Difesa dagli attacchi DDoS nel cloud ibrido

Sommario

Gli attacchi DDoS continuano a evolversi

Gli attacchi DDoS (Distributed Denial-of-Service), uno dei primi tipi di minacce informatiche, continuano ad evolversi e ora sono diventati uno strumento altamente sofisticato nelle mani di criminali informatici e hacktivisti che agiscono sulla base di motivazioni ideologiche. In realtà, gli attacchi DDoS pongono rischi per la sicurezza non solo alle aziende di piccole e grandi dimensioni, ma anche alle infrastrutture pubbliche critiche in vari settori come il settore sanitario, dei servizi di pubblica utilità e dell'energia, nonché del settore dell'istruzione.

A complicare ulteriormente questa dinamica si aggiunge la crescente adozione delle risorse di cloud computing da parte delle istituzioni pubbliche e private. Quando queste organizzazioni combinano il cloud con le loro risorse on-premise esistenti, l'ambiente ibrido risultante diventa molto più complesso. Applicazioni, API (Application Programming Interface), dati, microservizi e carichi di lavoro vengono ora trasmessi in un ambiente frammentato. Le diverse architetture di questi ambienti creano nuove vulnerabilità e una superficie di attacco frammentata che può essere sfruttata dai criminali informatici per sferrare attacchi DDoS sempre più sofisticati e devastanti.

Nell'intento di garantire la protezione delle loro infrastrutture digitali, le organizzazioni hanno bisogno di una piattaforma di protezione dagli attacchi DDoS integrata e ibrida in grado di proteggere le proprie infrastrutture on-premise (sul cloud privato) dagli attacchi DDoS brevi, ma potenti, e di trarre vantaggio dalla portata e dalla capacità di un servizio di scrubbing sul cloud per difendersi dagli imponenti attacchi DDoS volumetrici.

Le nuove tendenze suggeriscono che gli attacchi DDoS continueranno a diventare più potenti e frequenti. A febbraio 2023, Akamai ha mitigato il più vasto attacco DDoS mai sferrato contro un cliente di Akamai Prolexic situato nell'area Asia-Pacifico (APAC), che ha generato un picco di traffico pari a 900,1 gigabit al secondo e 158,2 milioni di pacchetti al secondo (Mpps). Questo episodio si è verificato solo pochi mesi dopo un altro attacco, il più vasto attacco DDoS mai sferrato contro un cliente di Akamai Prolexic in Europa, in cui il traffico è aumentato bruscamente fino ad arrivare a 704,8 Mpps nell'aggressivo tentativo di paralizzare le operazioni aziendali dell'organizzazione. Tutto ciò oltre al fatto che Akamai ha mitigato il più vasto attacco mai osservato fino ad oggi: un attacco da 1,44 terabit al secondo (Tbps) e 385 Mpps, che è stato distribuito a livello globale ed è durato quasi due ore. In realtà, in base alle sue informazioni sui modelli di traffico e degli attacchi, Akamai ha rilevato che, nel 2023, gli attacchi DDoS sono diventati più frequenti, prolungati e altamente sofisticati (con più vettori) e si sono focalizzati su obiettivi orizzontali (ossia, hanno colpito più destinazioni IP nello stesso attacco).

La crescente minaccia

La maggior parte degli attacchi DDoS è oggi multivettore, ossia vengono spesso impiegati più di 10 vettori di attacco per sovraccaricare i rudimentali sistemi e piattaforme per la protezione dagli attacchi DDoS. In effetti, secondo l'intelligence interna sulle minacce di Akamai, il numero di attacchi DDoS orizzontali e mirati a più obiettivi è raddoppiato dal 2022 al 2023. Nel contempo, nel 2023 la durata, la portata e le dimensioni complessive degli attacchi DDoS volumetrici sono risultate le più elevate mai registrate.

A complicare ulteriormente la pianificazione della sicurezza per le organizzazioni, i criminali ora usano diverse tattiche insieme agli attacchi volumetrici tradizionali.

Nel mirino degli autori degli attacchi DDoS rientrano tutti i potenziali point of failure, ad esempio:

- Siti web
- Applicazioni web e altri servizi aziendali
- Concentratori VPN per un accesso remoto alle risorse aziendali
- Controller SD-WAN
- API (Application Programming Interface)
- DNS (Domain Name System) e server di origine
- Data center e infrastrutture di rete

Infrastruttura DNS

Gli attacchi DDoS sferrati contro l'infrastruttura DNS delle organizzazioni sono diventati sempre più comuni, in particolare gli attacchi NXDOMAIN (anche noti come attacchi di sottodominio pseudocasuale, attacchi DNS Water Torture o attacchi di esaurimento delle risorse DNS). Più del 60% degli attacchi DDoS mitigati da Akamai nel 2023 ha presentato un componente DNS, di cui gli attacchi NXDOMAIN hanno costituito circa metà degli attacchi DDoS al DNS. Questi attacchi rappresentano un rischio significativo per il fatturato e la reputazione di un'azienda perché, se il sistema DNS di un'organizzazione si blocca, la sua presenza online scompare.

