SOTI

V10, NUMERO 04

10 YEARS
OF SECURITY INSIGHT

Le minacce alle architetture delle applicazioni moderne:

panoramica sull'area EMEA

Akamai

Stato di Internet - Security

Sommario

I principali risultati emersi dal rapporto

La panoramica sull'area EMEA è un documento integrativo del più ampio rapporto SOTI sulla sicurezza delle app dal titolo Le fortezze digitali sotto assedio: le minacce alle moderne architetture delle applicazioni (disponibile solo in inglese). All'interno di questo rapporto sono disponibili descrizioni dettagliate su come i criminali sfruttano la crescente superficie di attacco, alcuni suggerimenti per proteggere le organizzazioni e una spiegazione delle metodologie impiegate per condurre la nostra ricerca.

Panoramica

Nel corso degli ultimi due decenni, le applicazioni web sono cresciute esponenzialmente in numero e funzionalità, semplificando le attività aziendali, migliorando le customer experience e favorendo l'espansione aziendale tramite funzioni come la comunicazione in tempo reale, l'analisi dei dati e l'automazione dei processi. Anche le API, che fungono da base per le comunicazioni tra le applicazioni, sono proliferate e ora sono pronte per un ulteriore balzo in avanti.

Le applicazioni sono coinvolte praticamente in ogni aspetto delle attività aziendali, il che semplifica l'esecuzione di trilioni di connessioni, ma le rende anche più vulnerabili agli attacchi. In questa panoramica sull'area EMEA, che riguarda il periodo compreso tra gennaio 2023 e giugno 2024, abbiamo adottato una visione olistica delle minacce che influiscono sulle applicazioni, inclusi attacchi web, attacchi DDoS (Distributed Denial-of-Service) e minacce ai carichi di lavoro critici, con un'attenzione particolare alle relative implicazioni per le aziende.

Il numero degli attacchi DDoS ai livelli 3 e 4 è cresciuto costantemente nell'area EMEA (Europa, Medio Oriente e Africa), superando quello degli attacchi in Nord America registrato in cinque degli ultimi sette mesi. Il settore dei servizi finanziari ha sostenuto il peso maggiore di questi attacchi.

L'attività mensile degli attacchi alle applicazioni web e alle API nell'area EMEA ha registrato una tendenza al rialzo in questo periodo, crescendo del 21% dal 1° trimestre del 2023 allo stesso periodo del 2024, con un numero di attacchi che hanno preso di mira le API pari, in media, al 40% del numero di attacchi web mensili.

Il commercio è stato il settore maggiormente colpito dagli attacchi web nell'area EMEA con un'elevata percentuale di attacchi alle API ed è stato anche il settore più colpito dagli attacchi DDoS sferrati al livello 7.

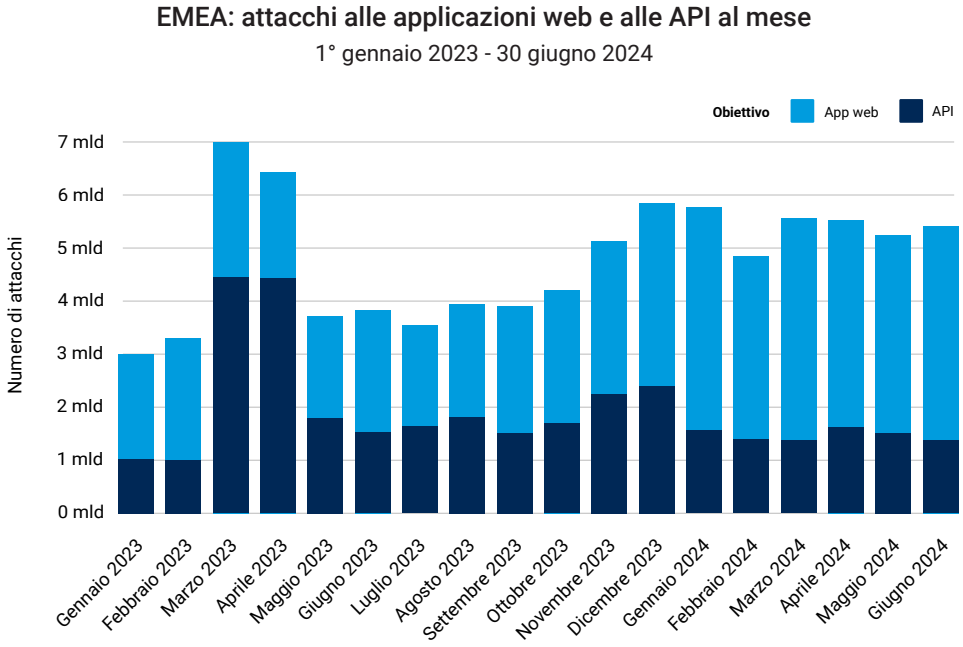
I ransomware e altri tipi di attacchi alle applicazioni, oltre ai carichi di lavoro tra di essi, rappresentano una crescente preoccupazione. Le organizzazioni stanno adottando la microsegmentazione basata su software per la visibilità e i controlli granulari richiesti per proteggere questa superficie di attacco in espansione.

