Lo chef della cybersicurezza:

le migliori ricette per la resilienza contro gli attacchi DDoS al livello 7

Sommario

Introduzione

Elaborare il giusto sistema di difesa dagli attacchi DDoS (Distributed Denial-of-Service) può risultare impegnativo anche per gli addetti alla sicurezza più esperti, specialmente nel caso di attacchi DDoS al livello 7, che comportano ulteriori complicazioni. A tal proposito, può risultare utile consultare alcune istruzioni dettagliate con diversi approcci per le diverse minacce, ovvero un "ricettario" per contrastare gli attacchi DDoS al livello 7.

Gli attacchi DDoS vengono preparati in modo diverso dai vari criminali. Gli attacchi ai livelli 3 e 4 sono basati maggiormente sulla forza. Chi ha maggiore capacità di rete: l'autore dell'attacco o il sistema di difesa? Gli attacchi al livello 7, invece, prendono di mira il livello di applicazioni del modello OSI (Open Systems Interconnection), che è responsabile direttamente dell'interazione con le applicazioni software, nell'intento di sovraccaricare un server web, un database o un'applicazione sfruttando le capacità, l'allocazione della memoria o le vulnerabilità presenti nel modo con cui questi sistemi gestiscono le richieste.

Gli attacchi DDoS al livello 7 presentano, pertanto, sfide specifiche in termini di mitigazione poiché queste richieste, spesso, sembrano traffico legittimo, il che rende difficile filtrare le richieste dannose senza influire sugli utenti legittimi. Inoltre, la disponibilità dell'automazione e le risorse cloud hanno reso per i criminali più semplice che mai sferrare questi attacchi rapidamente e su larga scala.

In questo articolo, verranno descritte le sfide legate alla mitigazione degli attacchi DDoS al livello 7 con "ricette" dettagliate che includono le tecniche e gli strumenti utilizzati dai criminali, le tattiche di rilevamento e mitigazione necessarie per contrastarli, nonché suggerimenti sul recupero e sull'analisi post-evento.

Grazie ad una lunga tradizione nei settori della delivery di contenuti e della cybersicurezza e ad una piattaforma cloud distribuita con oltre 4.200 PoP (Point-of-Presence) in tutto il mondo, Akamai può vantare una prospettiva esclusiva sugli odierni attacchi DDoS. Poiché gli attacchi DDoS a livello di applicazioni continuano a diventare più complessi e multilivello, è importante disporre di questa prospettiva e di una strategia di difesa approfondita. È proprio questo che forniamo:

questo "ricettario" fornisce la migliore ricetta per il successo ai professionisti della sicurezza in prima linea che hanno bisogno di assistenza con una specifica minaccia o vulnerabilità oppure ai CISO che cercano di migliorare il proprio sistema di sicurezza.

Esempi e obiettivi comuni degli attacchi DDoS al livello 7

Gli attacchi DDoS al livello 7 prendono di mira il livello principale del modello OSI, ossia il livello di applicazioni. Questi attacchi tendono a sovraccaricare le risorse di un obiettivo sfruttando il modo con cui le applicazioni web elaborano le richieste. Gli obiettivi comuni degli attacchi DDoS al livello 7 includono:

Server web: i criminali prendono di mira i server web per interrompere la delivery dei contenuti agli utenti legittimi, causando il rallentamento dei siti web o facendoli diventare completamente inaccessibili.

Applicazioni web: le applicazioni basate su database o servizi di back-end sono vulnerabili agli attacchi DDoS al livello 7 perché questo tipo di attacchi può sfruttare le vulnerabilità presenti nel modo con cui le applicazioni analizzano le query, elaborano le richieste o gestiscono le sessioni.

API (Application Programming Interface): le API sono componenti fondamentali delle applicazioni mobili e dei servizi web moderni. I criminali prendono di mira le API per interrompere l'interazione tra diversi servizi software, influendo sulle funzionalità delle applicazioni basate su queste API.

Servizi DNS: anche se gli attacchi DNS possono verificarsi su altri livelli, gli attacchi al livello 7 possono "bombardare" il servizio DNS con richieste dannose per interrompere la risoluzione dei nomi di dominio, causando diffusi problemi di accessibilità. L'incremento dell'adozione del DNS tramite il protocollo HTTP/TLS può determinare un aumento di tali attacchi.

Server e-mail: prendere di mira i server e-mail può interrompere le comunicazioni, influendo sulle e-mail in entrata e in uscita.

Gateway di pagamento e servizi finanziari: si tratta di obiettivi allettanti per i criminali che cercano di interrompere le transazioni e di seminare il caos nelle operazioni finanziarie.

I rapporti sullo stato di Internet (SOTI) e le informazioni sulla sicurezza di Akamai esaminano regolarmente il panorama degli attacchi DDoS al livello 7 in continua evoluzione, evidenziando la diversità dei vettori di attacco e i settori maggiormente a rischio.

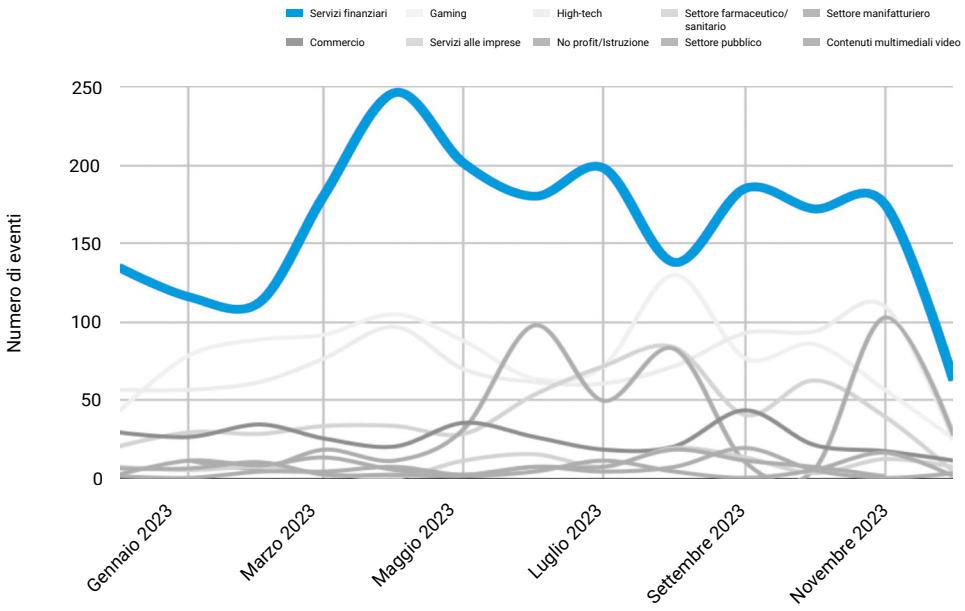
Vettori di attacco

- Attacchi alle applicazioni web e alle API: i criminali, di solito, prendono di mira i punti di accesso ai siti web, inclusi gli endpoint delle API che, generalmente, non vengono memorizzati nella cache a causa del loro contenuto o della loro configurazione. Alcuni di questi percorsi comunemente presi di mira includono: "/", "/home", "/en-us", "/pricing/", ecc.
- È frequente vedere vettori di attacco simili ai seguenti:
  • Attacchi HTTP GET/POST flood sulle home page
  • Attacchi HTTPS GET flood su stringhe di query e percorsi randomizzati
  • Attacchi Slow Read
  • Attacchi flood basati sul caricamento di file di grandi dimensioni

Inoltre, anche se il numero delle aziende che subiscono un attacco DDoS aumenta di anno in anno, oggi il "come" aumenta è cambiato. In primo luogo, il tipo e il volume delle proprietà presi di mira sono cambiati. Ad esempio, invece di 10 attacchi sferrati contro endpoint uguali o simili, ora possiamo osservare 100 attacchi diretti contro diversi IP nello spazio della rete. Questi attacchi non prendono di mira solo il livello 3, ma anche contemporaneamente il livello 7.

Settori presi di mira

Il numero degli attacchi DDoS (Distributed Denial-of-Service) contro i servizi finanziari, il settore del gioco d'azzardo e il settore manifatturiero ha registrato un'impennata nel 2023, in particolar modo nell'area EMEA, in cui ha superato quello di tutte le altre aree geografiche messe insieme.

