SOTI

V10, NUMERO 02

10 YEARS
OF SECURITY INSIGHT

Come contrastare la crescita degli

attacchi DDoS nell'area EMEA

Akamai

Stato di Internet - Security

Sommario

2 Gli attacchi DDoS sono in aumento nell'area EMEA

4 Il presente e il futuro degli attacchi DDoS

8 Analisi dei dati relativi agli attacchi DDoS nell'area EMEA

15 Contrastare gli attacchi rivalutando il potere dell'infosicurezza

17 Case study: una società di e-commerce europea subisce un attacco DDoS a livello di rete

18 Salvaguardia e mitigazione

20 Conclusione

21 Metodologia

23 Riconoscimenti

Gli attacchi DDoS sono in aumento nell'area EMEA

Gli attacchi DDoS (Distributed Denial-of-Service) aumentano a livello globale e diventano sempre più sofisticati. Questa impennata è particolarmente evidente nell'area EMEA (Europa, Medio Oriente e Africa), in cui i ricercatori di Akamai hanno osservato un significativo aumento del tasso di crescita degli attacchi DDoS; infatti, il numero di attacchi DDoS in quest'area geografica sta aumentando più rapidamente che altrove. Gli attacchi DDoS colpiscono i loro obiettivi con traffico dannoso indesiderato e ostacolano le operazioni di reti e siti web nell'area EMEA.

La nostra ipotesi è che gran parte di questo spostamento da un'area geografica all'altra sia dovuto alle attuali tensioni geopolitiche, come le attività criminali sostenute dai governi e l'hacktivismo in risposta alle guerre in corso, comprese le guerre tra Russia e Ucraina e tra Israele e Hamas. Inoltre, gli imminenti eventi importanti e le elezioni in Europa probabilmente aumenteranno ulteriormente il rischio di attacchi DDoS. Sebbene l'entità degli attacchi DDoS nell'area EMEA sia piuttosto ampia e in crescita, abbiamo anche assistito ad un aumento del numero di vettori di attacchi DDoS utilizzati dai criminali informatici e della loro durata.

In questo rapporto sullo stato di Internet (SOTI), vengono esaminate la natura e la frequenza degli attacchi DDoS nell'area EMEA e vengono analizzati alcuni dei principali settori verticali colpiti da essi, tra cui servizi finanziari, commercio e sanità. Inoltre, viene esaminata in dettaglio la nuova legislazione EMEA concepita per rafforzare la protezione contro l'aumento delle minacce alla cybersicurezza in quest'area e vengono fornite tecniche di mitigazione e protezione che insieme possono combattere la crescita degli attacchi DDoS nell'area EMEA.

I principali risultati emersi dal rapporto

I ricercatori di Akamai hanno osservato che il numero di attacchi DDoS nell'area EMEA è in costante aumento, con picchi più elevati, dall'inizio del 2019.

Più di un terzo di tutti gli attacchi DDoS a livello globale si verificano nell'area EMEA.

La complessità e la gravità degli attacchi DDoS nell'area EMEA sono state trasformate da motivi geopolitici, come l'hacktivismo, portando a conseguenze potenzialmente letali.

Secondo una ricerca di Akamai, tra tutti i tipi di attacchi DDoS, i più diffusi sono quelli sferrati contro il DNS. Nello specifico, abbiamo osservato il vettore NXDOMAIN (un dominio inesistente), noto anche come vettore del sottodominio pseudo-casuale, che "inonda" i server dei nomi DNS con richieste di domini inesistenti.

Per aumentare le probabilità di successo, oltre un terzo degli attacchi DDoS osservati ha utilizzato più vettori (fino a 12).

Nell'area EMEA, il segmento verticale con il numero più alto di attacchi DDoS di livello 3 e di livello 4 è rappresentato dai servizi finanziari, mentre per quanto riguarda gli attacchi di livello 7 è il settore del commercio.

I governi e le nazioni dell'EMEA hanno rivalutato il potere dell'infosicurezza adottando nuove misure legislative, come il NIS2 e il DORA, per contribuire a influenzare positivamente le strategie relative all'IT e alla cybersicurezza, incluso un miglior livello di resilienza e protezione dagli attacchi DDoS.

Il presente e il futuro degli attacchi DDoS

Gli attacchi DDoS, sia che vengano sferrati da singoli individui o da botnet, cercano di "inondare" i server di richieste e di sovraccaricarli di traffico, rendendo i servizi e i siti ospitati non disponibili per utenti e visitatori.

Gli attacchi DDoS si sono evoluti rispetto al periodo in cui i criminali utilizzavano strumenti open-source per eseguirli. Per questo gruppo, la motivazione era spesso semplicistica: forse erano insoddisfatti della nuova funzionalità di gioco, speravano di ottenere un vantaggio competitivo o semplicemente stavano cercando un passatempo. In generale, questo gruppo di criminali non ha dominato il panorama degli attacchi con la tendenza di prendere di mira ospedali o infrastrutture critiche né con l'obiettivo di danneggiare gravemente le reti o mettere in pericolo le vite umane.

L'hacktivismo ha cambiato radicalmente il panorama, sia in termini di identità dei criminali che della loro motivazione. Mentre alcuni attacchi di hacktivisti possono influire in modo solo limitato o fastidioso, altri prendono di mira il settore commerciale per ricavare notevoli guadagni finanziari e possono causare interruzioni dei servizi che durano giorni. Gli attacchi possono avere conseguenze potenzialmente letali, come abbiamo visto nel caso di alcuni attacchi sferrati contro i centri sanitari.

La capacità di sferrare attacchi DDoS è diventata più semplice negli ultimi anni, con l'emergere di servizi come il potenziamento degli attacchi DDoS, che consentono anche al criminale più inesperto di lanciare un attacco con il semplice clic di un pulsante e per una tariffa simbolica, a volte ad un costo irrisorio. Questi semplici attacchi causano poi un'enorme quantità di traffico, che provoca l'interruzione di interi siti web e reti, danneggiando le aziende sia a livello finanziario che operativo e privando clienti e utenti di servizi cruciali.

Focalizzazione sulla situazione geopolitica

Gli attacchi DDoS sono comunemente usati da hacktivisti che agiscono sulla base di motivazioni politiche e criminali sostenuti dai governi. Ad esempio, nella guerra informatica in corso tra ucraini e russi, gli attacchi DDoS svolgono un ruolo significativo poiché gli hacktivisti hanno scoperto l'efficacia di questi attacchi a basso costo.

Agli inizi del 2022, Akamai ha iniziato a sostenere il governo ucraino nella lotta contro la guerra informatica difendendo 20 diverse risorse web di enti governativi, tra cui l'URL president.gov.ua, che era stato il sito più attaccato, subendo, come era stato osservato, un elevato volume di attacchi DDoS con un picco di 1 milione di richieste dannose al secondo.

