Akamai

WHITE PAPER

Come evitare il caos

con la giusta piattaforma DDoS a livello di applicazione

Cosa sono oggi per noi gli attacchi DDoS a livello di applicazione

Come purtroppo sanno bene gli esperti di sicurezza di tutto il mondo, un DDoS (Distributed Denial-of-Service) è un attacco informatico che tenta di rendere non disponibile un sito web o una risorsa di rete sovraccaricandoli con un'elevata quantità di traffico dannoso e rendendoli, così, inutilizzabili. Gli attacchi DDoS rappresentano ancora la tecnica usata più comunemente dai criminali e sono aumentati negli ultimi cinque anni. Ad esempio, uno dei più recenti attacchi di grandi dimensioni in termini di PPS (pacchetti al secondo) ha raggiunto un picco di 809 MPPS in circa due minuti.

Una tendenza che abbiamo riscontrato in questo aumento di attacchi è il maggior numero di istanze di attacchi DDoS a livello di applicazione. Noti anche come attacchi DDoS di livello 7, questi attacchi prendono di mira e distruggono applicazioni web specifiche (non intere reti). Non solo questi attacchi sono difficili da prevenire e mitigare per gli addetti alla sicurezza; l'elevata adozione di tecnologie quali l'automazione e i servizi cloud hanno offerto ai criminali un facile accesso agli strumenti necessari per lanciarli, rendendo sempre più facile compromettere il livello delle applicazioni.

La verità è che in questo tipo di attacco vengono utilizzate richieste simili a quelle normalmente eseguite dagli utenti finali, pertanto non è facile valutarne la complessità. L'efficienza di un attacco nel colpire sia il server che la rete presi di mira implica la sua capacità di arrecare più danni con una minore larghezza di banda totale. In breve, gli attacchi a livello di applicazione sono facili da implementare, difficili da rallentare o arrestare e mirati ad un obiettivo specifico.

Per comprendere come un attacco DDoS a livello di applicazione riesca a colpire in modo specifico le nostre organizzazioni, dobbiamo sapere in che modo questo tipo di attacco influisce su tutti i settori. Possiamo paragonare le categorie di attacchi DDoS ai problemi che possono venirsi a creare durante una festa. Immaginate, ad esempio, di aver invitato alcuni ospiti a casa per festeggiare un'occasione speciale o per divertirvi nel weekend. Possono verificarsi due scenari:

Tipi di attacchi DDoS

Scenario 1
Attacco volumetrico

I vostri ospiti sono così entusiasti della festa da condividere troppe informazioni (magari sui social media). Si diffonde la notizia che la vostra festa è un evento da non perdere e, il giorno della festa, si presenta a casa vostra un numero considerevole di persone che non conoscete. Questo scenario rappresenta un attacco DDoS volumetrico perché tutte le vostre risorse vengono utilizzate da persone che non avete invitato.

Scenario 2
Attacco ai protocolli

Si è verificata una fuga di informazioni da parte di un ospite di cui vi fidate. Alcune persone che vogliono essere invitate alla vostra festa (e non hanno ricevuto l'invito) sommergono i vostri ospiti di domande per conoscere i dettagli dell'evento. Uno dei vostri ospiti cede e un gruppetto di persone non invitate riesce ad accedere alla vostra festa. Questo scenario rappresenta un attacco DDoS ai protocolli perché qualcuno che avrebbe dovuto tenere riservate le informazioni sulla vostra festa non l'ha fatto.

Scenario 3
Attacco alle applicazioni

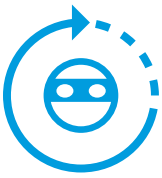
Un malintenzionato sente parlare della vostra festa e decide di presentarsi travestito da ospite per pianificare un furto e commettere una rapina in casa vostra. Questo scenario rappresenta un attacco DDoS alle applicazioni perché la persona in questione imita un ospite autenticato.

In tutti questi scenari, esiste una vulnerabilità comune: il fatto di aver aperto la vostra casa per un evento. Si tratta di una vulnerabilità inevitabile sfruttata dagli attacchi DDoS a livello di applicazione perché è il livello in cui la vostra organizzazione interagisce con l'utente. Inoltre, trattandosi del livello sul quale avete meno controllo perché viene gestito direttamente dagli utenti, può risultare più difficile mitigare questi attacchi DDoS, oltre al fatto che, in caso di problemi, dovrete sostenere costi aggiuntivi. Sia che si tratti di una maggior quantità di bevande e cibo o di estranei che vengono a conoscenza di informazioni su di voi oppure delle conseguenze di un'intrusione in casa vostra, una festa andata male può risultare molto costosa.