Applicazioni web e API: tanti rischi per la sicurezza

Gli attacchi alle applicazioni web e alle API proliferano mentre le organizzazioni si affrettano ad implementare le app appropriate per migliorare le customer experience e favorire le proprie attività aziendali. I criminali stanno traendo vantaggio dalle vulnerabilità presenti in questa superficie di attacco (ad es., applicazioni web con scarsa codifica e difetti di progettazione, vulnerabilità risalenti a diversi anni fa, ecc.). Inoltre, la rapida espansione dell'economia delle API ha offerto ai criminali informatici ulteriori opportunità di sfruttamento delle vulnerabilità e abuso della logica aziendale.

Le tendenze degli attacchi in cifre

Nel nostro primo rapporto SOTI del 2024, abbiamo esaminato le tendenze degli attacchi alle API nel 2023 all'interno del contesto degli attacchi alle applicazioni web nel complesso. Esaminando i 18 mesi compresi tra gennaio 2023 e giugno 2024, i ricercatori di Akamai hanno riscontrato che l'attività mensile degli attacchi alle applicazioni web e alle API nell'area in EMEA è cresciuta del 21% dal 1° trimestre del 2023 allo stesso periodo del 2024 ed è rimasta elevata per tutto il 2° trimestre del 2024. Gli attacchi sferrati contro le API hanno contribuito a far aumentare il livello di quest'attività, che rappresenta, in media, il 40% degli attacchi web mensili osservati in questo periodo (EMEA - Figura 1).

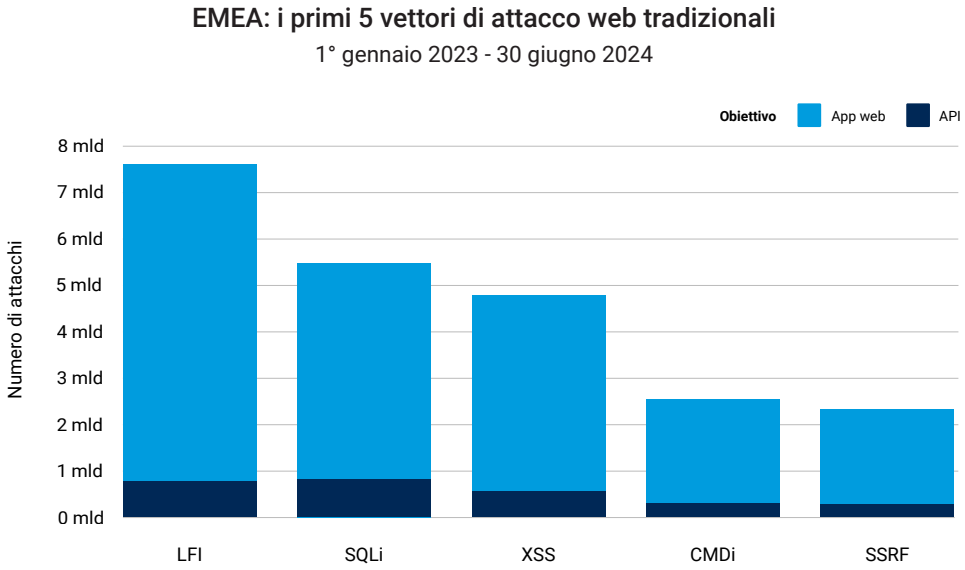


EMEA - Figura 1. Il numero mensile di attacchi alle applicazioni web e alle API rimane elevato nel 2024 (NOTA: il picco di attacchi alle API è correlato al settore del commercio in Spagna, un paese con una concentrazione di attacchi alle API già enorme.

All'interno dell'EMEA, il Regno Unito (20,5 miliardi), i Paesi Bassi (15,6 miliardi) e la Spagna (12,7 miliardi) hanno subito il maggior numero di attacchi alle applicazioni web e alle API. Germania (8,7 miliardi), Austria (7,4 miliardi), Francia (4,8 miliardi), Israele (3 miliardi), Italia (2,7 miliardi), Svizzera (2,5 miliardi) e Belgio (2,3 miliardi) seguono nell'elenco dei primi 10 paesi.

