

The logo for FOS (Forum of the Operators of the Italian Internet) is displayed in large, white, stylized letters. The background of the entire cover features a digital landscape with blue and purple wavy lines and a grid of small squares, suggesting a network or data environment.

FOS

V11, NUMERO 02

Lo stato della sicurezza di app e API nel 2025

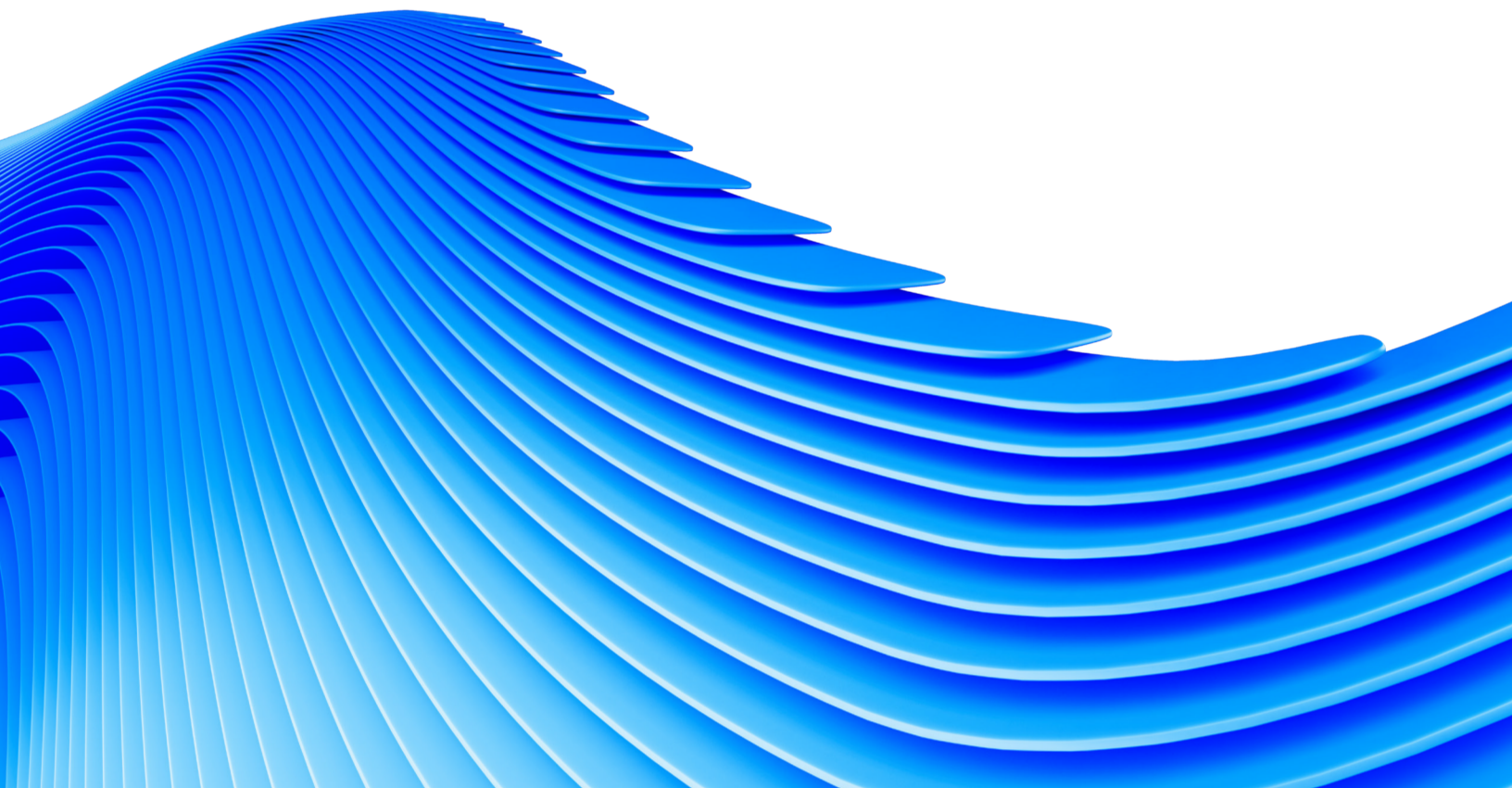
Come l'AI sta cambiando lo scenario digitale



Stato di Internet - **Security**

Contenuti

02	Introduzione
04	I principali risultati emersi dal rapporto
06	Sviluppo dell'intelligence di Akamai sulle minacce informatiche
13	Attacchi web: confronto e tendenze su base annua
17	Attacchi DDoS al livello 7: confronto e tendenze su base annua
21	Tendenze per settore
27	Tendenze per area geografica
39	Conformità
44	Mitigazione
46	Metodologia
47	Riconoscimenti



Introduzione

Agli inizi del 2025, il panorama relativo alla sicurezza delle applicazioni web si contraddistingue per un livello di evoluzione e complessità senza precedenti dei vettori di attacco. Le organizzazioni devono far fronte a un aumento marcato delle minacce che prendono di mira le applicazioni web e le API, un incremento direttamente correlato alla rapida adozione dei servizi cloud, delle architetture di microservizi e delle applicazioni basate sull'AI (intelligenza artificiale). Akamai, infatti, ha riscontrato oltre 311 miliardi di attacchi soltanto nel 2024, con un aumento del 33% su base annua. Inoltre, il [contesto geopolitico](#) ha aggravato ulteriormente la situazione. Il volume più elevato di attacchi DDoS (Distributed Denial-of-Service) al livello 7 (a livello di applicazione) si è registrato nei settori dell'high-tech, del commercio e dei social media. In particolare, i criminali informatici oggi [sfruttano](#) le kill chain generate dall'intelligenza artificiale per rendere automatica ogni fase del ciclo di vita degli attacchi.

Contemporaneamente, le API sono diventate uno degli obiettivi principali delle violazioni, con oltre 150 miliardi di attacchi documentati da Akamai da gennaio 2023 a dicembre 2024. Inoltre, l'integrazione degli strumenti SaaS (Software-as-a-Service) basati sull'intelligenza artificiale nelle piattaforme core ha determinato un notevole ampliamento della superficie di attacco. Le [conseguenze](#) economiche non sono trascurabili. Attualmente, i problemi correlati alla sicurezza delle API costano alle organizzazioni circa \$ 87 miliardi all'anno e si prevede che questa cifra, senza un intervento adeguato, potrebbe superare i \$ 100 miliardi (in dollari statunitensi) entro il 2026. Le API nascoste e zombie costituiscono un vettore di attacco particolarmente vulnerabile all'interno degli ecosistemi sempre più complessi delle API.



Il ruolo dell'intelligenza artificiale per la sicurezza delle applicazioni web e delle API

L'intelligenza artificiale sta rivoluzionando la sicurezza delle applicazioni web e delle API, creando al contempo nuovi problemi. Nelle applicazioni web, l'AI viene **utilizzata** per rendere automatico il rilevamento delle minacce, prevedere possibili violazioni e migliorare i tempi di risposta agli incidenti. Tuttavia, **consente** anche ai criminali di generare malware, impiegare strategie avanzate di web scraping e implementare metodologie dinamiche che automatizzano il ciclo di vita degli attacchi.

L'intelligenza artificiale ha un **ruolo** preponderante nella gestione e nella protezione delle interazioni fra le API su larga scala. Gli strumenti basati sull'AI sono indispensabili per il rilevamento delle anomalie, l'identificazione dei modelli di uso improprio e la reazione in tempo reale alle minacce. È certo che la gestione delle API basata sull'intelligenza artificiale continuerà a **evolversi** e garantirà una protezione avanzata contro attacchi sempre più sofisticati, attraverso l'integrazione di strumenti automatici per la sicurezza e l'analisi predittiva. Tuttavia, malgrado i progressi, nuovi **attacchi** come il credential stuffing e lo sfruttamento delle vulnerabilità insite nella logica aziendale restano un problema importante, che può essere contrastato con efficacia mediante l'impiego di sistemi di sicurezza affidabili.

Le strategie di attacco contro le API e le applicazioni web: divergenze e interrelazioni

Gli attacchi alle app web e alle API, pur essendo correlati, colpiscono elementi diversi dell'infrastruttura di un'applicazione:



Gli **attacchi alle applicazioni web** prendono di mira i componenti rivolti all'utente, come le pagine di accesso disponibili al pubblico, e spesso utilizzano tecniche meno avanzate.



Gli **attacchi alle API** puntano sulle vulnerabilità presenti negli endpoint delle API e nella logica di back-end delle applicazioni, pertanto richiedono una conoscenza più approfondita della struttura e del comportamento delle API.

Le differenze principali riguardano la superficie e la complessità degli attacchi. Nel primo caso, le violazioni sono in genere dirette contro le parti visibili di un'applicazione, mentre nel secondo caso sfruttano i canali di comunicazione tra i componenti diversi di un software. Tuttavia, quando vanno a buon fine, entrambi gli attacchi assicurano l'accesso non autorizzato ai dati sensibili e alle risorse di sistema.

Una conoscenza approfondita delle misure di cybersecurity è quindi indispensabile per proteggere contemporaneamente le app web e le API, perché le applicazioni moderne dipendono maggiormente dalle API per un corretto funzionamento. Nei prossimi due anni, le organizzazioni prevedono un **aumento** pari al 39% delle applicazioni web, che renderà ancora più evidente la stretta correlazione tra la sicurezza delle applicazioni web e quella delle API. Trascurando uno dei due aspetti, le organizzazioni possono diventare più **vulnerabili** agli attacchi multivettore sofisticati, che sfruttano i punti deboli presenti nel front-end e nel back-end delle applicazioni.

L'analisi esclusiva di Akamai: come identificare i modelli delle minacce

Akamai ha esaminato questa situazione complessa sulla scorta dei dati offerti dalla propria infrastruttura di rete, che elabora più di un terzo del traffico web mondiale e assicura una visibilità senza confronti sui modelli delle minacce. Questa prospettiva, insieme agli approfondimenti elaborati dai suoi team di ricerca e data science, consente ad Akamai di fornire un'intelligence utile e completa. I risultati raggiunti offrono ai responsabili della sicurezza i dati strategici necessari per decidere su quali aspetti concentrarsi per ridurre i rischi e aumentare al massimo il ritorno sull'investimento nei sistemi di sicurezza.

I principali risultati emersi dal rapporto

Le API basate sull'AI sono meno sicure delle loro controparti.

La maggior parte delle API basate sull'intelligenza artificiale è accessibile dall'esterno e spesso si basa su meccanismi di autenticazione inadeguati, una vulnerabilità che diventa più pericolosa se si considera l'incremento degli attacchi basati sull'AI a cui sono soggette.

L'AI favorisce il progresso tecnologico dei criminali.

Le tecniche più innovative comprendono i malware basati sull'intelligenza artificiale, le soluzioni per la scansione delle vulnerabilità, la violazione dei sistemi che integrano l'AI e funzionalità avanzate di web scraping.

+32%

Aumento degli incidenti correlati alle 10 principali vulnerabilità della sicurezza delle API riportate nell'elenco OWASP.

Gli incidenti di sicurezza delle API sono in aumento e l'elenco OWASP mette in luce le falle dei sistemi di autenticazione e autorizzazione che rendono visibili le funzionalità e i dati sensibili.

+30%

Aumento degli avvisi di sicurezza correlati al framework MITRE.

I criminali sfruttano le API attraverso l'impiego di tecniche avanzate, come l'automazione e l'intelligenza artificiale. Il framework MITRE può aiutare gli addetti alla sicurezza a identificare questi attacchi con maggiore efficienza e velocità.

+33%

Aumento degli attacchi web globali su base annua.

La diffusione degli attacchi è direttamente correlata alla rapida adozione di servizi cloud, microservizi e applicazione AI, che ampliano le superfici di attacco e pongono nuovi rischi per la sicurezza.

Oltre 230 miliardi

Attacchi web che hanno colpito il commercio.

Questo settore è stato il più colpito e ha segnalato un numero di attacchi quasi tre volte superiore a quello dell'high-tech (situato al secondo posto).

+73%

Aumento totale degli attacchi web su base annua nell'area API.

Gli incidenti sono passati da 29 miliardi nel 2023 a 51 miliardi nel 2024.

37%

Attacchi web diretti contro le API nell'area EMEA.

Questo dato indica che si sono concentrati in maggior misura nell'area EMEA rispetto a tutte le altre regioni geografiche.

+94%

Crescita degli attacchi DDoS al livello 7

tra il primo trimestre del 2023 e il quarto trimestre del 2024.

11,9 migliaia di miliardi

Attacchi DDoS al livello 7 sferrati in Nord America

nel corso dei due anni presi in esame (dal primo trimestre del 2023 al quarto trimestre del 2024).

7 migliaia di miliardi

Attacchi DDoS al livello 7 contro l'high-tech.

Dal gennaio del 2023 al dicembre del 2024, questo settore è stato il più colpito.

7,4 migliaia di miliardi

Attacchi DDoS al livello 7 sferrati nella regione API

nel corso dei due anni presi in esame (dal primo trimestre del 2023 al quarto trimestre del 2024).

20%

Attacchi DDoS al livello 7 contro le API nell'area EMEA.

Questo dato indica che si sono concentrati in maggior misura nell'area EMEA rispetto a tutte le altre regioni geografiche.

Sviluppo dell'intelligence di Akamai sulle minacce informatiche

L'acquisizione di Nonym Security da parte di Akamai ha migliorato in modo significativo le funzionalità di ricerca e di generazione dei rapporti sulle minacce per le API, fornendo dati più approfonditi sui relativi rischi. Grazie a questo nuovo dataset, ancora nelle fasi iniziali di integrazione, Akamai sta ottimizzando le analisi sulle minacce esistenti per fornire un quadro più completo sui problemi di sicurezza delle API.

Mappatura degli avvisi ai framework per la sicurezza

Nel corso del tempo, il dataset consentirà di mappare le informazioni più dettagliate sugli avvisi di sicurezza ai framework di cybersecurity e agli standard di conformità più importanti, tra cui:

- ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) di MITRE
- GDPR (Regolamento generale sulla protezione dei dati)
- PCI DSS (Payment Card Industry Data Security Standard)
- ISO (Organizzazione internazionale per la standardizzazione)
- OWASP (Open Worldwide Application Security Project)

Si tratta di un notevole progresso, che consentirà ad Akamai di fornire una protezione affidabile ed efficace ai propri clienti. Attraverso l'allineamento a questi framework, le organizzazioni potranno avere una visione più chiara del proprio livello di sicurezza, adeguarsi ai requisiti normativi e assegnare la giusta priorità alle iniziative incentrate sulla protezione. Questo approccio completo permetterà un'allocazione più ponderata delle risorse e lo sviluppo di interventi mirati per la salvaguardia delle API e dei dati sensibili.

Analisi di un campione mensile di dati

In questo rapporto, abbiamo esaminato un campione di dati, relativo a un periodo di 30 giorni, per offrire un quadro d'insieme sulle attività condotte dai malintenzionati, suddivisa in base a ciascun framework di cybersecurity e agli standard di conformità (Figura 1). Inoltre, abbiamo approfondito l'argomento degli avvisi MITRE e OWASP e analizzato in che modo i rischi e gli incidenti relativi alla sicurezza possono avere conseguenze negative sulla conformità.

	Attività in 30 giorni	Aumento mensile
OWASP	5.907.000	32%
MITRE	2.817.000	30%
ISO	832.000	22%
GDPR	669.000	21%
PCI DSS	881.000	16%

Fig. 1. Ripartizione degli avvisi in base ai framework di sicurezza e agli standard di conformità

Avvisi MITRE

Nell'arco di 30 giorni, tra i nostri clienti abbiamo riscontrato un aumento del 30% negli incidenti correlati alle tecniche MITRE. Scendendo nei particolari, i criminali hanno impiegato spesso il metodo T1078 (Valid Accounts), che consiste nell'utilizzare delle credenziali legittime, ossia degli account validi, per ottenere un accesso non autorizzato ai sistemi o alle reti aziendali. Siccome i token sono molte volte indispensabili per l'autorizzazione delle API, i malintenzionati che riescono a impadronirsene possono accedere ai dati sensibili senza essere individuati.

Inoltre, abbiamo rilevato una serie di attacchi T1566 (Phishing), che prevedono la sottrazione delle credenziali o dei token delle API attraverso una campagna di phishing. Con i dati sottratti, i criminali potranno sferrare nuovi attacchi. Le API espandono la superficie di attacco e di conseguenza i criminali se ne avvalgono con maggiore frequenza per introdursi nei sistemi. In aggiunta, gli avvisi relativi al metodo T1190 (Exploit Public-facing Application) hanno posto in evidenza il fatto che i malintenzionati si servono delle falle presenti nelle applicazioni per infiltrarsi nelle reti. T1580 (Cloud Infrastructure Discovery) è un'altra delle tecniche riscontrate. Si tratta di un attacco nel quale vengono originate delle chiamate API per effettuare una ricognizione e sondare gli endpoint esposti sul cloud.

Sebbene non disponga di una matrice dedicata alla sicurezza delle API, il framework MITRE continua ad essere indispensabile per le organizzazioni e i team addetti alla sicurezza che intendono ottenere informazioni utili sulle tecniche di attacco contro le API. Mappando le tecniche adottate dai criminali e i comportamenti specifici delle API, i team addetti alla sicurezza sono in grado di identificare le fasi di un attacco e le strategie, i metodi e le procedure correlati, ottimizzando la risposta agli incidenti. Questo approccio consente quindi di mitigare i rischi in modo più efficace.

Avvisi OWASP

L'elenco OWASP API Security Top 10 è un punto di riferimento indispensabile per ottenere informazioni utili sulla gravità e sulle conseguenze relative a una vulnerabilità. Grazie a questa risorsa, i team addetti alla sicurezza e gli sviluppatori possono stabilire con efficienza la priorità delle diverse iniziative e restare sempre aggiornati sui rapidi sviluppi nel panorama delle minacce.

Durante il periodo preso in esame, ossia nell'arco di 30 giorni, la nostra analisi ha riscontrato che gli incidenti correlati alle minacce dell'elenco OWASP hanno subito un aumento del 32%. In particolare, una serie specifica di vulnerabilità, come BOPLA (Broken Object Property Level Authorization), BFLA (Broken Function Level Authorization) e la violazione Broken Authentication espongono direttamente le informazioni sensibili o le funzioni più importanti alle attività dei malintenzionati. I meccanismi di autorizzazione inadeguati costituiscono uno dei vettori di attacco più pericolosi per le API, in quanto consentono ai criminali di effettuare l'escalation dei privilegi, assumere il controllo degli account e accedere a informazioni riservate.