Molte soluzioni per la sicurezza promettono sempre più di proteggere sistemi, risorse e informazioni sensibili dagli attacchi DDoS a livello di applicazione, che oggi sono molto comuni e tra i più difficili da cui difendersi. Vi siete affidati a queste soluzioni per proteggere ciò che offrite. In definitiva, l'efficacia dei sistemi di protezione dagli attacchi DDoS dipende dalla piattaforma alla quale vi affidate. Date un'occhiata ai cambiamenti e alle tendenze più recenti per individuare la piattaforma di protezione dagli attacchi DDoS a livello di applicazione più adatta a voi.

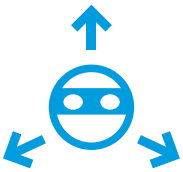
Quali sono le tendenze e come sta cambiando il panorama

Come sempre, una volta create le soluzioni per contrastare un attacco specifico, i criminali adattano la loro strategia per neutralizzarle. Dopo aver monitorato questa specie di competizione, vi presentiamo le quattro tendenze e i cambiamenti oggi più comuni:



1. Passaggio ad attacchi ripetuti e di breve durata

Gli attacchi DDoS stanno diventando sempre meno prolungati, ma aumentano le loro dimensioni e la loro frequenza. Akamai ha registrato attacchi complessi con più di nove vettori di attacco che combinano ARM, SYN flood, riflessione UDP (DNS, WS-Discovery, ecc.), HTTP flood, ecc.

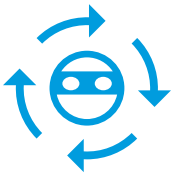


2. Uso più frequente di attacchi multivettore

Oltre il 20% dei criminali usa attacchi DDoS multivettore che combinano diversi metodi in un unico attacco breve, ripetendolo nuovamente subito dopo. Secondo Link11, il più alto numero di vettori simultanei che è stato registrato è 18 con un aumento del 50% rispetto al 2021.

3. Maggiore capacità di evitare il rilevamento e la successiva mitigazione

Distinguere tra il traffico di un attacco e il traffico normale è difficile, soprattutto nel caso del livello di applicazione. Ad esempio, una botnet lancia un attacco HTTP flood contro il server di una vittima. Dal momento che ogni bot invia richieste di rete apparentemente legittime, il traffico non è falsificato e può apparire "normale" in origine.



4. Prima l'automazione, poi la personalizzazione delle tattiche

Con la prevalenza di piattaforme cloud e IaaS/PaaS, i criminali hanno facile accesso all'automazione e alla potenza di elaborazione ed è facile automatizzare gli attacchi lanciandoli rapidamente su vasta scala. Pertanto, questi attacchi non sono semplicemente volumetrici, ma più distribuiti, casuali e creati in modo intelligente (randomizzando i parametri nelle richieste, ecc.).

Come notato nel caso della festa, la vostra casa potrebbe venire violata in tre modi: con l'utilizzo di risorse, tramite un ospite vulnerabile o un criminale travestito. Con le tendenze e i cambiamenti in corso negli attacchi a livello di applicazione, la vostra casa potrebbe sembrare esposta al caos, con l'intenzione sistematica di eludere il vostro controllo. Invece, il tutto è orchestrato in base alle tre categorie riportate sopra per poter agire nell'invisibilità. I criminali, ad esempio, effettuano controlli sulla vostra casa preventivamente per individuare quanti ingressi ci sono, cercano di scoprire qual è il dress code della festa in anticipo oppure creano falsi profili social per saperne di più su di voi, così possono ingannare i vostri ospiti inducendoli a pensare che vi lega una profonda amicizia.

A causa dell'aumento della complessità degli attacchi DDoS a livello di applicazione, è utile disporre di una strategia di protezione più olistica rispetto al passato. In precedenza, tutte le soluzioni WAAP (Web Application and API Protection), anche quelle create in-house, erano in grado di soddisfare le vostre esigenze. Ora, la vostra soluzione WAAP deve risultare più complessa degli attacchi a livello di applicazione sferrati attualmente.

Un approccio olistico alla protezione dagli attacchi DDoS a livello di applicazione

Ciò che rende difficile individuare un attacco DDoS a livello di applicazione è il fatto che, anche se gli attacchi multivettore presentano uno schema ovvio, un criminale motivato può monitorare la risposta all'attacco e modificarla per contrastare una determinata difesa. Per affrontare questa sfida in modo più coerente e accurato, dovete migliorare le vostre soluzioni WAAP con funzioni di rilevamento, mitigazione e self-service.

