WHITE PAPER

La rapida evoluzione e la crescente minaccia degli attacchi DDoS

Gli attacchi stanno diventando sempre più mirati, sofisticati e frequenti, pertanto tutte le aziende devono rimanere in stato di massima allerta.

Nessuna azienda si può più considerare realmente al sicuro dagli attacchi DDoS (Distributed Denial-of-Service). I cybercriminali, impegnati nelle loro attività di estorsione o hacktivismo oppure per farsi vendetta, possono facilmente mirare a qualsiasi organizzazione con attacchi sofisticati e di vasta portata. Ecco perché tutte le aziende orientate al digitale ora devono disporre di una difesa olistica dagli attacchi DDoS.

Uno dei primi tipi di attacchi su Internet

Il 22 luglio 1999, un computer dell'Università del Minnesota venne sommerso da pacchetti di dati superflui inviati da 114 computer compromessi rimanendo offline per due giorni.

Secondo la MIT Technology Review, si è trattato del primo attacco DDoS documentato.

Nelle settimane e nei mesi successivi, quando vennero interrotte le connessioni anche di importanti aziende come la CNN o Amazon, gli hacktivisti e altri cybercriminali si resero conto della semplicità con cui era possibile sferrare questi tipi di attacchi: ci volevano solo poche righe di codice.

L'attacco DDoS divenne una minaccia per qualsiasi azienda presente in rete.

Attacchi sempre più estesi e sofisticati

I sistemi di difesa dagli attacchi DDoS ne hanno fatta di strada dal 1999 e così pure i criminali. Oggi, per amplificare la portata delle loro attività, gli autori di attacchi DDoS possono sfruttare dozzine di vettori e toolkit a basso costo, nonché innumerevoli dispositivi vulnerabili presenti in rete. Nel 2016, i criminali misero fuori uso un'ampia porzione di Internet dopo aver violato delle telecamere di sorveglianza.

Da allora, centinaia di milioni di dispositivi IoT non protetti si sono connessi a Internet e, con l'avvento della rivoluzione del 5G, questo numero è destinato a raddoppiarsi, se immaginiamo soltanto la potenza e le dimensioni che avranno gli attacchi potenziati dai miglioramenti esponenziali apportati dal 5G in termini di velocità, capacità e latenza.

Non solo, è destinato a crescere a passi da gigante anche il numero di server in rete non protetti e non gestiti, di cui i criminali potranno assumere il controllo per sferrare attacchi di amplificazione e riflessione. Molti di questi server (di cui i criminali conoscono gli indirizzi IP) possono moltiplicare anche per 50.000 il numero delle richieste illegittime.

Mitigazione e protezione dagli attacchi DDoS 24/7

I clienti Akamai che subiscono un attacco DDoS possono contattare il SOCC (Security Operations Command Center) di Akamai.

I clienti non Akamai che desiderano ricevere una protezione in caso di emergenza possono compilare il modulo disponibile sulla nostra **pagina della linea diretta DDoS** o chiamare il numero **+1-877-425-2624** per assistenza immediata.

Nessun settore è immune agli attacchi DDoS

Attualmente, Akamai riesce a mitigare migliaia di attacchi DDoS ogni anno

e, in alcuni casi, per ovvi motivi. Un giocatore potrebbe usare gli attacchi DDoS per rallentare le reti e guadagnare un vantaggio competitivo sui suoi rivali. In un caso, alcuni studenti universitari hanno utilizzato attacchi DDoS mirati per frustrare il cliente di un ISP e favorire un'azienda concorrente.

A volte, tuttavia, i motivi sono più complessi o meno evidenti. Abbiamo osservato alcuni criminali utilizzare gli attacchi DDoS per distrarre i team impegnati nella risposta agli incidenti in una parte di un'organizzazione mentre tentavano di attaccare un'altra parte dell'azienda con un attacco più elusivo.

