FICHE PRODUIT AKAMAI

Fiche produit Brand Protector

Détectez et neutralisez les sites d'hameçonnage, les fausses boutiques et l'usurpation d'identité de marque afin d'éviter les préjudices causés à vos clients et de réduire le risque de fraude à grande échelle et d'attaques abusives.

Votre marque est reconnaissable et crée une valeur quantifiable aussi bien à l'extérieur qu'à l'intérieur de votre entreprise. La protection des éléments de votre marque permet à votre entreprise de conserver et de fidéliser ses clients tout en minimisant les pertes, les baisses de productivité et les mauvais avis de clients. Du point de vue de la sécurité, le contrôle de l'usurpation d'identité de marque bloque la chaîne d'attaque dans son élan, empêchant ainsi la collecte d'informations d'identification et l'abus de compte.

Malheureusement, toutes les attaques ne passent pas par la porte d'entrée de l'entreprise. Sur le Web, les attaquants usurpent l'identité de votre marque avec des sosies digitaux pour voler les données sensibles, les identifiants et les paiements directs de vos clients. L'usurpation d'identité de marque et l'hameçonnage représentent un défi croissant, en raison de leurs tactiques de campagne éphémères qui s'activent, se désactivent et se déplacent, rendant ainsi la détection et l'atténuation très exigeantes en termes de ressources.

Akamai Brand Protector exploite l'une des plus grandes bases de données de renseignements sur les menaces, combinant des flux de données internes et tiers pour accélérer les détections et améliorer la précision. Les capacités d'atténuation intégrées font de Brand Protector un outil efficace et essentiel pour éviter rapidement les attaques de fraude et d'abus.

Akamai Brand Protector détecte et atténue les attaques ciblées, notamment l'hameçonnage, les usurpations d'identité et l'usurpation de l'identité de marque sur les sites, les réseaux sociaux et les marketplaces d'applications. Avant toute chose, Brand Protector vous permet de préserver vos relations de confiance.

Plus de 50 000 nouveaux sites Web d'hameçonnage sont créés chaque semaine. Brand Protector inspecte chaque jour des milliers de milliards d'activités digitales, sur des sources internes et externes, afin de détecter rapidement et efficacement les atteintes à la marque et aux éléments de marque de votre entreprise, souvent avant le lancement d'une campagne d'attaque.

Pour ce faire, Brand Protector s'attaque au problème des usurpations d'identité grâce à une approche en quatre étapes : collecte d'informations, détection, visibilité et atténuation.

Avantages pour votre entreprise

Détection fiable des attaques
Notre réseau mondial propriétaire et nos flux supplémentaires offrent un avantage unique pour détecter les usurpations d'identité de marque

Précision et vitesse
La rapidité de détection de nos algorithmes peut émettre des alertes avant le lancement des campagnes d'attaque et minimiser les faux positifs

Informations exploitables
Des données complètes sont fournies sous forme d'informations exploitables, avec une évaluation des risques synthétisant la gravité et la portée de l'attaque d'un seul coup d'œil

Visibilité par client
Obtenez un recueil d'informations dédiées à votre marque, vos produits ainsi que les éléments associés sur les sites Web, les réseaux sociaux et les marketplaces d'applications

Facilité d'utilisation
Obtenez des informations en temps réel et initiez la résolution de ce vecteur d'attaque croissant en quelques minutes

Neutralisation et atténuation
Pour rester productif, tirez parti du service de neutralisation intégré dans Brand Protector ou choisissez d'interrompre le trafic avec une alerte de navigation

Collecte d'informations

Les défis de la détection de l'hameçonnage et des attaques d'usurpation d'identité de marque commencent avec la phase de collecte d'informations et de données.

En tant que plateforme cloud mondiale en bordure de l'Internet la plus massivement distribuée, la vision exclusive sur le trafic Web mondial d'Akamai permet d'analyser plus de 788 To de données par jour. La richesse des informations fournies par Brand Protector est renforcée par des flux de données tiers pour une visibilité globale sur les actions des attaquants. De plus, vous pouvez ajouter vos propres URL et domaines afin de les analyser grâce au cloud de détection Brand Protector.

Détection

La puissance et la vitesse de détection de Brand Protector proviennent d'une combinaison de flux d'informations et d'algorithmes d'analyse exclusifs d'Akamai pensée pour accroître la fiabilité de la détection et réduire les faux positifs.