Akamai tiene anche traccia di diversi vettori di attacco web. In questo rapporto, ci concentreremo sui primi cinque metodi tradizionali di attacco basati su vettore.

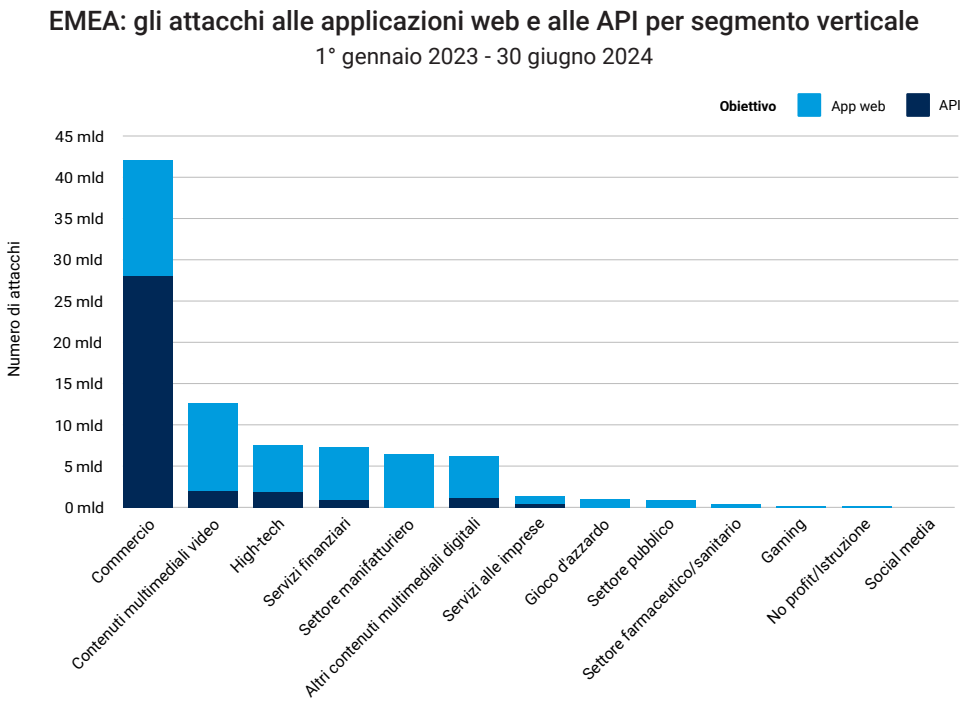
Coerentemente con i rapporti precedenti, l'LFI (Local File Inclusion) è rimasto il vettore di attacco preferito, ma anche altri vettori, come l'SQLi (Structured Query Language injection) e l'XSS (Cross-Site Scripting), destano preoccupazione (EMEA, Figura 2).



