DESCRIZIONE DEL PRODOTTO AKAMAI

Brand Protector - Descrizione del prodotto

Rilevazione e blocco di siti di phishing, falsi store e impersonificazioni dei brand al fine di prevenire danni ai clienti e ridurre il rischio di frodi e violazioni su larga scala.

Un brand riconoscibile genera un valore misurabile sia all'interno che all'esterno dell'organizzazione. Proteggere tutti gli elementi che compongono il brand consente alle organizzazioni di preservare e rafforzare la fedeltà dei clienti, riducendo al minimo le perdite di ricavi, i cali di produttività e i danni alla reputazione legati a recensioni negative dei clienti. Dal punto di vista della sicurezza, un controllo attento su eventuali impersonificazioni del brand interrompe tempestivamente la kill chain, impedendo la raccolta delle credenziali e la violazione degli account.

Non tutti gli attacchi vengono però sferrati frontalmente. Nel web i criminali informatici cercano di sfruttare il brand tramite l'impersonificazione digitale al fine di sottrarre i dati e le credenziali dei clienti e spingere questi ultimi a effettuare pagamenti diretti. L'impersonificazione del brand e gli attacchi di phishing rappresentano un problema sempre più complesso, a causa delle tattiche elusive messe in atto dai malintenzionati che creano campagne di breve durata e cambiano la posizione di attacco per rendere il rilevamento e la mitigazione molto dispendiosi in termini di risorse.

Akamai Brand Protector utilizza uno dei database di intelligence sulle minacce più ampio al mondo, combinando feed di dati proprietari e di terze parti per velocizzare i rilevamenti e migliorare la precisione. Le funzionalità di mitigazione integrate rendono Brand Protector uno strumento efficace ed essenziale per l'identificazione tempestiva di frodi e tentativi di violazioni.

Akamai Brand Protector consente di rilevare e mitigare attacchi mirati, tra cui phishing, impersonificazioni e atti di abuso dei brand, sferrati sui siti web, sui social media e sui marketplace di app. Cosa ancora più importante, Brand Protector permette di salvaguardare le relazioni con i clienti.

Ogni settimana vengono creati più di 50.000 nuovi siti web di phishing. Brand Protector ispeziona migliaia di miliardi di attività digitali al giorno, provenienti da fonti interne ed esterne, per individuare eventuali abusi ai danni dei brand e di singoli elementi dei brand in modo rapido ed efficiente, spesso prima che la campagna di attacco venga effettivamente lanciata.

Per far ciò, Brand Protector risolve il problema delle impersonificazioni fraudolente con un approccio costituito da quattro fasi: intelligence, rilevamento, visibilità e mitigazione.

Vantaggi per le aziende

Rilevamento attendibile degli attacchi
La nostra rete globale proprietaria e i feed aggiuntivi offrono una tecnologia unica di rilevamento delle impersonificazioni dei brand

Precisione e velocità
Il veloce processo di rilevamento tramite i nostri algoritmi è in grado di inviare avvisi prima del lancio delle campagne di attacco e di ridurre i falsi positivi

Utili informazioni
Vengono forniti dati completi, con un punteggio di rischio che riassume in un'unica schermata la gravità e la portata dell'attacco

Visibilità specifica per cliente
Una raccolta dedicata di informazioni per i brand, i prodotti e gli elementi associati in riferimento a siti web, social media e marketplace di app

Facilità d'uso
Informazioni in tempo reale e avvio della risoluzione dei problemi generati da questo vettore di attacco in pochi minuti

Rimozione e mitigazione
Per preservare la produttività, potete sfruttare il servizio di rimozione integrato di Brand Protector oppure scegliere di interrompere il traffico con un avviso di pericolo di navigazione

Intelligence

Il processo di rilevamento degli attacchi di phishing e di impersonificazione dei brand comincia dalla fase di intelligence e raccolta dati.