Alcuni gruppi di hacktivisti come Anonymous Sudan, NoName057(16) e Killnet sono rimbalzati sulle cronache da quando la Russia ha invaso l'Ucraina nel febbraio 2022. Killnet è stato il primo di questi gruppi ad emergere e ha iniziato la sua attività approssimativamente ad ottobre 2021, offrendo servizi DDoS-for-hire. Killnet ha attaccato agenzie governative, aziende sanitarie, società di media e altre organizzazioni che il gruppo considera alleati dell'Ucraina.

NoName057(16) è considerato da molti ricercatori delle minacce come un gruppo filorusso, che, come è stato osservato, sta ampiamente utilizzando gli attacchi DDoS basati su HTTP (livello 7). All'inizio del 2023, il gruppo filorusso Anonymous Sudan ha iniziato a sferrare attacchi DDoS contro varie entità situate in Danimarca, Svezia, Stati Uniti e in altri paesi. A giugno 2023, molti gruppi di criminali, tra cui ReVIL, Killnet e Anonymous Sudan, hanno rivolto la loro attenzione ad infrastrutture bancarie critiche, sfruttando il caos provocato dalla guerra tra Russia e Ucraina.

Più recentemente, Anonymous Sudan ha rivendicato la responsabilità dell'attacco all'app di messaggistica francese Telegram come parte dell'attacco DDoS da record sferrato contro la rete interministeriale statale del paese, causando l'interruzione di oltre 17.000 indirizzi IP e dispositivi e più di 300 domini. Si ritiene che questo attacco ai siti web e ai servizi del governo francese sia stato sferrato probabilmente in risposta all'annuncio fatto dal presidente francese Emmanuel Macron il 26 febbraio 2024 sulla possibilità di inviare truppe francesi in Ucraina.

Il conflitto tra Ucraina e Russia non è l'unica battaglia che sta causando un'ondata di attacchi DDoS nell'area EMEA. Anche la guerra tra Israele e Hamas ha provocato un aumento di questi attacchi. Anonymous Sudan ha rivendicato la responsabilità degli attacchi DDoS sferrati contro il Mossad, l'agenzia di intelligence nazionale israeliana, nonché contro il sito web e gli account Facebook del primo ministro israeliano e contro siti filoisraeliani collegati all'escalation del conflitto nel Mar Rosso. Anche il gruppo NoName057(16) ha attaccato i siti web israeliani in risposta a questo conflitto.

Una triplice minaccia

Storicamente, gli attacchi ransomware crittografavano i dati delle vittime, rendendoli inutilizzabili a meno che non venisse pagato un riscatto. Successivamente, sono stati escogitati gli attacchi a doppia estorsione, che hanno provocato maggiori danni alle vittime: i criminali riuscivano a creare una copia dei dati delle vittime prima di crittografare le loro reti, minacciando di pubblicarli o venderli a meno che non fosse stato pagato il riscatto richiesto. Un terzo tipo di attacco (a tripla estorsione) ha fatto la sua comparsa subito dopo. In questo tipo di attacchi, il criminale utilizza la tecnica DDoS per ostacolare le attività della vittima oltre alle altre due tattiche illustrate prima. Gli attacchi a tripla estorsione vengono spesso definiti RDDoS o Ransom DDoS.

Gli attacchi DDoS sono un elemento comune negli attacchi di estorsione, sia come copertura per distrarre i team addetti all'infosicurezza mentre gli hacker tentano di intromettersi nei sistemi presi di mira sia per aumentare la pressione sulla vittima. L'utilizzo di più vettori di attacco aumenta le possibilità che una vittima paghi il riscatto richiesto. Uno dei primi attacchi a tripla estorsione è stato sferrato contro la Vastaamo, una clinica di psicoterapia finlandese, ad ottobre 2020 mentre era in atto un processo di miglioramento della condivisione dei dati sanitari in tutta l'Unione europea.

Il settore sanitario continua a rimanere l'obiettivo principale dei criminali che utilizzano gli attacchi a tripla estorsione. Un esempio è il gruppo ransomware NoEscape, nato lo scorso anno dall'ex gruppo russo Avaddon con l'obiettivo di prendere di mira le aziende sanitarie. Pertanto, alcune società di cybersicurezza si stanno già preparando poiché in futuro sempre più gruppi prenderanno di mira il settore sanitario.

Sembra anche che il gruppo di ransomware russo LockBit abbia condotto l'operazione di ransomware più vasta e dannosa al mondo a partire da febbraio 2024, innescando un processo distruttivo costato miliardi di euro. Per contrastare il gruppo LockBit, le agenzie Europol ed Eurojust hanno collaborato per coordinare una task force internazionale nota come Operazione Cronos, nell'ambito della quale si sono verificati arresti, mandati, incriminazioni e la confisca di 34 server nell'EMEA, in Australia e negli Stati Uniti. Il gruppo LockBit era noto per aver sperimentato nuovi metodi per spingere le vittime a pagare i riscatti, come gli attacchi RDDoS.

Sebbene esistano altri gruppi noti che utilizzano la tecnica RDDoS, come Darkside, Lazarus, AvosLocker e BlackCat, l'impatto dell'Operazione Cronos sul gruppo LockBit è significativo perché per la prima volta le forze dell'ordine impegnate nella cybersicurezza si sono rivelate efficaci a questo livello, smantellando e assumendo il controllo completo dell'infrastruttura di un grande gruppo di ransomware mentre era ancora operativa.

La contromossa: contrastare gli attacchi DDoS con la stessa tecnica

L'idea di rispondere agli attacchi informatici con la stessa moneta è oggetto di dibattito da anni. Questa strategia è concepita sulla scia del detto "l'attacco è la miglior difesa" (nel senso che un attacco può proteggere le aziende dalle minacce internazionali) ma è anche percepita come un pericoloso precedente, che autorizza le società attive nella cybersicurezza a sferrare attacchi DDoS in tutto il mondo e potenzialmente destabilizzare le relazioni tra gli stati intensificando le tensioni diplomatiche. Inoltre, le ambiguità normative riguardanti i metodi per contrastare gli attacchi informatici, come la tecnica DDoS, sollevano questioni giuridiche molto complesse.

Come sappiamo, il gruppo LockBit ha utilizzato la tecnica DDoS come parte degli attacchi a tripla estorsione. Ironicamente, l'utilizzo di questo metodo da parte del gruppo è stato parzialmente influenzato da un attacco DDoS subito dallo stesso gruppo. Entrust, una società che si occupa di cybersicurezza, è stata aggiunta all'elenco delle vittime del gruppo LockBit a luglio 2022. Per rispondere a questa minaccia, Entrust ha sferrato un contrattacco DDoS che ha di fatto paralizzato i sistemi darknet utilizzati da LockBit per pubblicare i dati rubati.

I contrattacchi vengono anche utilizzati come tattica di guerra da alcuni stati. L'Ucraina ha reclutato alcuni volontari come parte di un "esercito IT" di hacker provenienti da tutto il mondo che difendono le sue reti rispondendo agli attacchi con la stessa moneta: una tecnica considerata come la prima del suo genere.

