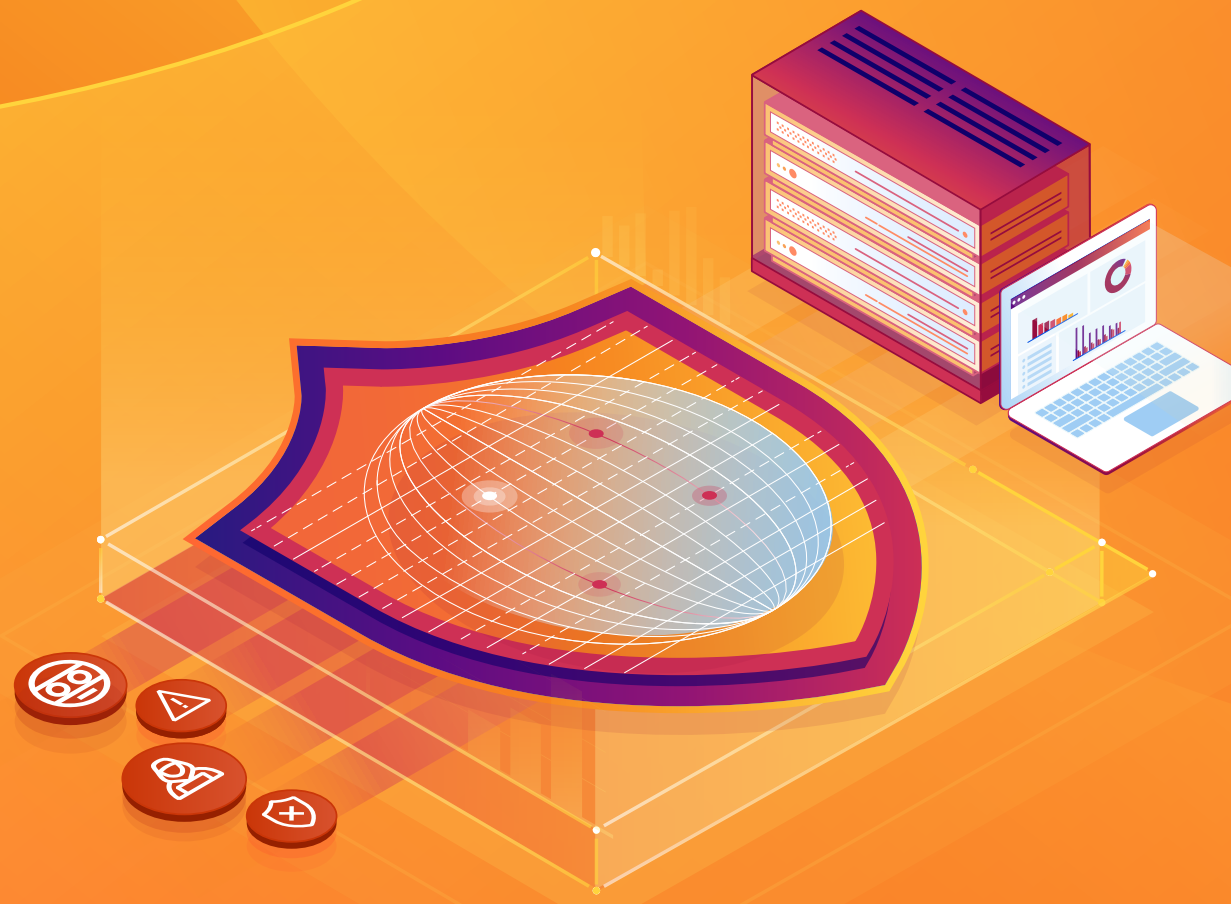
CLOUDFLARE

Report sulle tendenze DDoS di Cloudflare



Contenuto

3 **Sintesi**

4 **Punti salienti del report**

4 Tendenze DDoS per l'anno 2023

5 Zone di conflitto specifiche e attacchi DDoS: Elezioni generali a Taiwan e conflitto israeliano con Hamas

6 Eventi politici globali che innescano attacchi informatici tendenzialmente in aumento

6 Festività del quarto trimestre: gli attacchi guastafeste DDoS

7 Vettori di attacco emergenti a livello di rete

9 **Principali tendenze DDoS — Quarto trimestre 2023**

11 **Raccomandazioni e consigli**

Quarto trimestre 2023

Sintesi

Benvenuti alla sedicesima edizione del report sulle minacce DDoS di Cloudflare. Gli attacchi DDoS, o Distributed Denial-of-Service, sono un tipo di attacco informatico che mira a disturbare i siti Web (e altri tipi di proprietà Internet) per renderli non disponibili agli utenti legittimi sovraccaricandoli con traffico eccessivo. Immaginatelo come se causasse un ingorgo su una strada critica, impedendo alle persone di raggiungere la loro destinazione.