Attacchi a livello di applicazioni

Gli attacchi DDoS a livello di applicazioni (livello 7) sono diventati più sofisticati perché i criminali evolvono le proprie tattiche per sfruttare logica aziendale e workflow apparentemente benigni. Una vulnerabilità HTTP/2 scoperta nel 2023 ha condotto al più imponente attacco DDoS al livello 7 mai registrato.

DDoS-as-a-Service

I gruppi di criminali informatici organizzati, come Anonymous Sudan e Killnet, offrono servizi DDoS-as-a-Service. In questo caso, i gruppi criminali offrono i loro servizi, in genere una botnet, a pagamento e sferrano gli attacchi per conto di un client. Questi servizi DDoS-for-hire possono risultare estremamente redditizi per i gruppi criminali.

Ransomware + DDoS = RDDoS

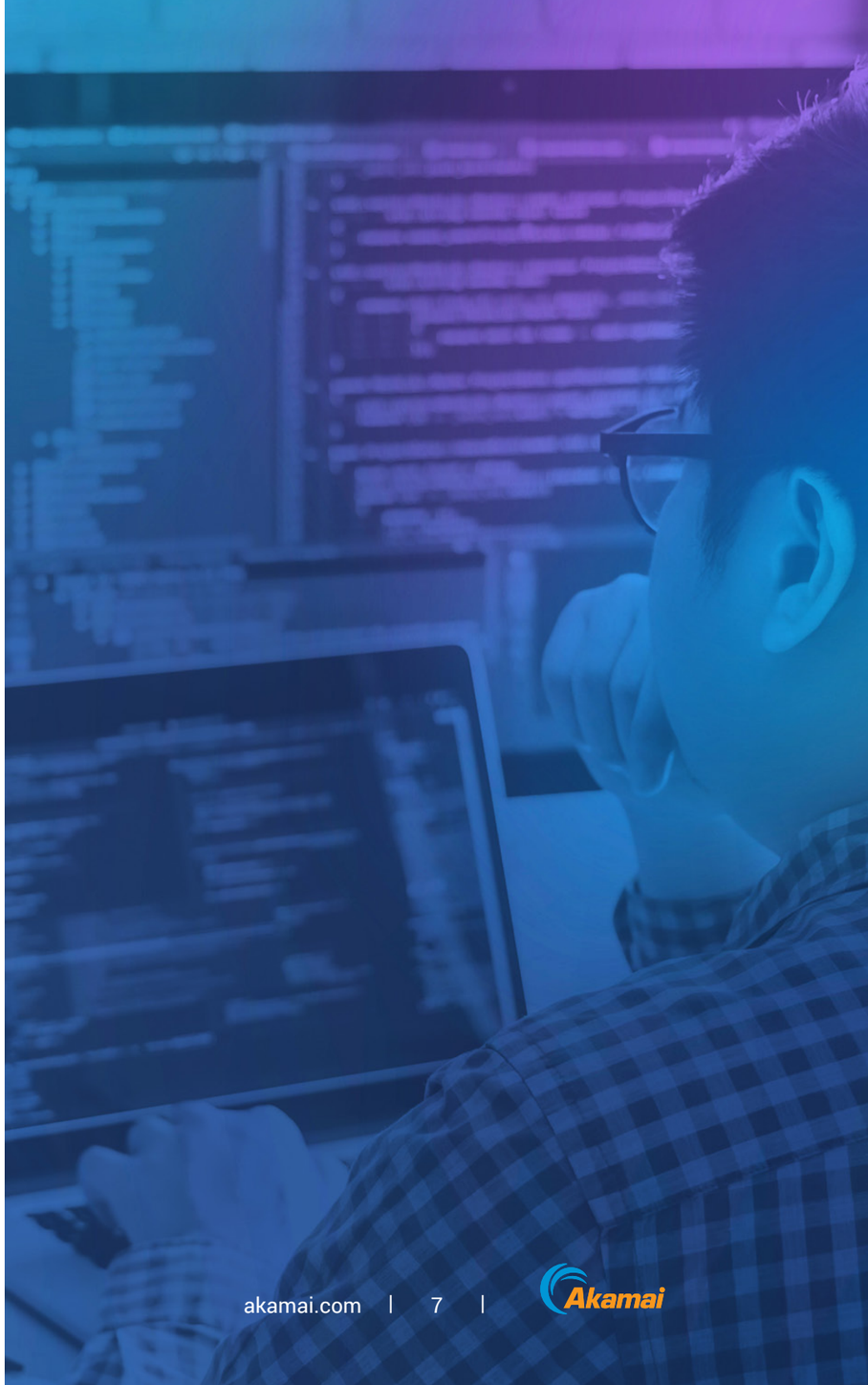
La disponibilità di sferrare attacchi come i servizi DDoS-as-a-Service rende più semplice, inoltre, per i criminali utilizzare gli attacchi DDoS come copertura per distrarre i team addetti alla sicurezza, che possono sferrare contemporaneamente un attacco ransomware o a tripla estorsione, anche detto attacco RDDoS (Ransom DDoS).