Analisi dei dati relativi agli attacchi DDoS nell'area EMEA

Gli attacchi DDoS sono in aumento in tutto il mondo, soprattutto nell'area EMEA. I ricercatori di Akamai, dopo aver analizzato i dati relativi agli attacchi DDoS nell'EMEA, notano come in quest'area il numero di attacchi DDoS tenda ad aumentare in modo più costante rispetto ad altre aree geografiche, compreso il Nord America, che è in testa a tutti gli altri paesi nel complesso (Figure 1a e 1b).

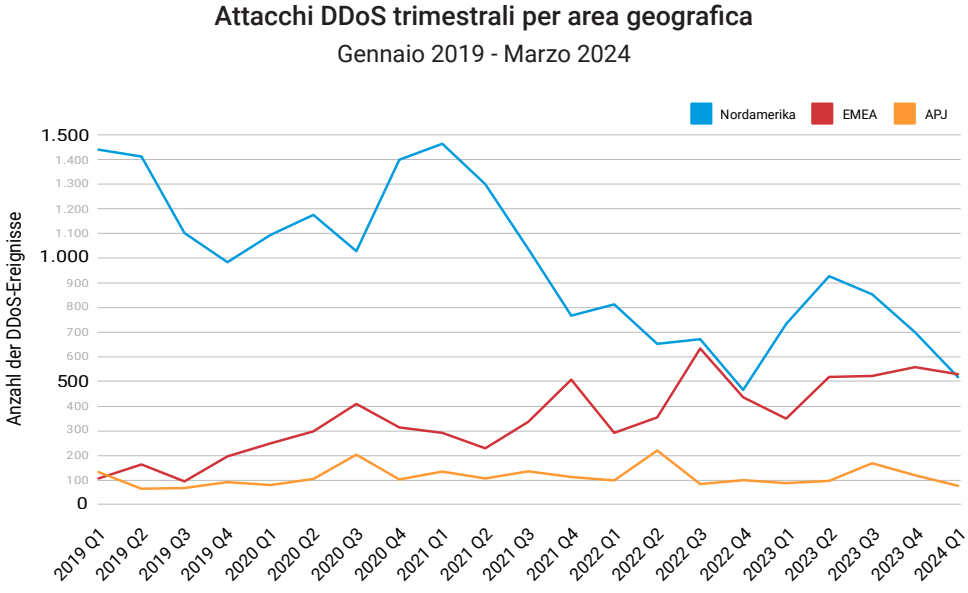


Figura 1a. Il numero di attacchi DDoS nell'area EMEA aumenta in modo più costante rispetto ad altre aree geografiche, compreso il Nord America

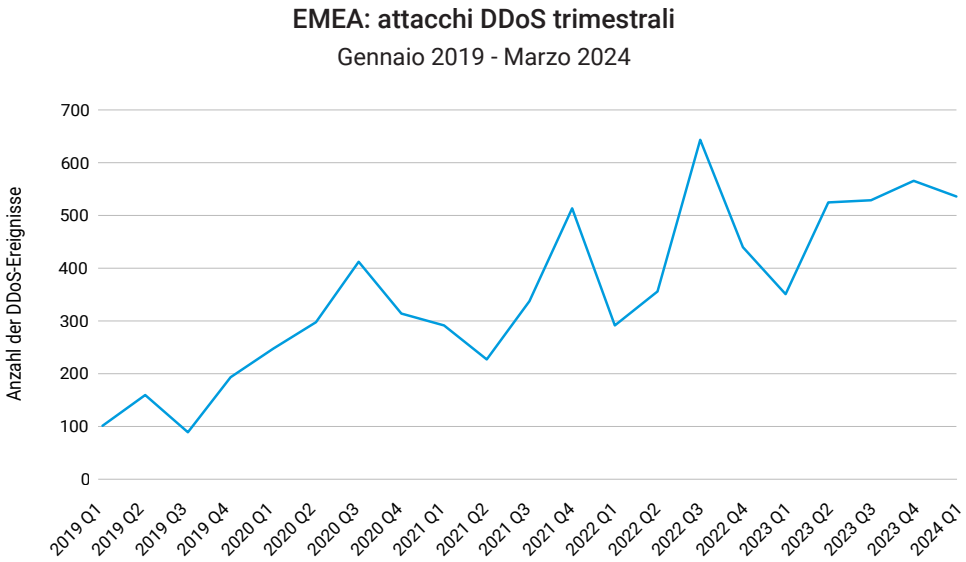


Figura 1b. La crescita degli attacchi DDoS nell'area EMEA

All'interno dell'area EMEA, il Regno Unito (26%), l'Arabia Saudita (22,3%) e la Germania (9,1%) sono in testa ai paesi con il maggior numero di attacchi subiti. Inoltre, dai risultati di Akamai emerge come più di un terzo di tutti gli attacchi DDoS a livello globale si verifichino nell'area EMEA (Figura 2).

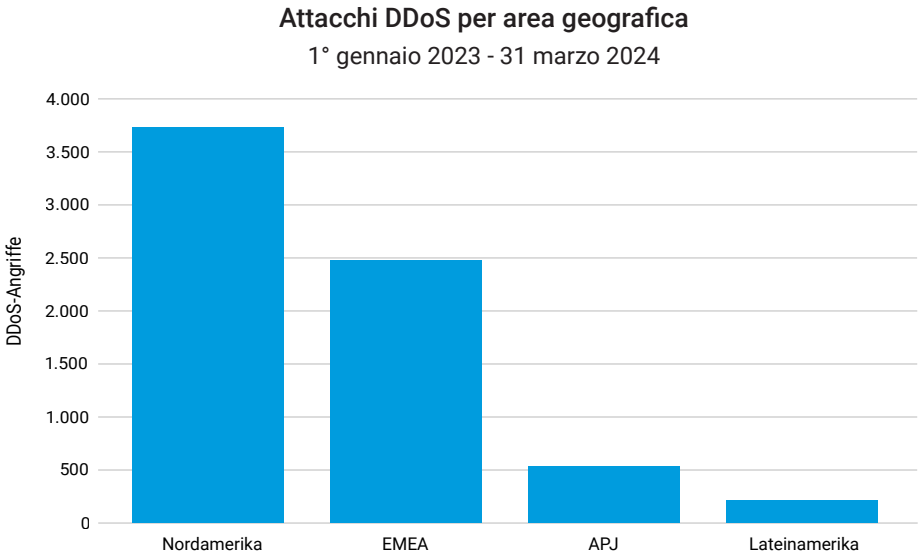


Figura 2. Dall'inizio del 2023 al primo trimestre del 2024, il numero di attacchi DDoS nell'EMEA è arrivato quasi a 2.500, una cifra più di tre volte superiore al totale complessivo di attacchi sferrati nell'Asia Pacifico e in Giappone (APJ) e in America Latina (LATAM)

Nel settore dei servizi finanziari, l'EMEA è l'area che subisce la maggiore quantità di traffico correlato ad attacchi DDoS di livello 3 e 4 (Figura 3). Come accennato in precedenza, alcuni gruppi di hacktivisti russi hanno dichiarato l'intenzione di sferrare attacchi DDoS contro il sistema bancario europeo e supponiamo che la ragione principale dell'aumento degli attacchi DDoS nel settore dei servizi finanziari sia proprio da ricondurre a questo hacktivismo geopolitico.