La violazione dell'autorizzazione a livello di oggetto, altrimenti definita BOLA, rimane una vulnerabilità critica per la sicurezza delle API, ma è difficile da rilevare perché è legata alle falle presenti nella logica aziendale. Questa situazione spesso comporta una bassa percentuale di rilevamento e una segnalazione inadeguata degli attacchi. Per risolvere il problema, le organizzazioni devono adottare soluzioni per la sicurezza delle API che stabiliscano relazioni chiare tra gli utenti e le risorse a cui accedono normalmente. A tale proposito, è necessario stabilire degli standard di riferimento relativi ai comportamenti, tramite algoritmi sofisticati di apprendimento automatico in grado di riconoscere i modelli di accesso anomali.

Un attacco BOPLA sfrutta i problemi di accesso granulari a livello di campo delle API, che spesso vengono ignorati durante l'esecuzione dei test di sicurezza. A differenza della vulnerabilità BOLA, che richiede la modifica di interi ID oggetto, questo tipo di attacco prende di mira determinate proprietà all'interno degli oggetti. Un esempio di vulnerabilità BOPLA è una chiamata DELETE API la cui risposta rende visibili i dati PII (informazioni di identificazione personale) più sensibili. Grazie a questo livello di sofisticazione, gli attacchi BOPLA sono più frequenti di quelli BOLA.

Un altro esempio pratico è il caso in cui viene utilizzato soltanto un indirizzo e-mail per inviare la richiesta di annullamento di un'iscrizione, alla quale l'API risponde includendo inavvertitamente anche il nome completo dell'utente. La causa che sottende alla divulgazione di informazioni sensibili a soggetti non autorizzati va rintracciata nei test sulla sicurezza, che solitamente sono eseguiti su interi oggetti anziché su singole proprietà. Questa circostanza fa sì che le attività per la valutazione della sicurezza delle API rilevino un numero maggiore di vulnerabilità BOPLA.

Un'altra vulnerabilità di importanza cruciale è l'utilizzo delle risorse illimitato, che innesca un'interruzione dei servizi in seguito a un attacco DDoS o a un esaurimento delle risorse. In questo caso, i rischi non si limitano soltanto alle ripercussioni sui servizi, ma comprendono un aumento dei costi operativi, causato dall'uso eccessivo delle risorse sul cloud, e una maggiore esposizione agli attacchi di forza bruta. Senza una limitazione adeguata della velocità, i criminali possono sondare rapidamente le API e compromettere la sicurezza. Inoltre, questi attacchi danno origine a una notevole quantità di traffico, che si traduce in un incremento esorbitante dei costi per le organizzazioni.

Un altro vettore è rappresentato dall'utilizzo non sicuro delle API, che dipende da fattori correlati all'integrazione delle API di terze parti, come l'inadeguatezza delle attività di convalida e filtraggio dei dati e l'assenza di sistemi di protezione. Si tratta di un problema che desta crescenti preoccupazioni, perché le organizzazioni impegnate nella trasformazione digitale dipendono in larga misura dalle API di terze parti. Secondo uno [studio recente](#), oltre l'80% delle organizzazioni coinvolte nel sondaggio ha riscontrato problemi con le API di terze parti, un dato che pone in evidenza quanto sia importante adottare un modello di sicurezza Zero Trust. Questa vulnerabilità, di per sé, non produce gravi conseguenze nell'immediato, ma in combinazione con altri punti deboli, come l'esecuzione di una convalida di bassa qualità e la presenza di dipendenze non protette, può costituire un grave rischio per la sicurezza. Ad esempio, un'API impiegata da una società finanziaria, se considera attendibili le transazioni non verificate di terze parti, potrebbe aprire la strada a una violazione della sicurezza.



Gli avvisi di sicurezza relativi ai requisiti PCI DSS e alla normativa GDPR sono aumentati rispettivamente del 16% e del 21%, mentre gli avvisi associati allo standard ISO 27001 sono arrivati al 22%.

Come garantire la conformità delle API

Per assicurare la conformità delle API, è possibile fare ricorso a una serie di best practice, come contrassegnare ogni avviso non conforme indicando gli standard normativi e i requisiti violati, fornire in tempo reale informazioni utili sui problemi di conformità più importanti e offrire alle organizzazioni istruzioni pratiche per risolverli. Attraverso questo approccio proattivo, le organizzazioni sono in grado di attenersi alle normative ed evitare di incorrere in pesanti sanzioni, ripercussioni legali e danni alla reputazione, che possono determinare gravi perdite economiche. Ad esempio, [una compagnia aerea ha dovuto pagare una multa di £ 20 milioni](#) dopo che una vulnerabilità API ha reso visibili i dati di 400.000 clienti. Questo episodio mette in luce le gravi conseguenze che può avere, ai sensi del GDPR, una protezione inadeguata delle API.

Gli standard di conformità rappresentano un punto di riferimento indispensabile per le organizzazioni che intendono proteggere i dati sensibili, tutelare i clienti e adempiere agli obblighi legali e normativi. Standard quali i requisiti PCI DSS (Payment Card Industry Data Security Standard), la normativa GDPR (Regolamento generale sulla protezione dei dati) e il provvedimento HIPAA (Health Insurance Portability and Accountability Act) impongono di gestire in sicurezza le informazioni sensibili, come i dati di pagamento e le PII. L'analisi dei dati in nostro possesso dimostra come gli avvisi di sicurezza relativi ai requisiti PCI DSS e alla normativa GDPR siano aumentati rispettivamente del 16% e del 21%, mentre gli avvisi relativi allo standard ISO 27001 siano arrivati al 22%.

GDPR

La normativa GDPR mette in risalto la necessità di integrare la protezione dei dati e la privacy dei clienti nell'intero ciclo di vita delle API. Questi obiettivi possono essere raggiunti attraverso una progettazione sicura, un livello avanzato di autenticazione e autorizzazione, l'introduzione di opzioni per la limitazione della velocità, l'esecuzione periodica di test sulle vulnerabilità, l'implementazione della crittografia e la valutazione costante dei rischi, anche nelle fasi iniziali di sviluppo. Con queste misure è possibile garantire la riservatezza, l'integrità e la disponibilità dei dati.

PCI DSS

Analogamente, i requisiti [PCI DSS](#) sottolineano l'importanza di proteggere le API che gestiscono i dati di pagamento delle carte di credito, estendendo le misure di sicurezza alle fasi di progettazione, codifica e test. Le organizzazioni sono obbligate a garantire la protezione dalle vulnerabilità web e a identificare e risolvere le falle nel sistema di sicurezza mediante l'esecuzione di test periodici.

I requisiti 10 e 11, nello specifico, richiedono la registrazione e il monitoraggio completi delle attività delle API, come le richieste e le risposte, i tentativi di autenticazione e le modifiche del sistema. I registri devono essere conservati per almeno 12 mesi, mentre quelli relativi ai tre mesi più recenti devono essere immediatamente accessibili per l'analisi. Inoltre, i requisiti PCI DSS consigliano alle organizzazioni di eseguire una scansione delle vulnerabilità esterne ogni qual volta vengano introdotte modifiche di una certa entità. Per assicurare la conformità e garantire la resilienza delle API ai rischi e alle minacce, le organizzazioni devono implementare sistemi di controllo rigorosi, che comprendano la limitazione della velocità, le opzioni di registrazione, il metodo RBAC (controllo degli accessi basato sui ruoli) e una gestione sicura delle sessioni.



ISO 27001

Lo standard ISO 27001 è un quadro di riferimento affidabile che consente alle organizzazioni di gestire con efficacia i rischi legati alla protezione delle informazioni, ottimizzare il livello di sicurezza e creare un clima di fiducia tra colleghi e clienti. Ecco alcune delle best practice consigliate:

- Implementazione del controllo degli accessi (ad esempio, chiavi API) per verificare l'identità dell'utente
- Utilizzo della crittografia end-to-end dei dati
- Monitoraggio delle API per rilevare la presenza di comportamenti anomali
- Esecuzione approfondita delle valutazioni dei rischi per identificare possibili vulnerabilità delle API

Questi criteri di conformità mettono in luce il legame fondamentale tra i quadri normativi e la sicurezza delle API. Un'implementazione adeguata consente non soltanto di proteggere i dati sensibili, ma anche di rispettare contemporaneamente diversi obblighi relativi alla conformità. Per ulteriori informazioni sugli standard globali, sia in vigore che in via di sviluppo, consultate la sezione [Conformità](#) di questo rapporto.

Le lacune delle API in termini di visibilità: i varchi nascosti per l'accesso ai dati

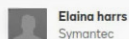
Abuso delle API

Nel novembre 2024, l'azienda [Bleeping Computer ha segnalato](#) un attacco condotto su larga scala contro un fornitore di soluzioni di firma digitale. I criminali sono riusciti a inviare fatture fraudolente a diversi utenti sfruttando un componente basilare dell'API utilizzata dal fornitore per la gestione e il monitoraggio dei documenti. Se le vittime firmavano per errore la fattura falsa, i malintenzionati ne potevano sollecitare il pagamento a diverse organizzazioni.

Questo incidente sottolinea le conseguenze nefaste legate all'abuso delle API, che possono essere sfruttate al di là degli scopi per cui sono state progettate e aprire involontariamente la strada a un attacco. Lo sviluppo dell'intelligenza artificiale generativa ha ingigantito questi rischi e ha agevolato la possibilità di sferrare attacchi più rapidi e sofisticati, automatizzando il rilevamento delle vulnerabilità e l'elusione delle limitazioni della velocità.

Fonte: [bleepingcomputer/Wallarm](#)

Please Review & Act on These Documents



Norton
Receipts & Invoice
[View More](#)

Norton
Internet Security
Powered by [docusign](#)

Please review the documents below.

[CONTINUE](#)

[OTHER ACTIONS](#)

Signature
 Initial
 Stamp
 Date Signed

Name
 First Name
 Last Name
 Email Address
 Company
 Title

- Comprehensive protection against viruses and malware
- Identity theft protection
- Performance optimization tools
- 24/7 customer support

DETAILS:

PRODUCT	TENURE	AMOUNT
Norton LifeLock 360	2 Users/1 Year	249.00 USD
	Activation Charges	49.00 USD
TOTAL		298.00 USD

POLICY:

We understand that circumstances can change and you may need to cancel your subscription. We

Difficoltà nel rilevamento degli abusi delle API

Durante le attività di rilevamento di un abuso delle API, i team addetti alla sicurezza incontrano grandi ostacoli, dovuti principalmente alla mancanza di uno standard di riferimento in grado di distinguere i comportamenti normali da quelli sospetti. Questo problema sottolinea che è assolutamente necessario monitorare il comportamento delle API in tempo reale, così da identificare le minacce e le anomalie in via preventiva.

Dal nostro [Studio sull'impatto della sicurezza API del 2024](#) emerge una tendenza preoccupante: solo il 13% delle organizzazioni che hanno partecipato al sondaggio eseguono un test quotidiano delle API, una percentuale in netto calo rispetto al 2023 (37%). Si tratta di un dato molto allarmante, se si considera lo scenario attuale delle minacce. La forte riduzione dei test quotidiani espone le organizzazioni a un aumento dei rischi per la sicurezza, in quanto limita notevolmente la capacità di rilevare e rispondere alle minacce in rapida evoluzione e lascia irrisolte le vulnerabilità più critiche per lungo tempo.

Le organizzazioni che eseguono frequentemente i test automatici durante i cicli di sviluppo sono in grado di identificare e risolvere i problemi tempestivamente ed evitare i costi legati alla mitigazione negli ambienti di produzione. In un'epoca in cui i metodi automatizzati e nascosti sono sempre più diffusi, l'esecuzione proattiva dei test svolge un ruolo cardine nella mitigazione dei rischi.

API non gestite: le tipologie ombra e zombie

La visibilità del patrimonio delle API, che comprende sia il monitoraggio delle API ufficiali che l'identificazione dei dati sensibili, costituisce tuttora un problema importante per le organizzazioni. Lo [Studio sull'impatto della sicurezza API 2024](#) ha posto in luce un divario significativo: il 47% dei team di AppSec, pur mantenendo un inventario completo, non è in grado di individuare le API che gestiscono i dati sensibili. Gli esperti della sicurezza si trovano ad affrontare questioni analoghe e segnalano lo stesso problema di supervisione nel 42% dei casi. Un dato allarmante è che il numero di imprese che posseggono inventari completi delle API e conoscono il livello di esposizione delle informazioni sensibili ha subito un calo drastico, passando dal 40% nel 2023 al 27% nel 2024. Il rapporto, inoltre, indica che le API ombra e zombie sono una delle cause principali alla base dei relativi incidenti di sicurezza.

Gli inventari incompleti non rilevano principalmente le API ombra e zombie. Le API zombie sono interfacce obsolete, vulnerabili ai vettori di attacco, che rimangono attive a causa di una rimozione incompleta, del turnover del personale o di altri motivi. Le API shadow, sviluppate come soluzioni rapide che non sono approvate mediante i processi standard, costituiscono una minaccia altrettanto pericolosa. [Una ricerca indica](#) che un terzo delle transazioni API dannose colpisce le API ombra.

Le misure di sicurezza tradizionali, come i WAF (Web Application Firewall), si dimostrano inefficaci contro queste minacce. Le organizzazioni necessitano di soluzioni avanzate per l'individuazione e il monitoraggio delle API, in grado di individuare con efficienza gli endpoint vulnerabili.

Un inventario completo delle API è il caposaldo di una strategia efficace per la sicurezza, in quanto consente alle organizzazioni di monitorare i modelli di utilizzo, tenere traccia della cronologia delle versioni, rilevare le vulnerabilità e rispettare i requisiti di conformità e normativi. Questo approccio strategico offre una chiara visibilità sull'infrastruttura digitale, che in ultima analisi può consolidare la gestione dei rischi e ottimizzare il livello di sicurezza generale dell'azienda.

Focus sulla sicurezza

Nel primo trimestre del 2025, abbiamo identificato un attacco sferrato contro un'azienda di e-commerce tramite l'abuso delle API. L'API in uso per l'invio di SMS non disponeva di un sistema di autenticazione adeguato. Per sfruttarla, i criminali hanno utilizzato oltre 200 indirizzi IP diversi, un singolo token di autenticazione e vari numeri di cellulare casuali (sia legittimi che falsi).

L'attacco ha messo in atto una strategia semplice ma efficace: ha registrato diversi numeri di cellulare e inviato messaggi SMS a quelli fraudolenti per sovraccaricare le attività dell'azienda e causare direttamente un danno finanziario. In seguito alla registrazione dei numeri di telefono, l'organizzazione colpita, che utilizza un servizio di gateway SMS a pagamento per semplificare lo scambio dei messaggi di testo fra le applicazioni e i dispositivi mobili, ha dovuto affrontare un costo imprevisto che poteva ripercuotersi sul brand e sulla reputazione aziendale. Una strategia di difesa approfondita, basata su misure di sicurezza a più livelli, può contrastare questo tipo di attacco e mitigare notevolmente i rischi associati.

I nostri avvisi hanno rivelato che i criminali, nel corso dell'attacco, hanno inviato 11.057 richieste POST e sono riusciti a ricevere 5.659 risposte (Figura 2).

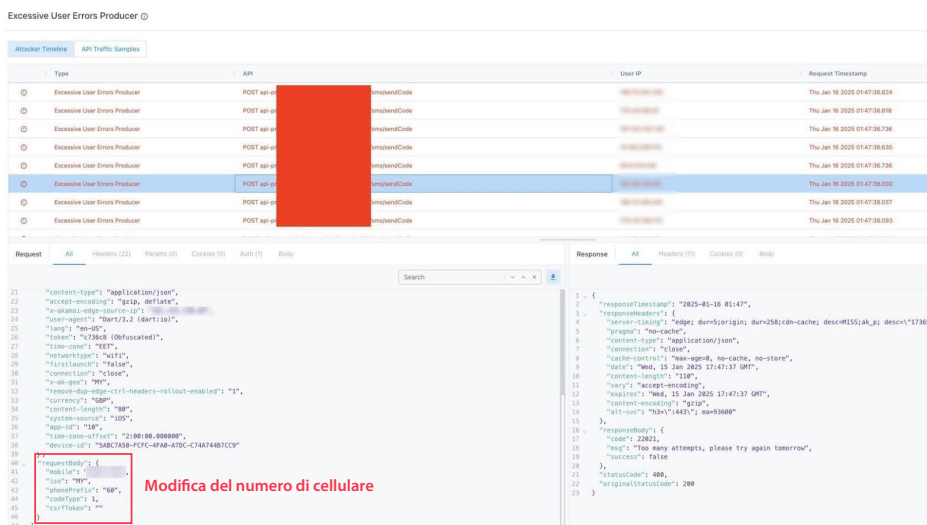


Fig. 2. I criminali inondano di richieste l'API non sicura

Le richieste automatizzate erano identiche, ad eccezione di un parametro fondamentale:

Body param **mobile**: the following pattern is detected - **<number>**

Tali richieste possono sovraccaricare il server, determinando una situazione di Denial-of-Service, oppure indicare l'esito positivo di un accesso non autorizzato all'API. I sistemi WAF (Web Application Firewall) tradizionali non sono in grado di individuare questi attacchi sofisticati. Tuttavia, le soluzioni avanzate per la sicurezza delle API, che creano uno standard di riferimento per i comportamenti normali, possono identificare tali attacchi tramite l'analisi del comportamento, mitigare i rischi in modo proattivo e impedire ai criminali di compiere danni più gravi.

Attacchi web: confronto e tendenze su base annua

Nel periodo esaminato (da gennaio 2023 a dicembre 2024), la ricerca di Akamai ha scoperto un notevole aumento degli attacchi web che hanno colpito le applicazioni web e le API (Figura 3). Il volume mensile degli attacchi è passato da quasi 14 miliardi all'inizio del 2023 a oltre 29 miliardi nell'ottobre 2024. Si tratta di un aumento del 65% dal primo trimestre del 2023 al quarto trimestre del 2024.

