SOTI

V10, NUMERO 01

10 YEARS
OF SECURITY INSIGHT

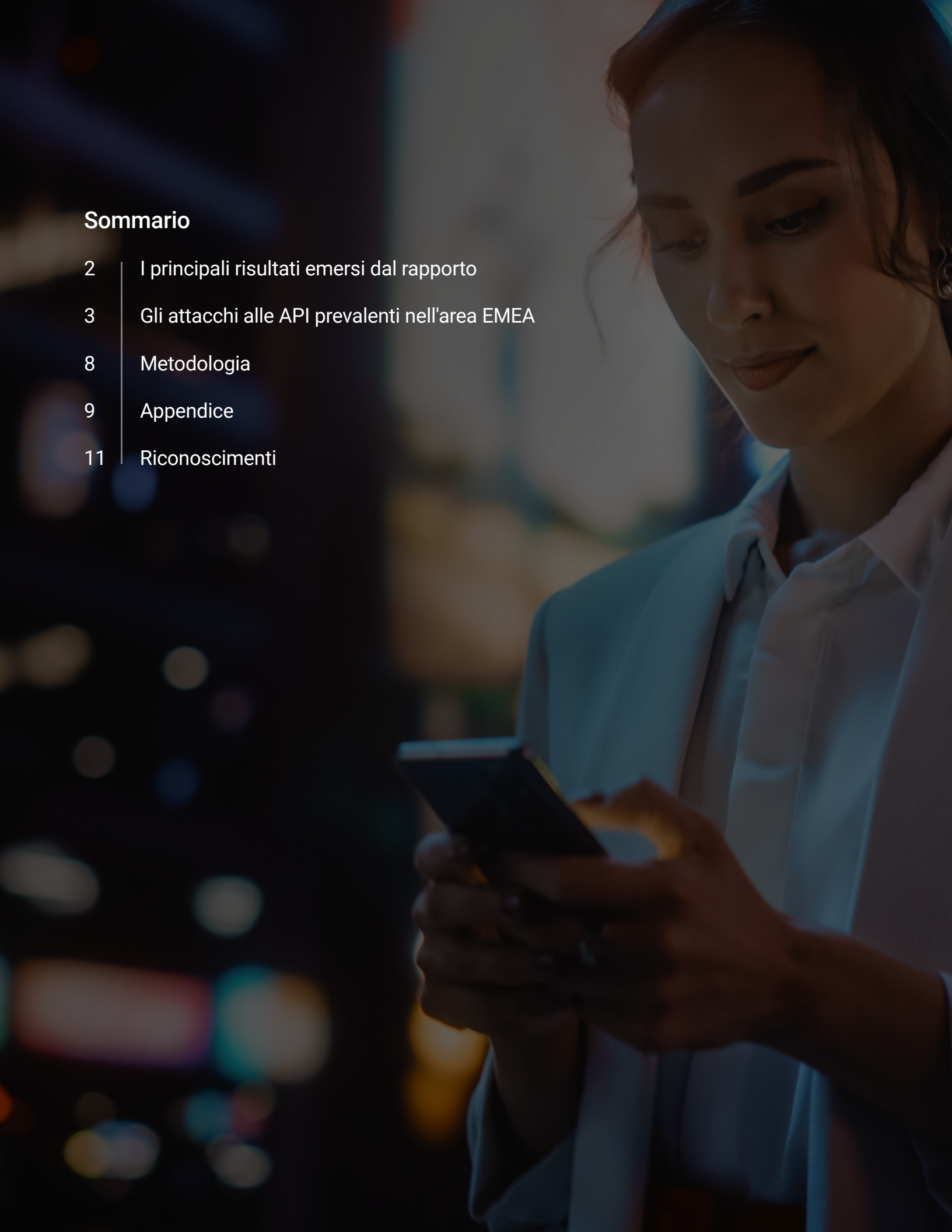
Le tendenze degli attacchi fanno luce sulle minacce delle API

Panoramica sull'area EMEA

Akamai

Stato di Internet - Security

Sommario



I principali risultati emersi dal rapporto

La panoramica sull'area EMEA è un documento integrativo del più ampio rapporto SOTI sulla sicurezza delle API dal titolo Minacce in agguato: le tendenze degli attacchi fanno luce sulle minacce delle API (disponibile solo in inglese). All'interno di questo rapporto sono disponibili descrizioni dettagliate su come i criminali sfruttano i vettori di attacco trattati in questa panoramica, alcuni suggerimenti per proteggere le organizzazioni e una spiegazione delle metodologie impiegate per condurre la nostra ricerca e dei nuovi dataset.