La nostra rete è una delle più grandi al mondo e comprende più di 310 città in oltre 120 paesi. Gestiamo un'enorme quantità di traffico Internet, servendo oltre 70 milioni di richieste Web al secondo al massimo ed elaborando 2,6 miliardi di query DNS al giorno. In media, ogni giorno contrastiamo 170 miliardi di minacce informatiche. Questo vasto volume di dati ci offre una prospettiva unica sul panorama delle minacce DDoS, consentendoci di condividere informazioni e tendenze preziose con la comunità della sicurezza informatica.

Nelle ultime settimane, abbiamo osservato un'impennata degli attacchi DDoS e di altri attacchi informatici, nel contesto delle elezioni generali che si sono concluse di recente a Taiwan e delle tensioni segnalate con la Cina. Mentre il conflitto militare tra Israele e Hamas continua, i siti Web palestinesi, così come quelli israeliani, hanno dovuto affrontare attacchi DDoS significativamente maggiori.

Da un confronto annuale emerge che gli attacchi DDoS a livello di applicazione diminuiscono del 20% su base annua nel 2023 rispetto al 2022. Ironicamente, il 2023 ha visto anche le più grandi campagne di attacchi DDoS a livello applicazione, attacchi che hanno superato i 100 milioni di richieste al secondo in più istanze, inclusa la campagna di attacco HTTP/2 Rapid Reset all'inizio di quest'anno. A livello di rete, abbiamo osservato una tendenza completamente diversa: un aumento dell'85% degli attacchi DDoS a livello di rete nel 2023 rispetto al 2022.

In particolare, le organizzazioni di servizi ambientali hanno registrato il volume più elevato di traffico di attacchi DDoS HTTP, che ha coinciso con la 28a Conferenza delle Nazioni Unite sui cambiamenti climatici (COP 28).

Una versione interattiva di questo report è disponibile su Cloudflare Radar.

Punti salienti del report

Tendenze DDoS per l'anno 2023

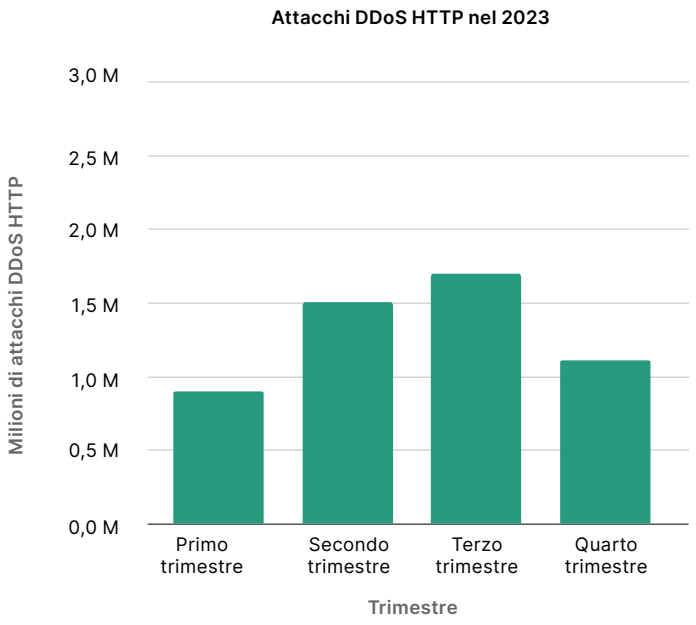
Una volta che la campagna ad alto volume si è calmata, abbiamo assistito a un calo inaspettato degli attacchi DDoS HTTP del 20% rispetto al 2022. Complessivamente nel 2023, le nostre difese automatizzate hanno mitigato oltre 5,2 milioni di attacchi DDoS HTTP costituiti da oltre 26 trilioni di richieste. Nonostante il calo nel numero di attacchi, il numero medio di attacchi bloccati è molto elevato: 594 attacchi DDoS HTTP bloccati e 3 miliardi di richieste mitigate ogni ora del 2023.