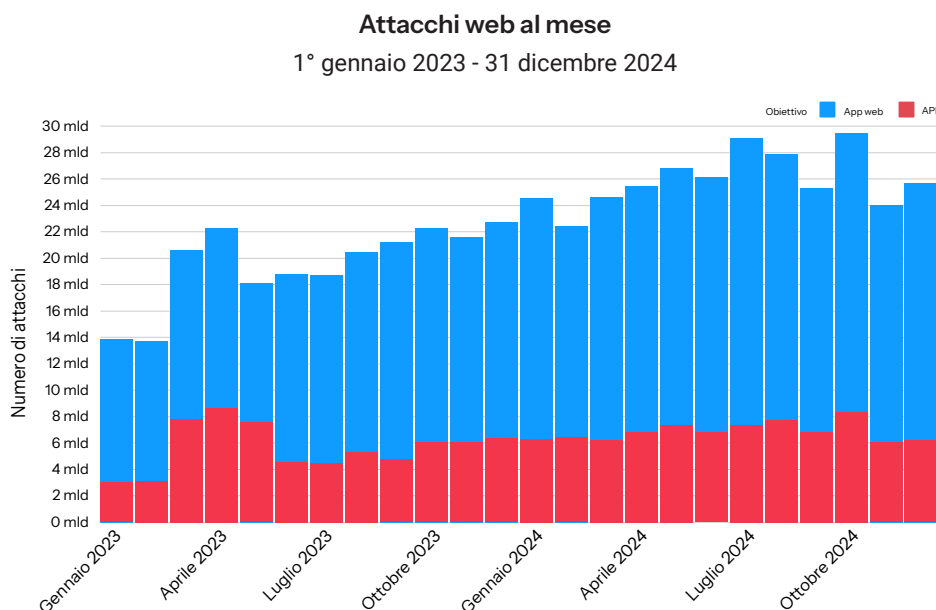


Fig. 3. Gli attacchi web tradizionali contro le API e le applicazioni web sono in costante aumento (+65% tra il primo trimestre del 2023 e il quarto trimestre del 2024)

Vettori principali: una combinazione di tecniche tradizionali e moderne basate sul comportamento

Gli esperti di cybersecurity che si occupano di proteggere le infrastrutture digitali da una varietà di minacce si trovano di fronte a una situazione sempre più complessa, caratterizzata sia dagli attacchi web tradizionali sia da tecniche moderne che sfruttano le configurazioni errate e le vulnerabilità intrinseche ai sistemi.

Violazione delle limitazioni delle richieste API: una minaccia in costante espansione

Da un'analisi completa degli endpoint API, che ha preso in considerazione un periodo di due anni, si evince come le violazioni delle limitazioni delle richieste API costituiscano una priorità per le organizzazioni (Figura 4). Queste violazioni si verificano quando le richieste o le risposte non rispettano i parametri predefiniti o i requisiti stabiliti, ad esempio quando superano i limiti di velocità o immettono dati non validi.

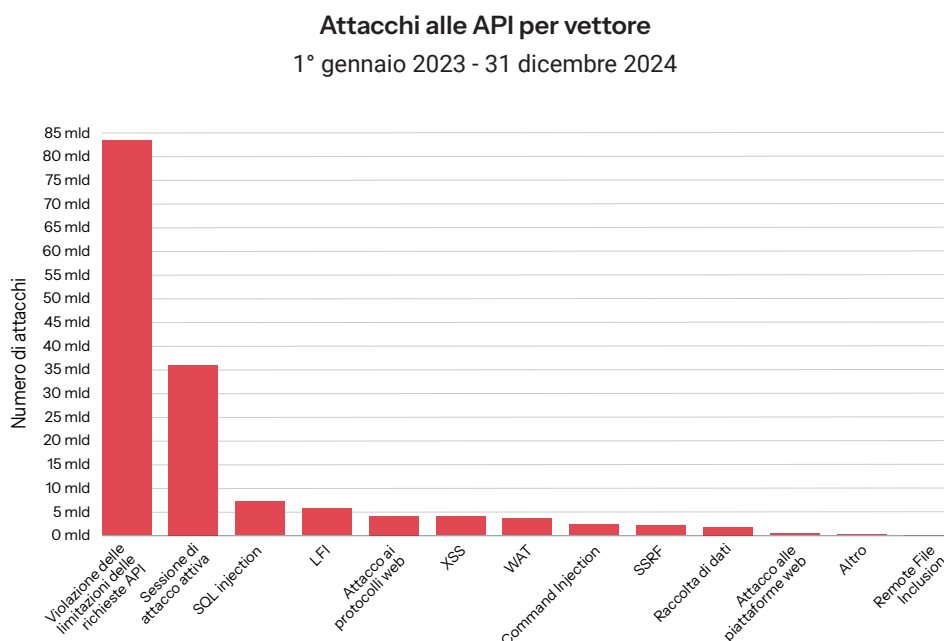


Fig. 4. Nell'arco di due anni sono stati rilevati oltre 83 miliardi di violazioni delle limitazioni delle richieste

Se si considera che, in due anni, si sono registrati oltre 83 miliardi di attacchi, la violazione delle limitazioni delle richieste API rappresenta una minaccia in costante crescita. Il brusco aumento di questo vettore (+24%) pone in evidenza i pericoli insiti nell'abuso delle API. La preponderanza di tali violazioni indica in modo eloquente la presenza di un abuso delle API, che può innescare a cascata una serie di effetti indesiderati, come il peggioramento delle performance di sistema, le interruzioni del servizio e una maggiore vulnerabilità agli attacchi mirati.

Sessioni di attacco attive: soluzioni creative per un problema unico nel suo genere

Le opzioni di sicurezza innovative integrate nelle soluzioni di Akamai consentono di contrastare i problemi peculiari degli attacchi specifici contro le API. Questi sistemi sono incentrati su un meccanismo proprietario che rileva le sessioni di attacco attive e funge da strumento strategico per la difesa. Sfruttando l'intelligence sulle minacce di Akamai, il sistema identifica e monitora i comportamenti sospetti e consente alle organizzazioni di neutralizzare le violazioni in via preventiva, prima che possano degenerare in un attacco su larga scala.

Inoltre, segnala i criminali informatici e integra funzionalità di "penalty box". Nel caso delle violazioni moderne, i malintenzionati fanno un uso prevalente dell'automazione per effettuare le attività ricognitive e sferrare gli attacchi. Akamai identifica rapidamente le sessioni di analisi delle vulnerabilità, interviene attraverso il blocco temporaneo del client e le contrassegna come sessioni di attacco attive. Questa strategia è un efficace deterrente per le attività criminali che puntano ad analizzare e sfruttare le vulnerabilità della rete.

Limitando le opportunità a disposizione dei malintenzionati, le organizzazioni possono migliorare notevolmente il livello di sicurezza delle API. Questo approccio offre una protezione efficace da un'ampia gamma di attacchi e ottimizza complessivamente la resilienza della cybersecurity.

Le informazioni in nostro possesso dimostrano quanto sia importante questa strategia. In una classifica generale, le sessioni di attacco attive si sono aggiudicate il primo posto come vettori diretti sia contro le app web che contro le API (Figura 5), per un totale di oltre 69 miliardi di violazioni nell'anno 2023. Nel 2024 sono aumentate a oltre 113 miliardi, con un incremento significativo pari al 63% su base annua.

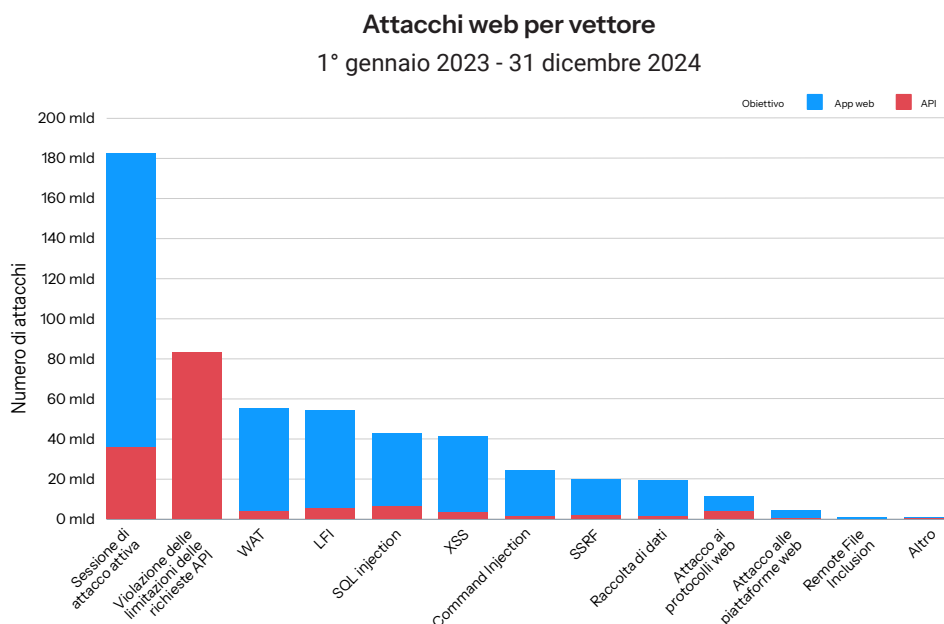


Fig. 5. Le sessioni di attacco attive si impongono su tutti gli altri vettori sia nel caso delle app web che nel caso delle API ed evidenziano come i criminali siano alla costante ricerca delle vulnerabilità presenti nelle reti delle organizzazioni

Perché è importante risolvere le vulnerabilità web tradizionali nelle infrastrutture moderne

Gli attacchi di tipo injection restano sempre molto efficaci, nonostante lo sviluppo di metodologie più sofisticate per le violazioni basate sul comportamento e la maggiore consapevolezza delle organizzazioni sulle vulnerabilità web tradizionali. I dati che abbiamo raccolto da gennaio 2023 a dicembre 2024 indicano un notevole aumento degli attacchi, con una crescita dei vettori SQLi (Structured Query Language Injection) e Command Injection rispettivamente pari al 60% e al 34% su base annua. Attraverso queste vulnerabilità, i criminali possono eseguire comandi non autorizzati, compromettere l'integrità del sistema e accedere ai dati sensibili che non sono protetti da adeguati sistemi di autenticazione, acquisendo un ruolo sempre più importante nel settore della cybersecurity.

La persistenza degli attacchi contro i database SQL, famosi perché consentono uno storage affidabile e scalabile dei dati, deriva paradossalmente dalla loro progressiva diffusione. In particolare, i [quattro database più utilizzati](#) dispongono di un'architettura basata su SQL, il che sottolinea la pericolosità di questo vettore di attacco.

Sebbene l'elenco OWASP delle 10 principali vulnerabilità per la sicurezza delle API sia stato oggetto di revisione (la versione aggiornata del 2023 ha sostituito gli attacchi di tipo injection con gli errori di configurazione del sistema di sicurezza), la pericolosità degli attacchi di tipo injection resta invariata. Allo stesso tempo, il volume di altri vettori consolidati, come LFI (Local file Inclusion) e XSS (Cross-Site Scripting), continua a mantenersi elevato. Sulla base dei dati relativi agli attacchi reali sferrati nel 2024, Akamai ha preparato la [Guida 2025 per gli addetti alla sicurezza](#), che descrive il livello sofisticato raggiunto dalle tecniche di sfruttamento delle vulnerabilità XSS, come l'inserimento di risorse remote, il furto dei cookie, il defacing dei siti web e le violazioni XSRF (Session Riding).

I risultati raggiunti evidenziano come sia prioritario implementare strategie di difesa multilivello. Per contrastare con efficacia questi attacchi sempre più complessi, gli esperti di cybersecurity devono fare ricorso a un insieme di strumenti che comprendano una codifica appropriata dell'output, policy affidabili per la sicurezza dei contenuti e opzioni WAF avanzate.

Attacchi DDoS al livello 7: confronto e tendenze su base annua

Da gennaio 2023 a dicembre 2024, la ricerca di Akamai ha documentato un drastico incremento degli attacchi DDoS al livello 7 (a livello di applicazione) contro le API e le applicazioni web (Figura 6). Il volume mensile è aumentato da una cifra appena superiore ai 500 miliardi nei primi mesi del 2023 a oltre 1,1 migliaia di miliardi nel dicembre 2024 (+94%).

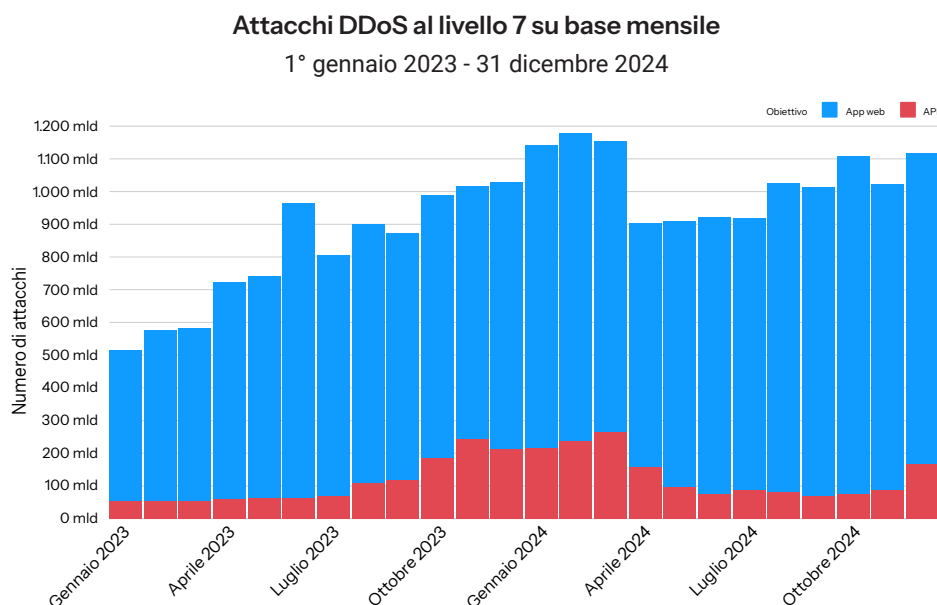


Fig. 6. Il numero di attacchi DDoS al livello 7 contro le API e le applicazioni web è in costante aumento, pari al 94% tra il primo trimestre del 2023 e il quarto trimestre del 2024

Attacchi DDoS al livello 7 contro app e API

Le violazioni [HTTP flood](#) restano il principale vettore in un contesto di progressivo sviluppo degli attacchi DDoS al livello 7 contro gli endpoint delle API e delle applicazioni web. In questo caso, la tecnica utilizzata consiste nell'inondare le API con volumi elevati di richieste, in apparenza legittime, dirette alle operazioni che richiedono un consumo ingente di risorse. Gli interventi di rilevamento e mitigazione sono resi più complicati dal fatto che i criminali hanno perfezionato la tecnica degli attacchi DDoS al livello 7, modificati in modo da sfruttare vulnerabilità specifiche presenti nelle API o nella logica delle applicazioni web. Anche gli attacchi basati sui bot hanno raggiunto un grado di avanzamento elevato, che consente di generare modelli di traffico molto simili a quelli di un uso legittimo delle API.

L'impulso offerto agli hacker dall'intelligenza artificiale: percorsi di attacco manuali e automatici contro le API

L'adozione diffusa e l'applicazione pratica delle API è stata favorita dalle tecnologie basate sull'AI generativa, che ha rivoluzionato le operazioni di integrazione aziendale attraverso l'utilizzo di queste interfacce. Le previsioni indicano che il mercato delle API basate sull'AI conoscerà una [crescita esplosiva](#), passando da \$ 44,41 miliardi nel 2025 a \$ 179,14 miliardi (in dollari statunitensi) entro il 2030, con un tasso annuo composto del 32,2%. Tuttavia, la proliferazione dei sistemi di intelligenza artificiale ha coinciso con un incremento marcato degli [attacchi basati sull'AI contro le API](#). La visibilità delle vulnerabilità delle API deriva in larga parte dalla strategia scelta dai criminali, che impiegano l'intelligenza artificiale per eseguire operazioni, sia manuali che automatiche, di analisi e sfruttamento.

Strategie di attacco contro le API basate sull'AI

-  **Attacchi mirati:** i criminali si avvalgono degli strumenti AI per identificare e analizzare componenti specifici delle API e sferrano attacchi mirati contro specifiche vulnerabilità mediante un [codice dannoso generato dall'intelligenza artificiale](#). In questo modo, le violazioni dirette contro i punti deboli delle API vengono eseguite in modo più preciso ed efficace.
-  **Attacchi automatizzati:** l'automazione degli attacchi consente ai criminali informatici di identificare e sfruttare rapidamente le vulnerabilità nella sicurezza delle API, con un risparmio notevole di tempo e impegno. In questo caso sono impiegati [bot basati sull'intelligenza artificiale](#), che rappresentano un grave pericolo sia per le aziende che per i singoli individui.
-  **Attacchi volumetrici:** l'intelligenza artificiale viene utilizzata come un'arma per sovraccaricare di traffico le API e inondare i sistemi di sicurezza con una velocità elevata e un volume ingente di traffico. Un esempio di questa strategia sono gli [attacchi DDoS automatizzati](#), durante i quali i bot basati sull'AI sferrano attacchi continui e si adattano dinamicamente alle misure di difesa.
-  **Attacchi basati sul comportamento:** attraverso l'analisi dei modelli di traffico, l'intelligenza artificiale genera [attacchi ad attività bassa e lenta](#), che agiscono al di sotto delle normali soglie di avviso e riescono quindi a eludere il rilevamento. Questi attacchi spesso prendono di mira le vulnerabilità più comuni delle API, tra cui le tipologie BOLA e Broken Authentication.

Il paradosso delle API basate sull'IA

La contraddizione insita nelle API basate sull'intelligenza artificiale è che si sono dimostrate molto pericolose. Le [API basate sull'AI](#) sono accessibili dall'esterno e buona parte di esse dipende da sistemi di autenticazione non adeguati, che le rendono più vulnerabili agli attacchi. Come rivela il nostro [Studio sull'impatto della sicurezza delle API 2024](#), la causa principale degli incidenti segnalati dai team addetti alla sicurezza nei settori del retail e dell'e-commerce è da rintracciare nella presenza di API all'interno degli strumenti di AI generativa.

Il panorama in evoluzione delle minacce basate sull'AI

I progressi dell'intelligenza artificiale hanno svolto un ruolo significativo per l'evoluzione del panorama delle minacce legate alle API. Nel corso dell'anno precedente, si è registrato un [aumento record](#) delle vulnerabilità associate alle API che si basano sull'intelligenza artificiale. Secondo l'agenzia federale statunitense U.S. Cybersecurity and Infrastructure Security Agency, la maggior parte delle [vulnerabilità sfruttate](#) dagli attacchi è stata per la prima volta correlata alle API.

