Akamai

WHITE PAPER

I vettori di attacco che minacciano la fiducia dei clienti

La sicurezza e la fiducia nei brand non sono mai state così dipendenti l'una dall'altra. Mentre le applicazioni e le API determinano il modo con cui i brand si presentano nel mondo e il volume degli attacchi informatici sale vertiginosamente a livello globale, proteggere le applicazioni digitali senza soffocare le customer experience è diventato il compito principale dei team addetti alla sicurezza in tutto il mondo.

L'affidabilità delle customer experience costruisce la fiducia nei brand, influendo in modo tangibile sulle performance aziendali. Dalle performance dei siti web alla protezione dei dati, inclusi tutti gli aspetti ad essi correlati, le scelte effettuate dalle organizzazioni in materia di sicurezza influiscono troppo spesso negativamente sulle customer experience. I complessi controlli che proteggono le aziende possono causare problemi per i clienti, con conseguente perdita di fiducia e, in ultima analisi, di ricavi.

Le scelte in materia di sicurezza incidono anche sulla crescita e sull'innovazione. Mentre le aziende continuano ad espandersi digitalmente e a migrare dati e applicazioni nel cloud, un numero incalcolabile di criminali si concentra sui vettori di attacco scaturiti da queste decisioni. Le soluzioni per la sicurezza devono ora mirare ad evolversi in anticipo rispetto alle tattiche dei criminali in continua evoluzione e ai sofisticati attacchi multivettore (diversi tipi di attacchi sferrati contemporaneamente o in rapida successione) interagendo con altre soluzioni per proteggere le aziende e mantenere la fiducia risposta dai clienti nei brand.

Quali vettori di attacco dovrebbero essere tenuti nella massima considerazione?

L'ultimo importante obiettivo a rischio: le API

Le applicazioni danno impulso praticamente ad ogni aspetto delle attività aziendali e le API (Application Programming Interface), che collegano parti di software e consentono la comunicazione tra varie applicazioni, sono diventate il nuovo obiettivo preferito dai criminali. Perché? Troppo spesso, le applicazioni e i processi aziendali che coinvolgono le API vengono avviati e distribuiti più velocemente di quanto i team addetti alla sicurezza riescano a valutarli, creando così errori di configurazione e vulnerabilità. Questi difetti sono proprio ciò i criminali cercano: sfruttando la logica aziendale, gli attacchi alle API consentono di accedere agli ambienti aziendali, in cui i criminali possono rubare dati e persino sferrare altri attacchi. Ma i criminali non prendono di mira solo le API che passano attraverso le soluzioni WAF (Web Application Firewall). Anche se autenticate dalle soluzioni WAF, le API possono comunque diventare vulnerabili agli attacchi a indicare che i criminali ora conducono regolarmente operazioni di ricognizione allo scopo di identificare specifiche API da sfruttare.

È importante ricordare che qualsiasi API può potenzialmente essere presa di mira. In settori come quello sanitario, l'interoperabilità dei dispositivi IoT, ad esempio, ha reso le API un enorme bersaglio per i criminali che cercano di rubare informazioni di identificazione personale (PII) o di sferrare attacchi ransomware. Per proteggere le API, è necessario quindi innanzitutto conoscere il proprio patrimonio delle API, ossia tutte le API associate ad una specifica organizzazione.

Akamai API Security aiuta ad inventariare il patrimonio delle API, quindi fornisce visibilità sul comportamento storico di ogni API, in modo da consentire di riconoscere il comportamento normale delle API rispetto ad un comportamento anomalo. Con queste informazioni a disposizione, potete scovare le minacce attive in modo da fermare rapidamente eventuali abusi, prima che i criminali raggiungano i loro obiettivi.

Più sofisticati e più facili da implementare che mai: i bot dannosi

I bot si muovono continuamente nei siti web, anzi, tutte le operazioni di ottimizzazione dei motori di ricerca mirano ad ottenere il loro favore. Tra i bot buoni, si nascondono, tuttavia, bot dannosi che lanciano una serie di attacchi informatici. I bot dannosi sono forse meglio noti per monopolizzare un inventario limitato, ad esempio per acquistare scarpe sportive in edizione limitata o enormi quantità di biglietti per concerti o alberghi, utilizzando comunque più o meno lo stesso metodo quando sovraccaricano le attività aziendali con un numero eccessivo di richieste in un attacco DDoS (Distributed Denial-of-Service), progettato per interrompere le operazioni online delle aziende.

Ciò che molti non sanno è che un attacco DDoS è diventato una forma di attacco relativamente semplice ed economica che viene utilizzata da un nuovo gruppo di criminali per bloccare aziende multimiliardarie e infrastrutture pubbliche critiche, tra cui scuole, ospedali, aeroporti e provider di servizi pubblici. Questi attacchi creano massicce interruzioni di servizio che costano alle vittime enormi quantità di ricavi al minuto. Diversamente dai tradizionali criminali del passato, questi attacchi sono quasi sempre sferrati da sofisticati hacker sostenuti dai governi, hacktivisti politici e criminali informatici professionisti con l'aiuto di botnet, ossia grandi reti di dispositivi connessi (sia dispositivi di utenti che semplici dispositivi IoT), che vengono infettati e controllati dai bot.