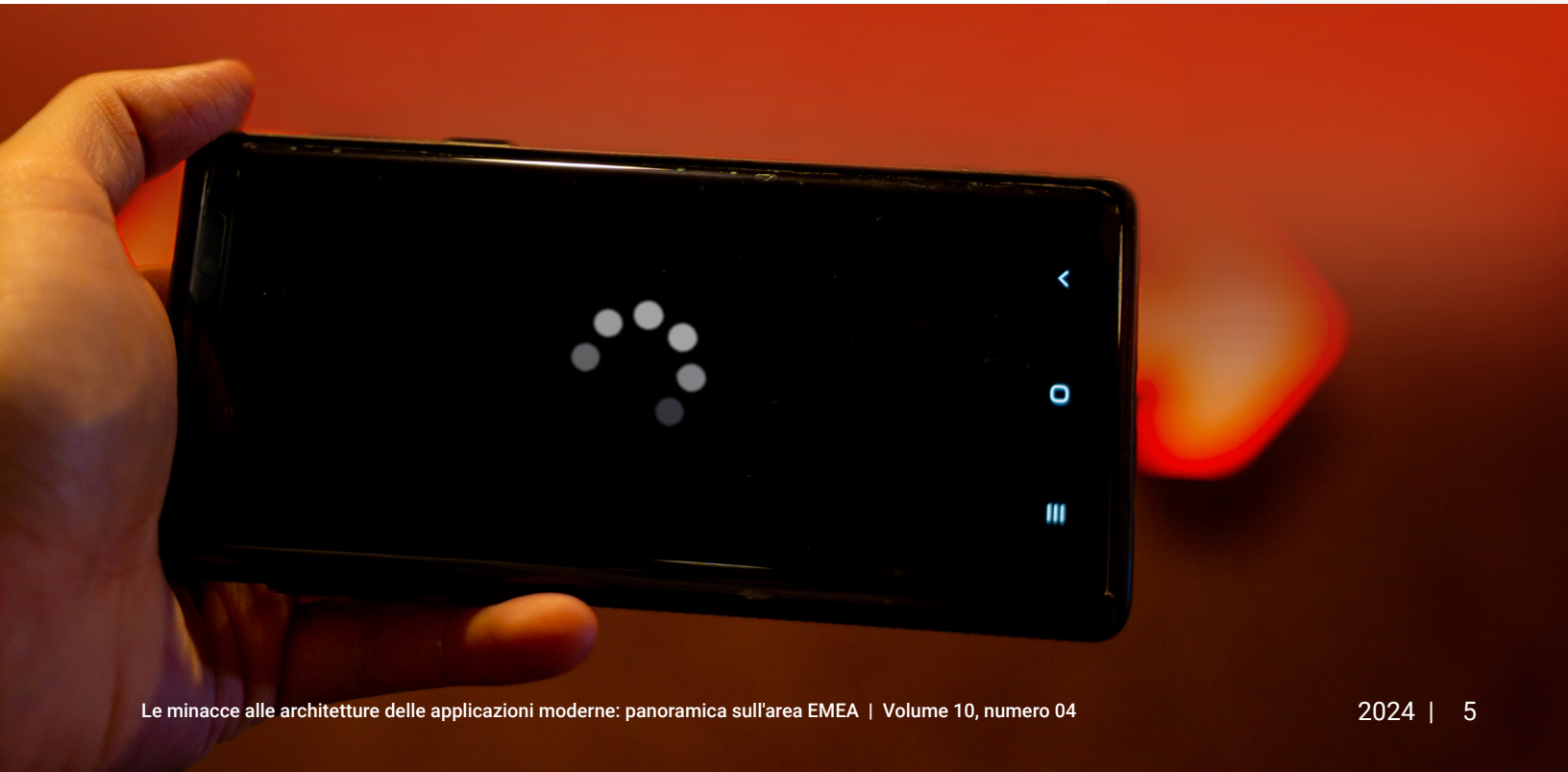
EMEA - Figura 2. I vettori LFI, SQLi e XSS favoriscono l'aumento degli attacchi alle applicazioni web e alle API

Non è insolito per i criminali utilizzare tattiche tradizionali, come l'LFI e l'SQLi, per accedere ai dati degli obiettivi presi di mira. Inoltre, l'LFI consente ai criminali di prendere piede nei sistemi presi di mira ed eseguire codice remoto, mettendo, pertanto, a repentaglio la loro sicurezza.

Continuando con la tendenza osservata nei rapporti precedenti, il commercio e i contenuti multimediali video sono stati i primi settori colpiti dagli attacchi alle applicazioni web e alle API nell'EMEA. Inoltre, come abbiamo segnalato nel nostro rapporto SOTI sulla sicurezza delle API, il commercio ha continuato a subire il maggior numero di attacchi alle API rispetto ad altri settori nella stessa area geografica (EMEA, Figura 3).



EMEA - Figura 3. A causa dell'enorme numero di attacchi alle API , il commercio è stato il settore più colpito dagli attacchi web, seguito dai contenuti multimediali video, dall'high-tech e dai servizi finanziari.



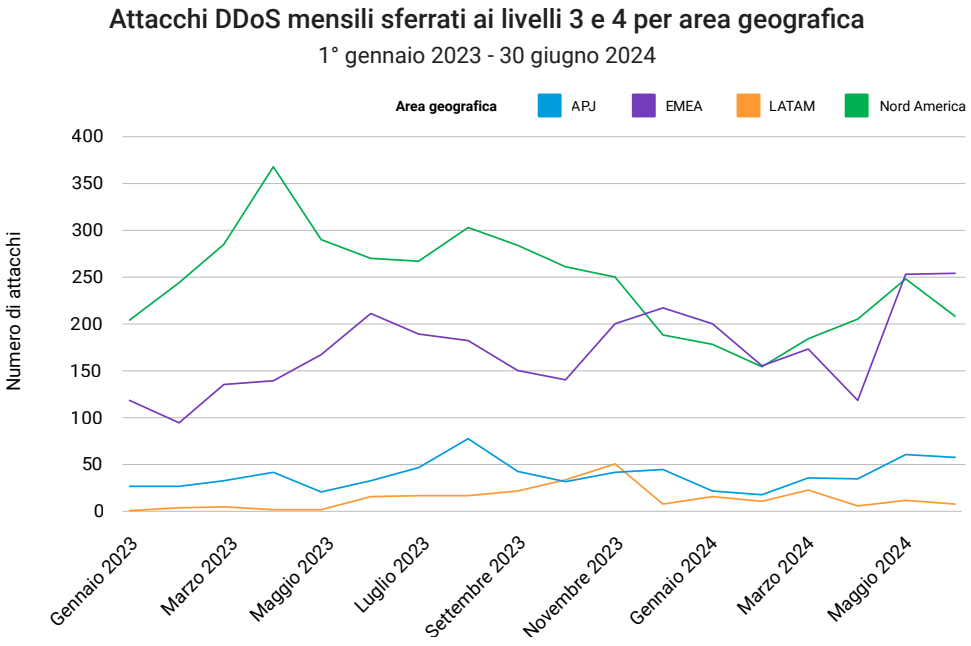
Gli attacchi DDoS minacciano i tempi di attività delle applicazioni