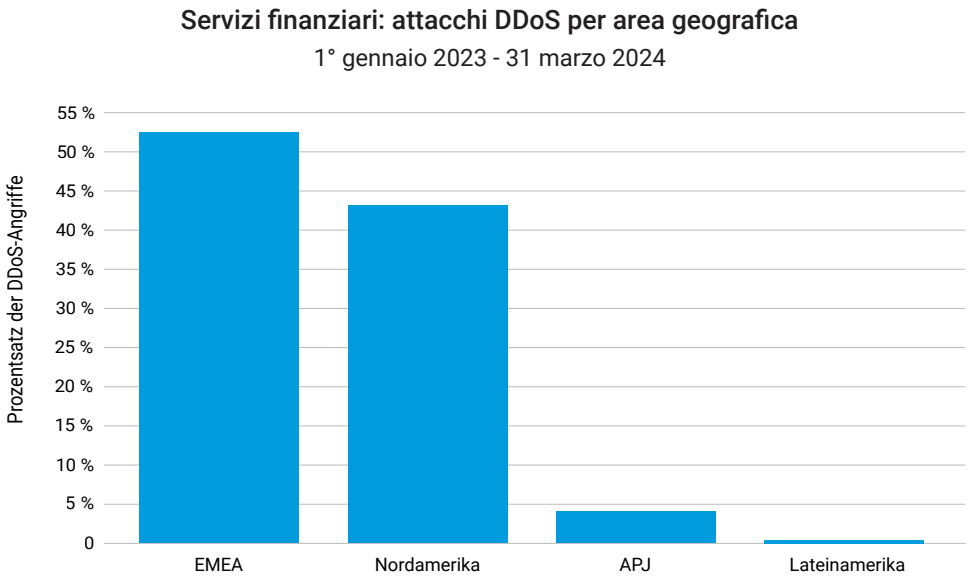


Figura 3. L'area EMEA ha subito il 52,5% del traffico degli attacchi DDoS di livello 3 e 4 nel settore dei servizi finanziari

Oltre agli attacchi di livello 3 e 4, le applicazioni dei servizi finanziari sono prese di mira dagli attacchi DDoS di livello 7. Tuttavia, il settore del commercio sta registrando il maggiore aumento degli attacchi DDoS di livello 7 nell'EMEA poiché subisce quasi il 30% di tutti gli attacchi osservati in quest'area geografica (Figura 4).

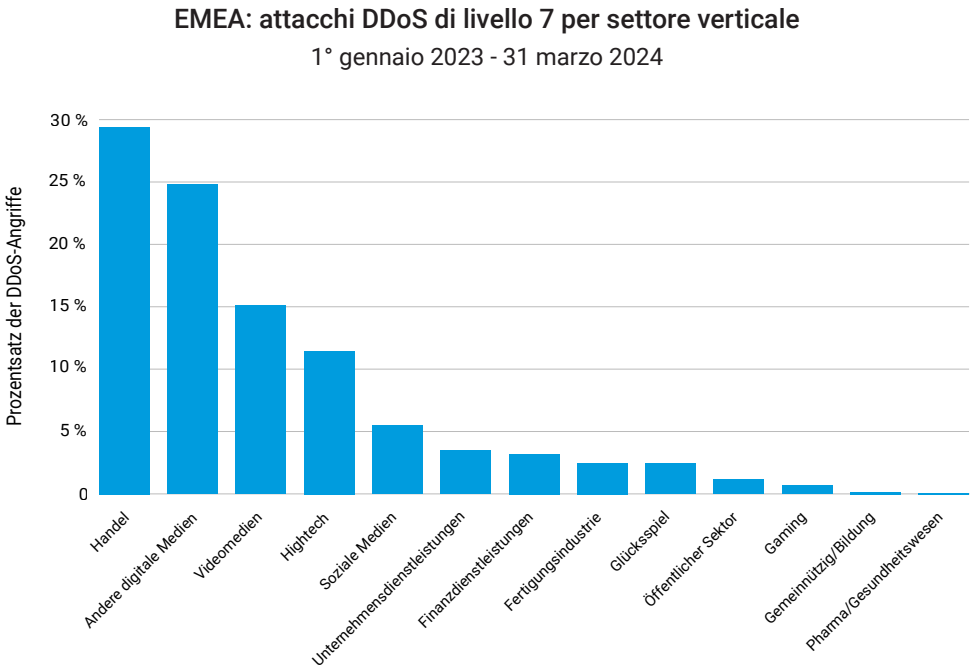
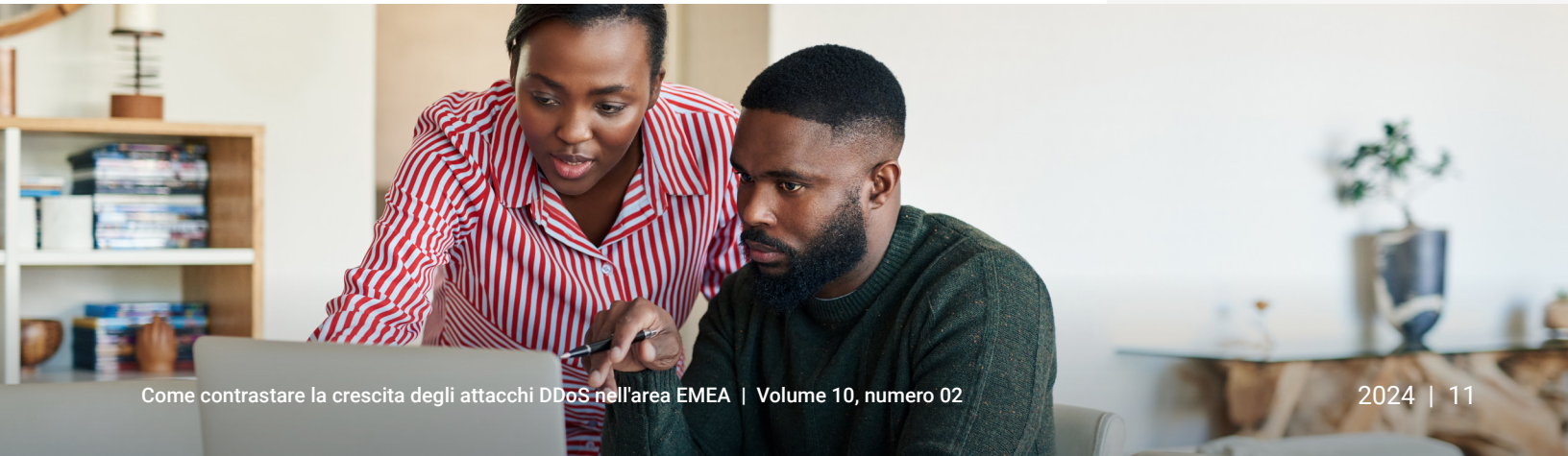


Figura 4. Il settore del commercio è interessato dal 29,4% del traffico degli attacchi DDoS di livello 7 nell'area EMEA

Gli attacchi DDoS a livello di applicazione, come gli attacchi HTTP flood, sono più frequenti nel settore del commercio probabilmente per i potenziali notevoli ricavi che questi attacchi offrono ai criminali. Questi tipi di attacchi sono particolarmente paralizzanti per le organizzazioni commerciali perché possono rendere inaccessibile un negozio online o non disponibile un sistema di prenotazione, determinando una significativa perdita di entrate per l'azienda presa di mira. Inoltre, questi attacchi possono essere utilizzati come tattica per distrarre le risorse che si occupano di risposta agli incidenti, mentre i criminali mirano a rubare i preziosi dati dei clienti (come i dati delle carte di credito) da altre aree presenti nella rete della vittima.