Attacchi alle applicazioni web basate sull'AI e strategie di difesa

L'intelligenza artificiale ha avuto un impatto considerevole sulla sicurezza delle applicazioni web: se da un lato ha consentito di sviluppare funzionalità di difesa innovative, dall'altro ha prodotto nuovi vettori di attacco. I malware ottimizzati per l'intelligenza artificiale, l'analisi delle vulnerabilità basata sull'AI, gli attacchi ai sistemi che adottano l'intelligenza artificiale, le strategie avanzate di web scraping e la violazione delle soluzioni WAF basate sull'IA sono alcuni dei principali fattori che hanno profondamente modificato il panorama della cybersecurity per le applicazioni web.

Malware ottimizzato per l'intelligenza artificiale

Come hanno osservato gli esperti di cybersecurity, alcuni malware sofisticati sfruttano l'intelligenza artificiale per colpire le applicazioni web. In una campagna e-mail che ha interessato gli utenti francesi nel 2024, i criminali hanno fatto ricorso a un codice dannoso, probabilmente progettato con l'ausilio dell'AI generativa, per eseguire il [malware AsyncRAT](#). Questo episodio mette in evidenza come la creazione e l'implementazione di malware attraverso l'intelligenza artificiale costituisca una tendenza in costante aumento, che pone nuovi problemi agli addetti alla sicurezza delle applicazioni web.

Analisi delle vulnerabilità basata sull'AI

L'intelligenza artificiale ha comportato una rivoluzione per l'[analisi delle vulnerabilità](#) associate alle applicazioni web, offrendo funzionalità che possono essere utilizzate sia per scopi difensivi che offensivi. Questi strumenti rendono automatica la ricerca delle vulnerabilità più diffuse, tra cui SQLi, XSS, CSRF (Cross-Site Request Forgery) e SSRF (Server-Side Request Forgery), effettuano un'analisi delle possibili conseguenze e offrono suggerimenti utili per le procedure di risoluzione.

Attacchi ai sistemi che integrano l'intelligenza artificiale

L'integrazione dell'AI nelle applicazioni web, soprattutto i modelli LLM (modelli linguistici di grandi dimensioni) ha generato una serie di [nuove vulnerabilità per la sicurezza](#). Passiamole brevemente in rassegna. Gli *attacchi di tipo injection dei prompt* puntano a superare le misure di difesa dei modelli per colpire i sistemi basati sull'AI. Un esempio rilevante è offerto da una [vulnerabilità di Slack](#), alla quale è stato nel frattempo posto rimedio, che ha consentito la raccolta di dati da canali privati tramite un attacco indiretto di prompt injection. Gli *attacchi di data poisoning* manipolano una percentuale ridotta di dataset per danneggiare il comportamento dei modelli di intelligenza artificiale e pertanto possono compromettere l'integrità dei sistemi. Le *tecniche di jailbreaking* consentono ai criminali di aggirare le limitazioni, estrarre dati sensibili e generare output dannosi attraverso il bypass dei sistemi di protezione dei modelli LLM. Questi nuovi vettori di attacco richiedono una vigilanza più approfondita e strategie di difesa innovative.

Web scraping di livello avanzato

L'ottimizzazione degli strumenti di web scraping attraverso l'intelligenza artificiale rappresenta un altro problema per la sicurezza delle applicazioni web. Questi strumenti migliorano l'efficienza dei metodi di estrazione dei dati e la capacità di eludere le misure difensive. Dal 2020 il [web scraping di livello avanzato](#) si avvale dell'AI per l'elaborazione dei dati, ma nell'ultimo periodo gli attacchi contro i modelli LLM sono diventati molto più frequenti. Questo fenomeno è dovuto in buona parte all'aumento dell'esecuzione di query basate sugli agenti, che rende necessario l'impiego di fonti di dati in tempo reale (non statiche).

Purtroppo, ciò ha determinato una crescita del costo unitario delle richieste di applicazioni web, che può variare da un minimo di \$ 0,01 a un massimo di \$ 0,50 (in dollari statunitensi), a seconda di fattori quali la complessità della richiesta, l'infrastruttura di hosting e così via. Se in origine il settore più colpito dalla crescita dello scraping dei modelli LLM era quello del commercio, la situazione è mutata radicalmente e altri settori, come quello dei servizi finanziari, del gioco d'azzardo, dei contenuti multimediali digitali e video, si trovano a sostenere il peso enorme di questo cambiamento.

Sistemi WAF basati sull'AI

Il lato positivo è che l'intelligenza artificiale consente ai sistemi WAF più avanzati di identificare e mitigare con maggiore efficacia un'ampia varietà di minacce informatiche, compresi i bot, gli attacchi DDoS, gli scraper e gli scanner. I [sistemi WAF basati sull'AI](#) sono utili per contrastare gli attacchi informatici più sofisticati, dal momento che i corrispettivi tradizionali, dotati di set di regole statici, incontrano difficoltà nel gestire le minacce zero-day e richiedono aggiornamenti manuali.

La strategia di apprendimento automatico multilivello consente il riconoscimento degli schemi, l'apprendimento adattivo, il rilevamento delle anomalie e il miglioramento dei tempi di risposta. L'addestramento eseguito sfruttando miliardi di eventi quotidiani e l'implementazione di un approccio multilivello con un monitoraggio continuo permette ai sistemi WAF basati sull'AI di prevenire proattivamente le minacce in continua evoluzione e di assicurare la protezione dei clienti.

Tendenze per settore

Se si considera il periodo compreso tra il primo trimestre del 2023 e il quarto trimestre del 2024 (Figura 7), il commercio spicca sopra tutti gli altri settori, con un volume complessivo di attacchi web quasi tre volte superiore a quello dell'high-tech (situato al secondo posto). Inoltre, il numero di violazioni segnalate contro le API supera enormemente il volume registrato negli altri nove settori.

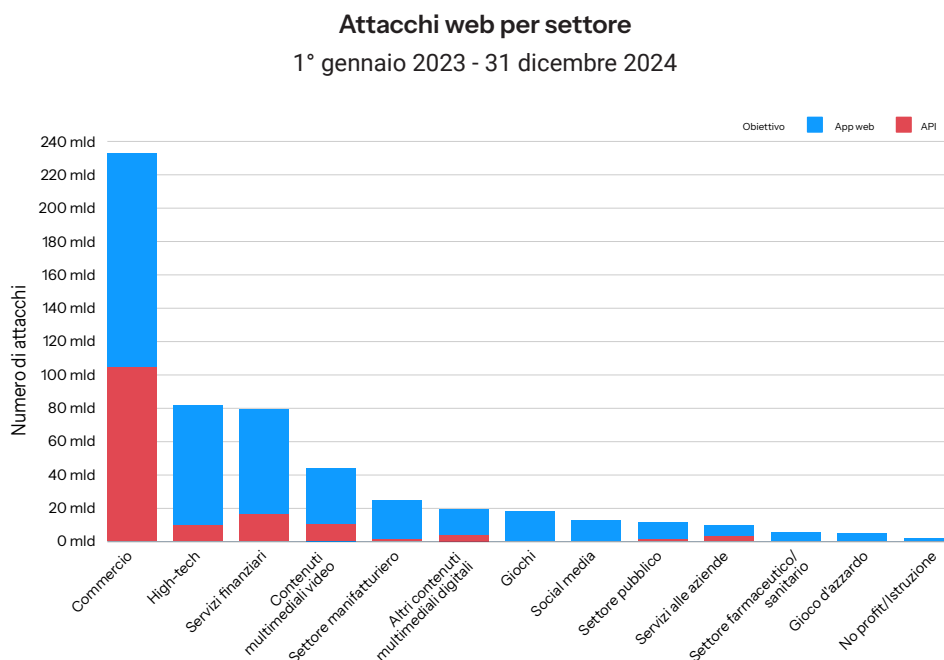


Fig. 7. I settori più colpiti dagli attacchi web sono stati quelli del commercio, dell'high-tech e dei servizi finanziari

Per quanto riguarda gli attacchi DDoS al livello 7 (a livello di applicazione), l'high-tech è stato colpito più degli altri settori, con un numero di violazioni che ha oltrepassato i 7 migliaia di miliardi. I social media e il commercio seguono con una cifra inferiore (Figura 8). Tuttavia, nello stesso arco di tempo, il volume di attacchi DDoS al livello 7 contro le API delle organizzazioni commerciali ha nuovamente superato in modo significativo quello di tutti gli altri settori.

Attacchi DDoS al livello 7 per settore

1° gennaio 2023 - 31 dicembre 2024

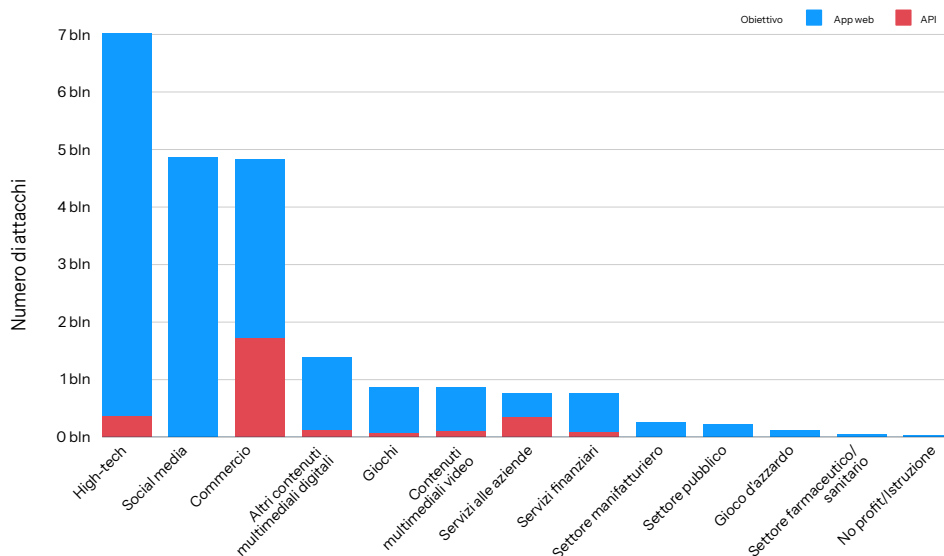


Fig. 8. Attacchi DDoS al livello 7 per settore

Commercio

Oltre ad aver subito più di 230 miliardi di attacchi web (oltre il 40% del totale), il settore del commercio ha dovuto gestire un incremento senza precedenti degli attacchi DDoS al livello 7, pari a oltre 4,8 migliaia di miliardi secondo i dati di Akamai.

Questo volume combinato rende evidente la strategia dei modelli di attacco, che colpiscono le applicazioni web nel 64,25% dei casi e le API nel restante 35,75%. Da questa distribuzione si evince quali sono i due vettori di attacco che i criminali utilizzano per compromettere le piattaforme commerciali ed emerge come l'attuale scenario delle minacce abbia un carattere multifaccettato.

Le aziende del settore sono un bersaglio molto remunerativo, perché concentrano nei loro sistemi le informazioni sensibili dei clienti, i dati relativi ai pagamenti e le transazioni finanziarie. Il furto delle credenziali per i pagamenti, la compromissione degli account dei clienti e la sottrazione delle PII offrono un percorso diretto verso la monetizzazione degli attacchi e rendono più allettante il settore dal punto di vista finanziario. A differenza di altri settori, nei quali sono necessari ulteriori passaggi per ottenere un vantaggio economico dalla compromissione dei dati, spesso le piattaforme commerciali includono risorse a disposizione diretta dei criminali.

Il settore retail come obiettivo principale

Nel più ampio settore del commercio, il comparto retail è quello maggiormente preso di mira con un volume di attacchi sproporzionato, in quanto presenta caratteristiche peculiari.

In genere, le operazioni retail si basano su ecosistemi digitali complessi, che integrano diversi sistemi e piattaforme. Le aziende del segmento portano avanti la trasformazione digitale attraverso un approccio aggressivo e danno precedenza al time-to-market a discapito della sicurezza globale, creando lacune nei sistemi di sicurezza. L'adozione delle strategie omnicanale rende inavvertitamente più variegata la superficie di attacco, mentre il ricorso esteso ai fornitori di terze parti crea una supply chain complessa, con molti punti deboli esposti a potenziali compromissioni.

I modelli di traffico cambiano da stagione a stagione e pertanto è possibile prevedere i momenti dell'anno caratterizzati da un volume elevato di transazioni. I criminali puntano soprattutto su questi periodi, con un aumento degli attacchi che oscilla tra **il 25% e il 30%** durante le festività natalizie, come rivela l'Internet Crime Complaint Center dell'FBI. Le minacce colpiscono con maggiore frequenza anche le piattaforme di e-commerce che, nel mese di dicembre, riscontrano un incremento degli attacchi informatici pari al **31%** rispetto alla media annuale.

L'evoluzione degli attacchi alle applicazioni web

Nell'ambito delle applicazioni web si assiste a una trasformazione importante degli attacchi, favorita dalle innovazioni tecnologiche e dal cambiamento delle metodologie impiegate dai criminali. Le tecniche dei cybercriminali sono sempre più sofisticate: puntano a sfruttare le vulnerabilità delle applicazioni web e adattano la propria strategia in modo da eludere le misure di sicurezza, anch'esse in evoluzione. L'aumento degli strumenti di attacco automatizzati, insieme all'integrazione degli algoritmi di apprendimento automatico, ha consentito di lanciare campagne più precise e mirate contro le applicazioni web dei retailer.

In aggiunta, l'adozione delle architetture di microservizi e lo sviluppo di soluzioni basate sulle API ha esteso la superficie di attacco, rendendo necessario rivalutare i paradigmi di sicurezza tradizionali. Questa evoluzione richiede un approccio proattivo da parte degli esperti di cybersecurity e mette in risalto l'importanza di un monitoraggio continuo, dei meccanismi di difesa adattivi e di una profonda conoscenza dei vettori di attacco che si stanno imponendo sullo scenario delle applicazioni web.

Il panorama delle minacce basate sui bot

Grazie alle innovazioni tecnologiche, lo scenario delle minacce basate sui bot sta cambiando rapidamente, soprattutto per l'impiego, da parte dei malintenzionati, delle funzionalità offerte dall'AI generativa. Questa evoluzione ha ottimizzato le strategie di attacco, includendo rapidi exploit zero-day e tecniche di elusione avanzate che aggirano le difese tradizionali. Alcuni dati confermano che le frodi di bot basate sull'AI ai danni dei retailer **sono aumentate** costantemente tra agosto 2022 e aprile 2024, raggiungendo un picco straordinario (+137%) nel gennaio 2024. I problemi di rilevamento rendono ancora più pericolose queste minacce: le aziende impiegano generalmente quattro mesi per individuare gli attacchi basati sui bot e nel frattempo subiscono danni finanziari e di immagine.

I bot sono diventati un vettore fondamentale delle minacce nel settore retail, in quanto semplificano il controllo degli account, le frodi legate alle carte di credito e l'abuso di buoni regalo. Attraverso i bot, i criminali possono lanciare campagne di attacchi più vaste, che sfruttano i dati sottratti da un sito compromesso per eseguire il credential stuffing contro altre vittime. Ciò innesca un effetto a catena negli ecosistemi del settore retail. Le frodi online stanno quindi conoscendo un processo di "industrializzazione", in quanto gli strumenti automatizzati permettono alle organizzazioni criminali a livello globale di ampliare le proprie attività ben oltre ciò che era possibile fare con i metodi manuali.

Per un elenco di suggerimenti su come migliorare la protezione delle API e delle applicazioni web nel settore retail dagli attacchi legati ai bot e all'AI, passate alla sezione [Mitigazione](#).

Servizi finanziari

Il settore dei servizi finanziari è diventato il principale obiettivo degli attacchi web e continua a subire attacchi DDoS al livello 7. Tra gennaio 2023 e dicembre 2024, i primi hanno raggiunto una cifra totale di 79 miliardi, mentre i secondi sono arrivati a superare i 761 miliardi sia nel caso delle applicazioni web che delle API.

Si tratta di un volume senza precedenti, che evidenzia la vulnerabilità del settore e la sua appetibilità per i criminali. Questo incremento è dovuto a una serie di fattori, tra cui il ruolo fondamentale dei servizi finanziari per l'infrastruttura economica globale, il valore elevato delle informazioni finanziarie e il rischio che si verifichino gravi [interruzioni](#) dei servizi.

La digitalizzazione dei servizi finanziari

I servizi finanziari digitalizzati hanno ampliato la superficie di attacco a disposizione dei criminali informatici. L'adozione di sistemi personalizzati basati sull'AI, dei modelli BaaS (Banking-as-a-Service) e di soluzioni finanziarie integrate hanno fatto emergere nuove vulnerabilità, mentre i conflitti geopolitici, in particolare la guerra tra Russia e Ucraina, hanno favorito le attività degli hacktivisti [mirate](#) agli istituti finanziari. L'[interesse](#) dei criminali nei confronti del settore è cresciuto anche per una serie di fattori economici, come la diffusione delle criptovalute e la possibilità di creare riserve di valute digitali.

Gli attacchi alle applicazioni web sono in rapida trasformazione e si stanno adattando alle nuove tecnologie per sfruttare le vulnerabilità emergenti. I criminali oggi impiegano algoritmi sofisticati di intelligenza artificiale e apprendimento automatico per eludere i sistemi di sicurezza tradizionali e sferrare attacchi continui e più mirati. L'aumento dei microservizi e delle architetture senza server ha dato origine a nuovi vettori di attacco, mentre l'impiego crescente delle API ha aumentato i potenziali punti di accesso a disposizione dei malintenzionati. Inoltre, l'adozione delle applicazioni mobili e basate su cloud ha costretto a rivalutare le strategie di sicurezza, dal momento che queste piattaforme presentano problemi peculiari in termini di controllo degli accessi e di protezione dei dati.

La prevalenza del comparto bancario tra gli obiettivi di attacco

Nel settore dei servizi finanziari, il segmento bancario si distingue come obiettivo principale degli attacchi web (Figura 9). Analogamente a quanto avviene nel settore del commercio, il [credential stuffing](#) sta diventando uno dei principali vettori di attacco contro gli istituti bancari.