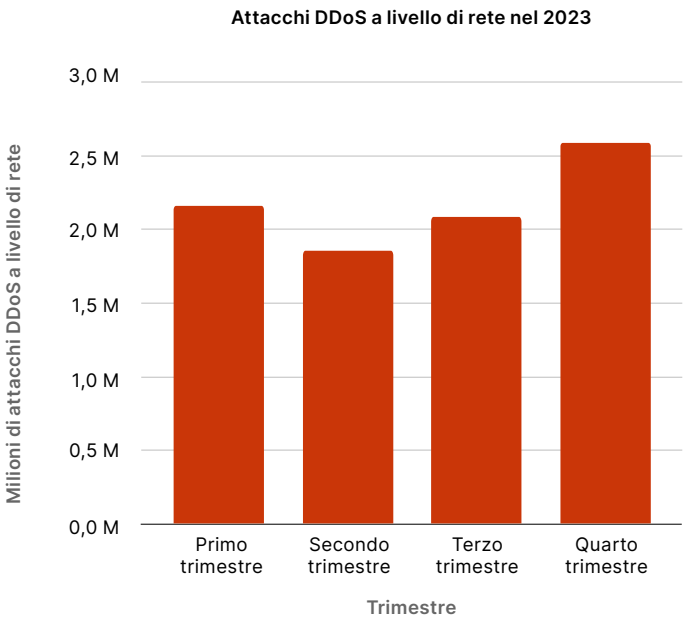
A livello di rete, abbiamo osservato una tendenza completamente diversa. Le nostre difese automatizzate hanno mitigato 8,7 milioni di attacchi DDoS a livello di rete nel 2023. Ciò rappresenta un aumento dell'85% rispetto al 2022. In media, i nostri sistemi hanno mitigato 996 attacchi DDoS a livello di rete e 27 terabyte ogni ora.

2023 - I numeri degli attacchi DDoS

Attacchi DDoS HTTP
5,2 milioni di attacchi mitigati nel 2023
-20% su base annua

Attacchi DDoS a livello di rete
8,7 milioni di attacchi 8.7 mitigati nel 2023
+85% su base annua





Zone di conflitto specifiche e attacchi DDoS: elezioni generali di Taiwan e conflitto israeliano con Hamas

L'ondata di attacchi contro regioni specifiche (Taiwan, Israele e territori palestinesi) sottolinea l'uso di DDoS come strumento nella guerra informatica, le capacità informatiche vengono sfruttate per esercitare pressioni politiche o interrompere infrastrutture digitali critiche.

Elezioni generali di Taiwan

Abbiamo riscontrato un aumento del 3.370% su base annua degli attacchi DDoS HTTP contro i siti Web di Taiwan. La stragrande maggioranza (82%) proveniva dalla Cina, il che è correlato all'accesa retorica politica in Cina e Taiwan in questo momento. Sorprendentemente, i siti web di intrattenimento per adulti sono stati presi di mira più dei settori comuni radicati nella vita quotidiana come i servizi finanziari, la sanità e i trasporti.

Guerra Israele-Hamas

Gli attacchi DDoS sono uno strumento di guerra e di disturbo accettato. Abbiamo assistito a un aumento dell'attività di attacchi DDoS nella guerra Ucraina-Russia, e ora lo stiamo vedendo anche nella guerra Israele-Hamas. Per prima cosa abbiamo segnalato l'attività informatica nel nostro post sul blog Attacchi informatici nella guerra Israele-Hamas, e a tutt'oggi continuiamo a monitorare quest'attività.

I territori palestinesi sono stati la seconda regione più attaccata al mondo da attacchi DDoS HTTP e a livello di rete nel quarto trimestre. Gli attacchi DDoS hanno rappresentato oltre il 68% di tutto il traffico di livello 3 e livello 4 verso le reti palestinesi e oltre il 10% di tutte le richieste HTTP verso i siti web palestinesi. 9 su 10 di questi attacchi DDoS HTTP hanno preso di mira siti Web bancari palestinesi.

Anche i siti Web israeliani hanno assistito a un traffico DDoS intenso, sebbene abbiano registrato un aumento più modesto del 27% nel traffico DDoS HTTP trimestre su trimestre. I settori dei giornali, dei media e dei software per computer hanno ricevuto quasi il 65% di tutti gli attacchi DDoS HTTP contro i siti Web israeliani.

I nostri dati suggeriscono uno sforzo concertato per danneggiare le industrie radicate nella vita quotidiana da entrambe le parti.

Eventi politici globali che innescano attacchi informatici tendenzialmente in aumento

Stiamo assistendo a una tendenza crescente secondo cui gli eventi globali possono diventare punti di innesco per attacchi informatici. La 28a Conferenza delle Nazioni Unite sui cambiamenti climatici (popolarmente nota come COP 28) si è conclusa il 13 dicembre 2023. Abbiamo assistito a un aumento sconcertante (oltre il 61.000%) degli attacchi DDoS HTTP contro le organizzazioni di servizi ambientali tra ottobre e dicembre 2023 rispetto allo stesso periodo del 2022. Il modello non è stato isolato solo da questo evento.