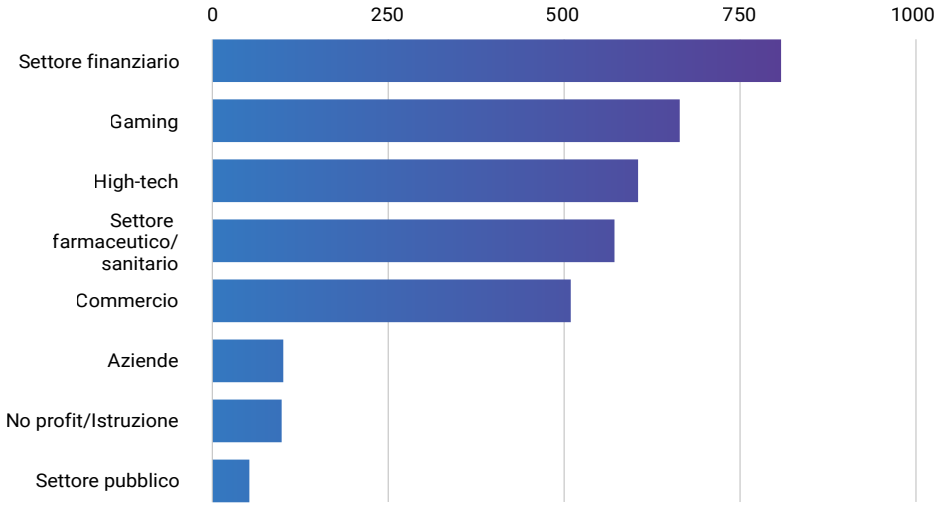


Gli attacchi DDoS non sono un fenomeno passeggero, marzo 2024

I servizi finanziari, in particolare, sono diventati un bersaglio sempre più preso di mira dagli attacchi DDoS al livello 7. Dal 2021, Akamai ha osservato un chiaro e notevole aumento nel numero di attacchi DDoS contro le società di servizi finanziari. Nel 2023, oltre un terzo (il 35%) degli attacchi sferrati contro tutti i settori ha colpito il settore dei servizi finanziari, rendendolo un bersaglio più allettante del settore del gaming. Dall'analisi di Akamai, risulta che il settore bancario ha subito il 63% degli attacchi DDoS a livello globale. Quasi i tre quarti (il 72%) degli attacchi nell'EMEA e il 91% nell'area APAC si sono focalizzati sul settore bancario. Nelle Americhe, invece, gli attacchi DDoS sono stati sferrati in modo più uniforme contro il settore bancario e quello assicurativo, nonché contro altre società di servizi finanziari.

Americhe: i servizi finanziari hanno subito il 28% degli attacchi DDoS

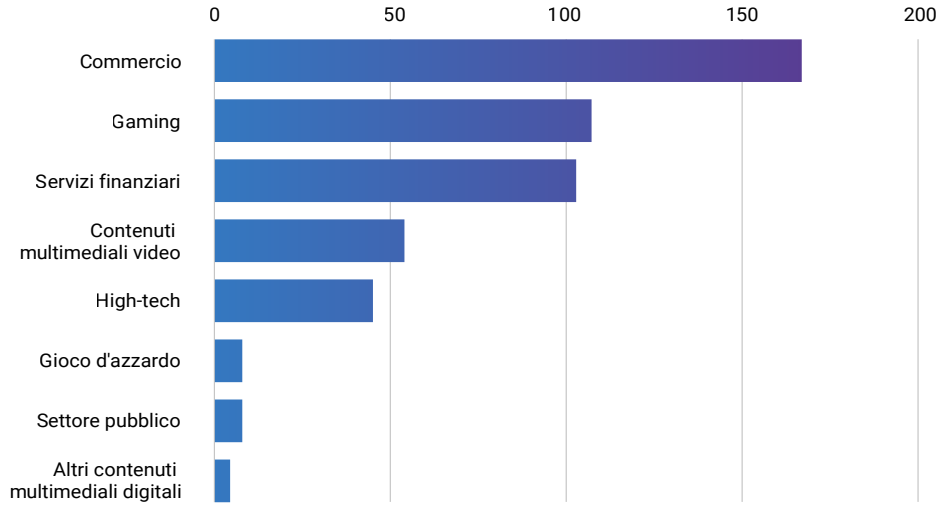
Giugno 2023 - Dicembre 2023



Gli attacchi DDoS non sono un fenomeno passeggero, marzo 2024

APAC: i servizi finanziari hanno subito l'11% degli attacchi DDoS

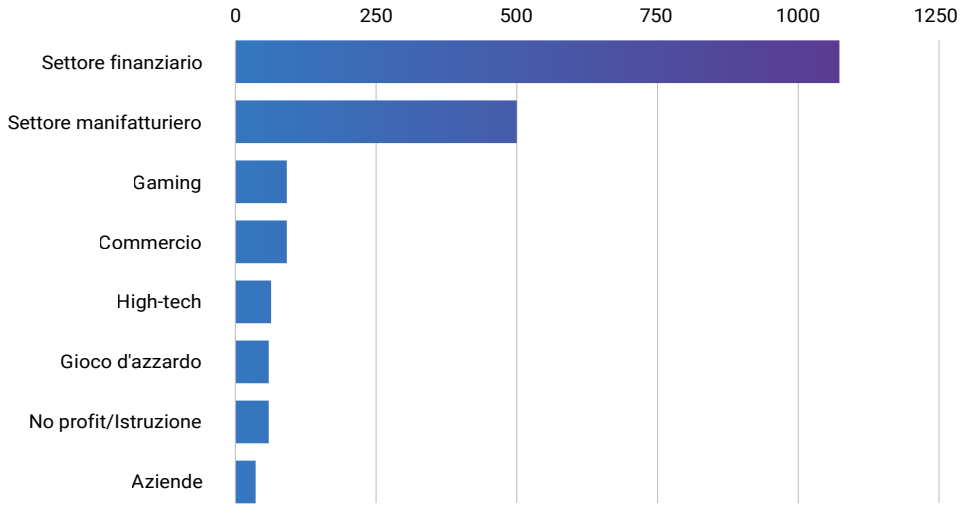
Giugno 2023 - Dicembre 2023



Gli attacchi DDoS non sono un fenomeno passeggero, marzo 2024

EMEA: i servizi finanziari hanno subito il 66% degli attacchi DDoS

Giugno 2023 - Dicembre 2023



Gli attacchi DDoS non sono un fenomeno passeggero, marzo 2024

In un recente esempio di un sofisticato attacco DDoS al livello 7 che ha preso di mira uno dei clienti di Akamai che opera nel settore dei servizi finanziari, i criminali informatici hanno utilizzato un metodo di automazione per creare un attacco altamente distribuito. Questo attacco di tipo HTTP GET flood ha preso di mira URL perlopiù non memorizzabili nella cache (come quelli di endpoint di accesso e home page). Utilizzando vari controlli proattivi, questo attacco è stato mitigato senza influire in alcun modo sull'origine del cliente. Questa mappa termica con le origini degli attacchi sottolinea il crescente utilizzo di fornitori di servizi cloud, nodi di uscita Tor e nodi proxy anonimi o aperti:

Attacchi DDoS provenienti da un sistema autonomo (AS)

Visualizzazione di un attacco a livello di applicazioni sferrato contro un'istituzione finanziaria nel 2024 in più di 100 paesi, che è stato mitigato con l'aiuto di Akamai

Gli autori di attacchi DDoS riescono a creare e coordinare un'infrastruttura di attacco ampiamente distribuita, sfruttando gli indirizzi IP dinamici grazie alla presenza di reti di vaste dimensioni dislocate in diversi paesi e aree geografiche in tutto il mondo.

Tecniche e strumenti utilizzati dai criminali

Sfortunatamente, gli autori di attacchi DDoS e i loro metodi non rimangono invariati. Man mano che i criminali continuano a trovare modi per trarre profitto dalle loro azioni, adattano le loro tecniche, utilizzando nuovi strumenti e trovando nuovi metodi di attacco. Ci sono moltissimi fattori che dimostrano questa evoluzione.

Automazione: i criminali utilizzano bot e script automatizzati per imitare il comportamento degli utenti legittimi, rendendo il rilevamento molto più difficoltoso. Inoltre, i criminali stanno adottando gli algoritmi di apprendimento automatico, che sono in grado di adattarsi e di eludere i metodi di rilevamento tradizionali.

Attacchi multivettore: i criminali utilizzano sempre più strategie multivettore, combinando diversi tipi di attacchi (come gli attacchi GET e POST flood) e minacce al DNS (come gli attacchi di amplificazione e frammentazione) con altri metodi per sovraccaricare le risorse della rete e delle applicazioni.

Attacchi alle API: poiché le aziende si basano sempre più sulle API per le loro applicazioni, i criminali stanno trovando nuove opportunità di sfruttare le vulnerabilità delle API nei loro attacchi DDoS. Questi attacchi mirano ad esaurire le risorse del server, richiedendo simultaneamente migliaia di connessioni, o a sfruttare i difetti di logica, causando interruzioni nei servizi.

Sfruttamento dei dispositivi IoT: la proliferazione di dispositivi IoT scarsamente protetti apre il campo ad un esercito di botnet. Questi dispositivi vengono spesso violati e utilizzati per sferrare massicci attacchi DDoS, sfruttando la loro connettività di rete e la loro potenza computazionale.

Aumento della complessità

Parallelamente alla diffusione di questi nuovi strumenti e tecniche, si è registrato un corrispondente aumento della complessità e della frequenza degli attacchi DDoS, in cui i criminali hanno utilizzato metodi sofisticati per bypassare i sistemi di difesa tradizionali. Tra le tendenze di maggior rilievo, figurano le seguenti:

Crittografia: una notevole svolta verso gli attacchi DDoS basati su HTTPS ha reso la mitigazione più difficoltosa. Questi attacchi, che sono crittografati, si spacciano per traffico legittimo, il che li rende più difficili da rilevare e filtrare perché i sistemi tradizionali di protezione dagli attacchi DDoS presentano limitazioni nella decrittografia del traffico SSL/TLS a livello di applicazioni.

Botnet e proxy: considerando la notevole crescita delle botnet DDoS e la prevalenza ad utilizzare proxy anonimi da parte dei criminali, le richieste ora vengono inviate da una moltitudine di indirizzi IP (in genere, più di 10.000 indirizzi IP per attacco). I criminali utilizzano questa strategia per bypassare le misure di mitigazione che considerano le richieste provenienti da un solo IP. La prevalenza delle piattaforme di hosting su cloud e l'adozione di servizi basati su cloud rendono solo più semplice preparare questi attacchi ad alta intensità e altamente distribuiti.