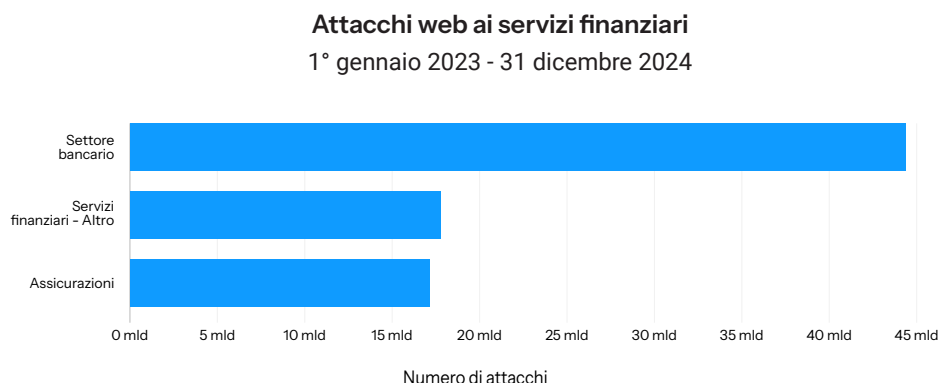


Fig. 9. Il comparto bancario è il segmento più colpito dagli attacchi web ai servizi finanziari

La grande diffusione dei servizi di online banking, unita alle criticità insite nell'accesso agli account, è una fonte di attrattiva per i criminali informatici, che sono incentivati dai vantaggi economici derivanti dagli attacchi in caso di successo. Infatti, per ottenere enormi guadagni, è sufficiente compromettere un numero esiguo di account. La vulnerabilità del comparto è stata involontariamente [aggravata](#) dalla resistenza delle aziende all'impiego di sistemi di sicurezza più restrittivi, come l'autenticazione multifattore, che potrebbero incidere sulla user experience.

Altri fattori complicano ulteriormente la posizione del segmento bancario. Il downtime è un evento sensibile che espone al rischio di estorsioni, in quanto i cybercriminali fanno leva sulle [preoccupazioni](#) delle aziende in merito all'interruzione dei servizi. Inoltre, la progressiva evoluzione delle tecniche di attacco, come l'uso dell'intelligenza artificiale e dell'apprendimento automatico per eludere le attività di rilevamento, pone enormi [problemi](#) per i meccanismi di difesa tradizionali. Il contesto normativo, che prevede criteri di conformità rigorosi e cospicue sanzioni in seguito a una violazione della sicurezza, rende ancora più intricato lo scenario della cybersecurity in questo segmento.

High-tech

L'high-tech resta uno dei settori maggiormente presi di mira dagli attacchi web e DDoS al livello 7. Ai fini del nostro rapporto, abbiamo preso in considerazione i comparti delle telecomunicazioni e quello delle soluzioni hardware e software, rivolte sia alle imprese che ai consumatori. Secondo i dati di Akamai, l'high-tech è secondo soltanto al commercio per il volume complessivo di attacchi web, che hanno superato la cifra di 81,7 miliardi nel biennio 2023 - 2024. Inoltre, si situa al primo posto per il numero di attacchi DDoS al livello 7, che hanno superato la cifra di 7 migliaia di miliardi.

I contenuti dinamici e le query complesse dei database, che trovano largo impiego nelle applicazioni web dell'high-tech, generano vulnerabilità che i criminali sfruttano per [semplificare il sovraccarico dei server](#) e concorrono all'elevata percentuale di attacchi DDoS al livello 7 riscontrati nel settore. In particolare, le [reti blockchain](#), pur disponendo di un'architettura decentralizzata, hanno registrato un incremento elevato degli attacchi DDoS, sferrati da cybercriminali che impiegano tecniche come le transazioni spam e l'HTTP flood per bloccare le transazioni legittime. I downtime operativi hanno conseguenze economiche importanti per il settore dell'high-tech e questa circostanza incentiva i criminali a sferrare attacchi DDoS in grado di rendere inutilizzabili i servizi essenziali. La dipendenza dalle architetture incentrate sulle API per lo sviluppo moderno dei software rappresenta un elemento di rischio aggiuntivo, in quanto i criminali sfruttano gli endpoint dotati di codice non sicuro per effettuare attacchi HTTP flood.

La situazione è analoga nel comparto delle telecomunicazioni

Il segmento delle telecomunicazioni, che è interessato da un elevato numero di attacchi alle API, deve far fronte a problemi analoghi per la cybersecurity. Le minacce alle API e alle applicazioni web spaziano dalla violazione dei dati agli attacchi DDoS e agli exploit dei punti deboli presenti nella supply chain. Diverse violazioni dei dati di alto profilo sono state causate proprio da queste vulnerabilità.

Nel gennaio 2025, per esempio, si è scoperto che un'[importante rete di telecomunicazione](#) impiegava delle API altamente vulnerabili, che hanno esposto 3.000 aziende a gravi rischi per la sicurezza. L'indagine ha messo in luce ingenti lacune nelle soluzioni di sicurezza, tra cui una procedura inadeguata per le verifiche KYC (Know Your Customer) e una falla nelle API di back-end, che rendeva vulnerabile l'organizzazione ad attacchi path traversal e concedeva l'accesso ai sistemi interni.

L'IoT (Internet of Things) dà origine a nuovi vettori di attacco

Il settore dell'high-tech non riesce a restare al passo con l'evoluzione delle vulnerabilità presenti nelle API e nelle applicazioni web, per via dei rapidi progressi tecnologici che caratterizzano la nostra epoca. In questo contesto, l'adozione diffusa dei dispositivi IoT, molti dei quali non dispongono di sistemi difensivi efficaci, apre la strada a nuovi vettori di attacco. L'adozione a ritmo sostenuto delle infrastrutture multicloud spesso comporta una configurazione inadeguata degli ambienti e la creazione di punti di ingresso che possono essere sfruttati dai criminali.

I sistemi cloud e i dispositivi IoT che vengono sviluppati senza prestare attenzione alla sicurezza stanno diventando l'obiettivo privilegiato degli [attacchi basati sull'AI](#). Le [piattaforme SaaS](#) sono dotate di un'estesa superficie di attacco e corrono un rischio maggiore di subire attacchi contro le API. Una situazione analoga caratterizza il settore dell'high-tech, dove la proliferazione delle soluzioni di intelligenza artificiale e la maggiore dipendenza dalle piattaforme SaaS di terze parti hanno ampliato significativamente la superficie di attacco complessiva delle API. Con la progressiva adozione di queste tecnologie, le organizzazioni sono sempre più esposte ai pericoli informatici e possono proteggersi soltanto con un attento monitoraggio e con l'introduzione di soluzioni affidabili per la sicurezza.

Tendenze per area geografica

NOTA: il formato del rapporto sulle aree geografiche è stato modificato in modo da rendere più fruibili i dati per i lettori e offrire una panoramica immediata delle tendenze in ogni regione: N. America (Nord America), APJ (Asia-Pacifico e Giappone), EMEA (Europa, Medio Oriente e Africa) e LATAM (America Latina). La Figura 10 riporta un grafico che riassume a colpo d'occhio le informazioni discusse in questa sezione.

Dati attacchi web

Dati attacchi DDoS al livello 7

Area geografica	Numero di attacchi web	Numero di attacchi DDoS al livello 7	Principali attacchi web Vettori	Principali obiettivi per area	Principali obiettivi per settore
APJ	80 mld, il 14% contro le API	7,4 bln, il 6% contro le API	Sessione di attacco attiva, LFI, XSS	Australia (20,3 bln), India (17,3 bln), Singapore (15,9 bln)	Servizi finanziari, commercio, social media
				Singapore (4,7 bln), India (607 bln), Corea del Sud (283 mld)	Social media, altri contenuti multimediali digitali, commercio
EMEA	116 mld, il 37% contro le API	2,6 bln, il 20% contro le API	Sessione di attacco attiva, violazione delle limitazioni delle richieste API, LFI	Regno Unito (30,3 mld), Paesi Bassi (19,5 mld), Spagna (14,2 mld), Germania (12,8 mld)	Commercio, contenuti multimediali video, servizi finanziari
				Germania (569 mld), Regno Unito (506 mld)	Commercio, altri contenuti multimediali digitali, contenuti multimediali video
LATAM	3 mld, il 12% contro le API	258 mld, il 18% contro le API	Sessione di attacco attiva, WAT, SSRF	Brasile (19,3 mld), Messico (2 mld)	Commercio, servizi finanziari
				Brasile (175 mld), Messico (39 mld)	Commercio, servizi finanziari
N. America	327 mld, il 29% contro le API	11,9 bln, il 16% contro le API			

Fig. 10. Panoramica sulle aree geografiche, gennaio 2023–dicembre 2024. LFI è l'acronimo di Local File Inclusion, XSS di Cross-Site Scripting, WAT di Web Attack Tool e SSRF di Server-Side Request Forgery



Due tendenze negli attacchi contro le API e le applicazioni

Akamai ha messo a confronto gli attacchi alle applicazioni web e alle API e gli attacchi DDoS al livello 7 che hanno interessato le diverse aree geografiche nell'arco di 24 mesi, da gennaio 2023 a dicembre 2024, e ha rilevato due tendenze prevalenti (Figure 11).

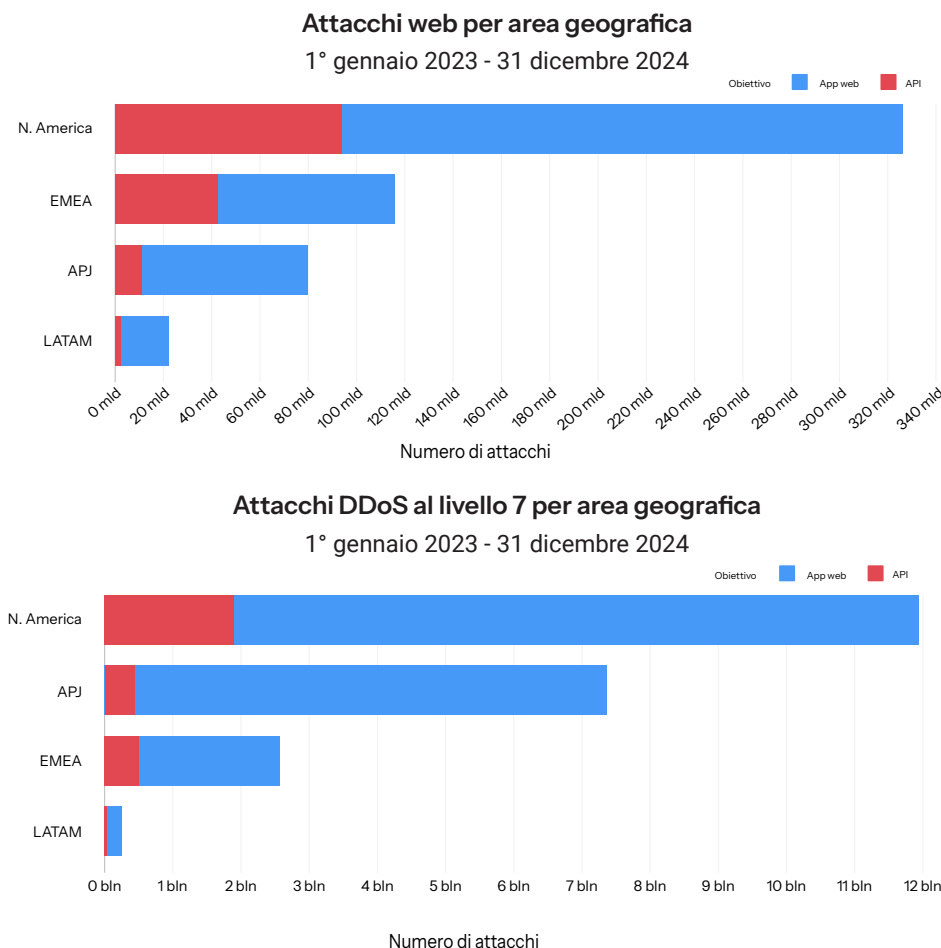


Fig. 11. A livello globale, durante il biennio esaminato, l'area EMEA ha registrato la più alta percentuale di attacchi alle API, mentre l'area APJ è seconda per il numero più elevato di attacchi DDoS al livello 7

Primo trend: gli attacchi alle API si sono verificati in modo diffuso nell'area EMEA. Tra le possibili cause, rientrano il [tasso elevato di adozione delle API, superiore a quello delle altre aree geografiche](#), il ricorso alle soluzioni di open banking e lo standard [PCI DSS v 4.0](#), che promuovono un maggiore utilizzo delle API e possono quindi comportare rischi per la sicurezza. Per un esame approfondito sui rischi specifici legati alle API, consultate la sezione [Sviluppo dell'intelligence di Akamai sulle minacce informatiche](#).

Nell'area EMEA prosegue la tendenza che abbiamo [osservato nel 2023](#). Durante il periodo analizzato, è stata rilevata la massima concentrazione di attacchi web contro le API: su un totale di 116 miliardi di attacchi web, il 37% ha preso di mira le API. Al contrario, nel Nord America si è registrato un volume complessivo di 327 miliardi di attacchi web, che hanno colpito le API nel 29% dei casi. L'area APJ si è posizionata subito dopo con 80 miliardi di attacchi web, il 14% dei quali è stato sferrato contro le API, mentre nell'area LATAM la percentuale è stata più bassa e si è attestata al 12% su 3 miliardi di attacchi web.

Inoltre, la regione EMEA ha avuto la più alta concentrazione di attacchi DDoS al livello 7 contro le API (20%), seguita dall'area LATAM (18%), dal Nord America (16%) e dall'area APJ (6%). In generale, questo tipo di violazione ha interessato una percentuale relativamente piccola sul totale degli attacchi web rilevati in ogni regione. Secondo le nostre previsioni, le percentuali aumenteranno nel tempo per diversi motivi, come lo sviluppo di attacchi più sofisticati basati sui bot e l'aumento degli attacchi basati sull'AI che sfruttano le vulnerabilità delle API.

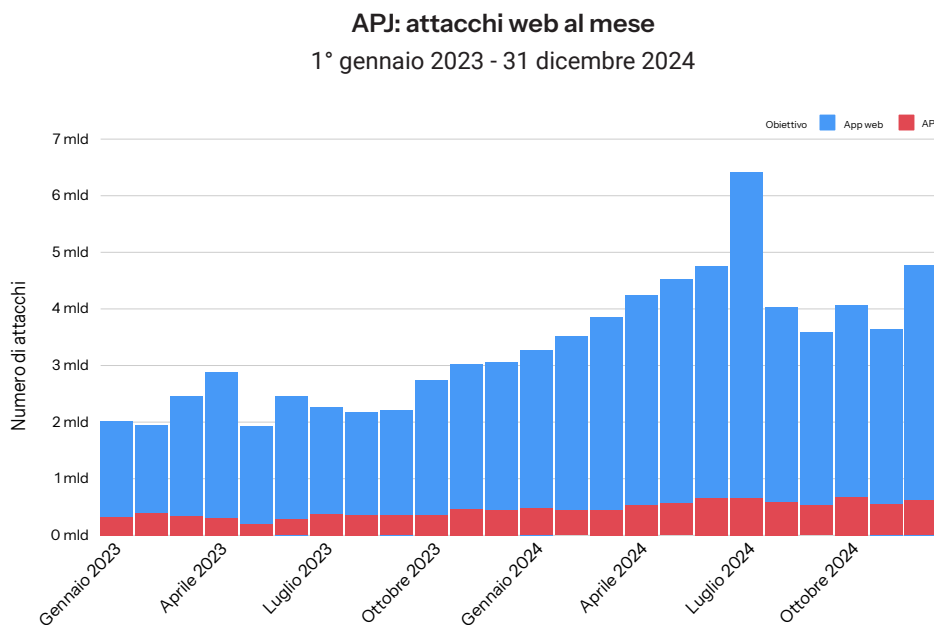
Secondo trend: a livello globale, l'area APJ si è situata al secondo posto per il numero di attacchi DDoS al livello 7 (7,4 migliaia di miliardi), preceduta soltanto dal Nord America con 11,9 migliaia di miliardi di violazioni. Seguono quindi l'area EMEA, con 2,6 migliaia di miliardi, e l'area LATAM, con 258 miliardi. Questa tendenza, descritta per la prima volta nel nostro [rapporto SOTI "Le fortezze digitali sotto assedio"](#), va ancora attribuita all'alto tasso di tentativi di attacco contro i social media che ha interessato l'area APJ.

Focus sulle aree APJ, EMEA e LATAM

In questa sezione vengono presentate alcune delle principali tendenze emerse nelle aree APJ, EMEA e LATAM. All'interno di queste regioni, abbiamo individuato alcune aree specifiche, per le quali era disponibile un numero di informazioni sufficiente a fornire dati statisticamente rilevanti sugli eventi di attacco.

Attacchi alle applicazioni web e alle API: analisi del traffico

Se si confrontano le tendenze mensili negli attacchi web, emerge un marcato contrasto tra le diverse aree geografiche (Figura 12).