Les attaques de marque automatisent les sites Web malveillants éphémères. Malheureusement, la plupart des technologies ne sont pas assez rapides pour détecter et atténuer ces attaques avant qu'elles n'affectent vos clients. Toutefois, l'approche d'Akamai est différente, car nous traçons le trafic en direct pour détecter les usurpations de l'identité de marque au lieu de nous appuyer sur des listes actualisées ou des flux retardés. Avec Brand Protector, votre équipe de sécurité peut détecter les sites d'hameçonnage dès la première requête HTTP/HTTPS, souvent avant que la campagne n'atteigne vos clients.

Visibilité

L'ingénierie et la conception centrées sur le client offrent à votre équipe un plus grand nombre d'informations essentielles sur la sécurité, le tout dans un seul tableau de bord.

Après réception des informations, les signaux de données sont soumis à une série de détecteurs heuristiques et d'intelligence artificielle. Bien qu'une quantité importante de données et de preuves soit collectée, l'interface utilisateur simplifiée d'Akamai offre à vos clients une compréhension instantanée des menaces actives via les usurpations d'identité.

Les données sur le trafic, la détection et les menaces spécifiques aux clients sont intégrées dans des informations exploitables sur le portail client d'Akamai. Les résultats sont classés en fonction d'un indice de menace résumé. Il vous suffit de cliquer sur une alerte pour afficher les données de menace analysées, notamment le score de confiance, l'indice de gravité, le nombre d'utilisateurs affectés et le calendrier des attaques.

Chaque détection est étayée par des preuves. Notez que vous pouvez afficher le code, les captures d'écran, les indicateurs de détection et les détails du domaine dans un seul écran de détection.

Atténuation

Les services de neutralisation intégrés ferment la boucle pour lutter contre la fraude à la marque.

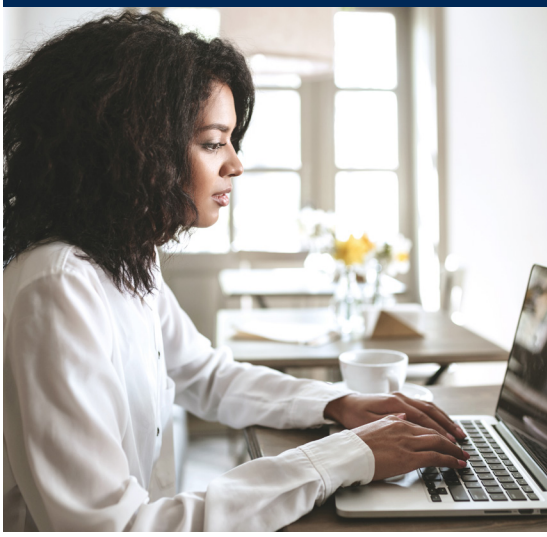
Brand Protector permet à votre équipe d'émettre une demande de neutralisation du site abusif directement depuis l'écran de détection. Les demandes de neutralisation (envoyées à un partenaire tiers d'Akamai) pour Brand Protector joignent automatiquement les preuves de la détection ainsi que des détails supplémentaires pour faciliter l'utilisation. Pour suivre et afficher l'état des mesures d'atténuation, il vous suffit de consulter le portail.

Conçu pour votre marque

Protection de zone
Cette solution de notre portefeuille de protection en bordure de l'Internet permet d'étendre la visibilité de votre équipe de sécurité à la protection précoce de la chaîne d'attaque. Elle recherche de manière proactive les permutations des domaines de votre marque qui pourraient être utilisées pour transformer les clients en victimes d'hameçonnage.

Surveillance des réseaux sociaux
Face à la montée de l'usurpation d'identité de marque sur les réseaux sociaux, notre nouvelle capacité améliorée de surveillance des réseaux sociaux détecte et neutralise la fraude en ligne, protégeant ainsi votre marque et ses clients sur diverses plateformes.

Détection des applications indésirables
La surveillance des marketplaces d'applications est une nouvelle fonctionnalité qui analyse les référentiels d'applications officiels et non officiels pour détecter les applications trompeuses qui abusent de l'identité de la marque, offrant ainsi une défense complète dans le paysage digital.



©2024 Akamai Technologies | Assistance |
| Publication : 11/24