Attacchi DDoS provenienti da un sistema autonomo (AS)

Visualizzazione di un recente attacco DDoS a livello di applicazioni (650.000 transazioni al secondo (TPS), 20 Gbps, oltre 9 miliardi di richieste in totale) sferrato contro un cliente di Akamai che opera nel settore dei servizi finanziari

Un approccio emergente attualmente utilizzato dagli addetti alla sicurezza consiste nel tracciare le richieste per ogni fingerprint TLS, che è costituito da più segnali di livello TLS, come i tipi di sequenze cifrate e il relativo ordine. Anche se questo approccio è suscettibile ai falsi positivi, se usato correttamente può fornire una mitigazione più efficace nel caso in cui un criminale utilizza vari computer e diversi indirizzi IP perché lo stesso software viene installato sui dispositivi violati. Questi dispositivi presentano caratteristiche ambientali simili, una delle quali è la libreria TLS condivisa.

Gli autori di attacchi DDoS sono in grado di creare e coordinare un'infrastruttura di attacco estremamente distribuita per la maggior parte dei fornitori di servizi cloud.

Provenienza degli ingredienti

Mentre gli strumenti disponibili sul mercato cambiano frequentemente, l'evoluzione delle tecniche di attacco suggerisce una svolta verso metodi più sofisticati e meno rilevabili, che includono:

- **Dispositivi IoT violati:** i criminali continuano ad utilizzare dispositivi IoT violati nelle botnet come metodo per sferrare attacchi DDoS su larga scala, il che evidenzia la costante vulnerabilità di questi dispositivi.
- **Servizi DDoS-for-hire:** la disponibilità dei servizi DDoS-for-hire ha reso più facile lanciare gli attacchi, consentendo a persone senza vaste conoscenze tecniche di sferrare attacchi su larga scala.

- **Tecniche di elusione:** ora vengono utilizzate più comunemente avanzate tecniche di elusione, come i parametri randomizzati delle intestazioni e gli argomenti dinamici delle richieste. Queste tecniche mettono alla prova i tradizionali approcci di rilevamento e mitigazione rendendo più difficile distinguere il traffico dannoso dalle richieste legittime.

Vulnerabilità solitamente sfruttate negli attacchi di questo tipo

Le vulnerabilità sfruttate dai criminali negli attacchi DDoS al livello 7 sono spesso correlate ai modi con cui le applicazioni web elaborano gli input degli utenti e gestiscono i dati. Per mitigare queste vulnerabilità, è fondamentale utilizzare una combinazione di misure di sicurezza.

Recentemente, una delle vulnerabilità più significative che sono state sfruttate dai criminali durante il lancio di attacchi DDoS a livello di applicazioni è stata la vulnerabilità HTTP/2 Rapid Reset pubblicata alla fine del 2023. Questi attacchi hanno sfruttato una falla presente nel protocollo HTTP/2, che è fondamentale per il funzionamento di Internet e di tutti i siti web. Lo sfruttamento di questa vulnerabilità ha portato ad un incremento complessivo del 65% nel traffico degli attacchi HTTP di tipo DDoS in un trimestre rispetto a quello precedente a sottolineare la gravità e l'impatto degli attacchi che sfruttano questa vulnerabilità.

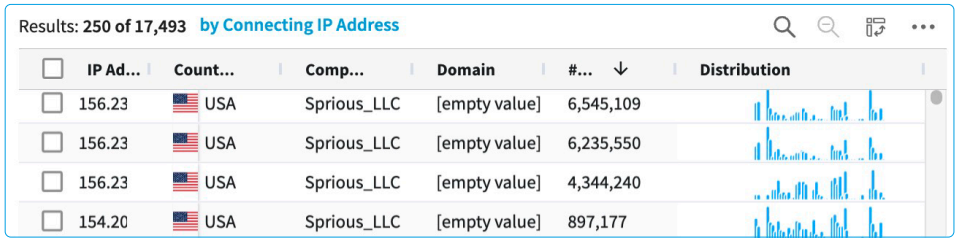
Questa particolare vulnerabilità ha consentito ai criminali di causare un maggior impatto utilizzando le piattaforme di cloud computing e sfruttando il protocollo HTTP/2, il che ha consentito di sferrare attacchi DDoS ipervolumetrici con botnet relativamente piccole. Tra i settori più colpiti da questi attacchi, figuravano i seguenti: gaming, IT, criptovalute, software informatici e telecomunicazioni, mentre i primi paesi da cui si sono originati questi attacchi erano, nell'ordine: Stati Uniti, Cina, Brasile, Germania e Indonesia.

In risposta a questa situazione, grazie ad uno sforzo congiunto a livello di settore è stata divulgata la vulnerabilità HTTP/2 Rapid Reset (CVE-2023-44487) per far luce sugli attacchi DDoS basati su questa vulnerabilità, che ha preso di mira vari provider, tra cui i principali fornitori di servizi cloud e CDN.

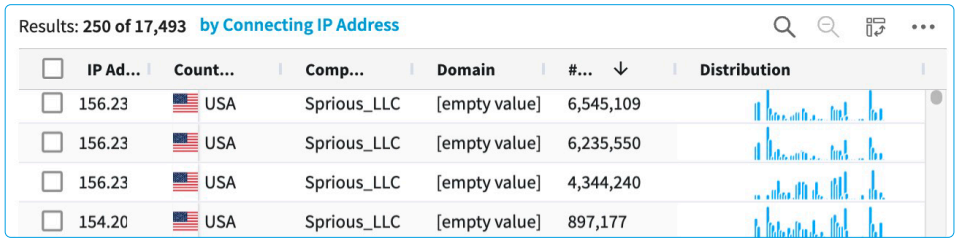
Esempi reali: l'utilizzo dell'automazione in un attacco DDoS

I criminali spesso utilizzano più strumenti DDoS per sferrare gli stessi attacchi DDoS, ciascuno dei quali utilizza diverse tecniche combinate una con l'altra per bypassare i prodotti per la sicurezza o, perlomeno, per renderli meno efficienti. Un esempio di questo tipo di attacco viene descritto di seguito tramite Akamai Web Security Analytics.

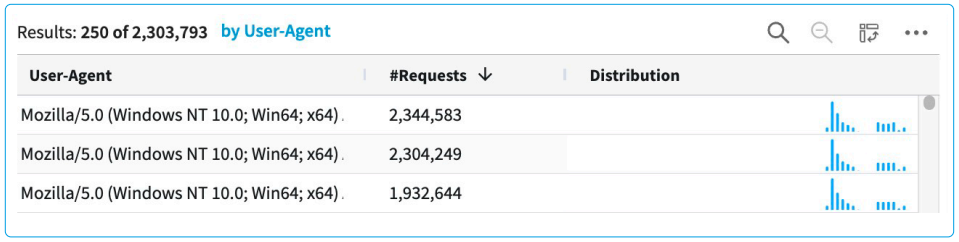
- Attacco proveniente da più di 17.000 indirizzi IP



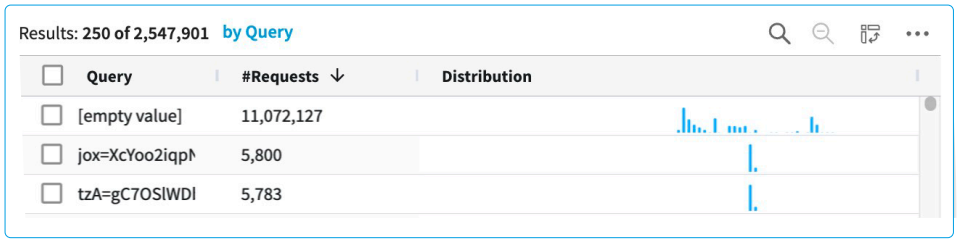
- Attacco proveniente da più di 400 reti



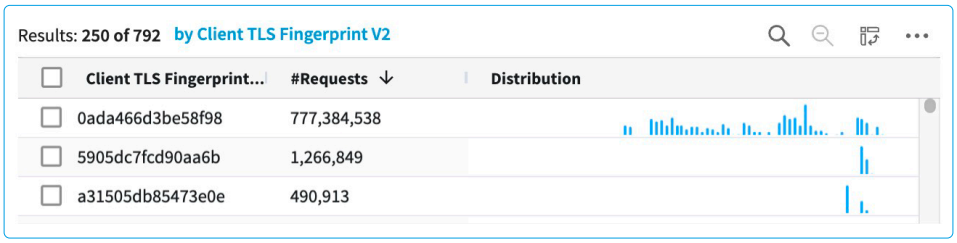
- 2.303.793 user agente univoci



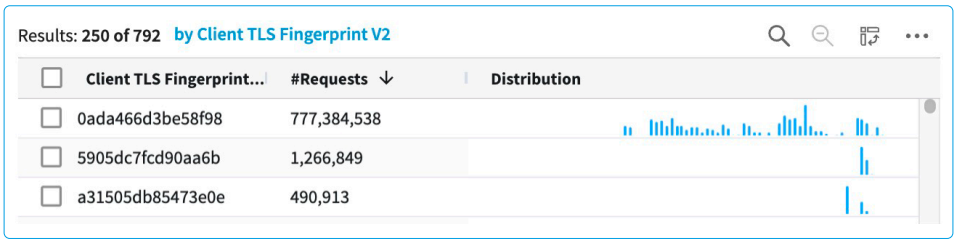
- 2.547.901 stringhe di query univoche e casuali



- Rotazione delle intestazioni HTTP (ad es. Accept-Language, Referer)



- Rotazione delle impostazioni TLS



La mitigazione di questi attacchi sofisticati richiede una strategia di protezione multilivello. Al riguardo, può risultare utile implementare controlli proattivi e reattivi, come una combinazione avanzata di corrispondenze di richieste e caratteristiche del traffico di origine nella limitazione della velocità, o controlli della reputazione di origine.