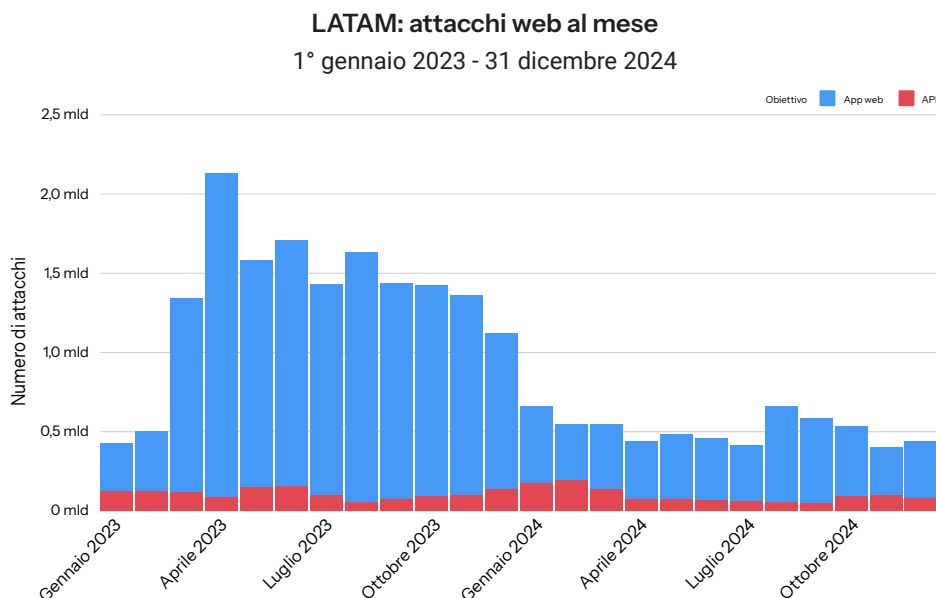
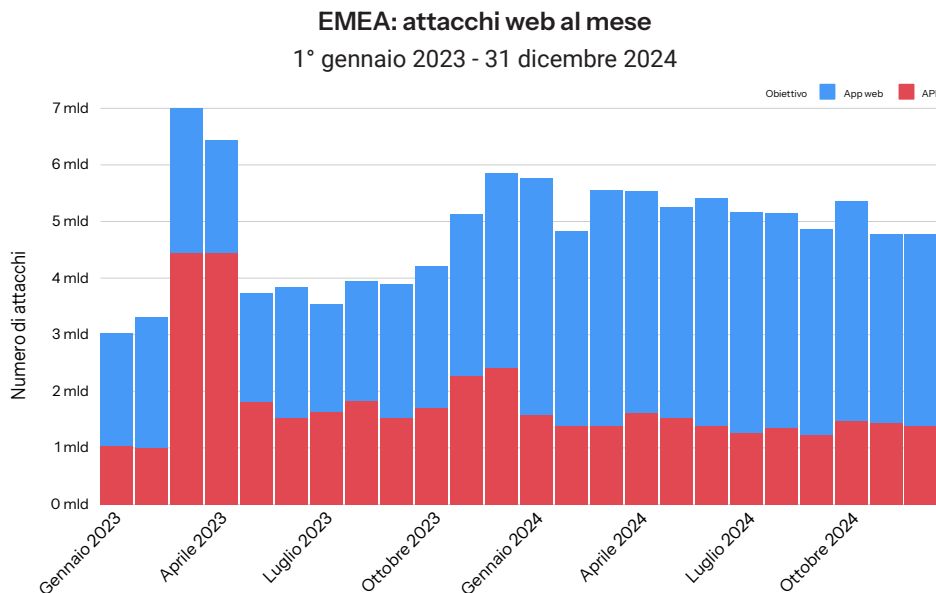


Fig. 12. Le attività dei cybercriminali contro le applicazioni web hanno contribuito ad aumentare il numero totale di attacchi web nelle aree APJ ed EMEA, mentre nell'area LATAM si è verificata una netta diminuzione

Se prendiamo in esame i dati su base annua, l'area APJ ha registrato un forte incremento (+73%) degli attacchi web totali, che sono passati da 29 miliardi nel 2023 a 51 miliardi nel 2024. Nell'area EMEA la crescita si è fermata a un modesto 16% (da 54 a 62 miliardi). In realtà, se non si tenesse conto di un evento eccezionale che ha influenzato i dati, la percentuale si avvicinerebbe al 33%. In America Latina, gli attacchi web totali sono diminuiti notevolmente: da 16 miliardi nel 2023 a 6 milioni nel 2024, con un calo del 61%.

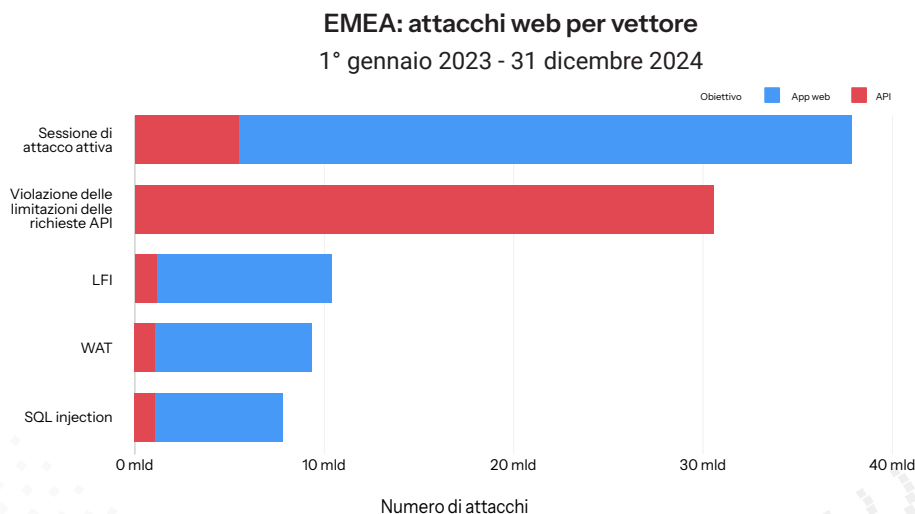
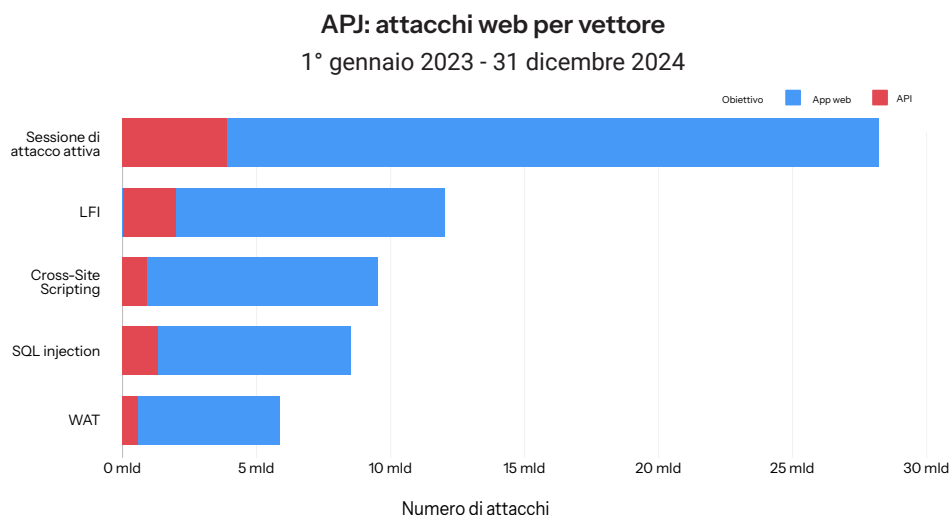
L'aumento degli attacchi alle applicazioni web sembra spingere al rialzo il volume complessivo degli attacchi web, dal momento che le violazioni contro le API sono rimaste a un livello contenuto, soprattutto nelle aree APJ e LATAM.

Nell'area EMEA, la situazione è molto diversa. Dopo il picco registrato nel primo semestre del 2023, causato dagli [attacchi su larga scala sferrati contro il settore del commercio spagnolo](#), le violazioni delle API sono diminuite, rimanendo a un livello più basso per tutto il 2024 (seppur relativamente superiore a quello di altre aree).

In America Latina, la riduzione degli attacchi web è dovuta al fatto che i criminali hanno spostato la propria attenzione dal commercio ad altri settori, come quello farmaceutico e dei servizi aziendali, e si sono focalizzati su altri tipi di attacco, come il [ransomware](#).

Attacchi alle applicazioni web e alle API: tendenze relative alle tattiche

Negli ultimi due anni, i criminali hanno continuato ad avvalersi dei metodi tradizionali, ampiamente collaudati, ma hanno anche iniziato a impiegare in misura maggiore i vettori moderni basati sul comportamento (Figura 13).



LATAM: attacchi web per vettore

1° gennaio 2023 - 31 dicembre 2024

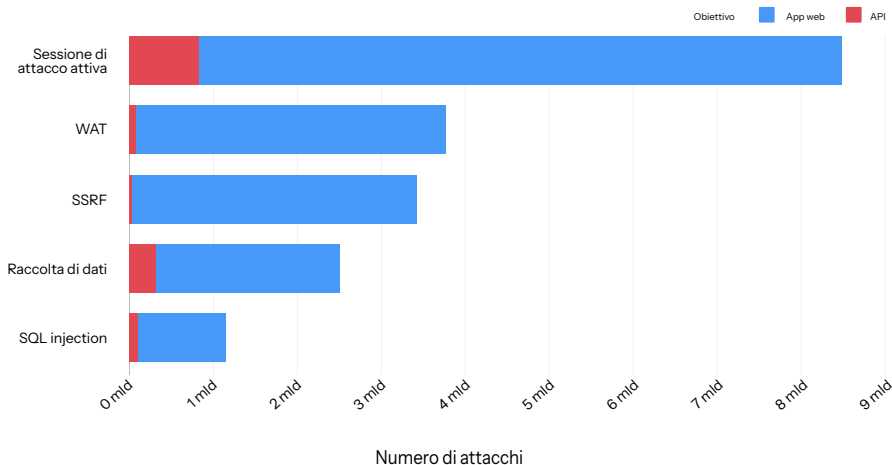


Fig. 13. In tutte le aree geografiche, i principali vettori di attacco hanno combinato sia i metodi tradizionali che le tecniche moderne basate sul comportamento, progettate specificamente per l'abuso delle API

In linea con le tendenze globali, i vettori di attacco tradizionali, come le tecniche LFI, SQLi e XSS, persistono in tutte le aree geografiche, mentre nell'area LATAM sono presenti anche attacchi SSRF. Nella nostra [Guida 2025 per gli addetti alla sicurezza](#), abbiamo evidenziato come gli attacchi XSS siano difficili da estirpare e continuino ad avere una grande importanza per la difesa dalle tradizionali vulnerabilità web.

Ciò che è cambiato in questo periodo, oltre a un progressivo interesse dei cybercriminali nei confronti dell'abuso delle API, è l'incremento dei problemi causati dai vettori di attacco tradizionali basati sul comportamento. I malintenzionati si avvalgono di questi vettori per scoprire e sfruttare le vulnerabilità. Monitorando i vettori a livello locale, i ricercatori di Akamai sono giunti a queste conclusioni:

- Il principale vettore in ogni area geografica è rappresentato dalle sessioni di attacco attive, contro le quali i controlli intelligenti di Akamai agiscono bloccando in modo proattivo e per un determinato periodo di tempo le richieste provenienti da autori noti delle minacce.
- La violazione delle limitazioni delle richieste API è al secondo posto tra le minacce più diffuse nell'area EMEA, dove si è concentrata la maggior parte degli attacchi contro le API. I criminali tentano di effettuare l'abuso delle API mediante l'elusione dei requisiti aziendali, come i limiti di velocità e l'immissione dei dati.
- In ogni area geografica, gli attacchi WAT sono presenti nelle prime cinque posizioni. I criminali utilizzano questo vettore per analizzare il bersaglio e ricavare informazioni sulla sicurezza, sulle configurazioni o sulle vulnerabilità che potrebbero sfruttare per scopi illeciti.

Per ulteriori informazioni su questi vettori, consultate la sezione [Attacchi web](#).

Attacchi alle applicazioni web e alle API: obiettivi principali

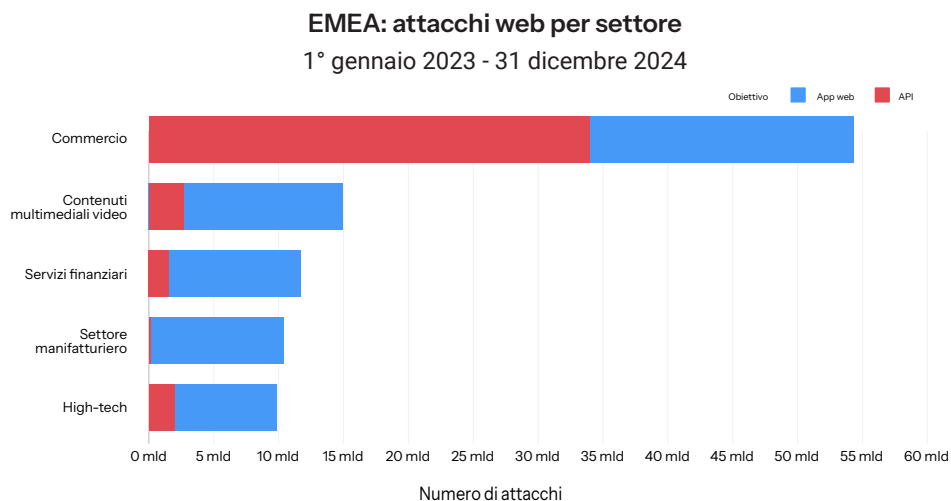
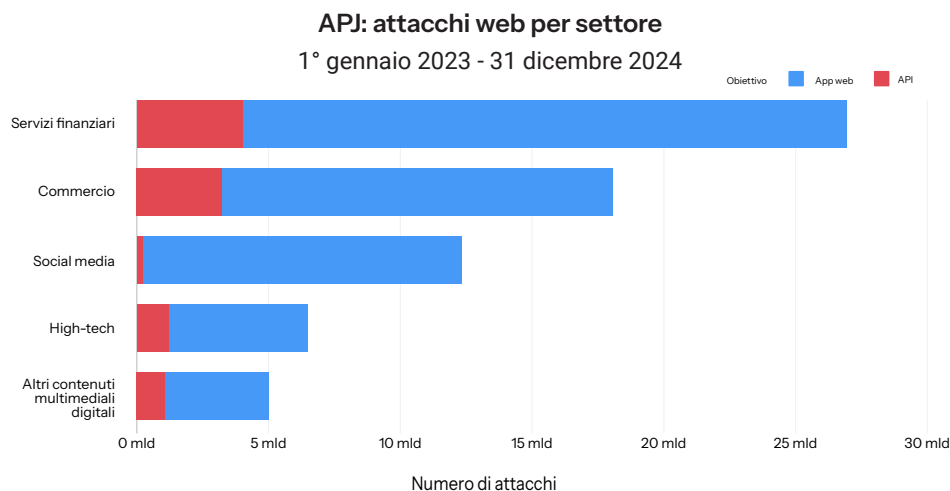
Esaminando nello specifico gli obiettivi presi di mira a livello regionale, si nota che l'area APJ, l'Australia (20,3 miliardi), l'India (17,3 miliardi) e Singapore (15,9 miliardi) hanno sostenuto il peso maggiore degli attacchi alle applicazioni web e alle API, seguiti dal Giappone (6,3 miliardi), dalla Cina (6,2 miliardi), dalla Corea del Sud (4,9 miliardi), dalla Nuova Zelanda (2,9 miliardi) e dalla Regione amministrativa speciale di Hong Kong SAR (2,2 miliardi).

Nell'area EMEA, i tre paesi più colpiti sono stati il Regno Unito (30,3 miliardi), i Paesi Bassi (19,5 miliardi), la Spagna (14,2 miliardi) e la Germania (12,8 miliardi). Seguono l'Austria (8,2 miliardi), la Francia (7,5 miliardi), l'Italia (4,1 miliardi), la Svizzera (3,7 miliardi), il Belgio (3,5 miliardi) e Israele (3,3 miliardi).

Nell'area LATAM gli attacchi si sono concentrati in Brasile (19,3 miliardi), quindi in Messico (2,0 miliardi) e in Cile (0,4 miliardi), che rappresentano tuttavia solo una piccola parte del totale.

Obiettivi per settore

Le ricerche condotte in base alle tendenze per settore hanno rilevato che nelle aree APJ, EMEA e LATAM, il commercio e i servizi finanziari sono stati sempre tra i primi tre settori colpiti dagli attacchi web (Figura 14).



LATAM: attacchi web per settore

1° gennaio 2023 - 31 dicembre 2024

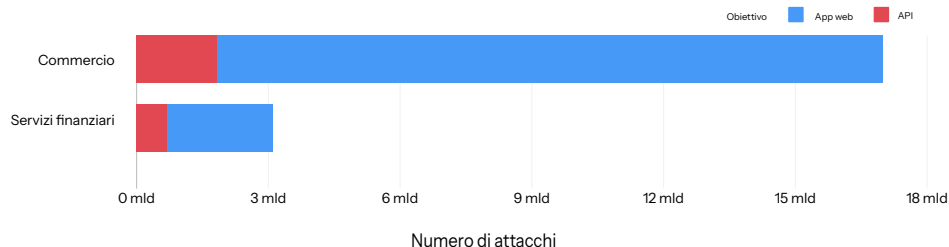


Fig. 14. Il commercio e i servizi finanziari sono due dei tre settori più colpiti nelle aree APJ, EMEA e LATAM

Nell'area APJ, i servizi finanziari hanno segnalato il maggior numero di attacchi web (27 miliardi), mentre il commercio è al secondo posto con 18 miliardi. Si tratta di una crescita, rispettivamente, del 52% e del 161% su base annua. Il settore più interessato dagli attacchi alle API è stato quello degli altri contenuti multimediali digitali (22%), seguito dal commercio (18%) e dai servizi finanziari (15%).

Nell'area EMEA è stato preso di mira soprattutto il commercio, con 54 miliardi di attacchi web, un volume quasi tre volte superiore a quello indicato dal settore più prossimo. Nonostante l'elevata concentrazione, gli attacchi web totali contro le aziende del commercio sono diminuiti del 10% su base annua, perché il picco verificatosi nel 2023 ha alterato i dati relativi a quest'area geografica. La regione EMEA ha comunque registrato un aumento del 16% su base annua degli attacchi web totali, causato da un incremento negli altri settori, tra cui i servizi finanziari (152%) e il comparto manifatturiero (96%). Da un'attenta analisi degli attacchi rivolti contro le API, si osserva come nel 63% dei casi abbiano interessato le API impiegate dalle aziende commerciali.

Una tendenza analoga si può notare nell'area LATAM, dove gli attacchi web diretti contro il commercio hanno raggiunto un totale di 17 miliardi, un volume di gran lunga superiore a quello degli altri settori. Tuttavia, su base annua, le violazioni sono diminuite del 76%. Contemporaneamente, il settore dei servizi alle imprese e quello farmaceutico hanno registrato un aumento, rispettivamente, del 107% e del 129%. Inoltre, l'11% degli attacchi contro il settore del commercio ha preso di mira le API, mentre i servizi finanziari hanno riscontrato una percentuale ancora più alta (23%).