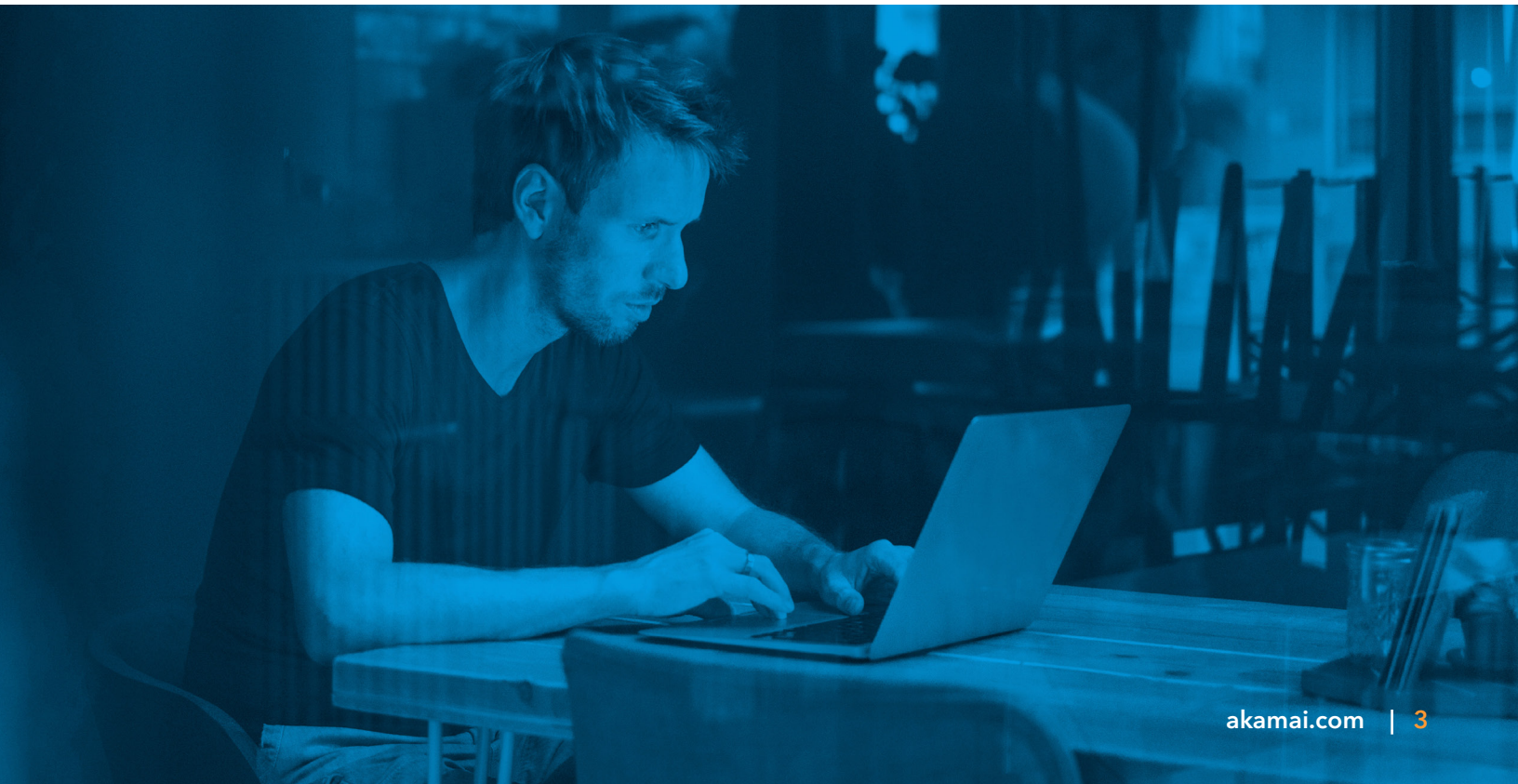
Per i criminali più inesperti, nel darknet esistono tante aziende da assoldare per sferrare attacchi DDoS, con prezzi che variano da 5 dollari per un attacco di 5 minuti fino a salire a 400 dollari per un attacco della durata di 24 ore. Se si vuole sferrare un attacco contro un'azienda, le si possono far perdere milioni spendendo soltanto 200 - 300 dollari.

Nel 2020 attacchi più ampi e sofisticati

Nella prima metà del 2020, Akamai ha bloccato massicci attacchi di 1,44 terabit al secondo (Tbps) e 809 milioni di pacchetti al secondo (Mpps) sferrati con il più imponente evento di questo tipo mai registrato.

Anche se mitigati in meno di un secondo, questi attacchi riflettono una tendenza orientata ad utilizzare dimensioni anche superiori a 100 Gbps. Molti attacchi impiegano complesse combinazioni di più vettori nell'intento di sommergere o eludere i sistemi di difesa e sfruttare le risorse impegnate nella risposta agli incidenti.

Si registra, inoltre, un aumento di attacchi la cui mitigazione richiede l'intervento umano, non solo risposte automatizzate.



La più vasta campagna di attacchi DDoS sferrati a scopo di estorsione nella storia

Nell'agosto 2020, il team di ricerca dell'intelligence sulla sicurezza di Akamai ha pubblicato un avviso per allertare le aziende di vari settori che avevano ricevuto e-mail di estorsione con la minaccia di attacchi DDoS. I criminali minacciavano di paralizzare le attività aziendali causando, pertanto, enormi problemi di downtime e pesanti perdite finanziarie se non fosse stato pagato un riscatto in bitcoin.

Solo alcune settimane dopo, l'FBI ha riferito che migliaia di organizzazioni in tutto il mondo avevano ricevuto simili e-mail di estorsione. I criminali attaccano e minacciano le aziende che operano in un settore per poi passare successivamente a colpire altri settori. I criminali più organizzati, spesso, ritornano a minacciare aziende già colpite in precedenza.