In qualità di piattaforma edge e cloud distribuita più grande al mondo, l'analisi proprietaria di Akamai sul traffico web mondiale esamina giornalmente più di 788 TB di dati. La straordinaria intelligence di Brand Protector è ulteriormente migliorata dai feed di dati di terze parti, per una visibilità olistica e completa sulle azioni dei malintenzionati. Inoltre, potete aggiungere URL e domini personalizzati per l'analisi tramite il cloud di rilevamento di Brand Protector.

Rilevamento

La potenza e la velocità di rilevamento di Brand Protector si basano su una combinazione di algoritmi di analisi e feed di intelligence proprietari di Akamai, in grado di aumentare l'efficacia del rilevamento e ridurre i falsi positivi.

Gli attacchi ai brand automatizzano la creazione di siti web dannosi e di breve durata. La maggior parte delle tecnologie non è abbastanza veloce da rilevare e mitigare questi attacchi prima che colpiscano i clienti. L'approccio di Akamai è diverso perché, piuttosto che affidarsi a elenchi aggiornati o feed differiti, monitora il traffico in tempo reale per rilevare gli abusi ai danni dei brand. Grazie a Brand Protector, i team di sicurezza possono rilevare i siti di phishing quando viene inviata la prima richiesta HTTP/HTTPS, spesso prima che la campagna raggiunga i clienti.

Visibilità

La progettazione e l'ingegneria improntata al cliente forniscono ai team approfondite informazioni di sicurezza in un'unica vista del dashboard.

Dopo aver ricevuto le informazioni di intelligence, i segnali di dati vengono trasmessi attraverso una serie di rilevatori euristici e di intelligenza artificiale. Sebbene venga raccolta una quantità enorme di dati e prove, l'interfaccia utente semplificata di Akamai assicura ai clienti una comprensione immediata delle minacce attive tramite impersonificazioni.

Il traffico specifico dei clienti, i sistemi di rilevamento e i dati relativi alle minacce vengono sintetizzati in utili informazioni all'interno del portale dei clienti di Akamai. I risultati vengono classificati in base a un punteggio riepilogativo sulla pericolosità delle minacce. Potete fare clic su un avviso per visualizzare i dati analizzati, tra cui il punteggio di affidabilità, il livello di gravità, il numero di utenti interessati e una cronologia degli eventi di attacco.

Ogni rilevamento è corroborato da prove (ad esempio, codici, screenshot, indicatori di rilevamento, ecc.) visualizzabili in un'unica schermata di rilevamento.

Mitigazione

I servizi integrati per la rimozione rappresentano l'ultimo passaggio nella lotta alle frodi ai danni dei brand.

Brand Protector consente al vostro team di inviare una richiesta di rimozione del sito abusivo direttamente dalla schermata di rilevamento. Per una maggiore facilità d'uso, a tali richieste (inviate a un partner di terze parti Akamai) vengono allegate automaticamente le prove a supporto del rilevamento e ulteriori dettagli. Lo stato della mitigazione è consultabile e monitorabile all'interno del portale.

Pensato per il vostro brand

Protezione delle zone
Questa soluzione, inclusa nel nostro portafoglio di prodotti per la protezione dell'edge, consente ai team addetti alla sicurezza di intervenire per fermare tempestivamente gli attacchi informatici nella kill chain. Ricerca proattivamente le varianti dei domini dei brand che potrebbero essere utilizzate per trasformare i clienti in vittime di phishing.

Monitoraggio dei social media
Per contrastare l'aumento delle impersonificazioni dei brand sui social media, la nostra nuova funzionalità avanzata di monitoraggio dei social media rileva e neutralizza le frodi online proteggendo i brand e i clienti su varie piattaforme.

Rilevamento di app non autorizzate
La nuova funzionalità di monitoraggio dei marketplace di app esegue la scansione dei repository di app ufficiali e non ufficiali per rilevare applicazioni ingannevoli che utilizzano l'identità dei brand, offrendo una difesa completa all'interno dell'intero panorama digitale.