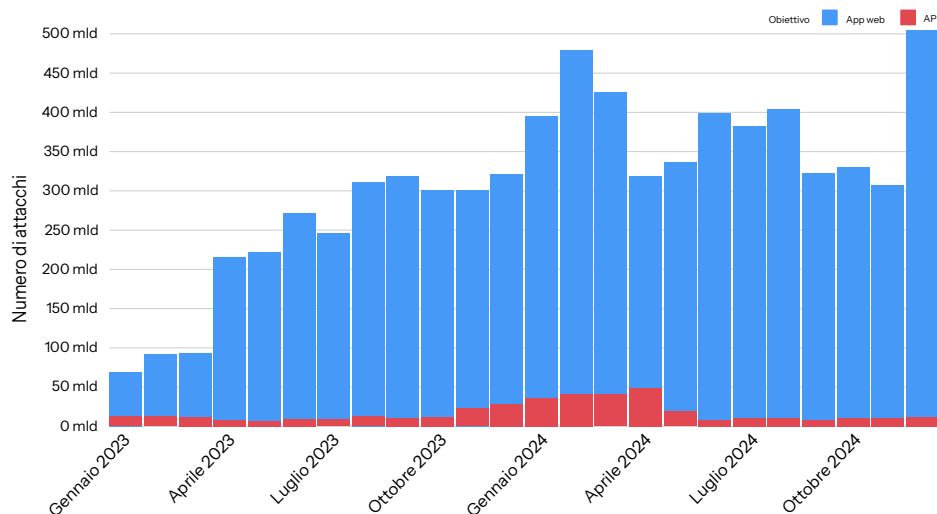
Questi ultimi due settori hanno alcune caratteristiche in comune che li rendono un bersaglio allettante per gli attacchi alle applicazioni web e alle API: entrambi operano all'interno di ecosistemi complessi, si avvalgono in larga parte delle API e dispongono di dati preziosi. Per conseguire i propri obiettivi, i cybercriminali utilizzano pertanto una combinazione di tecniche nuove e tradizionali.

Attacchi DDoS al livello 7: analisi del traffico

Se si confrontano le tendenze sul piano geografico e su base mensile, l'area APJ è stata al centro degli attacchi DDoS al livello 7, mentre le aree EMEA e LATAM hanno segnalato un andamento irregolare (Figura 15).

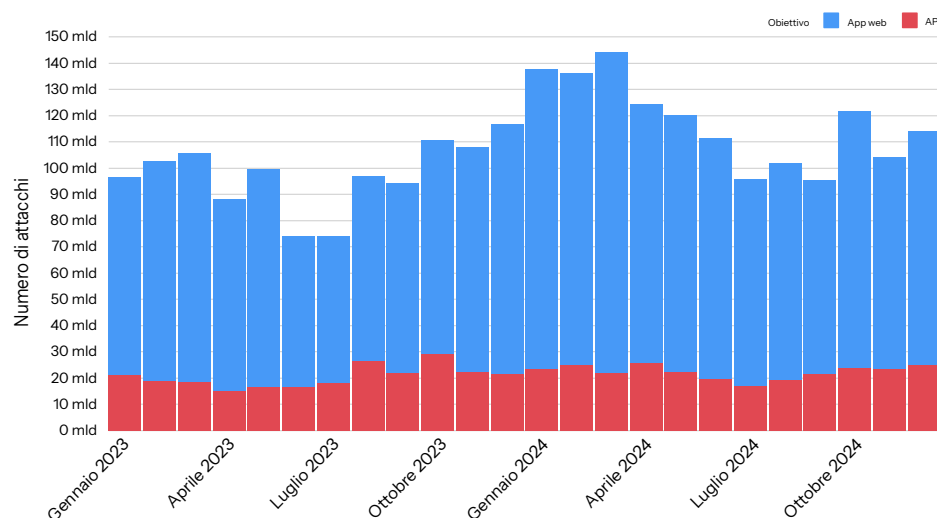
APJ: attacchi DDoS al livello 7 su base mensile

1° gennaio 2023 - 31 dicembre 2024



EMEA: attacchi DDoS al livello 7 su base mensile

1° gennaio 2023 - 31 dicembre 2024



LATAM: attacchi DDoS al livello 7 su base mensile

1° gennaio 2023 - 31 dicembre 2024

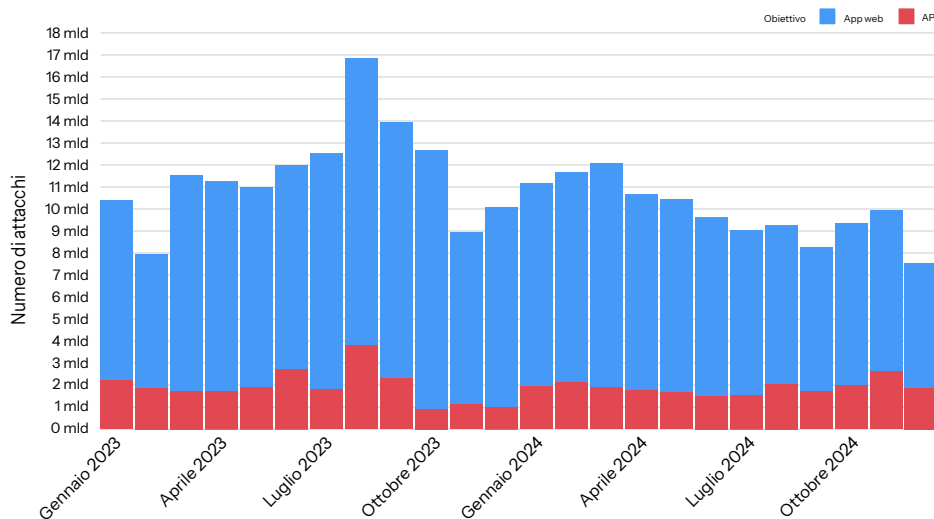


Fig. 15. Nel 2024, gli attacchi DDoS al livello 7 sono aumentati nelle aree APJ ed EMEA e diminuiti nell'area LATAM

L'area APJ ha segnalato una crescita del 66% su base annua, che si è consolidata progressivamente e ha raggiunto il picco dei 504 miliardi nel dicembre 2024. Ad alimentare questo fenomeno sono state le violazioni contro il settore dei social media.

Nell'area EMEA, questi attacchi hanno raggiunto il culmine nel marzo 2024, sfiorando i 145 miliardi di eventi. Dopo un periodo di contrazione, la crescita è ripresa raggiungendo il 20% su base annua. È possibile attribuire questo fenomeno a una confluenza tra fattori geopolitici e tecnologici. Le attuali tensioni geopolitiche hanno favorito un'impennata delle attività degli hacktivisti, mentre la diffusione delle piattaforme DDoS-as-a-Service e degli strumenti ottimizzati per l'AI hanno indebolito gli ostacoli che impediscono l'accesso ai sistemi.

Agli inizi del periodo considerato, l'area LATAM ha segnalato un aumento notevole dei tentativi di attacco DDoS al livello 7, in concomitanza con l'incremento degli [attacchi HTTP flood](#) che mirano a sovraccaricare le risorse API (esamineremo più approfonditamente questo vettore nella sezione [Attacchi DDoS al livello 7: confronto e tendenze su base annua](#)). Nell'agosto 2023, l'attività ha raggiunto il culmine con 16,8 miliardi di eventi, per poi calare fino a 7,5 miliardi nel periodo restante, con una contrazione annua del 15%.

Attacchi DDoS al livello 7: obiettivi principali

Rispetto alla nostra [precedente analisi sugli attacchi DDoS al livello 7](#), non si osservano sostanziali modifiche dal punto di vista dei settori e delle aree geografiche colpiti.

Nell'area APJ, è Singapore il paese in cui si è concentrato il maggior numero di attacchi (4,7 migliaia di miliardi), seguito dall'India (1,1 migliaia di miliardi), dalla Corea del Sud (607 miliardi), dall'Indonesia (283 miliardi), dalla Cina (246 miliardi), dal Giappone (111 miliardi), dall'Australia (108 miliardi) e da Taiwan (81 miliardi).

Nell'area EMEA spiccano invece la Germania (569 miliardi) e il Regno Unito (506 miliardi), quindi Israele (205 miliardi), la Svezia (193 miliardi) e Malta (160 miliardi). L'Italia (158 miliardi), la Svizzera (147 miliardi), la Francia (129 miliardi), l'Olanda (111 miliardi) e la Spagna (96 miliardi) completano l'elenco dei primi 10 paesi.

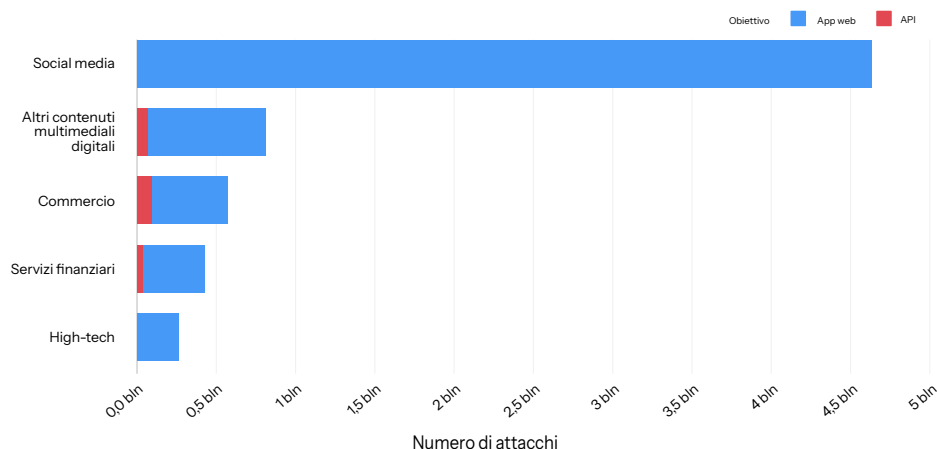
Nell'area LATAM, il Brasile si situa al primo posto (175 miliardi), il Messico al secondo (39 miliardi) e il Costa Rica al terzo (19 miliardi).

Obiettivi per settore

I principali settori colpiti nell'area APJ ed EMEA (Figure 16) sono gli stessi indicati nel nostro [rapporto SOTI precedente sulla sicurezza delle app](#). Come abbiamo approfondito in dettaglio nel suddetto rapporto, gli attacchi DDoS al livello 7 contro le piattaforme di social media hanno subito una crescita vertiginosa nell'area APJ, con riferimento al periodo gennaio 2023 – giugno 2024. L'aumento è correlato ai conflitti militari in corso in altre aree e all'estesa copertura mediatica riservata agli eventi elettorali su scala mondiale. Durante i periodi di crisi geopolitica, è infatti prevedibile che le piattaforme di social media ricevano un volume di traffico molto più elevato. La tendenza si è accentuata negli ultimi mesi del 2024, come abbiamo anticipato, per via delle elezioni in corso sia nell'area APJ che negli Stati Uniti. Questi fattori hanno contribuito ad aumentare del 130% il volume degli attacchi contro il settore dei social media.

APJ: attacchi DDoS al livello 7 per settore

1° gennaio 2023 - 31 dicembre 2024



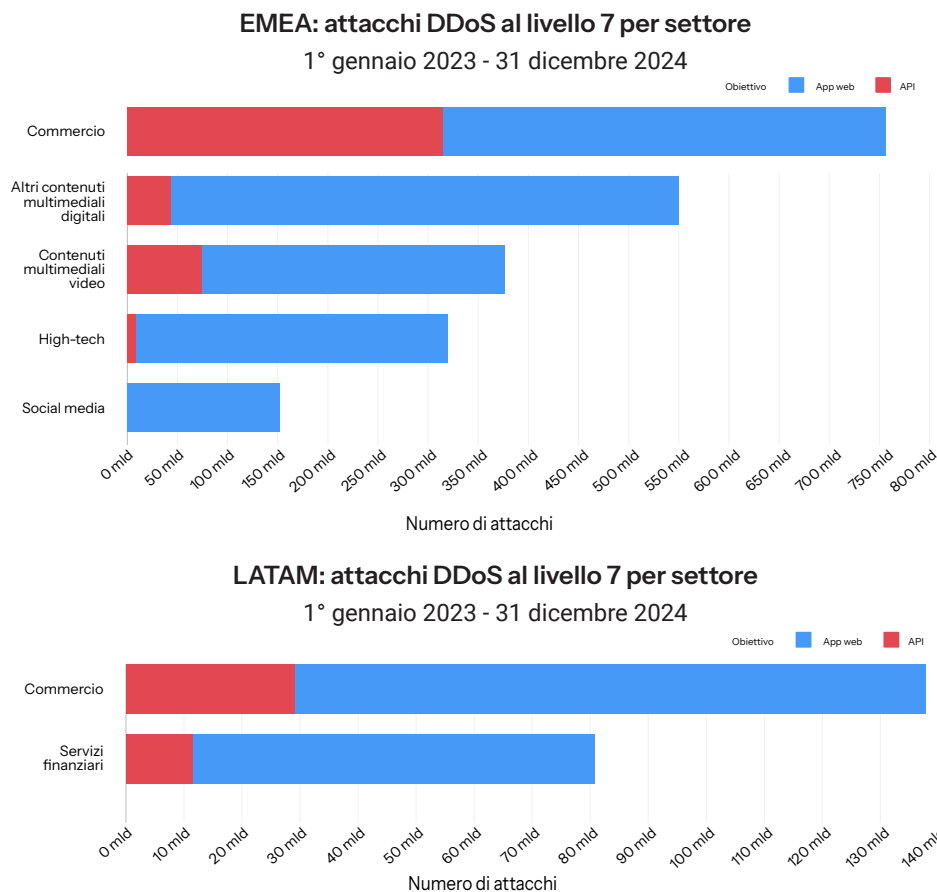


Fig. 16. I settori più colpiti sono gli stessi indicati nel precedente rapporto Akamai. Il commercio è al primo posto per gli attacchi DDoS al livello 7 contro le API

Nell'area EMEA, il settore più interessato dagli attacchi DDoS al livello 7 è rimasto quello del commercio, seguito da quelli degli altri contenuti multimediali digitali e dei contenuti multimediali video. La crescita più marcata su base annua è stata osservata nei settori dell'high-tech (+70%), dei social media (+23%) e del commercio (+14%). Questi cambiamenti mostrano come i cybercriminali riescano a spostare rapidamente l'attenzione da un'area geografica all'altra e da un settore all'altro, quindi è consigliabile monitorare le tendenze in modo più ampio.

Anche il commercio è stato il settore più colpito nell'area LATAM, seguito dai servizi finanziari. Nel periodo esaminato, il livello di attacchi DDoS al livello 7 si è mantenuto piuttosto uniforme tra un settore e l'altro.

In ogni area geografica è il settore del commercio ad aver subito il maggior numero di attacchi contro le API, un dato che rispecchia la tendenza globale. Nello specifico, gli attacchi hanno preso di mira le API in percentuale variabile: 43% nell'area EMEA, 21% nell'area LATAM e 16% nell'area APJ.

Per diversi motivi, fra i quali si ricordano le tensioni geopolitiche e il potenziale impatto economico derivante dalle interruzioni dei servizi ad alta visibilità, i settori del commercio, dei contenuti multimediali e dei servizi finanziari sono stati il principale bersaglio degli attacchi DDoS al livello 7, sia nell'area EMEA che nell'area LATAM, nel corso degli ultimi due anni. Per un approfondimento sulle cause e sulle tecniche alla base dell'alta percentuale di attività contro i settori del commercio e dei servizi finanziari, consultate la sezione [Tendenze per settore](#).

Conformità

Il quadro normativo nel mondo e nel Nord America

Nel 2025, il panorama della cybersecurity a livello globale presenta un livello inedito di complessità e volatilità. Le tensioni geopolitiche, in particolare i conflitti in atto in Ucraina e in Medio Oriente, hanno intensificato il volume degli attacchi sostenuti dai governi nazionali e delle minacce informatiche, mentre la diffusione dell'hacktivismo, praticato soprattutto da gruppi filorussi ai danni dei paesi europei, ha aggiunto un ulteriore elemento di complessità allo scenario delle minacce. Sul piano economico, l'accelerazione della trasformazione digitale osservata in tutti i settori ha ampliato la superficie di attacco, consentendo ai cybercriminali di incrementare le operazioni contro le infrastrutture di importanza cruciale e di sfruttare tecnologie più avanzate, come l'intelligenza artificiale, per affilare le proprie armi.

Questi fattori, unitamente alle pressioni economiche globali e all'instabilità politica di alcuni paesi chiave, hanno dato vita alla tempesta perfetta che sta preoccupando gli esperti di cybersecurity a livello mondiale. La protezione delle applicazioni web e delle API è dunque una priorità per le organizzazioni. Alle iniziative portate avanti dagli hacker etici, dagli esperti di cybersecurity e da organizzazioni come Akamai per dare una risposta all'esigenza fondamentale di difendere i punti di ingresso, si aggiunge la questione più urgente del rispetto della conformità.

In ogni paese, gli enti normativi stanno imponendo requisiti più restrittivi nell'ambito della cybersecurity delle applicazioni. Nel Nord America, l'attenzione è attualmente rivolta verso le strategie complete per la gestione dei rischi e la segnalazione obbligatoria degli incidenti. La legge [Cyber Incident Reporting for Critical Infrastructure Act](#) degli Stati Uniti, che si prevede entrerà in vigore nel 2026, richiede alle organizzazioni dotate di infrastrutture critiche di effettuare almeno annualmente le seguenti attività: creare un inventario dei sistemi informatici, categorizzare i rischi e valutare il livello di cybersecurity aziendale. La normativa sottolinea la necessità di implementare sistemi di sicurezza affidabili per le applicazioni, soprattutto in settori cruciali come quello energetico, chimico e informatico.

Analogamente, il Canada e il Messico si stanno allineando con gli standard internazionali, adeguando i regolamenti legislativi in materia di protezione dei dati e sicurezza delle infrastrutture di importanza critica. Sebbene le singole normative possano variare l'una dall'altra, la tendenza globale procede nella direzione di una definizione più rigorosa dei requisiti di sicurezza delle applicazioni, che comprendano la convalida avanzata degli input, l'introduzione di pratiche di sviluppo sicure e l'esecuzione periodica di controlli sulla sicurezza.

Questioni analoghe devono trovare una risposta anche nel panorama della sicurezza delle API, che stanno diventando il principale bersaglio dei cybercriminali in quanto svolgono un ruolo fondamentale per lo scambio dei dati e l'integrazione dei servizi. A livello globale, gli enti normativi intervengono attraverso la promulgazione di [regolamenti più restrittivi](#), che richiedono alle organizzazioni di adottare sistemi affidabili per la sicurezza delle API.

Inoltre, le nuove normative rendono obbligatoria l'introduzione di soluzioni per la protezione e per il monitoraggio e il rilevamento continui delle API, indispensabili per contrastare le minacce in costante evoluzione. La legislazione del Nord America è orientata a una valutazione approfondita dei rischi associati agli ecosistemi delle API e pone particolare enfasi sulle pratiche di sviluppo sicure, sui meccanismi di autenticazione affidabili e sulle funzionalità per il rilevamento delle minacce in tempo reale. La rapida adozione di strumenti SaaS basati sull'AI, che spesso vengono integrati attraverso le API, ha portato a una notevole estensione della superficie di attacco e ha indotto gli enti normativi a richiedere un approccio più avanzato nel campo della cybersicurezza.

