem acessar ou tocar em um ativo cresceu. Isso significa que o número de possíveis fissuras em sua armadura de segurança também cresceu.

Tome como exemplos freelancers e casas de pós-produção. Normalmente, eles não se consideram alvos e podem não ter os recursos ou, ainda que os tivessem, podem não ter a experiência para colocar em prática a higiene de segurança adequada. Isso os torna alvos ideais.

Por exemplo, o famoso hacking da série *Orange Is the New Black* de 2018 foi resultado da capacidade de invasores financeiramente motivados de comprometer uma casa de pós-produção que trabalha na nova temporada desse sucesso da Netflix. Eles roubaram os arquivos com qualidade média e pediram um resgate.[1]

Em um recente retiro de portas fechadas sobre *Segurança virtual para emissoras* realizado nos Estados Unidos para mais de vinte e quatro empresas, entre os principais pedidos estavam a proteção do acesso remoto e a segurança dos prestadores de serviços.

Estas duas ferramentas podem ajudar:

1. Aplique uma estratégia de privilégio mínimo usando uma ferramenta de acesso à rede Zero Trust para funcionários e prestadores de serviços que buscam acesso aos principais recursos
2. Detecte e bloqueie tráfego mal-intencionado originado dentro da rede usando um gateway seguro da Web (SWG)

Essas abordagens de Zero Trust reduzirão a probabilidade de o ladrão entrar no "cofre" e, se isso acontecer, limitarão a capacidade dele de chegar ao "carro de fuga".

> *Meu pai era um ladrãozinho barato. Ele disse: "Todo mundo rouba. É assim que funciona. Eu roubo, filho. Mas eu não sou pego." "*
>
> *– Christian Slater como Mr. Robot, "Mr. Robot" (2015)*

Ponto 2 da trama: vídeo sob ataque

Em 2013, a série de televisão de terror psicológico "Hannibal" foi cancelada devido a "avaliações ruins". No entanto, a série foi classificada como a quinta série com mais downloads ilícitos daquele ano. Sua produtora, Martha De Laurentiis, disse que o cancelamento de "Hannibal" tinha muito a ver com a pirataria.[2]

Em junho de 2019, a emissora Qatari BeIN Media Group anunciou que estava demitindo 300 funcionários devido à queda da receita. O motivo? A BeIN afirma que o serviço concorrente beoutQ pirateia seu conteúdo esportivo de alta qualidade.[3]

A pirataria de mídia faz parte do nosso cenário desde a época dos filmes mudos. A mudança para o streaming e a globalização da distribuição simplesmente tornam mais fácil e mais rentável para esses infratores. Estudos sobre o impacto da pirataria variam drasticamente, mas analistas acreditam de maneira consistente que a pirataria de vídeo gera pelo menos 1 bilhão de dólares por ano para os piratas nos Estados Unidos[4] e mais 1 bilhão de euros na Europa.[5]

A pirataria também é um ecossistema multifacetado, com amadores que fazem transmissões ao vivo para os amigos nas mídias sociais, "anarquistas da informação" que obtêm e compartilham conteúdo em primeira mão por meio de grupos de lançamentos, invasores financeiramente motivados que executam serviços sofisticados de vídeo e, claro, nações que usam a pirataria como parte de sua campanha de guerra da informação.

É um osso duro de roer. Nós da Akamai trabalhamos com muitos dos maiores produtores e distribuidores de mídia de vídeo do mundo, e temos colaborado em uma abordagem que chamamos de Proteger, Detectar e Aplicar. Em resumo:

Proteger: Impedir que o conteúdo e as credenciais sejam roubados

- Proteger contra o roubo de sistemas de produção e armazenamento de vídeo
- Proteger contra o roubo de informações do espectador para evitar o re-streaming
- Proteger contra violações geográficas e de direitos
- Proteger contra violações de reprodução

Detectar: Descobrir quem está usando os arquivos após seu roubo

- A inspeção profunda de registros pode fornecer uma imagem em tempo real da atividade de violação
- A detecção de proxy pode localizar usuários de serviços de VPN
- A marca d'água pode identificar e rastrear arquivos roubados

Aplicar: Eliminar piratas que usam sua propriedade intelectual

- A revogação de acesso ao token pode impedir o streaming de endereços IP invasores
- A modificação do streaming pode substituir o streaming pirateado por conteúdo alternativo
- O bloqueio de proxy pode impedir que o usuário detectado use esse IP de proxy

> *Nosso mundo inteiro está dentro de um computador. Seus registros de DMV. Sua segurança social. Seus cartões de crédito. Seus registros médicos. Está tudo bem ali, implorando para alguém pegar. E sabe de uma coisa? Eles fizeram isso comigo, e quer saber? Eles vão fazer isso com você."*
>
> *– Sandra Bullock como Angela, "A Rede" (1995)*

A evolução: espectadores sob ataque

Em 2019, um novo e importante serviço de assinatura foi lançado nos Estados Unidos com enorme sucesso. Mas em 24 horas, alguns novos clientes lotaram as redes sociais reclamando que suas contas haviam sido bloqueadas. Nesse caso, o motivo não era uma violação dos dados, mas um ataque de credential stuffing.

Quando os serviços OTT (over the top) descobrem que a conta de um espectador foi comprometida, muitos respondem exigindo que o cliente pagador faça uma redefinição de conta para evitar mais roubos. Isso protege a propriedade intelectual da empresa, mas resulta em uma experiência insatisfatória do cliente.

Muitos desses ataques assumem a forma de "preenchimento de contas" automatizado, e uma defesa que pode reduzir a necessidade de bloqueio e redefinição de contas é usar uma ferramenta de gerenciamento de bots. Ferramentas boas conseguem identificar proativamente quando uma pessoa real faz login e bloquear bots que fingem ser a mesma pessoa.

E como a identidade é um dos elementos fundamentais da revolução de OTT, permitindo uma excelente experiência do espectador, bem como modelos de negócios mais rentáveis baseados em assinaturas e com suporte a anúncios, é essencial para proteger essas identidades.

O desfecho: o regresso do herói

Enquanto produtores e distribuidores de vídeo concluem sua jornada rumo a um ecossistema mais seguro, eles certamente sabem que os invasores estão apenas lambendo suas feridas e preparando seu próximo ataque.

Como parceira-chave para entrega de vídeo e segurança na nuvem, a Akamai está bem posicionada para uma parceria com você. Veja como podemos ajudar a proteger sua empresa e suas aplicações e APIs, como podemos ajudá-lo a definir o escopo e enfrentar o desafio da pirataria, e como nossas soluções de gerenciamento de bots podem reduzir o ataque dos clones.

Vejo você na sequência.

REFERÊNCIAS

1) Netflix hackeada, vazados 10 novos episódios de Orange Is the New Black
2) Os piratas mataram "Hannibal"? | The Hill
3) Funcionários da BeIN alegam impactos nos lucros causados pela pirataria
4) White Paper da Sandvine - Pirataria de vídeo e televisão: Ecossistema e impacto
5) Relatórios do EUIPO: Cerca de 1 bilhão de euros em streaming ilícito de "IPTV" em 2018; pequena queda da pirataria em geral

Akamai *Experience the Edge*

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 multinuvem. 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 de 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 mundiais confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou @Akamai no Twitter. Encontre nossas informações de contato globais em www.akamai.com/locations. Publicado em 06/20.