Parallelamente alla continua espansione della superficie di attacco, aumentano anche i tipi di attacchi DDoS che influiscono sulle applicazioni. Come discusso in maggior dettaglio nel rapporto SOTI globale, gli attacchi DDoS sferrati contro l'infrastruttura tradizionale (livelli 3 e 4) sono in circolazione da più tempo rispetto ad altri tipi di attacchi e mirano a sovraccaricare la capacità della rete o del server delle applicazioni. Gli attacchi DDoS a livello di applicazioni (livello 7) sfruttano le vulnerabilità, le falle e/o i difetti della logica aziendale presenti a questo livello, causando potenziali danni significativi anche con una quantità relativamente piccola di traffico dannoso. Indipendentemente dal vettore di attacco, l'impatto di un attacco DDoS si traduce in problemi di downtime delle applicazioni.

La gamma di tipi e tendenze degli attacchi DDoS in quest'area geografica è stata esaminata in dettaglio nel nostro recente rapporto SOTI sull'area EMEA del 2024. In questo rapporto, sono stati inclusi alcuni dati aggiornati che mostrano il costante aumento degli attacchi DDoS sferrati ai livelli 3, 4 e 7 contro l'infrastruttura alla base delle applicazioni, nonché contro le stesse applicazioni.

Attacchi DDoS all'infrastruttura

Nel periodo di 18 mesi (da gennaio 2023 a giugno 2024) oggetto del rapporto, i ricercatori di Akamai hanno riscontrato che il numero degli attacchi DDoS sferrati ai livelli 3 e 4 è cresciuto costantemente nell'area EMEA, superando il numero di attacchi DDoS mensili registrato in Nord America in cinque degli ultimi sette mesi (EMEA, Figura 4).



EMEA - Figura 4. Il numero di attacchi DDoS mensili sferrati ai livelli 3 e 4 nell'area EMEA ha superato quello degli attacchi registrato in Nord America in cinque degli ultimi sette mesi

Nell'area EMEA, i primi paesi interessati dagli attacchi DDoS sferrati ai livelli 3 e 4 sono stati Arabia Saudita (957) e Regno Unito (576), seguiti da Svizzera (240), Turchia (205), Italia (203), Germania (189) e Polonia (115).

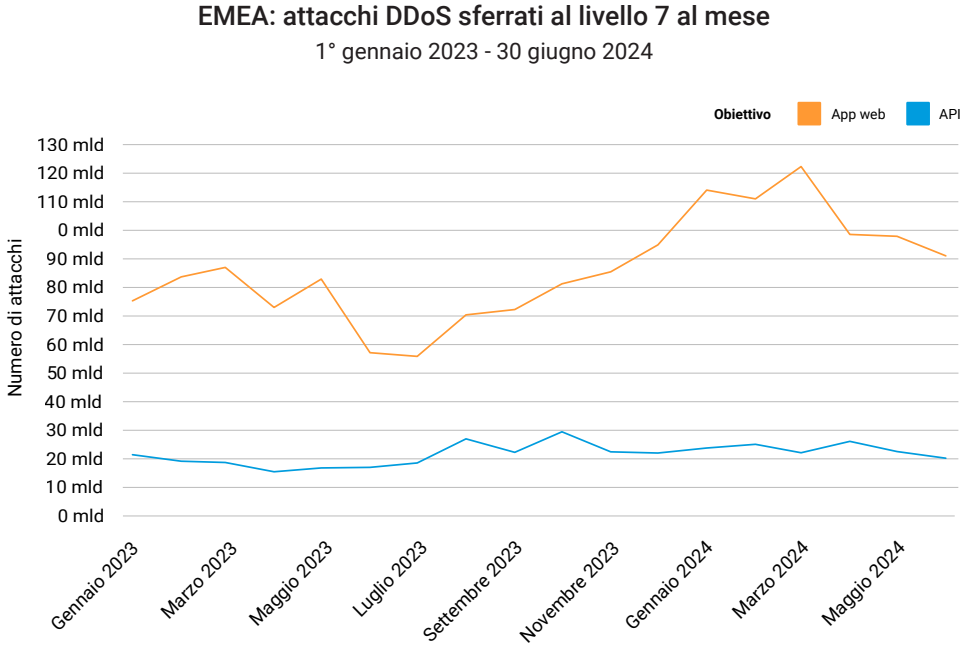
Come descritto nel nostro rapporto SOTI sull'area EMEA, gli attacchi DDoS sono comunemente usati da hacktivisti che agiscono sulla base di motivazioni politiche e criminali sostenuti dai governi. Inoltre, la guerra tra Russia e Ucraina e il conflitto tra Israele e Hamas hanno condotto ad un incremento degli attacchi.