Le conseguenze di un attacco DDoS

Negli attacchi DDoS sferrati a livello di rete (livello 3) e trasporto (livello 4), gli attacchi volumetrici e quelli basati su protocolli tentano di congestionare la struttura Internet, sovraccaricare i server ed esaurire le voci delle tabelle di stato per rendere reti e servizi non disponibili. Negli attacchi al livello 7, i criminali tentano di interrompere web performance e user experience sferrando attacchi "nascosti e lenti" e HTTP flood per provocare problemi di downtime con conseguenze sui profitti. Gli attacchi DDoS al DNS possono risultare un po' più complessi poiché, a seconda del tipo di attacco, possono influire su diversi livelli della rete di un'organizzazione. Ad esempio, gli attacchi DDoS di amplificazione e riflessione al DNS possono produrre traffico sui livelli 3 e 4 di una rete aziendale, mentre gli attacchi DDoS di tipo NXDOMAIN o DNS flood, spesso, colpiscono il livello di applicazioni di una rete.

Le ripercussioni dei problemi di downtime non influiscono solo sui costi derivanti dalla mancata disponibilità delle applicazioni e dei servizi presi di mira. Secondo il Ponemon Institute, il costo medio di un attacco DDoS per un'organizzazione corrisponde a 1,7 milioni di dollari all'anno, una cifra determinata dall'aumento dell'assistenza tecnica necessaria, dell'utilizzo delle risorse richieste per risolvere i problemi, delle escalation interne, delle spese legali, delle interruzioni operative e della perdita di produttività da parte dei dipendenti. Inoltre, per le aziende basate sulle interazioni con la clientela, come le società di servizi finanziari, e-commerce, gaming e media, un'interruzione della connessione Internet non arreca solo danni economici, ma, cosa più importante, può causare danni irreparabili alla loro reputazione.

È chiaro che la posta in gioco è alta e può solo aumentare, visto l'incremento della migrazione alle infrastrutture nel cloud ibrido.

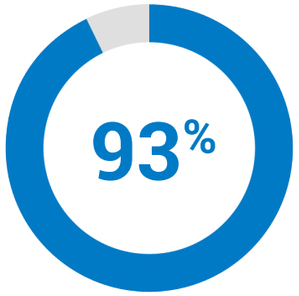


Gli ambienti ibridi e multicloud continuano a rendere la sicurezza complessa

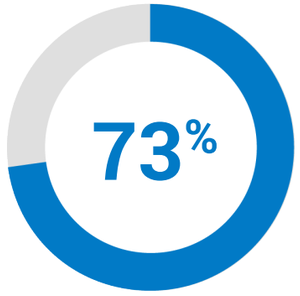
Visto che molte organizzazioni mantengono alcuni carichi di lavoro nei cloud privati o nei data center on-premise e spostano altre applicazioni in ambienti ospitati nel cloud pubblico, questo approccio ibrido nei confronti delle infrastrutture rende estremamente complesso riuscire a garantire un sistema di sicurezza affidabile. Analogamente, le aziende spesso dispongono di un'infrastruttura DNS ibrida in cui alcune zone del DNS autoritativo vengono gestite nel cloud, mentre le altre zone sono gestite da server dei nomi on-premise e strumenti di bilanciamento del carico del server globale (GSLB). Le organizzazioni continuano a mantenere alcune infrastrutture DNS on-premise per vari motivi, tra cui, ad esempio, perché hanno già investito ingenti capitali nella configurazione di un'infrastruttura on-premise che soddisfa i requisiti di conformità vigenti. La complessa migrazione di tutto il sistema DNS nel cloud potrebbe non essere finanziariamente sostenibile.

I criminali, ben consapevoli delle vulnerabilità derivanti da un ambiente così frammentato, cercano in tutti i modi di sfruttare le vulnerabilità del sistema e dell'architettura di un'organizzazione, che sono causate da requisiti e policy di sicurezza non coerenti, nonché di trarre vantaggio dalle difficoltà associate alla risoluzione dei problemi in un'infrastruttura cloud diversificata e frammentata.

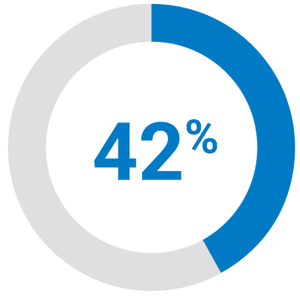
Sfortunatamente, la responsabilità della sicurezza negli ambienti basati sul cloud pubblico può risultare incoerente da un fornitore all'altro, poiché molte organizzazioni suppongono erroneamente di poterli lasciare sguarniti. Ad esempio, il 73% delle aziende che sono state sottoposte ad un sondaggio condotto da IBM ritiene che i fornitori di servizi sul cloud pubblico (CSP) sono i principali responsabili della sicurezza dei servizi SaaS (Software-as-a-Service), mentre il 42% pensa che i CSP siano principalmente responsabili della sicurezza dei servizi IaaS (Infrastructure-as-a-Service) nel cloud. Questa mancanza di chiarezza circa le responsabilità relative al controllo della sicurezza può condurre ad una violazione: un rischio che nessuna organizzazione è disposta ad accettare.