Guardando indietro ai dati storici, in particolare durante la COP 26 e la COP 27, così come altre risoluzioni o annunci delle Nazioni Unite relativi all'ambiente, emerge uno schema simile. Ciascuno di questi eventi è stato accompagnato da un corrispondente aumento degli attacchi informatici rivolti ai siti web dei Servizi Ambientali.

Festività del quarto trimestre: gli attacchi guastafeste DDoS

Abbiamo riscontrato un aumento dell'attività DDoS HTTP che ha preso di mira siti web di vendita al dettaglio, spedizioni e pubbliche relazioni tra il Black Friday, Natale e le festività di Capodanno. A livello applicazione, il settore dell'imballaggio e della consegna delle merci è stato il secondo più preso di mira (dopo il settore dei servizi ambientali) rispetto al traffico HTTP complessivo di ciascun settore. Questo settore è alla base del successo del Black Friday e dell'esperienza di shopping delle vacanze invernali. I regali e i beni acquistati devono arrivare a destinazione in modo accurato e puntuale. Gli autori di attacchi potrebbero aver tentato di interferire. Anche gli attacchi DDoS a livello applicazione contro le aziende di vendita al dettaglio sono aumentati del 16% rispetto all'anno precedente, il 2022.

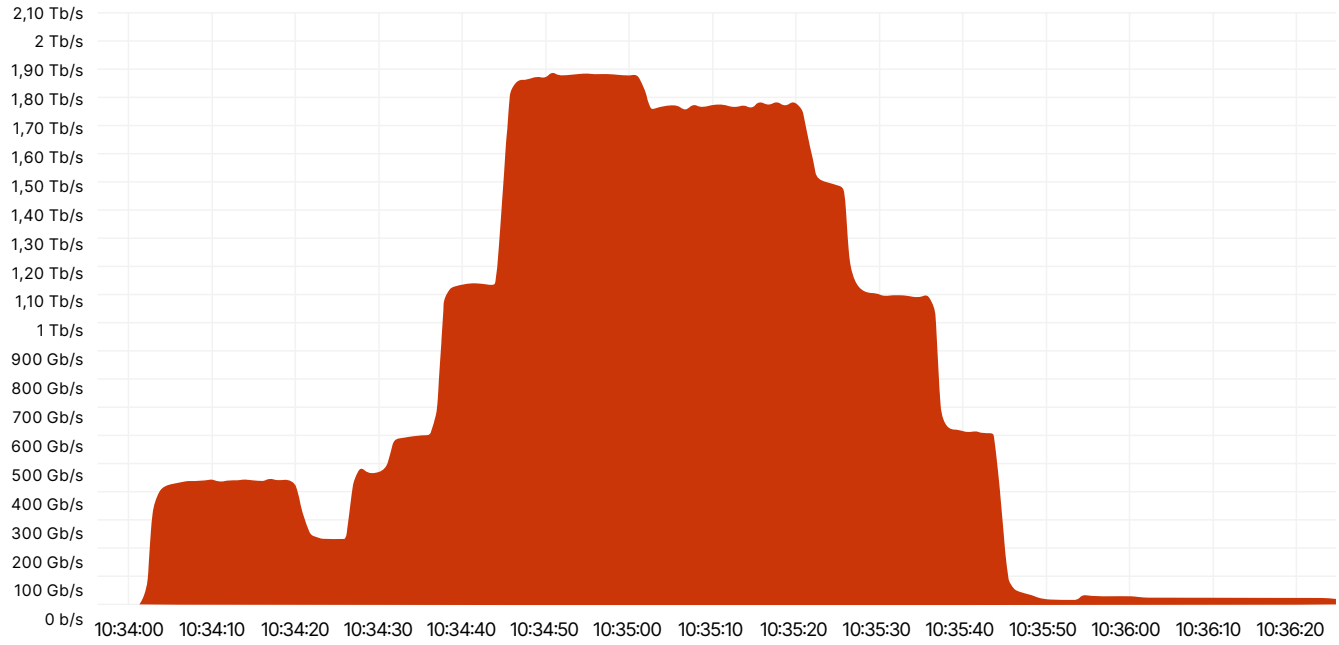
A livello di rete, il settore delle pubbliche relazioni (PR) e delle comunicazioni è stato il settore più preso di mira — Il 36% del suo traffico era dannoso. Interrompere le operazioni di questo settore può avere impatti reputazionali immediati e diffusi. I mesi da ottobre a dicembre e la fine dell'anno vedono spesso un aumento delle attività di PR e comunicazione a causa delle vacanze, dei riepiloghi di fine anno e dei preparativi per il nuovo anno. In breve, è un periodo operativo critico — uno che gli autori di attacchi potrebbero voler interrompere.