Avversari sempre più sofisticati: l'impersonificazione dei segnali TLS

Da osservazioni recenti, è emerso che i criminali utilizzano più frequentemente i segnali TLS nei propri strumenti DDoS per eludere i sistemi di rilevamento facendo sembrare che tali connessioni provengano da browser Chrome legittimi. Invece di utilizzare una versione headless di Chrome ad elevato utilizzo di risorse, che potrebbe rallentare l'attacco, i criminali potrebbero impiegare una versione modificata della libreria TLS per impostare e impersonificare i segnali TLS di un browser legittimo. Anche se alcuni strumenti sono progettati per replicare il fingerprinting TLS, non sono comunemente presenti negli strumenti utilizzati per gli attacchi DDoS. L'utilizzo di questo tipo di attacchi implica l'aumento delle competenze tecniche e una profonda conoscenza dei sistemi di difesa da parte dei criminali: ecco perché le strategie di difesa dagli attacchi DDoS al livello 7 devono includere l'esecuzione di ricerche regolari sulle ultime tendenze negli attacchi. Inoltre, questo aspetto sembra suggerire una maggiore diffusione degli strumenti DDoS che includono lo spoofing TLS.

Uno sguardo alla valutazione dei rischi e all'identificazione delle vulnerabilità

Potete migliorare notevolmente la strategia di mitigazione degli attacchi DDoS al livello 7 identificando le vostre risorse critiche e stabilendo se potrebbero risultare vulnerabili ad un attacco DDoS. Questa valutazione dei rischi aiuta a dare priorità alle risorse da proteggere in base alla loro importanza e al loro livello di vulnerabilità. Comprendendo i potenziali vettori di attacco e il loro impatto, le organizzazioni possono implementare specifiche contromisure, come la limitazione della velocità, le soluzioni WAF (Web Application Firewall) e l'analisi comportamentale, per mitigare i rischi in modo efficace. Inoltre, una valutazione continua dei rischi consente di realizzare una strategia di difesa in grado di evolversi per rispondere alle nuove minacce e ai mutevoli requisiti aziendali.

Diversi settori e aziende potrebbero adottare un approccio diverso alla valutazione dei rischi per gli attacchi DDoS a livello di applicazioni, come, ad esempio:

> **E-commerce:** prima di un importante evento di vendita, una valutazione dei rischi potrebbe identificare il processo di pagamento come una vulnerabilità critica. Le misure di mitigazione potrebbero includere l'implementazione di una soluzione WAF (Web Application Firewall) e la limitazione della velocità per proteggere il servizio.
>
> **Servizi finanziari:** per un'applicazione di banking, la valutazione dei rischi potrebbe individuare la pagina di accesso come il principale bersaglio degli attacchi DDoS. La banca in questione potrebbe, quindi, utilizzare una combinazione di funzioni di rilevamento dei comportamenti e limitazione della velocità in base agli endpoint per distinguere gli utenti legittimi dal traffico degli attacchi.

Comprendere le specifiche vulnerabilità consente di attivare la difesa dei sistemi presi di mira e di migliorare i servizi critici durante un attacco.

Il troppo stroppia: ruoli e responsabilità

Stabilire chiaramente ruoli e responsabilità è un passaggio cruciale in un'efficace strategia di difesa dagli attacchi DDoS al livello 7 perché massimizza l'opportunità di rispondere in modo coordinato ed efficiente in caso di attacco. Senza una chiara definizione dei ruoli, le risposte possono diventare caotiche, creando una sovrapposizione delle mansioni e lacune nel sistema di difesa. La definizione delle responsabilità aiuta ad identificare le specifiche attività di ciascun membro del team, dal monitoraggio del traffico e dall'identificazione delle anomalie all'implementazione di strategie di mitigazione e alla comunicazione con le parti interessate. Questa coordinazione aiuta a minimizzare l'impatto degli attacchi, a mantenere la disponibilità del servizio e a proteggere le risorse critiche.

In effetti, se sono presenti troppi responsabili decisionali senza ruoli chiari, durante un attacco DDoS si possono verificare ritardi nelle risposte. Ad esempio, se i team addetti alle operazioni di rete e alla cybersicurezza decidono in modo indipendente sui diversi approcci di mitigazione senza coordinarsi, potrebbero inavvertitamente neutralizzare i loro sforzi reciproci o trascurare alcune vulnerabilità critiche. La giusta strategia richiede la definizione dei ruoli, come un responsabile designato per la risposta agli incidenti, il coordinatore delle comunicazioni e il team addetto alle risposte tecniche, per garantire azioni tempestive e unificate contro gli attacchi, minimizzando i problemi di downtime e semplificando l'analisi post-incidente.

Come scegliere gli strumenti giusti in cucina

Rilevare e mitigare un attacco a livello di applicazioni possono risultare operazioni impegnative perché è difficile distinguere il traffico legittimo da quello dannoso. Per rispondere a queste minacce in continua evoluzione, si consiglia di adottare un approccio alla difesa multilivello:

- **Scegliete un approccio always-on anziché on-demand:** assicuratevi che i controlli di sicurezza DDoS siano sempre attivi e aggiornate i piani di risposta agli incidenti per rispondere tempestivamente alle minacce emergenti.
- **Stabilite un'architettura resiliente e affidabile:** anticipate un single point of failure in quanto i criminali prenderanno probabilmente di mira più servizi, inclusi DNS, applicazioni web, API e infrastrutture di rete e data center. L'utilizzo dell'architettura appropriata è cruciale per la protezione dagli attacchi DDoS al livello 7. Queste considerazioni sull'architettura potrebbero includere la scelta di un sistema di protezione dagli attacchi DDoS sull'edge o sulla CDN, che è sempre disponibile. Non sopravvalutate la vostra affidabilità. La portata degli odierni attacchi DDoS può sovraccaricare facilmente la maggior parte delle infrastrutture.
- **Valutate gli SLA offerti dal vostro provider** e allineateli alla vostra strategia.
- **Verificate la capacità di risposta del vostro provider:** scegliete un provider che riesamina regolarmente i suoi componenti di rete critici e che valuta diversi meccanismi di protezione dagli attacchi DDoS per ottenere informazioni sulla sua efficacia contro i metodi di attacco correnti.
- **Verificate il vostro playbook di risposta agli attacchi DDoS:** riunite il personale IT e operativo, nonché i team addetti alla sicurezza e alle comunicazioni con i clienti per ottimizzare il loro livello di preparazione in caso di attacco.
- **Protezione dagli attacchi DDoS di emergenza:** in caso di emergenza, dovete predisporre un piano per contattare un provider di soluzioni di mitigazione degli attacchi DDoS. Se potete rivolgervi ad un partner del vostro vendor per la protezione dagli attacchi DDoS, tenete a portata di mano il suo numero di assistenza telefonica.

Le ricette per efficaci operazioni di rilevamento e mitigazione

Un'efficace protezione dagli attacchi DDoS al livello 7 richiede diverse strategie di rilevamento e mitigazione. Esistono varie metodologie da applicare, ognuna delle quali con propri punti di forza e considerazioni principali.

Rilevamento basato su comportamenti/anomalie

Punti di forza: questo approccio si basa sull'utilizzo dell'apprendimento automatico e dell'analisi statistica per comprendere i normali modelli di traffico e per identificare, quindi, le deviazioni che potrebbero indicare un attacco DDoS. Questo approccio risulta estremamente efficace contro attacchi complessi e sconosciuti.

Considerazioni: un rilevamento efficace richiede un periodo di apprendimento anche di diverse settimane per stabilire uno standard di riferimento per un traffico "normale", durante il quale il rilevamento potrebbe non risultare così efficace. Il modello potrebbe restituire falsi positivi se non addestrato accuratamente.

Rilevamento basato su velocità e throughput

Punti di forza: semplice da implementare, questo metodo si basa sul monitoraggio della velocità e del volume di richieste, attivando avvisi o processi di mitigazione se il traffico supera le soglie predefinite. È un metodo efficace per identificare rapidamente gli attacchi volumetrici su larga scala.

Considerazioni: i picchi di traffico legittimo, come quelli registrati nel caso di eventi promozionali, possono essere erroneamente considerati attacchi DDoS. Questo metodo potrebbe non rilevare gli attacchi a basso volume e a bassa velocità che rimangono nascosti.

Rilevamento basato su firme

Punti di forza: confrontando il traffico rispetto ad un database di modelli di attacco noti, questo metodo può identificare e bloccare rapidamente le minacce riconosciute. Questo approccio risulta estremamente efficace contro vettori di attacco comuni e identificati in precedenza.

Considerazioni: questo metodo non riesce a rilevare attacchi nuovi o modificati che non corrispondono a firme esistenti. Gli aggiornamenti regolari sono necessari per garantire l'efficacia del metodo.