I bot vengono utilizzati anche allo scopo di sferrare attacchi di credential stuffing per il controllo degli account. Il credential stuffing si verifica quando un criminale utilizza un elenco di nomi utente e password ottenuti durante una violazione di dati di grandi dimensioni, quindi invia tali credenziali tentando in modo massiccio di accedere ad altre istituzioni. I bot vengono utilizzati per effettuare milioni di tentativi di controllo degli account e, poiché molte persone tendono a riutilizzare le stesse combinazioni di nome utente e password, solo una piccola parte funzionerà. Una volta che il criminale ottiene l'accesso a un account, si tratta di un attacco per il controllo degli account.

Il credential stuffing è solo uno dei tanti metodi utilizzati dai criminali per impossessarsi di account legittimi e, una volta acquisito il controllo di un account, possono sottrarre punti fedeltà e trasferire risorse digitali, prosciugare il saldo dei buoni regalo ed effettuare acquisti fraudolenti utilizzando i dati della carta di credito memorizzata o persino vendere l'intero account a un altro criminale. Se i vostri clienti riscontrano questi problemi, perdono quasi sempre irrimediabilmente la loro fiducia nei vostri confronti. Tuttavia, anche gli attacchi di credential stuffing non riusciti possono risultare dannosi per i brand, perché il traffico dei bot che inonda i siti durante questi tentativi può ridurre significativamente la disponibilità delle risorse e rallentare i tempi di risposta, creando experience frustranti per i clienti e i visitatori dei siti.

Infine, i bot scraper vengono utilizzati sia per scopi buoni che dannosi, ma ciò che è meno ovvio è che la loro presenza può rallentare le performance dei siti e manipolare le metriche necessarie alle aziende per prendere decisioni importanti, rendendo i loro effetti collaterali potenzialmente peggiori per il brand rispetto ai contenuti esfiltrati.

Akamai offre una suite di soluzioni appositamente progettate per mitigare le minacce introdotte dai bot dannosi:

Akamai App & API Protector con Malware Protection è fondamentale per proteggersi dal furto di dati, PII e altre informazioni sugli account e per bloccare gli attacchi DDoS basati sui bot, nonché ransomware, malware e molto altro. Inoltre, questa soluzione consente ai vostri clienti di accedere costantemente alle vostre proprietà web e garantisce che le performance del sito non rallentino quando si verifica un attacco.

Akamai Bot Manager rileva il traffico dei bot e mitiga i bot dannosi sull'edge, utilizza modelli di intelligenza artificiale per analizzare il comportamento dei bot e implementa algoritmi di browser fingerprint e di apprendimento automatico (ML) per rendere il rilevamento sempre più accurato, riducendo i problemi per gli utenti e proteggendoli da attività fraudolente.

Akamai Content Protector impedisce agli scraper di sottrarre contenuti web che possono poi essere utilizzati per scopi illeciti, mitigando, al tempo stesso, il deterioramento delle performance del sito. Con il rilevamento basato sull'apprendimento automatico, l'attività potenzialmente dannosa dei bot scraper viene classificata in base al rischio per fornire la risposta appropriata.

Un'altra soluzione fondamentale per proteggere i clienti è migliorare la sicurezza dell'accesso agli account. Akamai Account Protector contrasta le frodi perpetrate dall'uomo, spesso coordinate dai bot, consentendo, al tempo stesso, ad utenti fidati un accesso semplice e sicuro al sito, incoraggiandoli a rimanere connessi più a lungo e a ritornarvi spesso.

Il costo degli script dannosi: le minacce lato client

Analogamente ai bot, gli script di terze parti eseguono perlopiù operazioni lecite, consentendo di utilizzare funzionalità, strumenti di marketing, analisi e molto altro per migliorare, in generale, le user experience (UX) complessive, ma trasformano anche il browser web in una superficie di minaccia critica sul lato client.

Le minacce lato client mirano a indurre i clienti ad accedere a contenuti dannosi, sfruttando i punti deboli delle applicazioni in esecuzione sul computer gestito direttamente dall'utente (di solito, il cliente), in questo caso denominato client. La sicurezza lato client comprende quindi le tecnologie e le policy utilizzate per proteggere i clienti da attività dannose che si verificano sulle pagine web.