Vettori di attacco emergenti a livello di rete

Esaminiamo un attacco specifico per esplorare il panorama in evoluzione a livello di rete DDoS.

Uno degli attacchi più grandi tra ottobre e dicembre 2023 è stato un attacco botnet Mirai che ha preso di mira un noto provider cloud europeo per meno di dieci minuti e ha avuto origine da oltre 18.000 indirizzi IP univoci (si presume sia stato falsificato). È stato rilevato e mitigato automaticamente dalle difese di Cloudflare.

Grave attacco botnet Mirai al provider cloud europeo

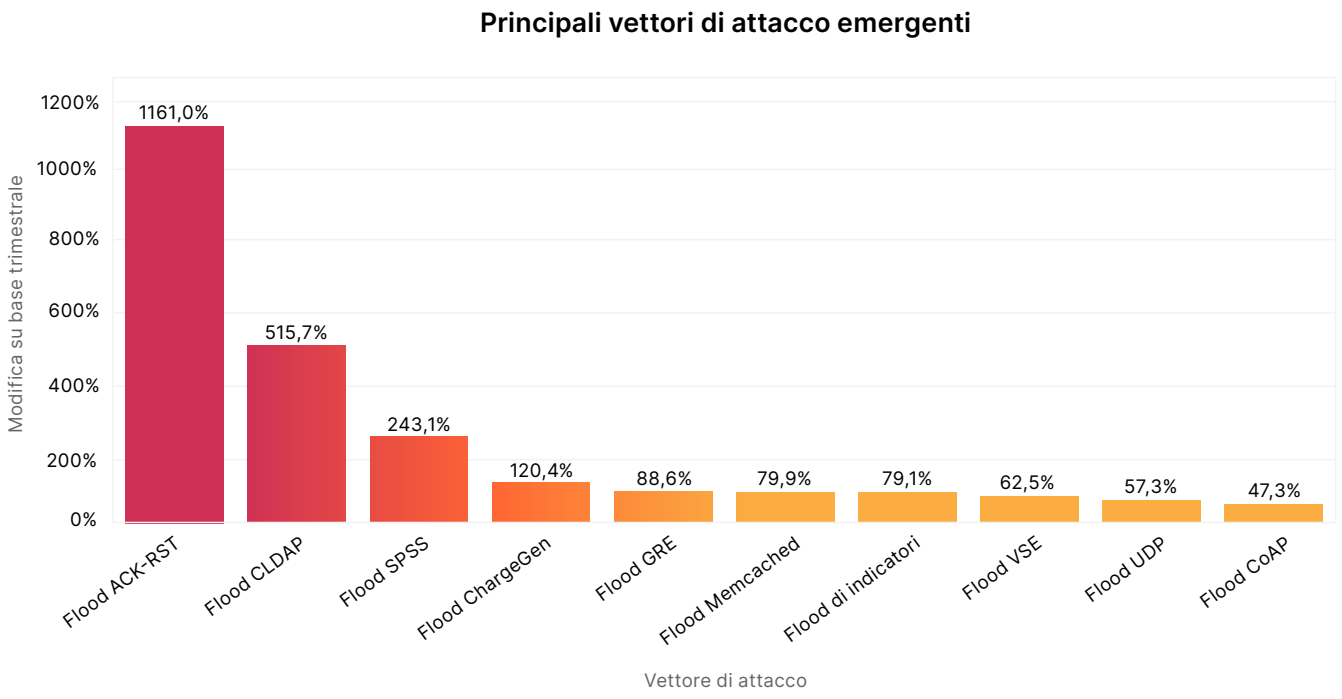


Questo attacco era unico in termini di elevata velocità di bit al secondo e natura di attacco multi-vettore, eppure è durato solo per un breve periodo. Ha raggiunto il picco di 1,9 terabit al secondo e ha combinato diversi metodi di attacco tra cui il flood di frammenti UDP, il flood UDP/Echo, il flood SYN, il flood ACK e i flag TCP malformati. Attacchi con velocità di bit al secondo così grandi sono rari. Ancora più sofisticato è che gli attacchi combinino più metodi.