Percentuale di aziende che hanno adottato una strategia multicloud



Percentuale di partecipanti al sondaggio secondo cui i CSP sono responsabili della sicurezza dei servizi SaaS



Percentuale di partecipanti al sondaggio secondo cui i CSP sono responsabili della sicurezza dei servizi IaaS nel cloud

Le organizzazioni si rivolgono ora a fornitori di soluzioni per la protezione dagli attacchi DDoS in grado di offrire una piattaforma integrata, altamente scalabile e completa per proteggere le loro applicazioni, le API, il DNS e l'infrastruttura sottostante su cui si basano.

Non tutte le soluzioni di mitigazione degli attacchi DDoS sono progettate in modo uguale

Poiché le aziende continuano ad investire nelle infrastrutture cloud, i team addetti alla sicurezza si trovano di fronte alla sfida di garantire controlli coerenti in ambienti ibridi. Inoltre, visto che diventa sempre più difficile proteggere le applicazioni implementate in diverse infrastrutture di back-end nel cloud, molte organizzazioni cercano un unico punto di controllo in grado di gestire i sistemi di difesa.

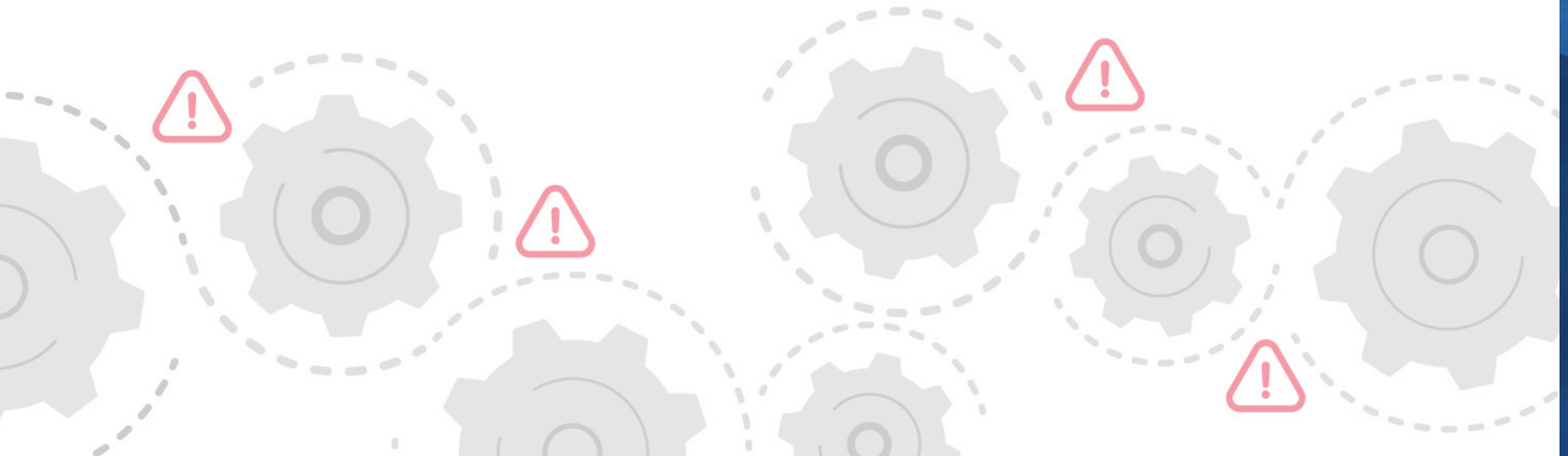
Poiché lo stack tecnologico dedicato alla sicurezza diventa sempre più complesso, molte organizzazioni desiderano disporre di una visione consolidata del proprio ambiente, non solo per ottimizzare la visibilità, ma anche per generare facilmente rapporti da poter trasmettere tramite le API ai sistemi di correlazione dei dati degli eventi.