Migliori sono le difese, minori sono le probabilità di attacco

I cybercriminali non sono uguali agli altri: preparano il campo d'azione esaminando le eventuali vulnerabilità presenti. Prima di sferrare un attacco DDoS, cercano un punto debole nel DNS, nelle applicazioni web e nei data center online della vittima designata.

Se notano una vulnerabilità nelle risorse, nei siti o nei servizi, cercano di accedervi. Se, invece, si trovano davanti solidi sistemi di difesa, nella maggior parte dei casi lasciano perdere.

In realtà, per la maggior parte, i clienti Prolexic che si rivolgono a noi per ricevere assistenza in caso di emergenza, dopo aver subito un attacco prima di instradare il traffico sulla piattaforma, non sono stati colpiti nuovamente una volta implementati i sistemi di difesa Prolexic. Per un cybercriminale potrebbe sembrare una perdita di tempo affrontare i sistemi di difesa messi in atto da Prolexic, soprattutto se altrove esistono obiettivi più vulnerabili.

Come funziona una difesa olistica dagli attacchi DDoS

Akamai fornisce un'approfondita difesa dagli attacchi DDoS attraverso una combinazione di soluzioni di mitigazione basate su edge dedicato, DNS distribuito e scrubbing su cloud, con oltre 175 Tbps di capacità di rete totale. Queste soluzioni sul cloud appositamente studiate sono progettate per rafforzare le strategie di sicurezza DDoS, riducendo, al contempo, le superfici di attacco. Questa protezione DDoS end-to-end è concepita per migliorare la qualità della mitigazione e ridurre i falsi positivi, aumentando, così, la resilienza rispetto agli attacchi più vasti e complessi.

Inoltre, è possibile ottimizzare la soluzione in base ai requisiti specifici delle applicazioni web e dei servizi basati su Internet.

Difesa sull'edge

Akamai ha progettato l'Intelligent Edge Platform distribuita globalmente come un proxy inverso che accetta il traffico solo tramite le porte 80 e 443. Tutti gli attacchi DDoS a livello di rete vengono subito interrotti sull'edge grazie ad uno SLA (accordo sul livello di servizio) immediato.

Per gli eventi a livello delle applicazioni, compresi gli attacchi sferrati tramite le API, Kona Site Defender assorbe gli attacchi, garantendo, al tempo stesso, l'accesso agli utenti legittimi.

Difesa del DNS

Il servizio DNS autoritativo di Akamai, Edge DNS, filtra anche il traffico sull'edge. A differenza di altre soluzioni DNS, Akamai ha progettato Edge DNS specificamente per offrire caratteristiche di disponibilità e resilienza contro gli attacchi DDoS. Edge DNS assicura, inoltre, performance superiori con ridondanze delle architetture a più livelli, inclusi server dei nomi, punti di presenza, reti e persino cloud IP Anycast segmentati.

Difesa dello scrubbing su cloud

Prolexic protegge tutti i data center e le infrastrutture ibride dagli attacchi DDoS, su tutte le porte e i protocolli, con 20 scrubbing center globali e 8,2 Tbps di capacità di difesa DDoS dedicata. Questa capacità è studiata per mantenere a disposizione le risorse su Internet: fondamento essenziale in ogni programma di tutela della sicurezza delle informazioni.

In qualità di servizio completamente gestito, Prolexic è in grado di costruire modelli di sicurezza positivi e negativi. Il servizio combina sistemi di difesa automatizzati con la mitigazione esperta della rete globale offerta dai SOCC di Akamai. Prolexic offre anche un **immediato** SLA di mitigazione leader del settore attraverso controlli di difesa proattivi.

Come Prolexic ha bloccato un attacco da record

Nel giugno 2020, si è registrato il più imponente attacco PPS (pacchetti al secondo) mai osservato su Internet con dimensioni pari a 809 Mpps. A differenza dei più comuni attacchi BPS (bit al secondo), che cercano di sovraccaricare il traffico Internet in entrata, gli attacchi PPS hanno l'obiettivo di esaurire la capacità delle reti nei data center o sul cloud.

Questo attacco di proporzioni straordinarie ha riguardato un numero enorme di indirizzi IP di origine, di cui oltre il 96% non era mai stato coinvolto in altri attacchi in precedenza. Le dimensioni dell'attacco sono cresciute da 418 Gbps a 809 Mpps in soli due minuti.

Fortunatamente, l'azienda presa di mira utilizzava la soluzione Prolexic, supportata da uno SLA immediato. Il SOCC di Akamai ha collaborato con l'azienda per comprendere i suoi profili di traffico "in tempo di pace", implementando le policy di sicurezza e i controlli necessari per bloccare immediatamente gli attacchi DDoS.

Pianificate un briefing personalizzato sulle minacce

Visitate il sito all'indirizzo **akamai.com/ddos-briefing**