La velocità di pacchetti al secondo, pari a 160 milioni di pacchetti al secondo, non è stata la più alta mai vista, pari a 754 milioni di pacchetti al secondo nel 2020.

Al di là di questo attacco con le sue caratteristiche uniche, le organizzazioni non possono permettersi di utilizzare scrubbing center manuale per le proprie difese DDoS. Hanno bisogno di sistemi di difesa automatizzati in linea.

Tra le minacce emergenti che monitoriamo, abbiamo registrato un aumento del 1.161% delle inondazioni ACK-RST, nonché un aumento del 515% delle inondazioni CLDAP e un aumento del 243% delle inondazioni SPSS, in ogni caso rispetto allo scorso trimestre. Esaminiamo alcuni di questi attacchi e il modo in cui sono destinati a causare interruzioni.



Flood ACK-RST

Un flusso ACK-RST sfrutta il protocollo di controllo della trasmissione (TCP) inviando numerosi pacchetti ACK e RST alla vittima. Ciò travolge la capacità della vittima di elaborare e rispondere a questi pacchetti, portando all'interruzione del servizio. L'attacco è efficace perché ogni pacchetto ACK o RST richiede una risposta dal sistema della vittima, consumandone le risorse. I flood ACK-RST sono spesso difficili da filtrare poiché imitano il traffico legittimo, rendendo difficoltosi il rilevamento e la mitigazione.

Flood CLDAP

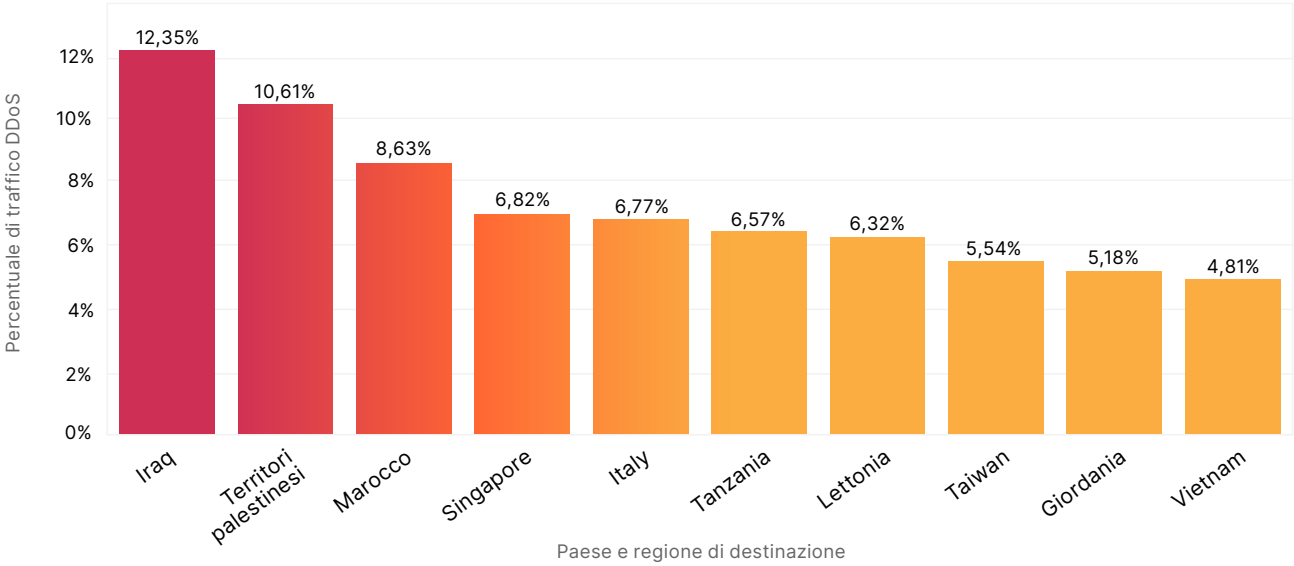
Il CLDAP (Protocollo di accesso leggero alla directory senza connessione) è una variante di LDAP (Protocollo di accesso alle directory leggero). Viene utilizzato per interrogare e modificare i servizi di directory in esecuzione su reti IP. Il CLDAP è senza connessione e utilizza UDP anziché TCP, rendendolo più veloce ma meno affidabile. Poiché utilizza UDP, non esiste alcun requisito di handshake che consenta agli autori di attacchi di falsificare l'indirizzo IP consentendo così agli autori di attacchi di sfruttarlo come vettore di riflessione. In questi attacchi, piccole query vengono inviate con un indirizzo IP di origine falsificato (l'IP della vittima), facendo sì che i server inviino risposte di grandi dimensioni alla vittima, sopraffacendola. La mitigazione prevede il filtraggio e il monitoraggio del traffico CLDAP insolito.