Se è vero che il numero di attacchi DDoS è in aumento, abbiamo d'altra parte osservato anche un notevole incremento del numero di vettori utilizzati per sferrare gli attacchi DDoS (Figura 5a). Tra i vettori più comunemente utilizzati, figurano gli attacchi DNS Flood, UDP Fragment e NTP Reflection (Figura 5b). Inoltre, abbiamo osservato che gli attacchi sono durati più a lungo.

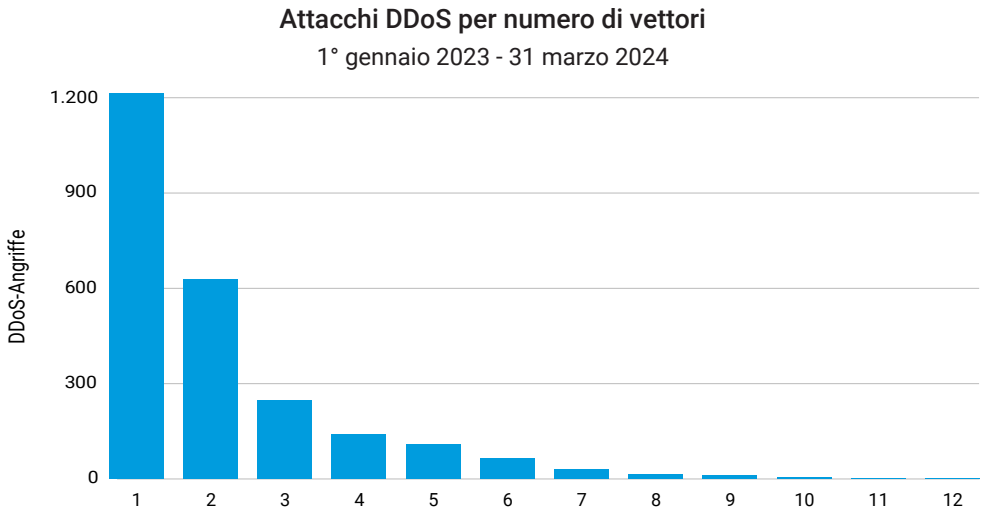


Figura 5a. Il numero di attacchi utilizzati per sferrare gli attacchi DDoS è aumentato notevolmente

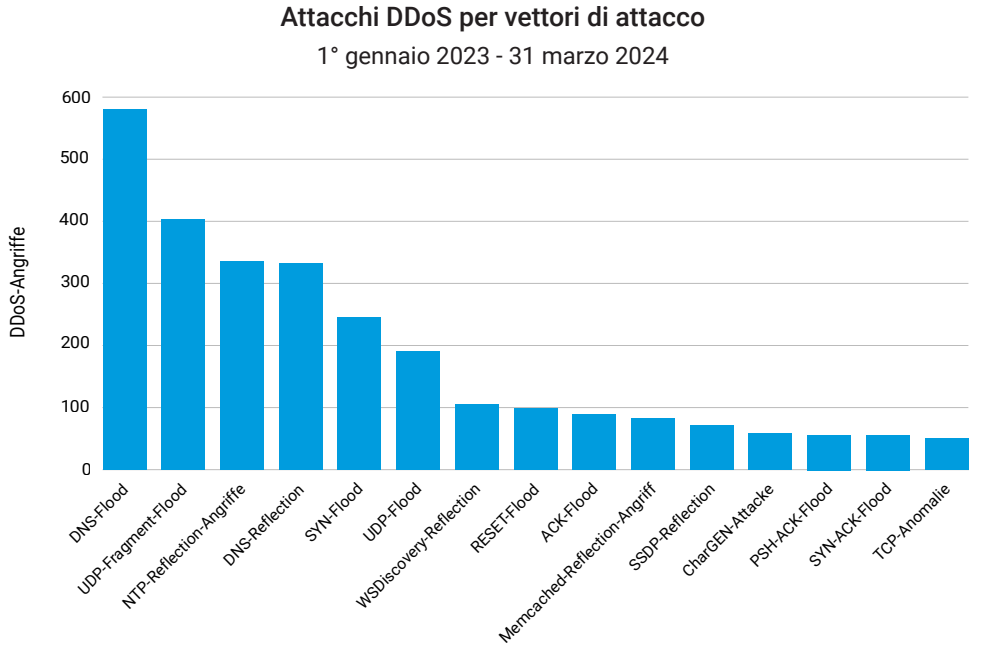


Figura 5b. Tra i vettori DDoS più comunemente utilizzati nell'area EMEA, figurano gli attacchi DNS Flood, UDP Fragment e NTP Reflection

Gli attacchi prolungati ostacolano la produttività e la capacità delle attività di preservare la loro continuità operativa quando vengono individuate altre minacce e sono richieste azioni di risposta. Le tecniche DDoS che comportano attacchi di maggiore durata e l'uso di più vettori di attacco sono strategie efficaci per i criminali, che, in tal modo, possono esaurire meglio le risorse prese di mira e sopraffare i team addetti alla sicurezza delle reti aziendali.

Il nuovo obiettivo di tendenza degli attacchi DDoS: il DNS

Tra tutti i tipi di attacchi DDoS, i più diffusi sono quelli sferrati contro il DNS (Domain Name System) (Figura 6), un obiettivo comunemente preso di mira dagli attacchi DDoS a causa dell'impatto che il traffico dannoso può avere su questo servizio essenziale e fondamentale. Un attacco DNS riuscito ha il potenziale per distruggere letteralmente la presenza di un'azienda su Internet.