Test di verifica/risposta

Punti di forza: questo approccio emette sfide per il traffico in entrata verificando se è stato o meno generato da un bot. Le sfide computazionali CAPTCHA o JavaScript possono mitigare in modo efficace i bot e gli strumenti di attacco automatizzati.

Considerazioni: le sfide possono influire negativamente sulle user experience se sono implementate in modo aggressivo. Poiché i bot più sofisticati possono riuscire a passare alcuni test di verifica/risposta, sono richiesti regolari aggiornamenti ai meccanismi di verifica.

Approcci ibridi

La combinazione di diverse strategie di rilevamento e mitigazione può offrire una protezione più completa. Ad esempio, l'utilizzo di un rilevamento basato sulle anomalie per segnalare potenziali attacchi, con l'aggiunta di metodi basati sulla velocità e sulle firme per una maggiore copertura, offre meccanismi di difesa più solidi. I test di verifica/risposta possono distinguere meglio i bot più avanzati dagli utenti legittimi.

Metodi convenzionali

Filtraggio di indirizzi IP e aree geografiche: bloccare o limitare il traffico proveniente da alcuni intervalli IP/CIDR e da alcune aree geografiche non rilevanti per le vostre attività aziendali può ridurre l'esposizione agli attacchi che si originano da queste zone. Anche se questo metodo può risultare utile nel caso l'origine degli utenti aziendali sia nota e limitata, spesso può presentare problemi perché richiede di eseguire continuamente la manutenzione e l'aggiornamento dell'elenco delle origini accettate. Inoltre, hacker esperti possono utilizzare dei proxy per bypassare il blocco geografico. In ogni caso, comunque questo metodo viene adottato comunemente e rimane la strategia di difesa iniziale dagli attacchi DDoS al livello 7.

Analisi del protocollo a livello di applicazioni: questo metodo può mitigare gli attacchi DDoS al livello 7 esaminando i dati presenti nei protocolli a livello di applicazioni per rilevare le anomalie o i modelli dannosi, attivando meccanismi di difesa proattivi. Questo metodo può prevenire sofisticati attacchi DDoS che bypassano le convenzionali misure di sicurezza, ma può utilizzare un elevato numero di risorse per l'ispezione approfondita dei pacchetti e può aumentare le possibilità di ricevere falsi positivi, che potrebbero inavvertitamente bloccare il traffico legittimo.

Come creare la ricetta bilanciata per una strategia di difesa dagli attacchi DDoS multilivello

Preparare una strategia di difesa dagli attacchi DDoS multilivello richiede un approccio differenziato e personalizzato in base allo specifico profilo di rischio di un'organizzazione e al panorama delle minacce informatiche in continua evoluzione. Fondamentalmente, questa strategia richiede una valutazione iniziale per identificare le risorse critiche e i probabili vettori di attacco, seguita dall'implementazione di sistemi di protezione basilari, come la limitazione della velocità e i firewall. I passaggi più avanzati richiedono una combinazione di funzioni di rilevamento basato sulle anomalie per le nuove minacce, rilevamento basato su firme per gli attacchi noti e meccanismi di verifica/risposta per filtrare i bot.

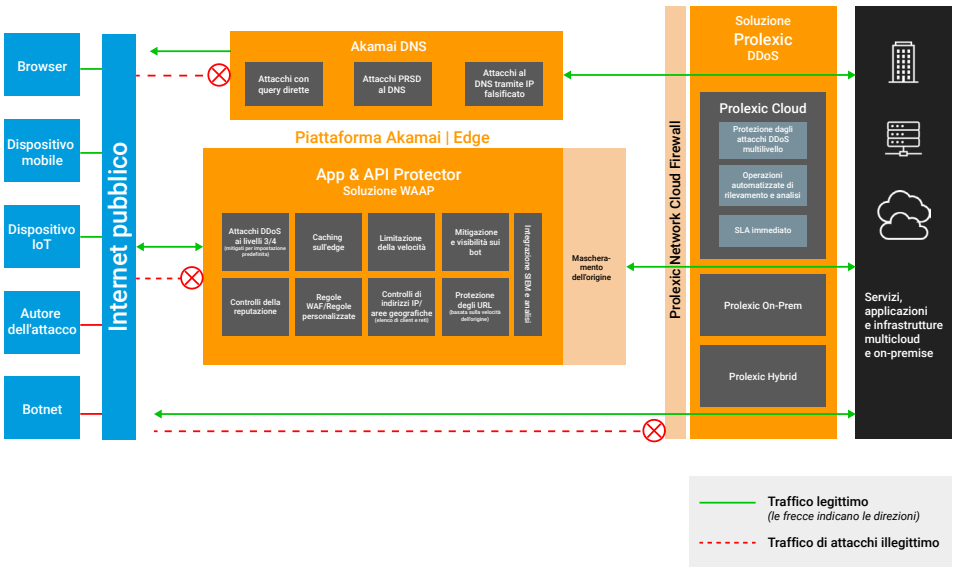
Integrando un'intelligence sulle minacce adattiva, come gli algoritmi che stabiliscono i modelli di fingerprint TLS per gli attacchi DDoS noti ed emergenti, il sistema di sicurezza può adattare automaticamente la sua mitigazione in modo da bloccare o emettere sfide al traffico che mostra tale fingerprint, mitigando efficacemente l'attacco. Un piano di risposta agli incidenti e recupero completo è fondamentale per minimizzare i danni e mantenere la fiducia durante e dopo un attacco. L'apprendimento continuo e le modifiche basate sugli attacchi precedenti e sulle tendenze emergenti mantengono la strategia di difesa efficace e resiliente.

Un'istituzione finanziaria che subisce sofisticati attacchi DDoS multivettore offre un chiaro esempio dell'importanza di disporre di una strategia di difesa multilivello bilanciata. L'impatto potenzialmente esercitato dai problemi di downtime sulle operazioni e sulla fiducia dei clienti rendono le istituzioni di questo tipo i principali bersagli dei criminali.

Integrando una combinazione di metodi di rilevamento e mitigazione, come il rilevamento delle anomalie del traffico, tramite metodi convenzionali come la limitazione della velocità, il filtraggio di indirizzi IP/aree geografiche, la reputazione dell'IP e l'intelligence sulle minacce in tempo reale, insieme ad un solido piano di risposta agli incidenti, queste istituzioni possono proteggere le loro risorse critiche da eventuali interruzioni, garantendo, al contempo, la continuità del servizio per i loro clienti. Questo approccio completo è indicativo del modo con cui le organizzazioni possono difendersi dalla natura sfaccettata degli attacchi DDoS nell'odierno scenario digitale.

Come prepararsi ad una strategia di difesa approfondita con l'architettura edge di Akamai

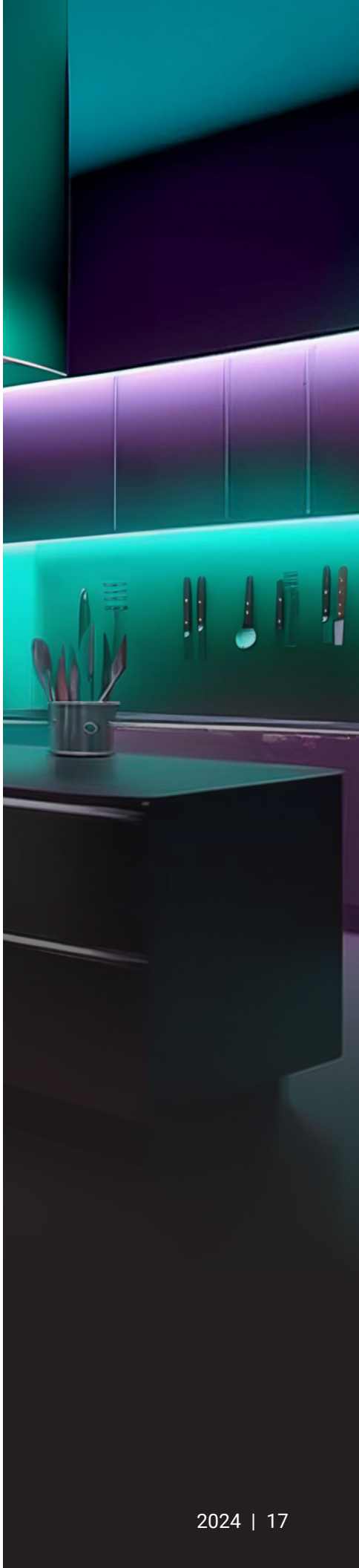
L'approccio di Akamai alla protezione dagli attacchi DDoS a livello di applicazioni è multilivello, completo e adattivo ed è progettato per salvaguardare siti web, applicazioni e API dagli attacchi più sofisticati. App & API Protector utilizza varie funzionalità principali, che forniscono una protezione completa, combinando WAF, visibilità e mitigazione dei bot, sicurezza delle API e protezione dagli attacchi DDoS al livello 7 in un unico prodotto per offrire un'ampia protezione.



Architettura di riferimento per una protezione olistica dagli attacchi DDoS con le soluzioni Edge DNS, App & API Protector e Prolexic

La strategia di protezione dagli attacchi DDoS di Akamai è basata su un'architettura di difesa sull'edge che instrada il traffico tramite la piattaforma di Akamai ampiamente distribuita, sulla quale ogni richiesta viene esaminata in tempo reale. Questa configurazione difende dagli attacchi DDoS, alle app web e alle API, nonché dai bot dannosi direttamente sull'edge, evitando che raggiungano le applicazioni o l'infrastruttura. In tal modo, la continuità aziendale risulta migliorata grazie ad un'architettura rapida, altamente sicura e sempre disponibile, in grado di scalare con gli attacchi.