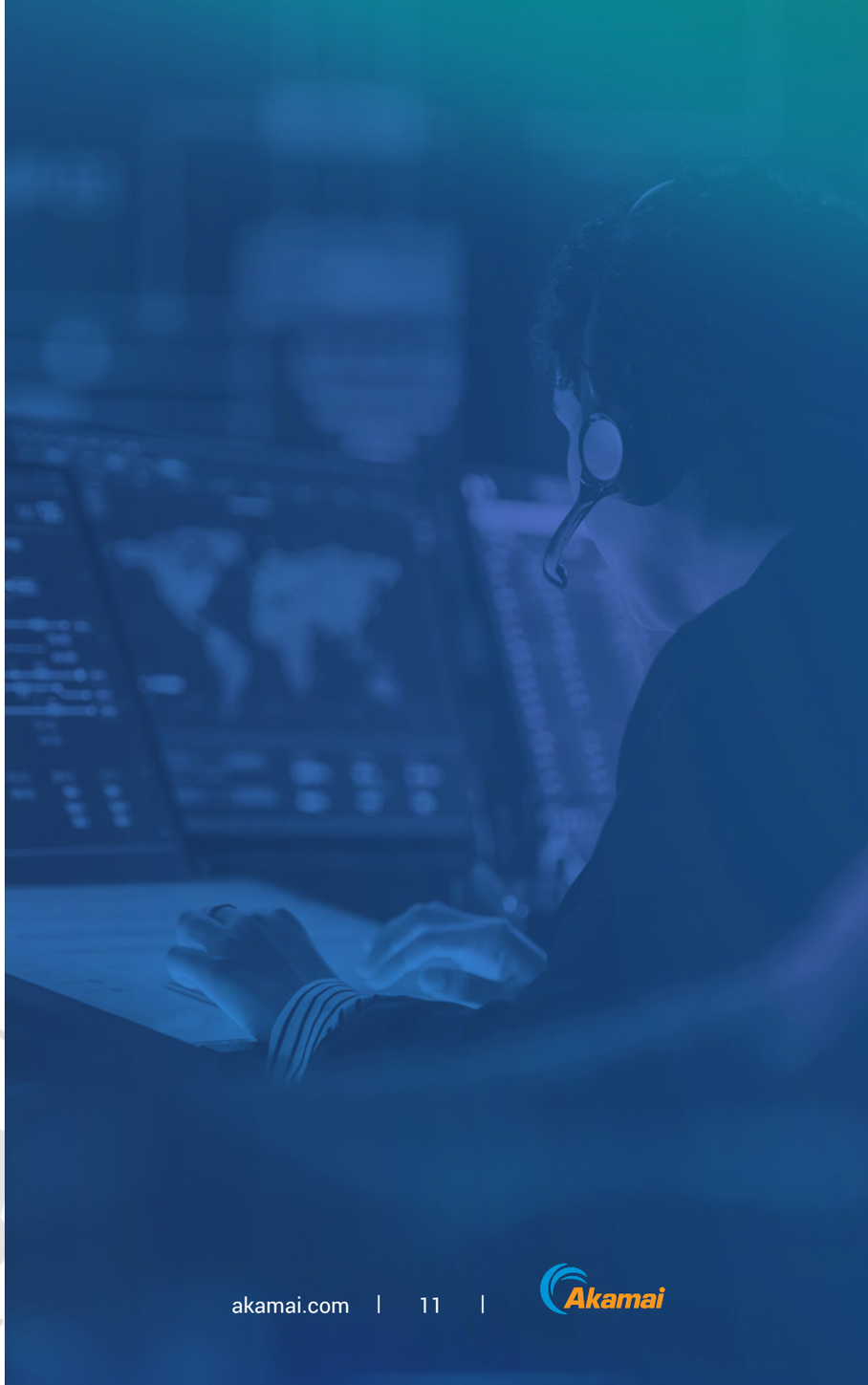
Per risolvere questo problema, le organizzazioni si rivolgono ora a fornitori di soluzioni per la protezione dagli attacchi DDoS in grado di offrire una piattaforma integrata, altamente scalabile e completa per proteggere le loro applicazioni, le API, il DNS e l'infrastruttura sottostante su cui si basano. Le organizzazioni hanno bisogno di sistemi di difesa scalabili e reattivi, indipendentemente dalla posizione in cui risiedono i servizi aziendali (on-premise, nel cloud o in un ambiente ibrido), per rispondere direttamente all'aumento della complessità operativa richiesta per integrare, implementare e gestire i sistemi di difesa DDoS nell'ambiente di un CSP. Inoltre, la situazione si fa ancora più complessa se consideriamo le numerose risorse online dislocate su più cloud pubblici e privati.

A complicare ulteriormente le cose, molte soluzioni per la mitigazione degli attacchi DDoS in sede fornite dai CSP sono prive di alcune funzionalità chiave, ossia visibilità, SLA (accordo sul livello di servizio) e generazione dei rapporti, il cui utilizzo è imprescindibile per gli esperti di sicurezza aziendale di oggi.

Per i team addetti alla sicurezza, la questione è tutta incentrata sul modo con cui ottenere visibilità e informazioni utili per ottimizzare la preparazione e la risposta ai problemi. Alcune soluzioni DDoS offerte dai CSP offrono una trasparenza minima (se non nulla) in termini di generazione di rapporti, visibilità e analisi post-attacco, pertanto non meraviglia il fatto che molti team si riferiscano ai CSP come alla "scatola nera" dell'analisi e della generazione di rapporti. Anche se alcuni CSP consentono ai team addetti alla sicurezza di un'organizzazione di impostare controlli e mantenere l'autonomia su specifici ambienti dei clienti, di solito, rifiutano qualsiasi responsabilità nei confronti del traffico degli attacchi DDoS e finiscono per addebitare ai clienti il volume astronomico del traffico dannoso derivante da un attacco DDoS, sia che si tratti o meno di un attacco DDoS a livello di applicazioni o di rete oppure al DNS.