Da un punto di vista industriale, i servizi finanziari (1.523) e il settore manifatturiero (890) hanno subito il maggior numero di attacchi DDoS ai livelli 3 e 4, seguiti dal gaming (189), dal commercio (151), dal gioco d'azzardo (105) e dall'high-tech (95).

Attacchi DDoS a livello di applicazioni

Oltre agli attacchi DDoS sferrati ai livelli 3 e 4, quest'area geografica è stata anche colpita dagli attacchi DDoS a livello di applicazioni (livello 7). Nel periodo di 18 mesi (da gennaio 2023 a giugno 2024) oggetto del rapporto, i nostri ricercatori hanno riscontrato che l'area EMEA è stata la terza area geografica maggiormente colpita dagli attacchi DDoS sferrati al livello 7, subendo 1,9 trilioni di attacchi rispetto agli 8,7 trilioni registrati in Nord America e ai 5,1 trilioni nell'area APJ.

Anche se in numero inferiore rispetto ad altre aree geografiche, è importante notare che gli attacchi DDoS sferrati al livello 7 sono in aumento nell'area EMEA. Dopo il calo a 74 miliardi registrato a maggio 2023, il numero mensile di attacchi DDoS sferrati al livello 7 ha registrato una notevole tendenza al rialzo, quasi raddoppiando a marzo 2024 prima di finire il 2° trimestre del 2024 con una media mensile di 119 miliardi di attacchi che hanno preso di mira applicazioni web e API (EMEA, Figura 5).



EMEA - Figura 5. Gli attacchi DDoS sferrati al livello 7 sono aumentati notevolmente da giugno 2023, finendo il 2° trimestre del 2024 con una media mensile di 119 miliardi di attacchi

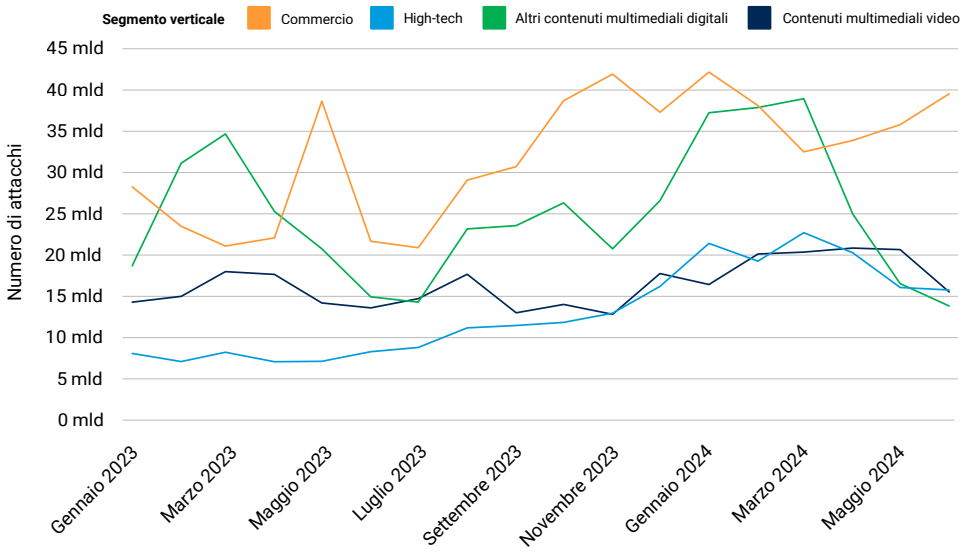
In questo periodo, gli attacchi DDoS sferrati contro le API sono rimasti alquanto stabili e hanno rappresentato il 25% di questo tipo di attacchi. Pertanto, oltre a proteggere dai vettori di attacco descritti in precedenza relativamente agli attacchi alle applicazioni web e alle API (EMEA, Figura 2), difendere le API dagli attacchi DDoS è un chiaro imperativo, specialmente ora che le direttive e le normative continuano a far crescere l'uso delle API.