La solida serie di strumenti e ingredienti di Akamai fornisce controlli proattivi e reattivi, ognuno dei quali con uno scopo distinto nella strategia di difesa complessiva.



Controlli proattivi

I controlli proattivi aiutano a prevenire gli attacchi, focalizzandosi sul rafforzamento del sistema di sicurezza per minimizzare le vulnerabilità, tra cui:

- **Controlli IP (IP di blocco, intervalli CIDR e ASN):** questi controlli rappresentano un livello di difesa fondamentale in quanto bloccano gli indirizzi IP dannosi che riconoscono o gli intervalli identificati tramite l'intelligence sulle minacce.
- **Controlli geografici (blocco di alcune aree geografiche):** consentendo o limitando il traffico proveniente da specifiche aree geografiche, le organizzazioni possono limitare preventivamente l'esposizione agli attacchi originati da zone ad alto rischio.
- **Regole WAF (Web Application Firewall):** l'implementazione di regole contro vulnerabilità e vettori di attacco noti, ad esempio gli strumenti DDoS come FiberFox, offre una solida difesa iniziale.
- **Controlli della reputazione dell'IP:** l'utilizzo dell'intelligence tramite l'euristica di risorse dannose note per attacchi DDoS, web scraping e altre attività dannose consente di bloccare o controllare preventivamente il traffico sospetto.
- **Intelligence sugli attacchi DDoS dalla piattaforma:** le informazioni sugli attacchi DDoS provenienti dalla piattaforma edge di Akamai distribuita a livello globale possono aiutare a creare una strategia di mitigazione proattiva nella lotta contro gli attacchi DDoS a livello di applicazioni.
- **Memorizzazione nella cache:** ottimizzare la memorizzazione dei contenuti nella cache può ridurre notevolmente il carico sui server di origine, mitigando indirettamente l'impatto degli attacchi DDoS mediante la gestione delle richieste dalla cache sull'edge.
- **Site Shield:** il mascheramento dell'origine per consentire solo le richieste indirizzate all'origine tramite la rete edge di Akamai può ridurre ulteriormente i carichi del server.

Controlli reattivi

I controlli reattivi sono le risposte fornite ad un attacco rilevato, che mirano a mitigare il suo impatto e a mantenere la disponibilità del servizio.

- **Limitazione della velocità (policy di velocità):** questi controlli sono fondamentali per mitigare gli improvvisi picchi di traffico che possono indicare un attacco DDoS. È possibile impostare e personalizzare la configurazione appropriata in base ai profili di traffico specifici per i clienti. Spesso, la limitazione della velocità aiuta come metodo di difesa iniziale a proteggere l'origine del cliente dagli attacchi DDoS volumetrici e distribuiti.
- **Protezione Slow POST:** focalizzandosi specificamente sugli attacchi Slow HTTP POST, questo controllo rileva i modelli anomali di traffico che mirano ad esaurire le risorse del server.

- **Regole personalizzate nella soluzione WAF:** questo controllo consente di personalizzare rapidamente le regole per rispondere alle minacce emergenti, offrendo meccanismi di difesa flessibili e dinamici.
- **Mitigazione e visibilità sui bot:** con l'apprendimento automatico che rileva gli attacchi di impersonificazione del browser, potete identificare e bloccare i sofisticati attacchi DDoS originati tramite l'automazione.
- **Protezione degli URL con l'eliminazione del carico intelligente:** questi controlli che limitano le richieste eccessive all'origine e danno priorità agli utenti legittimi rispetto al traffico dannoso possono aiutarvi a mantenere il tempo di attività del servizio durante un attacco DDoS.
- **Intelligence sugli attacchi DDoS dalla piattaforma:** l'eliminazione del carico è una categoria nella protezione degli URL che utilizza le informazioni sugli attacchi DDoS provenienti dalla piattaforma di Akamai distribuita a livello globale e che consente ai nostri clienti di creare una strategia di mitigazione proattiva nella lotta contro gli attacchi DDoS a livello di applicazioni.

La ricetta per mescolare gli ingredienti in modo bilanciato

- **Esempio:** una grande società di servizi finanziari combina una strategia di difesa approfondita con la soluzione WAAP di Akamai

Alcune organizzazioni potrebbero venire colpite dagli attacchi DDoS più frequentemente di altre. Ad esempio, secondo una ricerca di Akamai, oltre un terzo degli attacchi DDoS nel 2023 ha preso di mira le istituzioni finanziarie. Un'importante società di servizi finanziari, anche cliente di Akamai, ha dovuto affrontare un attacco sferrato contro la sua pagina di accesso ed è riuscita a difendersi seguendo una "ricetta" di comprovata validità. Anche voi potete fare lo stesso.


Profilo del criminale: hacktivista


Obiettivo: endpoint di accesso


Metodo: attacco HTTP POST flood


Origini dell'attacco: ~66.000 indirizzi IP e ~140 paesi

Akamai

La ricetta per
mitigare un attacco HTTP POST flood

Ingredienti

Controlli proattivi:

- **Controlli di indirizzi IP**: utilizzate l'intelligence sulle minacce per bloccare gli indirizzi IP o gli intervalli CIDR associati con entità dannose note.
- **Controlli di aree geografiche**: bloccate il traffico proveniente da aree geografiche note per dare asilo a gruppi di hacktivisti, come le zone associate al gruppo "Anonymous Sudan".
- **Regole WAF (Web Application Firewall)**: implementate regole specificamente progettate per contrastare tattiche e strumenti DDoS noti, tra cui i modelli tipici degli attacchi HTTP GET flood.
- **Controlli della reputazione dell'IP**: monitorate attentamente o bloccate attivamente (in tempo reale) il traffico proveniente da origini con scarsi punteggi di reputazione.
- **Intelligence sugli attacchi DDoS dalla piattaforma**: applicate le informazioni provenienti dai dati sugli attacchi DDoS di Akamai a livello globale per anticipare e contrastare i vettori di attacco emergenti.
- **Site Shield**: attivate gli ACL (Access Control List) del firewall in modo da consentire solo il traffico proveniente dalla rete edge di Akamai e bloccare il resto.

Controlli reattivi:

- **Limitazione della velocità**: stabilite policy relative alla velocità per mitigare gli improvvisi picchi di traffico, impostando soglie appropriate per le richieste inviate ogni secondo alla home page. Per ottimizzare la limitazione della velocità, dovete (1) ridurre le finestre temporali necessarie per misurare la velocità di una richiesta al secondo e (2) applicare la limitazione della velocità in base all'area geografica e al punteggio di reputazione delle origini IP di connessione, creando, al contempo, un elenco di origini consentite, come quelle dei partner e degli indirizzi IP aziendali dell'istituzione finanziaria.
- **Regole personalizzate nella soluzione WAF**: create regole personalizzate per rispondere alle specifiche caratteristiche di un attacco una volta rilevato. L'utilizzo dei controlli di campionamento del traffico nelle regole personalizzate vi aiuterà a cercare in modo più efficiente le principali origini dell'attacco nell'analisi del traffico, mentre l'uso dei controlli di indirizzi IP/aree geografiche nelle regole personalizzate potrà aiutarvi a velocizzare le operazioni di mitigazione.
- **Mitigazione e visibilità sui bot**: il rilevamento dell'impersonificazione del browser vi consente di identificare e bloccare le richieste che imitano il comportamento degli utenti legittimi, ma che, in realtà, fanno parte dell'attacco flood.
- **Protezione degli URL**: applicate i controlli di limitazione della velocità delle richieste indirizzate in modo specifico agli URL di accesso, conservando la larghezza di banda per gli utenti legittimi. La configurazione dell'eliminazione del carico intelligente con categorie come proxy, nodi di uscita Tor, bot di base, IP a bassa reputazione, ecc. vi aiuterà a dare priorità al traffico degli utenti reali rispetto ad origini potenzialmente dannose.

Metodo di preparazione

Fase di revisione:

- **Rivedete la configurazione**: eseguite un'accurata revisione del vostro attuale sistema di sicurezza. Configurate i controlli proattivi in base agli elementi individuati, assicurandovi che tutti i controlli di indirizzi IP/aree geografiche pertinenti vengano gestiti nel modo corretto.
- **Ottimizzazione della configurazione**: regolate la configurazione in modo da poter riconoscere e mitigare i modelli di traffico insoliti, inclusi quelli tipici degli attacchi HTTP POST flood.

Fase di rilevamento e mitigazione:

- **Monitoraggio e creazione di avvisi**: l'architettura di difesa sull'edge di Akamai può monitorare il traffico in entrata alla ricerca di modelli che potrebbero indicare un attacco DDoS. Potete configurare la creazione di avvisi in caso di modelli o picchi di traffico insoliti che corrispondono a metodi DDoS noti, come gli attacchi HTTP POST flood.
- **Rilevamento e mitigazione**: se configurati correttamente, diversi controlli proattivi, come la reputazione degli IP, la memorizzazione nella cache e i controlli di indirizzi IP/aree geografiche, offrono automaticamente le funzionalità di rilevamento e mitigazione.