Inoltre, alcuni CSP e vendor di soluzioni per la sicurezza non offrono uno SLA con chiare tempistiche di mitigazione (TTM), ma offrono invece crediti di servizio all'organizzazione che ha subito un attacco. È importante capire se la clausola TTM include il tempo necessario per identificare un attacco. Infatti, se una piattaforma richiede vari minuti o persino ore per identificare un attacco DDoS prima di attivare i suoi protocolli di mitigazione, l'organizzazione che ha subito l'attacco potrebbe rimanere offline per molto tempo. Nei casi in cui il fattore tempo è fondamentale, le organizzazioni devono avere la certezza che il loro fornitore si assumerà l'impegno di mantenere la disponibilità e i tempi di attività richiesti senza compromettere le performance.





Inoltre, è ugualmente (se non anche più) importante per i team addetti alla sicurezza o alle organizzazioni acquirenti capire se i vendor di soluzioni per la protezione dagli attacchi DDoS e i CSP offrono **una capacità di difesa DDoS dedicata** o se la capacità di difesa viene condivisa con la loro rete CDN. La difesa DDoS dedicata è simile ad un team SWAT focalizzato esclusivamente sulla lotta agli attacchi DDoS, che non condivide risorse o infrastrutture con altri aspetti delle attività aziendali, come la delivery dei contenuti, garantendo così un impatto minimo anche durante un attacco DDoS da record. Le organizzazioni che valutano una soluzione per la protezione dagli attacchi DDoS devono capire che gli stessi vendor, a volte, devono affrontare gli attacchi DDoS e tenere nella dovuta considerazione il fatto che riescano o meno ad offrire un tempo di attività/disponibilità regolato da uno SLA.

Infine, molti CSP e vendor di soluzioni per la sicurezza non forniscono un accesso on-demand al SOC (centro operativo per la sicurezza) globale 24/7 oltre all'assistenza prima, durante e dopo l'attacco. Se fornito, questo servizio aggiuntivo risulta spesso più costoso rispetto ad una soluzione ibrida per la mitigazione degli attacchi DDoS offerta dai principali fornitori del settore. Con una soluzione ibrida per la protezione dagli attacchi DDoS completamente gestita, i fornitori di servizi agiscono come un'estensione del team addetto alla risoluzione dei problemi di un'organizzazione, offrendo, al contempo, le competenze degli esperti necessarie per rispondere rapidamente agli eventi DDoS.

Nell'attuale panorama delle minacce, è chiaro che le aziende moderne si rivolgono a partner per la mitigazione degli attacchi DDoS in grado di supportare un'agevole experience di sicurezza in ambienti ibridi e di ridurre la complessità della superficie di attacco. Un partner per la protezione dagli attacchi DDoS deve facilitare, non ostacolare, l'adozione di una strategia ibrida o multicloud e allinearsi ai vostri obiettivi aziendali.

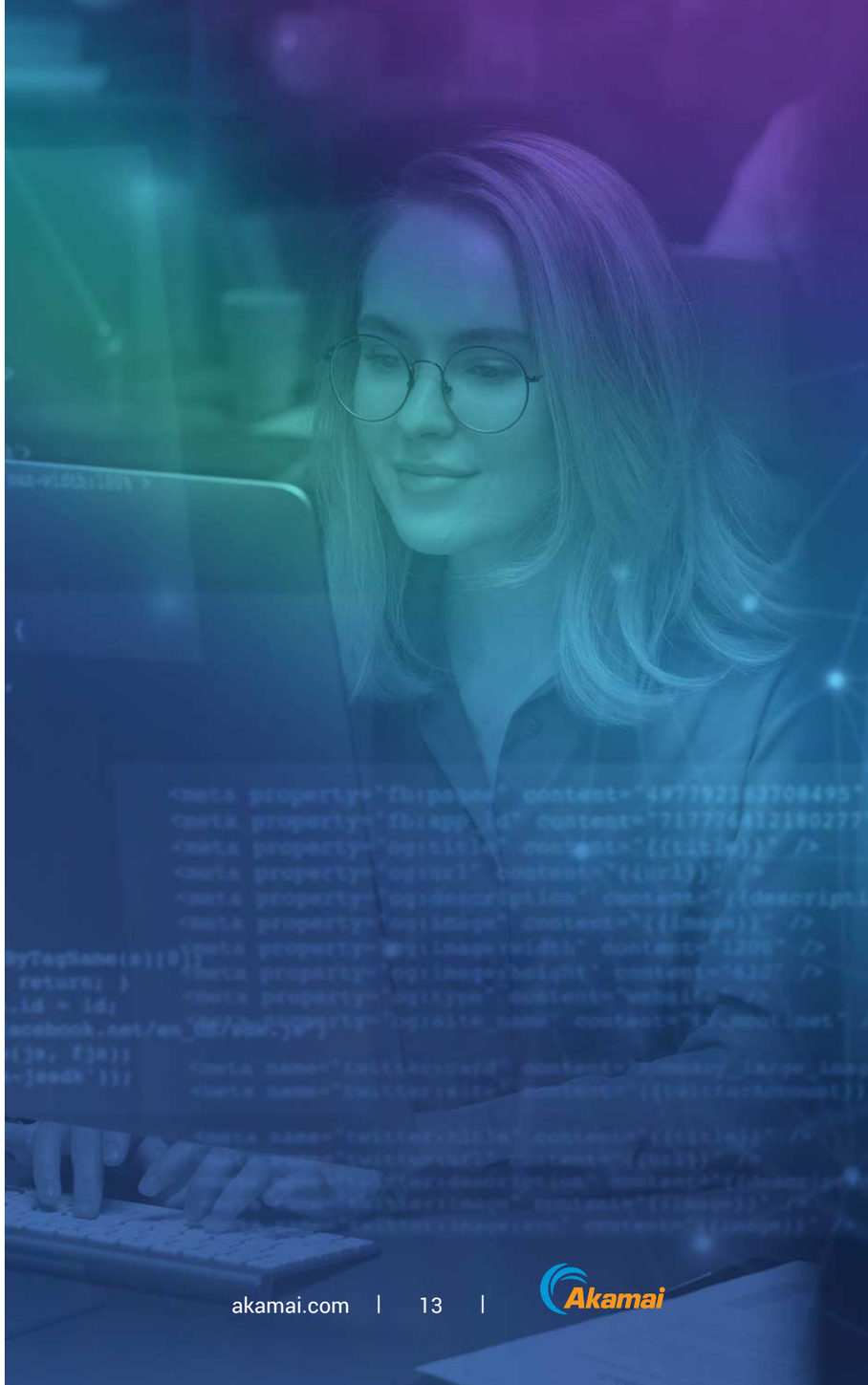
Mitigazione degli attacchi DDoS appositamente progettata con Akamai