Gli attacchi basati su script possono causare notevoli danni finanziari alle organizzazioni e diminuire la fiducia nei confronti di clienti, partner e responsabili del trattamento dei dati delle carte di pagamento. Non sorprende che la sicurezza lato client sia un obiettivo chiave dei nuovi requisiti previsti dallo standard per la sicurezza dei dati nel settore delle carte di pagamento (PCI DSS v4.0). Per soddisfare i requisiti di conformità, le organizzazioni che elaborano carte di pagamento online devono sapere quali script vengono eseguiti sui loro siti, quando cambiano e quando non vengono più eseguiti.

Difendersi da questi attacchi non è facile. Gli script di terze parti sono numerosi e cambiano continuamente, il che li rende estremamente difficili da monitorare. Gli attacchi basati su script assumono anche varie forme, come il web skimming e il formjacking. Interi gruppi di criminali (di cui il più noto è Magecart) si sono organizzati attorno a questo tipo di tecniche per rubare dati delle carte di pagamento e PII.

Nel nostro mondo fatto di pagamenti digitali, shopping e ricerche online, la sicurezza lato client è più importante che mai, soprattutto al momento del checkout e nelle pagine di pagamento, in cui vengono raccolti dati personali e finanziari. Per difendervi dagli attacchi, dovete disporre di una visibilità su tutti gli script in esecuzione sul vostro sito, della capacità di rilevare eventuali comportamenti sospetti e di misure di mitigazione in atto. Akamai offre una soluzione specifica contro queste minacce:

Client-Side Protection & Compliance mantiene la privacy e la fiducia dei clienti all'interno del browser proteggendo tutti gli utenti dagli attacchi lato client come web skimming, formjacking e Magecart.

Proteggere l'infrastruttura per proteggere le customer experience

Le customer experience sono incentrate sull'infrastruttura digitale sottostante che potenzia tutto ciò che riguarda il brand. La sicurezza, l'affidabilità e le performance del DNS garantiscono ai clienti di accedere ai servizi ogni volta che ne hanno bisogno. I sistemi DNS essenzialmente equivalgono alla vostra presenza online. Se vengono interrotti, si blocca anche la vostra presenza digitale. Ecco perché i criminali prendono continuamente di mira i sistemi DNS delle loro vittime con attacchi DDoS. Considerando il campo d'azione estremamente competitivo che tutti i settori si trovano ad affrontare, è richiesta niente di meno che una disponibilità DNS ininterrotta e un tempo di attività del 100% per garantire ai clienti esistenti e a quelli potenziali il meglio che un brand ha da offrire.

Akamai offre un portfolio di soluzioni top di gamma per proteggere la vostra infrastruttura digitale da vari attacchi DDoS:

Per difendersi al meglio dagli attacchi DDoS, Akamai Prolexic offre più opzioni di protezione, inclusi vari scrubbing center dislocati in oltre 32 sedi globali, nonché una straordinaria capacità di difesa dedicata di 20 Tbps.

Akamai Edge DNS offre una soluzione di DNS autoritativo completa e personalizzata, che utilizza la portata, la sicurezza e la capacità di Akamai Connected Cloud per gestire le zone del DNS.

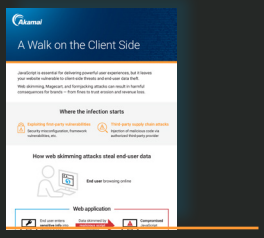
Akamai Shield NS53, una soluzione proxy DNS bidirezionale con applicazione dinamica delle policy di sicurezza, può essere utilizzata per proteggere i principali componenti dell'infrastruttura DNS di origine (on-premise, nel cloud o in ambienti ibridi) dagli attacchi di esaurimento delle risorse.

Noi e voi insieme per garantire la fiducia dei clienti

Noi di Akamai ci concentriamo sul modo con cui i brand si presentano nel mondo da oltre 25 anni. Dai nostri esordi pionieristici nel settore delle reti per la distribuzione di contenuti, abbiamo risolto i problemi di velocità per i primissimi negozi digitali. Negli ultimi dieci anni, abbiamo utilizzato la visibilità del traffico offerta dalla nostra rete di distribuzione di contenuti, una delle più grandi al mondo, per monitorare e analizzare quotidianamente le minacce, una ricerca che ci consente di evolvere organicamente le nostre soluzioni per la sicurezza man mano che i vettori di attacco continuano a crescere e cambiare. In qualità di partner chiave per la sicurezza dei nostri clienti, condividiamo l'impegno a mantenere le loro attività operative e a proteggere le loro customer experience, offrendo la sicurezza necessaria per provare nuove experience digitali leader dei relativi settori.

Passi successivi

Ecco alcune risorse utili per stabilire qual è il passo migliore da compiere per proteggere il vostro brand:



Rafforzate l'integrità delle pagine web con la protezione lato client.

Adottate una sicurezza centralizzata senza compromessi per siti web, applicazioni e API.

Scoprite le principali considerazioni da tenere presente per una strategia di gestione dei bot.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn.
Data di pubblicazione: 06/24.