Una volta rilevato un attacco, alcuni controlli, come la limitazione della velocità, la protezione degli URL e il rilevamento dell'impersonificazione del browser, vengono attivati automaticamente senza richiedere l'intervento dell'utente.

- **Analisi e adattamento**: analizzate continuamente i modelli di attacco e adattate le vostre misure difensive in tempo reale per contrastare le tattiche dei criminali in continua evoluzione. Ad esempio, potete creare policy di limitazione della velocità o regole personalizzate in base alle recenti analisi sul traffico degli attacchi.

Analisi delle operazioni di recupero e post-attacco:

- **Analisi dei registri**: dopo un attacco, potete eseguire un'analisi dettagliata dei registri sul traffico per identificare i vettori di attacco e l'efficacia dei controlli messi in atto.
- **Modifiche**: apportate le necessarie modifiche ai controlli proattivi e reattivi in base alle informazioni ricavate dall'analisi dell'attacco.

Suggerimenti per servire in tavola

- Rivedete e aggiornate regolarmente la vostra strategia di difesa per adattarla alle tattiche degli attacchi DDoS in continua evoluzione. Queste revisioni possono variare notevolmente da un'organizzazione all'altra poiché dipendono dalle specifiche esigenze aziendali, dal livello dell'esposizione alle minacce e dalle best practice di settore. Una società di servizi finanziari potrebbe avere la necessità di eseguire queste revisioni ogni trimestre, mentre una piattaforma di e-commerce potrebbe decidere di condurle due volte all'anno per prepararsi in vista dei picchi degli acquisti stagionali.
- Organizzate sessioni di formazione continua per consentire al team addetto alla sicurezza di riconoscere e rispondere adeguatamente ai nuovi vettori di attacco DDoS.
- Eseguite simulazioni degli attacchi per verificare l'efficacia delle misure messe in atto e per stabilire il livello di preparazione del team in caso di incidenti reali.

Analisi delle operazioni di recupero e post-attacco

Nella difesa dagli attacchi DDoS a livello di applicazioni (livello 7), la fase del post-attacco è fondamentale per rafforzare i futuri sistemi di difesa e per capire con chi si sta combattendo. Sono necessari due passaggi importanti: analizzare il modello dell'attacco e ottimizzare i sistemi di difesa in base all'analisi condotta. Questi passaggi sono cruciali per preparare una strategia di difesa resiliente e per garantire la continuità e l'integrità dei servizi online.

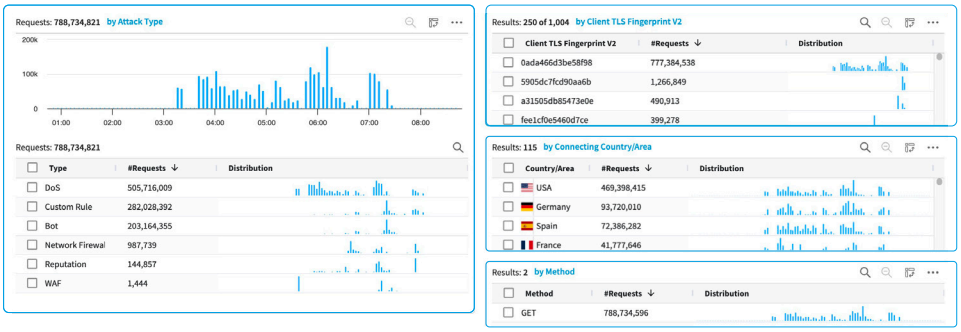
Analisi dei modelli di traffico e attacco

Dopo aver gestito un attacco, il passaggio successivo consiste nell'analizzare l'incidente per capire quale strategia ha funzionato e quale strategia non ha avuto l'esito previsto. Questa valutazione comprende fattori a lungo termine, come l'impatto sulla fiducia dei clienti, l'integrità dei dati e le potenziali perdite finanziarie. Sistemi di analisi della sicurezza completi come Akamai Web Security Analytics sono strumenti indispensabili in questa fase perché consentono alle organizzazioni di comprendere il traffico degli attacchi e il suo impatto.

Questa analisi implica l'esame delle tattiche, delle tecniche e delle procedure (TPP) utilizzate da parte dei criminali. Tra le principali domande a cui dovete rispondere, figurano le seguenti:

- Di quale natura era il picco di traffico?
- Sono state prese di mira specifiche funzionalità delle applicazioni?
- L'attacco ha sfruttato vulnerabilità note?

Akamai Web Security Analytics può identificare le anomalie presenti nei modelli di traffico, individuare l'origine geografica dell'attacco e classificare il tipo di attacco in base ai comportamenti osservati. Nell'esempio seguente, vengono mostrate alcune caratteristiche o dimensioni del traffico che possono essere applicate per analizzare un attacco DDoS.



Immagini tratte dalla soluzione Web Security Analytics, che offre una visibilità impareggiabile e un'analisi proattiva degli eventi di sicurezza

Come rivedere e aggiornare le strategie di difesa in base all'analisi degli attacchi

La revisione e l'aggiornamento delle strategie di difesa in base all'analisi degli attacchi sono fondamentali per rafforzare il sistema della cybersicurezza di un'organizzazione. Esaminando le specifiche di un attacco precedente, potete identificare le vulnerabilità presenti negli attuali sistemi di difesa e apportare modifiche oculate. Ecco alcuni esempi di come potete applicare questo processo tramite Akamai Web Security Analytics.

Esempio 1: aggiornamento delle regole WAF in base ai modelli di attacco

Scenario: un'organizzazione subisce un attacco DDoS al livello 7 che colpisce la sua applicazione web con una raffica di richieste dannose indirizzate alla home page dell'applicazione.

Esame: l'analisi dell'attacco rivela che le regole WAF (Web Application Firewall) esistenti hanno rilevato e bloccato in modo adeguato più del 90% del traffico degli attacchi, ma il rimanente 10% è sfuggito ai controlli perché era stato creato un elenco esplicito di aree geografiche consentite per cui le origini dell'attacco provenienti da queste zone sono riuscite a sovraccaricare l'applicazione.

Aggiornamento: in base a questa analisi, l'organizzazione ha aggiornato le configurazioni della sua soluzione WAF in modo da poter utilizzare una regola WAF personalizzata corrispondente a specifiche caratteristiche del traffico dell'attacco proveniente dalle aree geografiche consentite. Eventuali override possono mantenere le aree geografiche consentite, ma bloccando specifici attributi del traffico dell'attacco. Inoltre, le impostazioni della limitazione della velocità per le aree geografiche consentite sono state rese più rigorose.

Esempio 2: miglioramento della protezione dell'origine

Scenario: la procedura di accesso ad un sito di retail viene colpita da un attacco DDoS al livello 7 sofisticato e altamente distribuito che utilizza bot automatizzati.

Esame: l'analisi post-attacco indica che il traffico dell'attacco altamente distribuito proveniva da più di 150 paesi e centinaia di fingerprint TLS simili ai browser legittimi. Una buona porzione del traffico ha avuto origine dai fornitori di servizi cloud, alcuni dei quali erano inseriti in un elenco di elementi consentiti come origini di partner affidabili. Anche se l'attacco è stato mitigato in modo efficace, l'analisi ha rivelato la necessità di adottare ulteriori misure di difesa.

Aggiornamento: per proteggere gli URL che richiedono un'elaborazione elevata come i processi di pagamento, questa organizzazione ha implementato la protezione degli URL, una funzione appositamente progettata per proteggere gli URL che richiedono un'elaborazione elevata e gli endpoint delle API da attacchi DDoS a livello di applicazioni altamente distribuiti. Inoltre, un Security Architect ha attivato l'eliminazione del carico intelligente per bot, proxy, reputazione dell'IP, ecc., ossia una funzione secondaria della protezione degli URL che aiuta a dare priorità al traffico degli utenti reali negando prima le richieste provenienti da origini probabilmente dannose.

L'organizzazione ha anche deciso di attivare la funzionalità di protezione dai bot incorporata nella soluzione WAF a cui precedentemente non era stata attribuita la giusta considerazione dall'azienda per la presenza di una soluzione contro i bot on-premise, che, tuttavia, non era riuscita a garantire la necessaria scalabilità durante questo attacco ad alta velocità.

Esempio 3: implementazione della limitazione della velocità per gli endpoint delle API

Scenario: un endpoint delle API di un'applicazione di una società di servizi finanziari viene sovraccaricato da un numero eccessivo di richieste di transazioni fraudolente a indicare la presenza di un attacco DDoS al livello 7 sferrato con l'intento di esaurire le risorse del server.

Esame: l'analisi del modello di attacco mostra che i criminali hanno preso specificamente di mira gli endpoint delle API meno protette che non sono state in grado di elaborare un elevato numero di richieste.

Aggiornamento: l'organizzazione ha implementato, di conseguenza, una rigorosa limitazione della velocità su tutti gli endpoint delle API, specialmente quelli identificati come vulnerabili e ha adottato un componente aggiuntivo dedicato che fornisce livelli avanzati per la sicurezza delle API, tra cui il monitoraggio delle vulnerabilità delle API, le minacce delle API ombra e l'abuso della logica delle API.

Mosse strategiche

- **Monitoraggio e registrazione continui:** stabilite solidi sistemi di monitoraggio e registrazione per rilevare tempestivamente le anomalie e per valutare accuratamente i danni causati durante e dopo un attacco.
- **Gestione delle vulnerabilità:** aggiornate e applicate regolarmente le patch ai sistemi per mitigare le vulnerabilità note, riducendo il rischio di sfruttamento.
- **Analisi dei modelli di attacco:** utilizzate appropriati strumenti di visibilità per eseguire analisi approfondite sui modelli di attacco in modo da comprendere le metodologie e gli scopi dei criminali.