Così come le organizzazioni hanno bisogno di una strategia per l'infrastruttura digitale end-to-end che include ambienti ibridi e multicloud, devono anche considerare l'adozione di un adeguato sistema di protezione dagli attacchi DDoS. Adottando un approccio completo, Akamai agisce come una prima linea di difesa, fornendo la protezione richiesta con strategie che si avvalgono di un edge dedicato, un DNS distribuito e strategie ibride di mitigazione nell'intento di prevenire danni collaterali e single point of failure. A differenza di altre architetture di CSP, concepite come prodotti "all-in-one", le soluzioni DDoS appositamente progettate di Akamai offrono un miglior livello di resilienza, una capacità di difesa DDoS dedicata e una qualità di mitigazione superiore che è ottimizzata per soddisfare gli specifici requisiti delle applicazioni web o dei servizi basati su Internet. La soluzione per la difesa dagli DDoS di Akamai è disponibile per i clienti ovunque (on-premise, nel cloud o in ambienti ibridi) e nel modo richiesto (always-on oppure on demand). Questa protezione completa è integrata in tre prodotti principali:

Capacità di difesa DDoS dedicata

DNS distribuito

Mitigazione ibrida



Akamai Prolexic: una soluzione per la protezione dagli attacchi DDoS concepita per una sicurezza proattiva e positiva

Un'architettura moderna e scalabile

Akamai Prolexic utilizza un'architettura completamente definita dal software in grado di adattarsi alle mutevoli tendenze della rete relative all'Edge Computing, al 5G/6G e alla virtualizzazione. Con il passaggio ad ambienti software virtualizzati, Prolexic ha eliminato tutte le dipendenze da hardware specializzato. Questa implementazione standardizzata consente ad Akamai di soddisfare le mutevoli esigenze dei clienti più rapidamente, facilitare le implementazioni modulari per l'estensione della capacità, fornire una migliore copertura locale con collegamenti a bassa latenza e migliorare la ridondanza sulla piattaforma. Inoltre, l'architettura aiuta ad accelerare le avanzate funzionalità di apprendimento dei comportamenti di Prolexic che apprendono dalle firme degli attacchi, si adattano ai nuovi vettori di attacco e costruiscono in modo proattivo sistemi resilienti agli attacchi DDoS per i clienti. Prolexic Cloud si avvale di più **scrubbing center in 32 aree metropolitane globali e di oltre 20 Tbps di capacità di difesa dedicata**. Per guardare in prospettiva la capacità di difesa di Prolexic, possiamo affermare che il più grande degli attacchi DDoS di livello 3 e di livello 4 non rappresenta neanche il 10% della capacità disponibile per i clienti di Prolexic.

Una protezione dagli attacchi DDoS completa, flessibile e affidabile

Akamai Prolexic è disponibile nei prodotti Prolexic Cloud, Prolexic On-Prem e Prolexic Hybrid.

Prolexic Cloud è una soluzione innovativa nel settore della protezione dagli attacchi DDoS basata sul cloud, che offre ai clienti uno SLA con disponibilità della piattaforma del 100% e mitigazione immediata. I controlli di mitigazione aumentano la capacità in modo dinamico per bloccare gli attacchi sui flussi di traffico dei protocolli IPv4 e IPv6. Le risorse di elaborazione possono essere allocate dinamicamente in base alle esigenze di mitigazione.