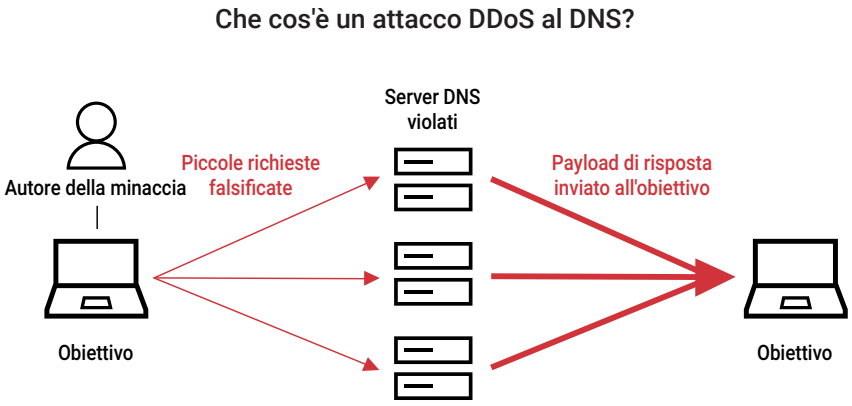


Figura 6. Un attacco DDoS al DNS compromette i server DNS con richieste falsificate, "inondando" l'obiettivo con un'enorme quantità di payload di risposta

Nello specifico, è stato osservato che gli attacchi NXDOMAIN (dominio inesistente), chiamati anche attacchi di sottodominio pseudocasuale (PRSD) o DNS Water Torture, "inondano" l'infrastruttura DNS con richieste di domini inesistenti. Questo tipo di attacco mira a raggiungere i server dei nomi di origine e a causare un carico elevato sui sistemi: l'elaborazione di una richiesta di un dominio inesistente è un'attività complessa che richiede molte operazioni, finendo per esaurire la capacità di risposta dei sistemi. Abbiamo assistito a molti attacchi brevi di questo tipo, che, in genere, vengono utilizzati per sondare la configurazione dell'infrastruttura DNS della vittima, per poi ritornare in seguito sferrando un attacco perfezionato in piena regola. Secondo i risultati di una ricerca condotta dai nostri 50 principali clienti finanziari che utilizzano Akamai Edge DNS, le richieste di domini inesistenti hanno costituito quasi il 60% del loro traffico Internet a marzo 2024 (Figura 7).

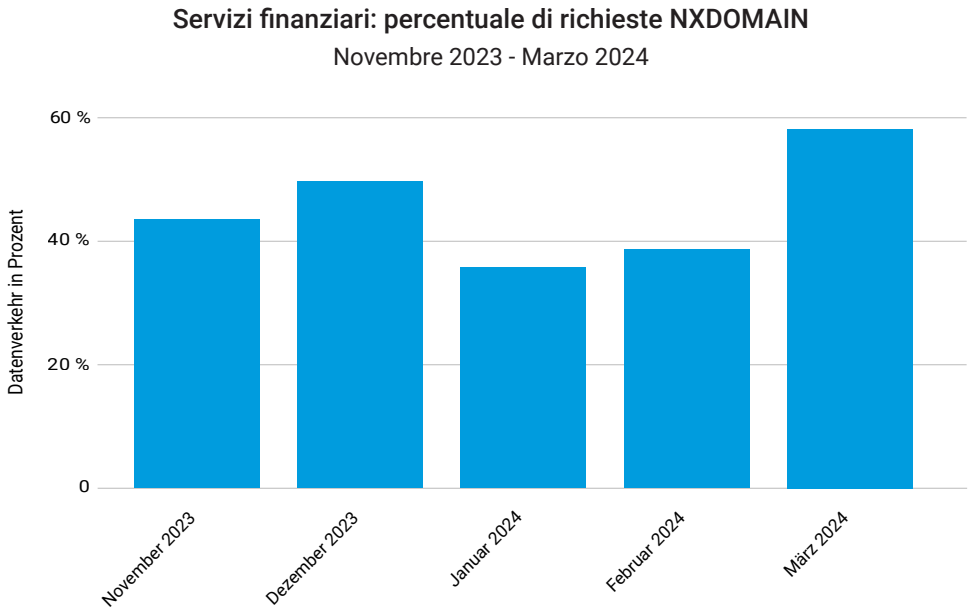


Figura 7. Dalla fine del 2023, si è registrato un picco di richieste NXDOMAIN (pari al 58%) a marzo 2024

Gli attacchi DNS Flood sono uno dei due gruppi principali di attacchi DDoS al DNS. L'altro gruppo è rappresentato dagli attacchi di amplificazione DNS, che includono attacchi di riflessione e comportano lo spoofing degli indirizzi IP creati dal criminale per inviare un numero considerevole di richieste DNS nel tentativo di paralizzare le risorse del sistema preso di mira. Un altro incentivo che porta il criminale a scegliere un attacco DDoS al DNS è la sua facilità di esecuzione poiché la maggior parte del traffico utilizza il protocollo UDP (User Datagram Protocol), che consente di falsificare gli indirizzi IP.

Contrastare gli attacchi rivalutando il potere dell'infosicurezza

Per combattere e prevenire l'aumento delle minacce alla cybersicurezza (inclusi gli attacchi DDoS) nell'EMEA, i governi e le nazioni di quest'area geografica stanno rivalutando il potere dell'infosicurezza. Il panorama in continua evoluzione comprende la nuova Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS2) e il Digital Operational Resilience Act (DORA), oltre a nuove misure legislative (ad esempio, il Regolamento generale sulla protezione dei dati [GDPR], il Cyber Resilience Act [CRA], il Programma europeo per la protezione delle infrastrutture critiche, ecc).

È fondamentale che le aziende implementino solide misure di sicurezza e valutino regolarmente le proprie applicazioni e reti per evitare e mitigare gli attacchi informatici, soprattutto per proteggersi dagli attacchi DDoS che non danno molto tempo per reagire. Inoltre, gli attacchi DDoS tendono a prendere di mira entità meno protette, che i criminali identificano tramite analisi di ricognizione e test accurati. È quindi importante per le organizzazioni stabilire efficienti procedure di sicurezza e disporre di piani di continuità operativa e di disaster recovery. Insieme, le nuove direttive e misure legislative possono contribuire alla sicurezza delle organizzazioni.

La Direttiva NIS2, adottata nel dicembre 2022 per abrogare e sostituire la NIS1, mira ad espandere, rafforzare e armonizzare l'implementazione del sistema di cybersicurezza esistente nell'Unione europea in risposta alla crescente vulnerabilità di quest'area geografica alle minacce informatiche. Gli Stati membri dell'UE hanno tempo fino al 17 ottobre 2024 per recepire la direttiva.

Importanti sono anche le procedure per la gestione dei fornitori, quali i soggetti terzi. Il DORA si incentra sulla regolamentazione dei servizi finanziari dell'UE e sarà applicabile a partire dal 17 gennaio 2025. Oltre a promuovere la resilienza informatica e ad aiutare le entità dell'UE operanti nel settore dei servizi finanziari a gestire i problemi legati alla cybersicurezza, il DORA fornisce linee guida per le procedure di gestione dei fornitori di terze parti. In tal modo, le istituzioni finanziarie possono garantire che i provider di servizi ICT (Information and Communication Technology) con cui stipulano contratti rispettino gli appropriati standard di sicurezza delle informazioni. Di seguito, vengono riportati i componenti chiave del modello del DORA, progettato per migliorare la resilienza informatica delle società operanti nei servizi finanziari e costituito da cinque pilastri, che sono: gestione del rischio, segnalazione degli incidenti, test di resilienza operativa digitale, rischio ICT di terze parti e condivisione di informazioni e intelligence.