Analisi post-attacco

La valutazione dei danni causati e l'analisi dei modelli di attacco sono componenti fondamentali in una solida strategia di difesa dagli attacchi DDoS al livello 7. Queste operazioni non solo aiutano a comprendere e mitigare l'impatto immediato di un attacco, ma forniscono anche informazioni utili per migliorare continuamente i meccanismi di difesa, garantendo un miglior livello di preparazione in vista delle future minacce.

Come mantenere e aggiornare le ricette

Mantenere un solido sistema di difesa dagli attacchi DDoS al livello 7 richiede un monitoraggio costante delle tendenze e delle tecniche più recenti.

I criminali combinano frequentemente vari modelli di attacco, sfruttando nuovi strumenti e vulnerabilità. Per contrastare queste minacce in modo proattivo, le organizzazioni devono investire tempo e fatica nelle operazioni di ricerca, monitoraggio, valutazione dei meccanismi di difesa, automazione dei sistemi di protezione e collaborazione con la community di intelligence sulle minacce.

Monitorare i principali forum sulla cybersicurezza è solo un buon punto di partenza, tuttavia, suggeriamo di adottare un approccio più ordinato:

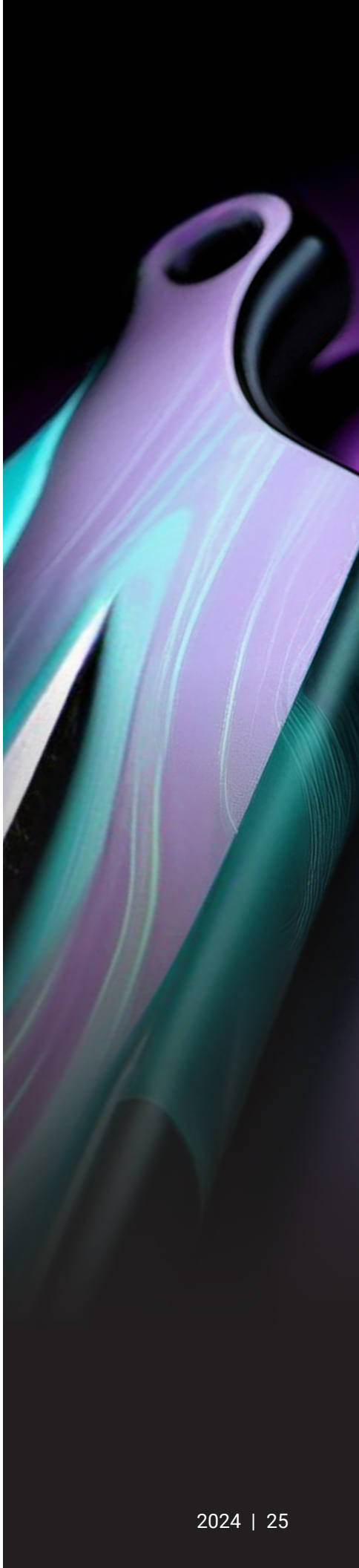
Effettuate continue operazioni di monitoraggio e valutazione: monitorate regolarmente le performance della rete e delle applicazioni per rilevare nuovi schemi o anomalie che indicano la presenza di nuove minacce. Utilizzate questi dati per valutare l'efficacia dei vostri attuali meccanismi di difesa, identificando le aree che necessitano di miglioramenti o modifiche.

Formate un team anti-DDoS: stabilite il team o la persona di riferimento all'interno della vostra azienda che si occuperà di effettuare ricerche e di monitorare il panorama degli attacchi DDoS, riferendo eventuali consigli e risultati importanti al resto dell'organizzazione almeno ogni trimestre.

Collaborate con la community di intelligence sulle minacce: i criminali comunicano tra loro sui metodi più recenti ed efficaci, quindi non c'è motivo per cui anche voi non dovreste comunicare con i vostri colleghi che operano in altre aziende e in altri settori relativamente ai migliori sistemi di difesa da adottare. Tenetevi informati sulle ultime intelligence sulle minacce. Potete abbonarvi per seguire i feed di sicurezza, prendere parte ai forum sulla cybersicurezza e collaborare con colleghi che operano nel vostro settore. Tali informazioni vi aiuteranno ad anticipare i nuovi vettori di attacco e ad adattare di conseguenza i vostri sistemi di difesa.

Affidatevi al vostro vendor di servizi di cybersicurezza: i fornitori di tecnologie, spesso, offrono gruppi di ricerca sulle minacce dedicati, mentre i fornitori con una rete per la distribuzione dei contenuti possono fornire informazioni che non sono disponibili altrove. Potrete trarre vantaggio da queste opportunità di apprendimento ovunque e in qualsiasi momento. Inoltre, è utile consultare periodicamente un esperto sulla sicurezza.

Eseguite test sui vostri sistemi di difesa: chi non riesce a prepararsi si sta preparando per non riuscire, ma i risultati si ottengono con la pratica, quindi qualunque sia la vostra strategia, ricordatevi che chi la dura la vince.



Dovete condurre revisioni periodiche e simulare gli scenari di attacco (esercizi di red team) per verificare la resilienza delle vostre strategie di difesa. Questi esercizi possono rivelare i punti deboli della vostra attuale configurazione e fornire informazioni su come i criminali potrebbero sfruttare il vostro sistema.

Dovete eseguire un test della vostra rete almeno una volta all'anno. I profili degli attacchi recenti possono anche essere un buon punto di riferimento per i test, in particolare gli attacchi che hanno subito le aziende del vostro settore.

Condividete le vostre conoscenze con la community: vale la pena ripetere che, come i criminali condividono le tattiche e gli strumenti che utilizzano, così anche le organizzazioni dovrebbero condividere le loro conoscenze sulle strategie di difesa più efficaci.

Documentando sia le esperienze positive che quelle negative, gli addetti alla cybersicurezza possono fornire informazioni realistiche per arricchire la knowledge base collettiva. Prendere parte ai forum di settore, offrire consulenza ai neofiti del campo e partecipare a progetti di collaborazione sono operazioni fondamentali per promuovere un solido ecosistema di difesa. Questi sforzi non solo contribuiscono a sviluppare strategie e strumenti più efficaci, ma offrono anche experience e informazioni diversificate in grado di adattarsi alle mutevoli tattiche dei criminali. Questo spirito collaborativo è essenziale per stare al passo nel panorama della cybersicurezza, rendendo ogni contributo importante per realizzare un mondo digitale più solido e resiliente.

La morale

Il panorama degli attacchi DDoS è dinamico perché i criminali cercano costantemente nuovi metodi per bypassare i sistemi di difesa. Mantenere e aggiornare le strategie di protezione dagli attacchi DDoS al livello 7 è un processo continuo che richiede vigilanza, adattabilità e un approccio proattivo. Rimanendo aggiornati, eseguendo regolarmente test e revisioni e promuovendo una cultura basata sul miglioramento continuo, potrete mantenere un solido sistema di difesa dalle minacce presenti e future.

Conclusione

È chiaro che gli attacchi DDoS al livello 7 non solo sono diventati più sofisticati, ma anche più semplici da sferrare grazie ai miglioramenti apportati all'automazione e al coordinamento dei criminali. Nel frattempo, le organizzazioni devono difendere un panorama più vasto e complesso, mentre aumentano i costi legati ad un eventuale insuccesso.

In realtà, elaborare una "ricetta" per la difesa non è un compito semplice. Nessun metodo da solo può risolvere tutti i problemi causati dagli attacchi DDoS al livello 7. Come abbiamo dimostrato, un approccio su più fronti che combina varie strategie di rilevamento e mitigazione offre la difesa più solida.

Inoltre, i metodi di difesa andrebbero scelti in base alle specifiche esigenze, ai modelli di traffico e al profilo di rischio dell'applicazione o del servizio da proteggere. Non potete costruire un sistema di difesa senza una perfetta comprensione delle vostre attività aziendali, del vostro traffico e delle vostre vulnerabilità. Apportare regolari aggiornamenti e modifiche a queste strategie è fondamentale per adattarle al panorama degli attacchi DDoS in continua evoluzione.

Infine, è chiaro anche che il vostro lavoro non finisce una volta terminato un attacco. Le analisi post-attacco e le conseguenti modifiche sono fondamentali per un successo costante e possono aiutare a svolgere una parte importante nella condivisione delle vostre conoscenze e nel vostro sviluppo professionale.

Fortunatamente, Akamai si trova in una posizione ideale per fornirvi il supporto necessario in ogni fase del vostro percorso. Molte aziende sfruttano l'opportunità di rivolgersi ad un solo provider per tutti i servizi di protezione dagli attacchi DDoS al livello 7 di cui hanno bisogno, dalla protezione di app e API ad esclusive informazioni sul traffico globale fino all'analisi post-attacco condotta dai nostri esperti.

Scoprite come funzionano i sistemi di protezione dagli attacchi DDoS al livello 7 di Akamai. Avviate una prova gratuita della soluzione App & API Protector.

Riconoscimenti

Editoria e stesura

Aseem Ahmed
Barney Beal

Revisione e contributi di esperti del settore

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing ed editoria

Georgina Morales Hampe
Shivangi Sahu