Infine, la vostra soluzione WAAP non deve limitarsi a proteggere solo la porta d'ingresso, ma deve difendere qualsiasi punto di accesso alla vostra casa, per consentirvi di identificare i criminali travestiti da ospiti, e deve risultare scalabile se subite più attacchi contemporaneamente. La buona notizia: ora potete adottare la giusta piattaforma per mitigare i problemi causati dagli attacchi DDoS a livello di applicazione e per proseguire le vostre attività aziendali come di consueto. La tecnologia di attenuazione DDoS deve diventare più olistica e concentrarsi sui seguenti elementi:

Scalabilità della piattaforma

Indipendentemente dalle sue performance quotidiane, la vostra soluzione WAAP risulterà presto un fallimento se non riuscirà a scalare per mitigare un attacco volumetrico. Ecco perché la piattaforma su cui si basa la soluzione WAAP è importante quanto la soluzione stessa. Inoltre, è fondamentale sapere dove viene eseguita la piattaforma. Akamai, ad esempio, dispone di sedi sull'edge in tutto il mondo, spesso nelle aree geografiche in cui hanno origine gli attacchi. È molto più facile bloccare un attacco DDoS se viene mitigato proprio dove si è originato. Inoltre, la scalabilità di una soluzione facilita di gran lunga le operazioni imprescindibili, come la limitazione della velocità e le regole personalizzate.

Risorse di dati e informazioni su cui si basano i vostri sistemi di protezione

Anche se qualsiasi soluzione WAAP può monitorare il traffico e inviare i dati generati, dovete prendere in considerazione una soluzione in grado di aggregare i dati da un punto di vista globale. Se il provider della vostra soluzione ha visibilità sul traffico di migliaia di aziende, i dati da voi generati possono essere contestualizzati tra varie organizzazioni che affrontano le vostre stesse minacce in modo da fornire migliori informazioni ai sistemi di apprendimento automatico implementati nella vostra soluzione. I vostri team interni potranno quindi reperire questi dati e utilizzarli per iterare e personalizzare la vostra soluzione.

Visibilità e accuratezza della vostra soluzione

Alcuni metodi di rilevamento, inclusi quelli basati su comportamenti/anomalie, dovrebbero già essere integrati nelle soluzioni per non concentrarsi solo sul traffico client in entrata ma risalire alla velocità di connessione e ai parametri sulle performance del server. Tuttavia, se disponete di una soluzione scalabile basata su un solido set di dati, la vostra soluzione WAAP sarà molto più mirata e accurata. Inoltre, potrete acquisire una comprensione più dettagliata del vostro traffico perché la soluzione è adattiva e in grado di capire se un attacco si nasconde, ad esempio, dietro un proxy aperto su Internet. In tal modo, potete assicurarvi di avvisare le persone giuste e di ridurre i falsi positivi.

Quindi, riassumendo, se volete organizzare una festa senza correre il rischio di farvi sfuggire la situazione di mano, dovete assicurarvi che la vostra casa sia abbastanza grande (= scalabile) per contenere eventuali ospiti aggiuntivi non invitati. Potreste parlare con altre persone che hanno avuto esperienze di feste (= risorse di dati) andate male così da sapere in anticipo quali sistemi di protezione mettere in atto. Inoltre, è consigliabile condividere in anticipo l'elenco degli ospiti e salutarli tutti prima che entrino a casa vostra (= visibilità e accuratezza) per garantire la sicurezza di tutti.

Infine, se non volete sobbarcarvi tutto questo lavoro da soli, potete affidarvi ad un supporto affidabile in grado di sostituirvi. I servizi gestiti possono monitorare tutti i segnali a cui dovete stare particolarmente attenti che vi consentono di distinguere un ospite da un malintenzionato. In più, in tal modo, potrete evitare di dover dedicare costantemente il tempo e le competenze del vostro personale alla prevenzione di questo tipo di attacco sempre più comune e difficile da rilevare.

La questione sugli attacchi DDoS a livello di applicazione presenta tante variabili e vulnerabilità, che fanno naturalmente parte del livello di applicazione. Inoltre, la questione riveste un'importanza critica perché questi attacchi possono risultare decisamente dannosi per la vostra organizzazione. Tuttavia, la difesa contro questo tipo di attacco non deve essere per forza complicata o caotica. Tutto ciò che vi serve è una soluzione strategica, scalabile e basata sui dati... poi la festa può iniziare.

Scoprite ulteriori informazioni su come Akamai può supportarvi con i sistemi di protezione DDoS di livello 7.