Flood SPSS

I flussi che abusano del protocollo SPSS (Source Port Service Sweep) sono un metodo di attacco di rete che prevede l'invio di pacchetti da numerose porte di origine casuali o contraffatte a varie porte di destinazione su un sistema o una rete mirata. Lo scopo di questo attacco è duplice: in primo luogo, sopraffare le capacità di elaborazione della vittima, causando interruzioni del servizio o interruzioni della rete, e in secondo luogo, può essere utilizzato per scansionare porte aperte e identificare servizi vulnerabili. Il flusso si ottiene inviando un grande volume di pacchetti, che possono saturare le risorse di rete della vittima ed esaurire le capacità dei suoi firewall e dei sistemi di rilevamento delle intrusioni. Per mitigare tali attacchi, è essenziale sfruttare le funzionalità di rilevamento automatico in linea.

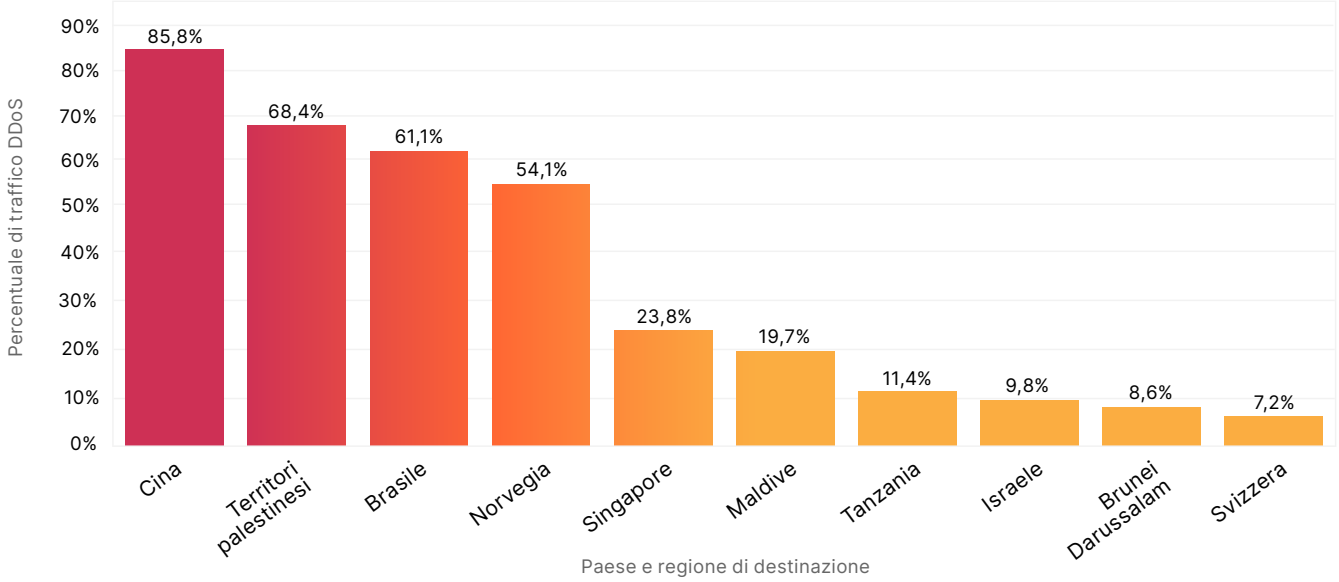
Regioni più attaccate

Principali paesi presi di mira dagli attacchi DDoS HTTP rispetto al traffico di ciascun paese



Iraq, territori palestinesi e Marocco sono in testa come regioni più attaccate rispetto al traffico totale in entrata. La cosa interessante è che Singapore arriva al quarto posto. Non solo Singapore ha dovuto affrontare la maggiore quantità di traffico di attacchi DDoS HTTP (il 4% di tutto il traffico DDoS globale), ma tale traffico dannoso ha anche costituito una quantità significativa del traffico HTTP totale diretto a Singapore. Al contrario, gli Stati Uniti sono stati il secondo paese più attaccato in termini di volume di traffico DDoS (3,8% di tutto il traffico DDoS globale), ma si sono piazzati al cinquantesimo posto se normalizzato in base al traffico HTTP totale diretto negli Stati Uniti.