Sia il NIS2 che il DORA includono linee guida sulle strategie che utilizzano il modello Zero Trust come metodo di resilienza. La fiducia e la disponibilità sono cruciali, soprattutto nell'universo online, e un attacco DDoS può erodere seriamente la fiducia. Pertanto, è importante che le aziende seguano procedure di salvaguardia adeguate, come pratiche di igiene informatica di base. Questo concetto include l'uso dei principi Zero Trust, che attuano un meccanismo di controllo degli accessi più granulare e sensibile al contesto che verifica continuamente l'identità e il comportamento di dispositivi e utenti prima di concedere l'accesso alle risorse sensibili. Inoltre, il concetto del privilegio minimo, una parte fondamentale delle pratiche di sicurezza Zero Trust, segmenta gli utenti a cui è consentito l'accesso. Le soluzioni Zero Trust aiutano poi a proteggere le risorse critiche delle organizzazioni dagli attacchi RDDoS.

Oltre alla legislazione relativa agli attacchi DDoS, è importante per le organizzazioni conoscere anche le altre normative vigenti nell'area EMEA che mirano a contrastare le minacce informatiche. Ad esempio, il nuovo CRA dell'Unione europea si focalizza sulle vulnerabilità software e hardware che i criminali sfruttano sempre più per infiltrarsi nelle organizzazioni e sferrare i loro attacchi ransomware. Inoltre, il GDPR ha creato obblighi per tutte le organizzazioni che trattano dati personali correlati ad aziende e a clienti europei.

Al di fuori dell'Unione europea, altri paesi stanno creando e applicando propri controlli, come la NCA (National Cybersecurity Authority) in Arabia Saudita, che ha introdotto leggi sulla protezione dei dati in modo simile al GDPR, e l'Africa Cybercrime Operations Desk dell'Interpol, che ha istituito vari programmi come l'Africa Cyber Surge.

Case study: una società di e-commerce europea subisce un attacco DDoS a livello di rete

Mantenere il tempo di attività e la resilienza di un sito web è fondamentale per incrementare le entrate di qualsiasi società di e-commerce. Ecco perché proteggere le risorse e le applicazioni web dagli attacchi DDoS per prevenire eventi che influiscono sulle loro attività (e sui loro clienti) è la massima priorità per i responsabili della sicurezza. Ma cosa accadrebbe se l'infrastruttura sottostante o i sistemi di back-end su cui si basa il ciclo degli ordini venissero interrotti o disconnessi completamente? Cosa accadrebbe se l'ordine effettuato da un cliente non potesse essere elaborato o evaso. Questo è quanto è successo ad una società di e-commerce europea quando un attacco DDoS sferrato a livello di rete ha colpito i servizi all'interno del data center in cui erano stati messi in atto controlli inadeguati.

Molti criminali lanciano comunemente campagne di attacchi nei fine settimana e nei giorni festivi quando è disponibile un minor numero di addetti alla sicurezza e di risorse che si occupano di risposta agli incidenti per porre rimedio ad una minaccia. Nel caso di questa società di e-commerce europea, gli autori degli attacchi DDoS hanno utilizzato una combinazione di vettori di attacco SYN e UDP Flood per prendere di mira il data center dell'organizzazione un venerdì pomeriggio e mettere fuori uso le sue risorse più vulnerabili, come il sistema di posta elettronica aziendale, impedendo quindi la trasmissione di dati importanti ad altre parti dell'organizzazione, inclusi i magazzini di evasione degli ordini.

Di conseguenza, l'infrastruttura della logistica, pur non subendo alcun impatto, non è riuscita a gestire e ad elaborare gli ordini ricevuti dalla piattaforma di e-commerce. Poiché l'organizzazione non era in grado di difendersi dal livello sostenuto di attacchi DDoS volumetrici, è stata richiesta l'assistenza di Akamai che è intervenuta con un'integrazione di emergenza per proteggere i data center aziendali del retailer. Nel giro di 24 ore, il sistema del cliente è stato migrato alla piattaforma Akamai Prolexic e la sua connettività ai servizi aziendali più importanti è stata ripristinata.

Conclusione: le società di e-commerce devono adottare un approccio olistico agli attacchi DDoS che includa la mitigazione degli attacchi di livello 7 (applicazione), di livello 3 (rete) e di livello 4 (trasporto) per prevenire problemi di downtime e garantire la resilienza durante l'intero ciclo degli ordini.

Salvaguardia e mitigazione

Dopo aver discusso delle principali tendenze e normative relative agli attacchi DDoS nell'area EMEA e fornito alcuni esempi di attacchi, diamo un'occhiata a cosa è possibile fare per proteggere la propria organizzazione. Oltre a seguire le misure legislative menzionate in precedenza, tra cui NIS2, DORA, GDPR e CRA, e ad utilizzare le soluzioni Zero Trust, i ricercatori di Akamai consigliano di adottare tre strategie per combattere gli attacchi DDoS in continua evoluzione.

1. **Prepararsi in modo proattivo con un sistema di protezione dagli attacchi DDoS per le risorse digitali.**
   Ciò comprende:
   - Garantire che siano in atto controlli di mitigazione per tutti gli indirizzi IP pubblici e per le sottoreti più importanti
   - Implementare i controlli di sicurezza DDoS in una strategia di protezione online
   - Assicurarsi che i piani e i team di risposta agli incidenti siano aggiornati e dedicati
   - Supportare il sistema di protezione dagli attacchi DDoS on-premise con una piattaforma ibrida dedicata per difendersi dagli attacchi che sovraccaricano le apparecchiature on-premise
   - Predisporre controlli di sicurezza proattivi tramite un firewall di rete cloud e una soluzione WAF (Web Application Firewall)
   - Configurare la limitazione della velocità
   - Memorizzare i contenuti nella cache su una CDN
   - Utilizzare un team SOCC (Security Operations Command Center) per alleggerire la pressione sulle risorse interne più importanti

2. **Proteggere la propria infrastruttura DNS.** Se il DNS di un'entità si blocca, lo stesso accade alla sua presenza online. Un firewall DNS tradizionale potrebbe non fornire una protezione adeguata se la configurazione gestisce zone sia on-premise che nel cloud. In tal caso, una piattaforma ibrida potrebbe risultare la soluzione ottimale. In generale, per ottenere un livello di sicurezza DDoS adeguato, è necessario esaminare attentamente tutto il traffico Internet che entra nella rete per mitigare e filtrare quello relativo agli attacchi prima che raggiunga le applicazioni, le API e l'infrastruttura, incluso il DNS.

3. **Non affidarsi a soluzioni "abbastanza buone".** Sembrerebbe più semplice utilizzare solo i sistemi di protezione essenziali, scelti in base ai requisiti e al budget a disposizione. Tuttavia, le aziende spesso scoprono che questo "risparmio" iniziale conduce ad una perdita successiva che comporta danni e spese di gran lunga superiori ai vantaggi del piano originale. È importante quindi eseguire test sotto stress dei propri sistemi di difesa dal punto di vista sia delle migliori pratiche che delle soluzioni tecniche. Questi test dovrebbero includere documentazione degli incidenti, processi, runbook e molto altro per garantire che le soluzioni forniscano un solido livello di cybersicurezza.

