RESUMO DO PRODUTO DA AKAMAI

Resumo do produto Brand Protector

Detecte e detenha websites de phishing, lojas falsas e apropriações indevidas de marca para evitar danos aos clientes e reduzir o risco de fraudes e ataques em larga escala.

Sua marca reconhecível cria valor mensurável dentro e fora da organização. A proteção dos elementos da sua marca permite que sua organização mantenha e aumente a fidelidade dos clientes enquanto minimiza perdas, quedas de produtividade e avaliações negativas por clientes. De um ponto de vista de segurança, controlar a apropriação indevida de marca interrompe a cadeia de destruição imediatamente, evitando a coleta de credenciais e a violação de contas.

Nem todos os ataques acontecem de forma escancarada. Na Web, os invasores se apropriam da sua marca com sósias digitais para roubar dados confidenciais, credenciais e pagamentos diretos de seus clientes. A apropriação indevida de marca e o phishing são desafios crescentes, devido às táticas de campanhas de curta duração que aparecem e desaparecem e mudam de local para tornar a detecção e a mitigação um desafio que consome muitos recursos.

O Akamai Brand Protector usa um dos maiores bancos de dados de inteligência de ameaças, combinando feeds de dados próprios e de terceiros para acelerar as detecções e melhorar a precisão. Seus recursos integrados de mitigação tornam o Brand Protector uma ferramenta eficaz e essencial para combater fraudes e violações nos estágios iniciais.

O **Akamai Brand Protector** detecta e mitiga ataques direcionados, incluindo phishing, apropriações indevidas e violações de marcas em websites, mídias sociais e marketplaces de apps. Acima de tudo, o Brand Protector permite que você proteja suas relações de confiança.

Mais de 50.000 novos websites de phishing são criados toda semana. O Brand Protector inspeciona trilhões de atividades digitais por dia, em fontes internas e externas, para detectar violações da marca e dos elementos da marca da sua organização com velocidade e eficiência, muitas vezes antes do lançamento de uma campanha de ataque.

Para isso, o Brand Protector aborda as apropriações fraudulentas em quatro etapas: inteligência, detecção, visibilidade e mitigação.

Benefícios para a sua empresa

Detecção de ataques confiável
Nossa rede global e nossos feeds adicionais patenteados fornecem uma vantagem exclusiva para detectar apropriações indevidas de marca

Precisão e velocidade
Nossa rápida detecção algorítmica pode fornecer alertas antes do lançamento de campanhas de ataque e pode minimizar falsos positivos

Insights práticos
Dados abrangentes são fornecidos como insights práticos com pontuação de risco resumindo a gravidade e o alcance do ataque rapidamente

Visibilidade por cliente
Inteligência dedicada para sua marca, produtos e elementos associados em websites, redes sociais e marketplaces de apps

Facilidade de uso
Obtenha insights em tempo real e inicie a correção nesse crescente vetor de ataque em apenas alguns minutos

Remoção e mitigação
Para manter a produtividade, use o serviço integrado de remoção do Brand Protector ou opte por interromper o tráfego com um alerta de navegação

Inteligência

Os desafios de detectar ataques de phishing e de apropriação indevida de marca começam na fase de inteligência e coleta de dados.

Como a maior plataforma global de edge e nuvem, a Akamai tem visão privilegiada de todo o tráfego mundial da Web e analisa mais de 788 TB de dados por dia. A profundidade da inteligência no Brand Protector é aprimorada com feeds de dados de terceiros para visibilidade holística das ações dos invasores. Além disso, você pode adicionar seu próprio URL e domínios para análise pela nuvem de detecção do Brand Protector.

Detecção

A força e a velocidade de detecção do Brand Protector vêm de uma combinação de algoritmo de análise e feed de inteligência exclusivos da Akamai para aumentar a confiabilidade da detecção e reduzir falsos positivos.

Os ataques a marcas automatizam websites mal-intencionados e que ficam ativos por pouco tempo. A maioria das tecnologias não é rápida o suficiente para detectar e mitigar esses ativos de ataque antes que eles tenham impactado seus clientes. A abordagem da Akamai é diferente porque rastreia o tráfego ao vivo para detectar a violação da marca em vez de depender de listas atualizadas ou feeds atrasados. Com o Brand Protector, sua equipe de segurança pode detectar websites de phishing quando ocorre a primeira solicitação HTTP/HTTPS, geralmente antes que a campanha chegue aos seus clientes.

Visibilidade

A engenharia e design centrados no cliente oferecem às equipes de segurança insights de segurança amplos em um único painel.

Depois de receber a inteligência, os sinais de dados são executados por meio de uma série de detectores heurísticos e de inteligência artificial. Embora uma grande quantidade de dados e evidências sejam coletados, a interface de usuário simplificada da Akamai fornece um entendimento imediato das ameaças ativas para seus clientes por meio de apropriações.

Tráfego, detecções e dados de ameaças específicos de clientes são traduzidos em insights práticos no portal de clientes da Akamai. Os resultados são classificados por uma pontuação de ameaça resumida. Clique em um alerta para visualizar os dados de ameaça analisados, incluindo pontuação de confiança, classificação de gravidade, número de usuários afetados e um cronograma de eventos de ataque.

Cada detecção é baseada em evidências: você pode visualizar códigos, capturas de tela, indicadores de detecção e informações de domínio em uma única tela de detecção.

Mitigação

Os serviços de remoção integrados fecham o ciclo para combater a fraude à marca.

O Brand Protector permite que sua equipe emita uma solicitação de remoção do website invasor diretamente na tela de detecção. As solicitações de remoção (enviadas a um parceiro externo da Akamai) do Brand Protector anexam automaticamente o suporte probatório da detecção e informações adicionais para facilitar o uso. Você pode acompanhar e visualizar o status de mitigação no portal.

Criado para sua marca

Proteção de zona
Essa solução do nosso portfólio de proteção de edge pode ampliar a visão da sua equipe de segurança para a proteção antecipada contra a cadeia de destruição. Ela procura proativamente por permutações dos domínios da sua marca que possam ser usadas para transformar clientes em vítimas de phishing.

Monitoramento de mídias sociais
Com o aumento da apropriação indevida de marca nas mídias sociais, nosso novo recurso aprimorado de monitoramento de mídias sociais detecta e neutraliza fraudes online, protegendo sua marca e seus clientes em várias plataformas.

Detecção de apps invasores
O monitoramento de marketplaces de apps é um novo recurso que verifica repositórios oficiais e não oficiais de apps para detectar aplicativos enganosos que fazem uso indevido da identidade da marca, oferecendo uma defesa abrangente em todo o cenário digital.

©2024 Akamai Technologies | Suporte | | Publicado em 11/24