Principali paesi presi di mira dagli attacchi DDoS a livello di rete rispetto al traffico di ciascun paese



Le tendenze a livello di rete per regione sono ancora più evidenti rispetto a quelle a livello applicazione.

La Cina continua a essere il paese più preso di mira a livello di rete nel 2023. Ancora più drammatico delle tendenze DDoS HTTP per Singapore, la Cina è il paese più attaccato sia dal traffico di attacchi DDoS a livello di rete, sia rispetto a tutto il traffico diretto in Cina. Quasi l'86% di tutto il traffico diretto in Cina è stato mitigato da Cloudflare come attacchi DDoS a livello di rete. Per altre tre regioni, territori palestinesi, Brasile e Norvegia, più di 1 byte su 2 in quella regione ha subito un attacco DDoS.

Raccomandazioni e consigli

Best practice	Ottimizza l'utilizzo di Cloudflare
Aggiorna o crea un piano di risposta al Denial of Service.	Assicurati che il tuo fornitore di sicurezza fornisca una hotline di emergenza 24 ore su 24, 7 giorni su 7 La hotline di Cloudflare Under Attack fornirà competenze, processi e tecnologia in materia di sicurezza per gestire gli attacchi in tempo reale. Metti alla prova il processo di risposta agli incidenti e gli accordi sul livello di servizio (SLA) dei tuoi fornitori di sicurezza prima di un vero attacco DDoS. Identifica e forma il personale sul piano di risposta DDoS documentato. Assicurati che leggano attentamente il Percorso di apprendimento DDoS di Cloudflare per ottimizzare i controlli di Cloudflare.
Distribuisci l'intelligence delle minacce e le soluzioni di mitigazione degli attacchi DDoS automatizzate in linea. Gli scrubbing center manuali non sono in grado di adattarsi ai moderni attacchi a volume elevato e a raffica breve.	Utilizza più tecniche di rilevamento per ottimizzare il tuo livello di sicurezza di fronte al panorama delle minacce in continua evoluzione: 1. Fingerprinting apolide dinamico 2. Classificazione basata sull'apprendimento automatico 3. Rilevamento traffico senza stato 4. Profilazione del traffico e mitigazione con stato 5. Intelligence delle minacce relative all'attività e alle tendenze DDoS attuali
Aggiorna la tua rete, DNS e infrastruttura applicativa per renderli più resilienti per il tuo profilo di traffico.	Assicurati che la capacità dei tuoi strumenti di mitigazione degli attacchi DDoS sia sufficientemente estesa da gestire il doppio degli attacchi più grandi mai registrati e il doppio della velocità massima del tuo traffico legittimo. Assicurati che il tuo fornitore di sicurezza possa mitigare le più recenti vulnerabilità dei protocolli a livello applicazione e rete. Scarica il traffico DNS su piattaforme cloud conformi e protette con il traffico instradato attraverso le reti edge più vicine all'utente.
Migliora le prestazioni della rete e delle applicazioni per evitare colli di bottiglia.	Sfrutta una sala d'attesa digitale per garantire che utenti e visitatori reali siano informati con garbo del periodo di attesa senza sovraccaricare i server delle applicazioni. Ottimizza la memorizzazione nella cache, gestisci meglio i carichi con una rete per la distribuzione di contenuti (CDN) e soluzioni di bilanciamento del carico basate su cloud.
Utilizza un modello di sicurezza positivo: assicurati che il traffico desiderato entri in modo affidabile.	Mantieni aperti i protocolli aziendali, gli IP, gli ASN, le porte e gli agenti utente per pulire il traffico. Utilizza la convalida dello schema e un gateway API per il traffico API.
Sfrutta l'intelligenza artificiale per stare al passo con le minacce emergenti.	Punteggi bot che possono essere utilizzati all'interno di firewall e regole di limitazione della frequenza. Scopri automaticamente le tue API rivolte al pubblico e proteggile dagli attacchi DDoS.

In Cloudflare, vogliamo fare in modo che per le aziende di ogni dimensione diventi ancora più semplice (e gratuito) proteggersi anche dagli attacchi DDoS più grandi e complessi. Forniamo a tutti i nostri clienti protezione gratuita da attacchi DDoS sin dal 2017.

Scopri di più sulla difesa dalle minacce DDoS più recenti con Cloudflare.

© 2024 Cloudflare Inc. Tutti i diritti riservati.
Il logo Cloudflare è un marchio di Cloudflare. Tutti gli altri nomi di società e prodotti possono essere marchi delle società cui sono rispettivamente associati.

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-5497.2024FEB08