Prolexic On-Prem offre una protezione DDoS del percorso dati/online di tipo fisico o logico always-on, che si integra in modo nativo con gli edge router per bloccare automaticamente più del 98% degli attacchi sull'edge della rete dei clienti senza reindirizzare il traffico. Si tratta della soluzione ideale per la grande maggioranza degli attacchi piccoli e rapidi, oltre che per le aziende che richiedono una protezione dagli attacchi DDoS a latenza ultra-ridotta.

Prolexic Hybrid combina la potenza, l'automazione e le performance di Prolexic On-Prem con l'innovativo livello di portata e capacità on-demand di Prolexic Cloud per proteggere le origini dei clienti dagli attacchi DDoS volumetrici più imponenti.

La sicurezza oltre gli attacchi DDoS

Akamai Prolexic viene fornito con Prolexic Network Cloud Firewall , una funzionalità totalmente self-service e configurabile dagli utenti, che consente ai clienti di definire, implementare e gestire facilmente i loro elenchi di controllo degli accessi (ACL) e le regole che desiderano applicare all'edge della loro rete. Si tratta di un firewall posizionato a monte di tutti gli altri firewall. Network Cloud Firewall, inoltre, suggerisce gli ACL più appropriati per ottenere il miglior sistema di difesa proattivo in base ai dati dell'intelligence sulle minacce di Akamai e fornisce i dati analitici delle regole esistenti. Network Cloud Firewall è una soluzione FWaaS (Firewall-as-a-Service) innovativa, che consente ai clienti di:

- Definire sistemi di difesa proattivi per bloccare immediatamente il traffico dannoso
- Ridurre il carico di lavoro sull'infrastruttura locale spostando le regole sull'edge
- Adattarsi rapidamente alle modifiche della rete tramite una nuova interfaccia utente

Akamai Edge DNS e **Akamai Shield NS53** proteggono e rafforzano l'infrastruttura DNS critica

Akamai Edge DNS vi offre una protezione completa da un'ampia gamma di attacchi sferrati contro l'infrastruttura on-premise, nel cloud o in ambienti ibridi. La soluzione offre anche un elevato livello di performance, resilienza e disponibilità del DNS. Basata sulla rete Anycast distribuita su scala globale, la soluzione Edge DNS può essere implementata come servizio DNS primario o secondario, sostituendo o espandendo l'infrastruttura DNS esistente in base alle necessità.

Akamai Shield NS53 è un proxy inverso DNS bidirezionale che protegge l'infrastruttura DNS on-premise e ibrida (inclusi GSLB, firewall e server dei nomi) dagli attacchi di esaurimento delle risorse DNS (anche detti attacchi NXDOMAIN). I clienti possono configurare autonomamente, amministrare, gestire e applicare le loro policy di sicurezza dinamiche in tempo reale. Le query DNS illegittime e gli attacchi DNS flood vengono interrotti sull'edge della rete di Akamai per proteggere l'infrastruttura DNS critica dagli attacchi DDoS al DNS.

Akamai App & API Protector protegge le applicazioni e le API dagli attacchi DDoS

Riconosciuta come la soluzione per la protezione delle applicazioni web e delle API (WAAP) leader del settore, App & API Protector riesce a bloccare immediatamente gli attacchi DDoS a livello di rete sull'edge (per le proprietà ospitate sull'Akamai Connected Cloud) e offre accurate strategie di difesa dagli attacchi DDoS a livello di applicazioni.

Perché Akamai?

Akamai offre le soluzioni per la mitigazione degli attacchi DDoS più affidabili al mondo. Sia per la protezione di singole applicazioni, di interi data center o dell'infrastruttura DNS critica, Akamai ha progettato la mitigazione degli attacchi DDoS con i massimi livelli di capacità, resilienza e mitigazione disponibili.

Siamo riusciti a mitigare alcuni dei più vasti attacchi DDoS al mondo. I nostri controlli di mitigazione proattivi offrono una reale mitigazione immediata e uno SLA leader del settore. Inoltre, siamo in grado di fornire servizi di protezione dagli attacchi DDoS per più clienti e contrastare più attacchi DDoS contemporaneamente.

Poiché i vettori di attacco DDoS continuano a cambiare con una portata sempre maggiore, una piattaforma DDoS affidabile deve continuamente innovare, sviluppare e implementare funzionalità tali da rilevare le minacce in modo proattivo, organizzare le strategie di mitigazione e minimizzare l'impatto dei danni. Akamai si impegna nell'intento di stare un passo avanti rispetto alle minacce mitigando gli attacchi tempestivamente.

La mitigazione degli attacchi DDoS deve potenziare la strategia ibrida e multicloud. Le innovative soluzioni DDoS di Akamai proteggono l'infrastruttura di rete digitale, le applicazioni e il sistema DNS on-premise, nel cloud o in ambienti ibridi e offrono i vantaggi combinati dell'intelligenza umana e artificiale.

Ulteriori informazioni

 | Data di pubblicazione 10/24