Conclusione

Gli attacchi DDoS, per la loro natura e l'impatto esercitato, si sono trasformati notevolmente fino a diventare sempre più gravi e complessi.

Questa escalation di attacchi DDoS ha colpito in particolar modo l'EMEA, in cui si è registrato un aumento di episodi di questo tipo nel settore pubblico, nei servizi finanziari, nel commercio e nella sanità. Lo spostamento in quest'area geografica può essere attribuito, in parte, alle tensioni geopolitiche e ai conflitti in corso nell'EMEA, che hanno favorito un aumento dell'hacktivismo e delle attività DDoS ad esso associate.

Inoltre, gli imminenti eventi importanti e le elezioni in Europa, comprese le elezioni del Parlamento europeo e quelle nel Regno Unito, nonché le Olimpiadi che si terranno quest'estate in Francia, potrebbero aumentare ulteriormente il rischio di attacchi DDoS. Questi eventi, che rivestono una notevole importanza politica ed economica, possono fungere da motivazione principale per i criminali che cercano di influire sui loro programmi tramite l'uso di tattiche DDoS.

I legislatori dell'EMEA stanno rivalutando il potere dell'infosicurezza e rafforzando le misure di sicurezza con l'emanazione di nuovi regolamenti e direttive. In generale, le aziende e le organizzazioni che rispettano queste normative e dispongono di misure di protezione hanno meno probabilità di essere considerate facili prede dai criminali informatici. Gli autori di attacchi DDoS tendono a prendere di mira obiettivi vulnerabili che non sono ben protetti e i criminali conducono continuamente operazioni di ricognizione per scoprire quali obiettivi sono più facili da violare con gli attacchi DDoS. A causa della moltitudine di vettori di attacco DDoS e dei numerosi percorsi disponibili tra i livelli di rete, trasporto e applicazione, è fondamentale utilizzare una combinazione di soluzioni per fornire una protezione completa da questo problema. Questo tipo di difesa è essenziale per contrastare al meglio gli attacchi DDoS in aumento nell'area EMEA.

Metodologia

DDoS (livelli 3 e 4)

La soluzione Akamai Prolexic Routed difende le organizzazioni dagli attacchi DDoS per bloccare le minacce e altro traffico indesiderato o dannoso prima che raggiungano le applicazioni, i data center e l'infrastruttura basata su Internet (pubblica o privata) ibrida e nel cloud, incluse tutte le porte e i protocolli utilizzati. Gli esperti del SOCC (Security Operations Command Center) di Akamai personalizzano i controlli di mitigazione proattivi per rilevare e bloccare immediatamente gli attacchi ed eseguono analisi del traffico rimanente in tempo reale per determinare ulteriori misure di mitigazione, in base alle necessità. Questi attacchi mitigati sono organizzati e raggruppati in eventi di attacco, i cui dati associati vengono registrati dal SOCC per l'analisi.

I dati inclusi in questo rapporto hanno riguardato un periodo di 15 mesi, dal 1° gennaio 2023 al 31 marzo 2024, salvo altrimenti specificato.

DDoS (livello 7)

Questi dati descrivono gli avvisi a livello di applicazione relativi al traffico osservato tramite la nostra soluzione WAF (Web Application Firewall). Gli avvisi sugli attacchi DDoS di livello 7 vengono attivati quando si rilevano anomalie volumetriche all'interno di una serie di richieste a un sito web, un'applicazione o un'API protetta. Questi avvisi possono essere attivati sia da richieste dannose che non dannose. Di solito, le richieste in sé non sono dannose, tuttavia un elevato numero di richieste può nascondere uno scopo illecito. Gli avvisi non indicano la corretta riuscita di un attacco. Sebbene questi prodotti consentano un alto livello di personalizzazione, i dati presentati in questo rapporto sono stati raccolti senza prendere in considerazione le configurazioni personalizzate delle proprietà protette.

I dati sono stati ricavati da uno strumento interno per l'analisi degli eventi di sicurezza rilevati sull'Akamai Connected Cloud, una rete di circa 340.000 server in più di 4.000 sedi su quasi 1.300 reti in oltre 130 paesi. I nostri team addetti alla sicurezza utilizzano questi dati, misurati in petabyte al mese, per effettuare ricerche sugli attacchi, segnalare comportamenti dannosi e includere ulteriori informazioni nelle soluzioni Akamai.

I dati inclusi in questo rapporto hanno riguardato un periodo di 15 mesi, dal 1° gennaio 2023 al 31 marzo 2024.

DDoS (NXDOMAIN)

Questi dati descrivono il traffico osservato tramite la nostra rete sull'edge per 50 dei nostri principali clienti di servizi finanziari. Le richieste rivolte agli NXDOMAIN vengono tracciate e documentate e possono essere effettuate sia con intenzioni dannose che non dannose. In generale, un aumento delle richieste NXDOMAIN osservato in uno specifico intervallo di tempo e/o area geografica indica un comportamento dannoso. I nostri team addetti alla sicurezza utilizzano questi dati per effettuare ricerche sugli attacchi, segnalare comportamenti dannosi e includere ulteriori informazioni nelle soluzioni di Akamai.

I dati inclusi in questo rapporto hanno riguardato un periodo di 5 mesi, da novembre 2023 a marzo 2024.

Riconoscimenti

Editoria e stesura

Lance Rhodes - Editor in Chief
Susan McReynolds - Case Study Writer
Maria Vlasak - Copy Editing

Revisione e contributi di esperti del settore

Christian Borggreen
Cheryl Chiodi
Sven Dummer
Jim Gilbert
Mitch Mayne
Richard Meeus
Craig Sparling
Carley Thornell

Analisi dei dati

Chelsea Tuttle

Materiali promozionali

Annie Brunholzl

Marketing ed editoria

Georgina Morales Hampe
Emily Spinks

Altri rapporti sullo stato di Internet - Security

Leggete i numeri precedenti e guardate le prossime uscite degli acclamati rapporti sullo stato di Internet - Security di Akamai sul sito **akamai.com/soti**

Ulteriori informazioni sulla ricerca delle minacce Akamai

Restate aggiornati con le ultime intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza. **akamai.com/security-research**

Accesso ai dati del rapporto

Potete visualizzare i grafici e i diagrammi citati in questo rapporto in versioni di alta qualità. L'utilizzo e la consultazione di queste immagini sono forniti a scopo gratuito, purché Akamai venga debitamente citata come fonte e venga conservato il logo dell'azienda: **akamai.com/sotidata**

Ulteriori informazioni sulle soluzioni di Akamai

Per ulteriori informazioni sulle soluzioni di Akamai per gli attacchi alle API, visitate le nostre pagine sulle **soluzioni Prolexic** e **App & API Security**.