Di pari passo con l'aumento della complessità negli ambienti API, conseguente soprattutto alla diffusione delle applicazioni di apprendimento automatico e intelligenza artificiale, i requisiti in materia di conformità si stanno evolvendo al fine di mitigare i rischi associati alle violazioni dei dati, agli accessi non autorizzati e all'interruzione dei servizi. Sebbene alcune aree geografiche, tra cui APJ, LATAM ed EMEA, stiano sviluppando normative in maniera autonoma, la tendenza globale punta a un'armonizzazione degli standard di sicurezza delle API, indispensabile per far fronte al carattere interconnesso delle architetture digitali moderne.

La situazione nell'area APJ

In quest'area, il quadro normativo sta mutando profondamente, attraverso l'introduzione di nuovi regolamenti che interessano le organizzazioni di tutti i settori. A Singapore, il [provvedimento in materia di cybersecurity](#) è stato recentemente modificato per ampliarne l'ambito di applicazione, in modo da includere i sistemi di infrastrutture, sia fisici sia virtuali, che gestiscono informazioni di importanza critica, compresi quelli ospitati nelle piattaforme sul cloud e quelli situati [oltreoceano](#). Il Giappone ha aggiornato le leggi del [National Center of Incident Readiness and Strategy for Cybersecurity](#), mentre l'India ha perfezionato il proprio atto sull'IT attraverso la promulgazione del [Digital Personal Data Protection Bill](#). L'Australia ha varato il provvedimento 2023 - 2030 Cyber Security Strategy, a ulteriore riprova dell'attenzione posta sul rafforzamento delle misure di cybersecurity nell'area APJ. La strategia perseguita comprende gli emendamenti apportati, verso la fine del 2024, all'Australian Security of Critical Infrastructure Act e la conversione in legge del [Cyber Security Act 2024](#). I requisiti di legge vengono quindi estesi a risorse secondarie come i dispositivi IoT, le applicazioni e le API in grado di elaborare dati sensibili. Le modifiche apportate alle normative costringono le organizzazioni a rivalutare e ottimizzare le procedure di sicurezza per le applicazioni web, concentrandosi in particolare sulla protezione dei dati sensibili e delle infrastrutture di importanza critica.

Si prevede che lo standard [PCI DSS v4.0.1](#) avrà un impatto importante sulle organizzazioni che gestiscono i dati relativi alle carte di pagamento. Il termine ultimo per adeguarsi è scaduto il 31 marzo 2025. La versione aggiornata comprende criteri più rigorosi per le applicazioni web, come l'implementazione di controlli per tutti gli script delle pagine di pagamento eseguiti nel browser dei clienti e l'impiego di soluzioni automatiche per il rilevamento e la prevenzione continua degli attacchi basati sul web. Le organizzazioni dell'area APJ devono ora svolgere analisi approfondite sulle lacune, aggiornare le proprie policy in materia di sicurezza e introdurre le modifiche tecniche indispensabili per rispettare gli avanzati standard di sicurezza previsti per le applicazioni web.

Per quanto riguarda le API, aumenta l'importanza attribuita alla loro sicurezza, un fenomeno in parte dovuto alla crescita delle iniziative di open banking. Sebbene questa regione geografica non abbia ancora adottato le normative per l'open banking nella stessa misura in cui sono state implementate nell'area EMEA, le organizzazioni hanno comunque la possibilità di rimediare proattivamente ai [problemi di sicurezza](#) delle API. I risultati di un [sondaggio](#) condotto nell'agosto 2024 rimarcano come l'accesso degli utenti esterni, nonostante l'impiego più diffuso delle API interne, rimanga un aspetto imprescindibile per il controllo degli accessi alle API. Le organizzazioni devono pertanto implementare sistemi di sicurezza affidabili per la protezione delle API, che comprendano protocolli di autenticazione e autorizzazione avanzati, la crittografia dei dati, l'individuazione e il monitoraggio continui. Mentre l'area APJ procede verso l'introduzione di direttive specifiche per l'[open banking](#), le organizzazioni dovranno attribuire una priorità esclusiva alla sicurezza delle API, in modo da risultare conformi alle normative in via di sviluppo e proteggersi dalle minacce più recenti.

Situazione attuale nell'area EMEA

La complicata interazione fra tensioni geopolitiche, innovazioni tecnologiche e modifiche legislative sta trasformando profondamente lo scenario della cybersecurity nell'area EMEA, che si trova ad affrontare sfide uniche nel suo genere. I conflitti in Ucraina e nel Medio Oriente concorrono all'intensificazione degli attacchi sostenuti dai governi nazionali e delle minacce informatiche, mentre la diffusione dell'hacktivismo, praticato soprattutto da gruppi filorussi contro i paesi europei, ha reso l'area EMEA il principale bersaglio dei cybercriminali che agiscono sulla base di motivazioni politiche.

Le stesse questioni influiscono sul panorama delle API nell'area EMEA. Le API sono diventate uno dei principali bersagli degli attacchi informatici, in quanto svolgono un ruolo indispensabile per l'integrazione dei servizi e lo scambio dei dati. La rapida adozione di strumenti SaaS basati sull'AI, che spesso vengono integrati attraverso le API, ha portato a un ampliamento significativo della superficie di attacco.

Per contrastare l'escalation di queste minacce, l'Unione europea ha introdotto un insieme esaustivo di normative in materia di cybersecurity. La [direttiva NIS2 \(Network and Information Systems\)](#), in vigore da gennaio 2025, prevede un campo di applicazione molto ampio, esteso a 18 settori fondamentali, e obbliga le aziende di medie e grandi dimensioni a implementare misure rigorose per la cybersecurity.

Nel settore finanziario, il regolamento [DORA \(Digital Operational Resilience Act\)](#), valido a partire dal 17 gennaio 2025, sostituisce la direttiva NIS2 e impone una serie di requisiti, tra cui l'introduzione di sistemi efficienti per la gestione dei rischi relativi ai servizi ICT (Information and Communication Technology), opzioni per la segnalazione degli incidenti e programmi in grado di testare la resilienza operativa digitale delle applicazioni utilizzate dai servizi finanziari. Inoltre, lo standard [PCI DSS v4.0.1](#), obbligatorio dal 31 marzo 2025, introduce nuovi criteri di conformità incentrati sulle esigenze di sicurezza in costante evoluzione, sui processi per la protezione continua, sulle metodologie flessibili e sulle procedure di convalida avanzata. La direttiva [PSD3 \(EU Payment Services Directive\)](#), in corso di pubblicazione, è intesa a risolvere le lacune presenti nella versione precedente (PSD2) attraverso il rafforzamento dei sistemi per la condivisione dei dati, dei requisiti di sicurezza e delle attività di supervisione nel settore dei servizi finanziari.

Il regolamento [CRA](#) (Cyber Resilience Act), che è entrato in vigore il 10 dicembre 2024, stabilisce standard di cybersecurity obbligatori per i prodotti con componenti digitali venduti all'interno dell'Unione Europea. In base al regolamento, le aziende sono tenute a implementare sistemi di sicurezza nell'intero ciclo di vita dei prodotti connessi in rete. Per gli utenti e gli sviluppatori delle applicazioni, il CRA considera gli smartphone e i tablet come importanti vettori di rischio, ragion per cui le organizzazioni devono gestire i terminali dei dispositivi mobili come un elemento essenziale della propria strategia complessiva di cybersecurity e introdurre misure adeguate in ogni fase del ciclo di vita delle applicazioni.

Nel Regno Unito sta per essere promulgato il [Cyber Security and Resilience Bill](#), che consentirà di migliorare le difese informatiche nazionali e proteggere i servizi pubblici di primaria importanza. Gli aggiornamenti che il progetto di legge introdurrà nel quadro normativo in vigore ne estenderanno l'ambito di applicazione, in modo da proteggere un numero maggiore di supply chain e servizi digitali, potenziare le attività di attuazione e incrementare i requisiti per la segnalazione degli incidenti.

La situazione nell'area LATAM

Nell'area LATAM, il panorama della cybersecurity continua a evolversi a un ritmo sostenuto, per effetto delle tendenze globali in ambito economico e della situazione economica e politica specifica di quest'area geografica. A tale proposito, l'accelerazione della trasformazione digitale in tutti i paesi sudamericani, a cui si aggiungono le vulnerabilità insite nei sistemi sempre più interconnessi, ha trasformato la regione in un obiettivo allettante sia per i cybercriminali sia per gli hacker sostenuti dai governi nazionali. Gli attacchi informatici colpiscono prevalentemente i settori del commercio e dei servizi finanziari, mentre i retailer online, le società di elaborazione dei pagamenti, gli istituti bancari, le compagnie assicurative, le startup FinTech e le piattaforme di scambio delle criptovalute sono estremamente [vulnerabili](#) agli attacchi che prendono di mira le infrastrutture digitali, soprattutto le API e le applicazioni web.

I paesi dell'area LATAM sono consapevoli di queste criticità e stanno compiendo grandi passi avanti nello sviluppo e nell'implementazione delle normative in materia di cybersecurity, incentrate sempre più spesso sulla sicurezza di applicazioni web e API. Il Brasile ha assunto un ruolo di primo piano attraverso l'implementazione della legge LGPD (Lei Geral de Proteção de Dados Pessoais), che prevede [requisiti](#) elevati per la protezione e la sicurezza dei dati. Sebbene non si rivolga nello specifico alle applicazioni web o alle API, il provvedimento ha indotto le organizzazioni a migliorare il livello di sicurezza complessivo, senza escludere le interfacce digitali.

Analogamente, il Cile ha attuato la legge [Framework Law on Cybersecurity](#), entrata in vigore il 1° gennaio 2025. Oltre a istituire la National Cybersecurity Agency, il provvedimento indica quali sono le misure più complete per prevenire, segnalare e risolvere gli incidenti relativi alla cybersecurity nei diversi settori, compresi quelli che dipendono maggiormente dalle applicazioni web e dalle API. Sempre nel gennaio 2025, l'Argentina ha pubblicato il [Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity \(2025–2027\)](#).

Ci sono progressi incoraggianti nell'ambito delle normative specifiche per le API. Il Messico, per esempio, ha implementato una [legislazione](#) incentrata sul settore finanziario (compreso il segmento FinTech), che delinea i requisiti necessari per uno sviluppo sicuro delle API impiegate nei centri di smistamento e nelle agenzie di informazioni creditizie. Questo approccio riflette la crescente consapevolezza di come le API abbiano un ruolo fondamentale per gli ecosistemi digitali moderni e di quanto sia importante introdurre regolamenti mirati per la sicurezza informatica. Inoltre, la [Federal Law on the Protection of Personal Data Held by Private Parties](#) disciplina l'elaborazione dei dati personali e stabilisce gli obblighi cui devono assolvere le aziende e le organizzazioni.

Anche la Colombia sta aggiornando il proprio [quadro](#) normativo e ampliando le iniziative sul piano giuridico, attraverso la divulgazione delle disposizioni rivolte agli enti pubblici in materia di cybersecurity e la realizzazione di un sistema per la gestione dei rischi digitali dotato di livelli diversi per la segnalazione delle risposte agli incidenti di sicurezza. Sebbene non riguardino esclusivamente le API, queste misure avranno inevitabilmente conseguenze sulle procedure per la sicurezza delle API implementate dalle organizzazioni.

Nell'intera area geografica, si delinea una tendenza crescente a effettuare [interventi](#) specifici per ciascun settore, come il quadro normativo in materia di Open Finance che stabilisce gli standard di sicurezza delle API necessari per proteggere i dati dei clienti. I quadri normativi hanno un'importanza essenziale nel settore finanziario, dove la sicurezza delle API è il presupposto necessario per garantire l'integrità delle transazioni finanziarie e salvaguardare le informazioni sensibili dei clienti. Se i paesi dell'area LATAM continueranno a dare precedenza alle innovazioni tecnologiche nel campo di sicurezza e a conformare le proprie normative sulla cybersecurity agli standard internazionali, è possibile prevedere che verranno sviluppate linee guida più specifiche e complete per la sicurezza di applicazioni web e API.

Mitigazione

In un contesto in cui le minacce continuano a evolversi e le tecniche di attacco diventano più complesse, la protezione delle applicazioni web e delle API rappresenta una priorità per le organizzazioni. Ecco alcune delle tecniche consigliate da Akamai per la protezione e la mitigazione degli incidenti:

- **Definizione di un piano completo per la sicurezza delle API:** implementate un approccio "shift-left" e "DevSecOps" che garantisca la sicurezza delle API durante ogni fase, dallo sviluppo alla post-produzione. Garantite un [rilevamento](#) e una visibilità continui per conoscere al meglio l'intera superficie di attacco, comprese le API nascoste (shadow, legacy, e zombie). Prevenite l'abuso delle API rafforzando i sistemi di sicurezza con soluzioni avanzate per l'autenticazione e l'autorizzazione (OAuth 2.0, mTLS, controllo degli accessi basato sui ruoli o sugli attributi), la limitazione della velocità e la mitigazione dei bot. Identificate e bloccate gli attacchi non appena si verificano implementando opzioni per la protezione del runtime, il monitoraggio delle anomalie e il rilevamento delle minacce in tempo reale. Preservate la sicurezza su larga scala attraverso la conformità a normative quali DORA, GDPR, HIPAA, NIS2 e PCI DSS e applicando le policy di governance delle API.
- **Implementazione di soluzioni affidabili per la cybersecurity:** utilizzate un [motore di sicurezza adattivo](#) in grado di monitorare gli attacchi e intervenire in tempo reale, fornendo intelligence sulle minacce e [protezione del runtime](#). Avvaletevi inoltre di [strumenti per i test delle API](#), come la soluzione DAST (Dynamic Application Security Testing), per garantire il rispetto dei requisiti di sicurezza, tra cui l'autenticazione, la crittografia e l'accesso sicuro.
- **Protezione proattiva contro le minacce:** sfruttate [strumenti di protezione DDoS specializzati](#), configurate la limitazione della velocità e il caching della CDN, implementando inoltre misure come la gestione delle patch, le policy di controllo degli accessi e la segmentazione della rete. Infine, proteggete la DNS Infrastructure attraverso un monitoraggio continuo del traffico e l'impiego di piattaforme ibride.
- **Mitigazione delle vulnerabilità delle API:** attenetevi a linee guida consolidate per la sicurezza, come quelle fornite dall'elenco [OWASP](#), per rafforzare la sicurezza delle API e risolvere i rischi correlati alle procedure di codifica inadeguate e agli errori di configurazione legati alle architetture delle API, che possono creare vulnerabilità sfruttate dagli hacker per ottenere un accesso non autorizzato o manipolare i dati.

- **Difesa contro le minacce ransomware:** impiegate un approccio su più livelli per contrastare il ransomware. Implementate le soluzioni Zero Trust per bloccare il traffico dannoso, eseguite la microsegmentazione per ottenere una visibilità approfondita e un controllo preciso degli accessi e avvaletevi del [MITRE ATT&CK framework](#) per scoprire i modelli di attacco e ottimizzare le strategie di risposta.
- **Preparazione agli attacchi basati sull'AI:** mettete in campo una strategia di difesa completa, che comprenda [soluzioni per la difesa dai bot](#), strumenti di sicurezza basati sull'intelligenza artificiale, firewall specializzati e misure proattive, come la valutazione continua e i modelli Zero Trust, in modo da far ai nuovi rischi per la sicurezza derivanti dall'[impiego crescente dell'AI](#). Inoltre, proteggete i sistemi basati sull'intelligenza artificiale attraverso un approccio variegato: Acquisite familiarità con i modelli e i dataset esistenti per affrontare minacce specifiche, come l'iniezione di prompt e il data poisoning, eseguite proattivamente i test di vulnerabilità e impiegate soluzioni consolidate, come il monitoraggio dei comportamenti, la convalida dei contenuti e l'automazione delle risposte agli attacchi, che sono integrate negli ambienti sia di sviluppo che di runtime.

Metodologia

Attacchi DDoS alle applicazioni web e al livello 7

In questa sezione vengono descritti gli avvisi a livello di applicazione 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'applicazione, un'API o un sito web protetto. Invece, gli avvisi sugli attacchi DDoS al livello 7 vengono attivati quando si riscontrano anomalie volumetriche all'interno di una serie di richieste a un'API, un'applicazione o un sito web protetto. L'attivazione è innescata sia dalle richieste dannose che da quelle non dannose. Le richieste, di per sé, non sono generalmente dannose, ma quando compaiono in un numero elevato, possono nascondere uno scopo illecito. Gli avvisi non indicano necessariamente che un attacco sia andato a buon fine. Sebbene i prodotti disponibili 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 in Akamai 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 24 mesi, dal 1° gennaio 2023 al 31 dicembre 2024.

Dati sugli attacchi alla sicurezza delle API

Grazie all'integrazione di Noname Security, Akamai ha ottimizzato le funzionalità di ricerca e rilevamento delle minacce. Occorre segnalare che il dataset è ancora nelle fasi di integrazione e analisi iniziali. Per questo rapporto, abbiamo preso in esame un campione di avvisi sulla sicurezza delle API, attivati in un periodo di 30 giorni nel primo trimestre del 2025, e li abbiamo esaminati in dettaglio a fronte degli standard di conformità e dei sistemi di sicurezza corrispondenti. Il dataset continuerà a evolversi e in futuro offrirà un quadro completo dei problemi relativi alla sicurezza delle API.



Riconoscimenti

Direttore della ricerca

Mitch Mayne

Editoria e stesura

Charlotte Pelliccia

Lance Rhodes

Badette Tribbey

Maria Vlasak

Revisione e contributi di esperti del settore

Tom Emmons

Reuben Koh

Richard Meeus

Stas Neyman

Steve Winterfeld

Analisi dei dati

Chelsea Tuttle

Materiali promozionali

Barney Beal

Ashley Linares

Marketing ed editoria

Georgina Morales Hampe

Emily Spinks

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

Ricerca sulle minacce di Akamai

Restate aggiornati sulle ultime novità in materia di intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersecurity consultando il sito akamai.com/security-research

Accesso ai dati del rapporto

Potete visualizzare i grafici e i diagrammi di questo rapporto in una versione 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

Ricerca sulla sicurezza di Akamai

Leggete il blog relativo alla ricerca sulla sicurezza di Akamai per una rapida panoramica sugli studi più importanti attualmente in corso.

akamai.com/blog/security-research



Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su [X](#) (in precedenza Twitter) e [LinkedIn](#). Data di pubblicazione: 04/25.