Nell'area EMEA, i paesi che hanno subito il numero più alto di attacchi DDoS sferrati al livello 7 sono stati Germania (461 miliardi) e Regno Unito (366 miliardi), seguiti da Svezia (167 miliardi), Israele (151 miliardi), Italia (125 miliardi), Malta (113 miliardi), Svizzera (112 miliardi), Francia (90 miliardi), Paesi Bassi (79 miliardi) e Spagna (77 miliardi).

Se guardiamo ai settori, notiamo che il commercio ha iniziato e finito il periodo osservato risultando il settore più colpito dagli attacchi DDoS sferrati al livello 7, seguito dagli altri contenuti multimediali digitali, dai contenuti multimediali video e dall'high-tech (EMEA, Figura 6).

EMEA: attacchi DDoS sferrati al livello 7 al mese per segmento verticale

1° gennaio 2023 - 30 giugno 2024



EMEA - Figura 6. Il settore del commercio è stato il più colpito dagli attacchi DDoS sferrati al livello 7

I criminali puntano ai carichi di lavoro delle applicazioni

Il modello Zero Trust viene solitamente descritto nell'ambito della sicurezza di rete. Tuttavia, anche le applicazioni web e i carichi di lavoro interni possono risultare vulnerabili a varie minacce, come i ransomware, che cercano un punto di ingresso e una strada per raggiungere gli obiettivi prefissati.

Come esaminato in dettaglio nel rapporto globale, per far funzionare le applicazioni (nel cloud, on-premise o in un ambiente ibrido), ogni singolo carico di lavoro deve essere operativo senza creare problemi. I carichi di lavoro attraversano diverse aree di sicurezza nel loro percorso all'interno della rete e ognuna di esse aggiunge un potenziale punto di ingresso per un criminale. La protezione di quest'ampia superficie di attacco è fondamentale per rafforzare la strategia di sicurezza complessiva, ma complica ulteriormente il lavoro già difficile dei team addetti alla sicurezza.

L'implementazione di un sistema Zero Trust da un approccio tradizionale basato su hardware richiede molte risorse e tempi lunghi, il che causa problemi di downtime. Inoltre, una reale implementazione Zero Trust richiede la microsegmentazione, che può proteggere dai ransomware o dagli attacchi contro i carichi di lavoro.

La microsegmentazione basata su software è rapida e semplice da implementare e rendere operativa, pertanto può risultare anche un valido metodo per rispondere agli incidenti e un controllo per isolare i sistemi critici a supporto della conformità normativa. Inoltre, offre un'accurata visibilità sulla rete e controlli di governance estremamente granulari. Grazie a questi vantaggi, le organizzazioni adottano sempre più questo approccio per rilevare e mitigare un carico di lavoro o un container a rischio nei propri data center, cloud e ambienti cloud ibridi.

Lezioni ricavate dal mondo reale sulla protezione dei carichi di lavoro delle applicazioni

In questa sezione, vengono presentati due case study osservati nell'area EMEA, che esemplificano il modo con cui le aziende stanno proteggendo i carichi di lavoro critici e l'innovazione del modello Zero Trust.

EMEA - Case study 1: per proteggere i sistemi critici e i dati sensibili, che sono correlati ai commercio e ai pagamenti, il CISO (Chief Information Security Officer) di un'importante banca che si occupa di investimenti esamina regolarmente la sicurezza della sua infrastruttura tecnologica per rafforzare il sistema di sicurezza di tutti i suoi domini. Fermare gli attacchi ransomware è un obiettivo importante per l'azienda, come sono anche fondamentali la scalabilità e il supporto di diversi sistemi operativi e ambienti cloud. Inoltre, il CISO cercava un modo per ridurre la superficie di attacco senza incorrere nei costi e nei ritardi associati all'aggiornamento dei firewall preesistenti. I carichi di lavoro sono stati isolati uno dall'altro mediante l'implementazione di una soluzione di microsegmentazione basata su software, che crea zone protette in tutti gli ambienti del data center. Se un carico di lavoro subisce un attacco, può essere isolato, impedendo al software dannoso di diffondersi in tutta la rete.

EMEA - Case study 2: un fornitore di media e software cercava un modo più semplice per innovare il suo sistema Zero Trust al fine di migliorare la protezione dei dati dei clienti e dei carichi di lavoro critici. Per realizzare questo miglioramento, era imprescindibile separare tra loro i componenti di alto valore come la gestione delle identità e i sistemi di pianificazione delle risorse aziendali con precise policy di segmentazione. L'obiettivo era quello di ridurre al minimo il traffico in entrata e in uscita, nonché inasprire le policy di accesso su centinaia di server aziendali. Nello stesso tempo, l'azienda voleva evitare di apportare importanti modifiche al proprio ecosistema che avrebbero potuto causare interruzioni delle attività e aumentare i rischi per la sicurezza. Un approccio alla microsegmentazione basata su software con una visibilità granulare sui modelli di interazione, nonché sugli avvisi, ha consentito al team di disporre di funzionalità tali da impedire il movimento laterale dannoso nell'intera rete.

Conclusione

In questa panoramica sull'area EMEA, abbiamo tentato di fornire una visione olistica dei diversi metodi con cui i criminali possono prendere di mira applicazioni e API. Dal punto di vista della gestione dei rischi e della sicurezza, è fondamentale per le organizzazioni comprendere e difendersi dalle minacce alle applicazioni e alle API, all'infrastruttura e ai carichi di lavoro critici. Inoltre, anche la legislazione futura (come già fanno le attuali normative) renderà questo approccio imprescindibile per proteggere le applicazioni.

All'interno dell'EMEA, nell'Unione europea, la legislazione fondamentale a tal riguardo include l'aggiornamento della direttiva NIS2 (Network and Information Systems), il DORA (Digital Operational Resilience Act), il CRA (Cyber Resilience Act), il Programma europeo per la protezione delle infrastrutture critiche, il nuovo PCI DSS (Payment Card Industry Data Security Standard) v4.0 e la direttiva europea PSD3 (Payment Services Directive) che verrà aggiornata a breve.

Le applicazioni sono più importanti che mai per le aziende, ma risultano anche più vulnerabili agli attacchi. Con funzionalità e best practice in grado di risolvere le sfide correlate ad una superficie di attacco in continua espansione, le organizzazioni possono proteggere le applicazioni create ovunque e in qualsiasi momento, senza compromettere le performance o le customer experience.

Per maggiori informazioni, potete consultare il rapporto SOTI globale sulla sicurezza delle API dal titolo "Le fortezze digitali sotto assedio: le minacce alle architetture delle applicazioni moderne".

Metodologia

Attacchi DDoS alle applicazioni web e al livello 7

Questi dati descrivono gli avvisi a livello di applicazioni relativi al traffico osservato tramite la nostra soluzione WAF (Web Application Firewall). Gli avvisi sugli attacchi alle applicazioni web vengono attivati quando si rileva un payload dannoso all'interno di una richiesta a un sito web, un'applicazione o un'API protetta. Gli avvisi sugli attacchi DDoS sferrati al 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 qui presentati 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.

Questi dati hanno riguardato un periodo di 18 mesi, dal 1° gennaio 2023 al 30 giugno 2024.

Aggiornamento dei dati nel 2024

Siamo lieti di annunciare alcuni aggiornamenti apportati ai nostri dataset per il nostro 10° anniversario! I nostri dataset relativi agli attacchi alle applicazioni web sono stati aggiornati. Il metodo di raccolta dei dati è stato trasformato, semplificato e ottimizzato. La portata e l'accuratezza delle nostre informazioni sono state migliorate. Sono state aggiunte le classificazioni per altri vettori di attacco, ad esempio l'SSRF. L'identificazione degli attacchi che hanno preso di mira gli endpoint delle API è stata, inoltre, aggiunta ai dataset. Siamo lieti di aver condiviso alcuni dei nostri nuovi miglioramenti in questo rapporto e speriamo di continuare a condividere questi aggiornamenti nel corso dell'anno (e oltre) per festeggiare così l'anniversario del rapporto SOTI - Security con i nostri lettori.

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.

Questi dati hanno riguardato un periodo di 18 mesi, dal 1° gennaio 2023 al 30 giugno 2024.

Riconoscimenti

Direttore della ricerca

Mitch Mayne

Editoria e stesura

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Revisione e contributi di esperti del settore

Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
Steve Winterfeld

Analisi dei dati

Chelsea Tuttle

Materiali promozionali

Barney Beal

Marketing ed editoria

Georgina Morales
Emily Spinks

Altri rapporti sullo stato di Internet - Security

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

Ulteriori informazioni sulla ricerca delle minacce di Akamai

Restate aggiornati con le ultime novità in materia di intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza consultando il sito **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 applicazioni e alle API, visitate la nostra **pagina sulla sicurezza di applicazioni e API**.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 08/24.