Panoramica

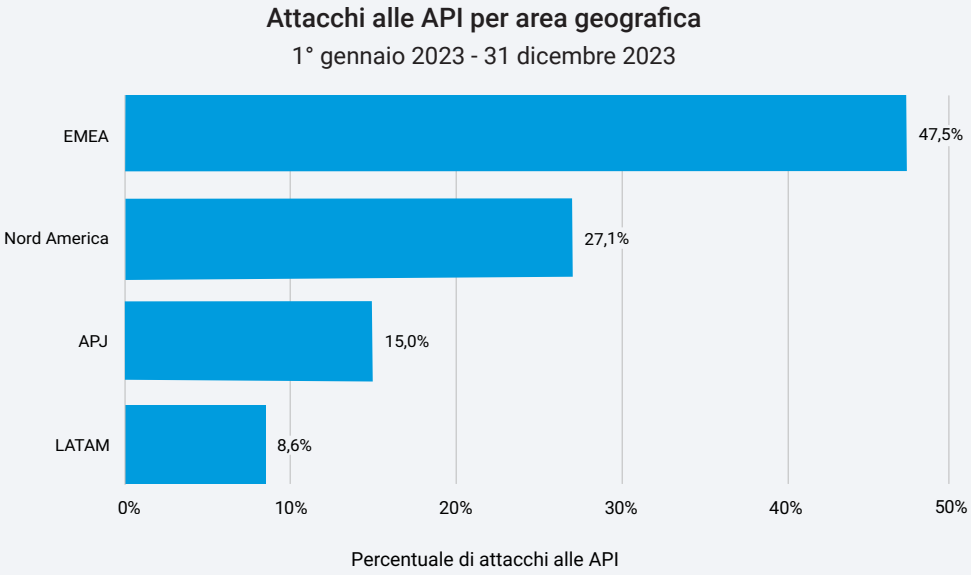
Man mano che l'innovazione digitale e l'economia delle API migliorano le experience di clienti e dipendenti, offrono ai criminali informatici anche nuove opportunità di sfruttamento delle vulnerabilità. Gli attacchi focalizzati sulle API possono danneggiare la reputazione, il brand e i profitti, nonché causare la perdita di dati riservati e della fiducia dei clienti. Considerando l'impennata prevista nel numero di attacchi alle API e l'incremento degli obblighi di segnalazione e controllo in base alle normative vigenti in materia di cybersicurezza dovuto all'aumento nell'utilizzo delle API per scambiare informazioni finanziarie sensibili, la sicurezza delle API è diventata più importante che mai.

Per comprendere meglio lo scenario degli attacchi alle API, anziché guardare complessivamente agli attacchi alle API e alle applicazioni web, nel 2024 stiamo usando un nuovo dataset che consente ai ricercatori di Akamai di distinguere tra due tipi di attacchi e di focalizzarsi sulla percentuale di attacchi che prendono di mira le API. In questa panoramica sull'area EMEA, che comprende 12 mesi (da gennaio 2022 a dicembre 2023), esaminiamo in modo approfondito le tendenze degli attacchi e le relative implicazioni per i consumatori.

- Dai dati globali, emerge come, nell'area EMEA (Europa, Medio Oriente e Africa), si sia registrata la più elevata percentuale di attacchi web che hanno preso di mira le API con un 47,5%, una cifra di gran lunga superiore al dato dell'area geografica più vicina, il Nord America, la cui percentuale si è attestata sul 27,1%.
- Coerentemente con la tendenza globale, gli attacchi al protocollo HTTP e SQLi (Structured Query Language Injection) sono stati i vettori di attacco predominanti per le API nell'area EMEA negli scorsi 12 mesi.
- Anche le richieste dei bot sono motivo di preoccupazione: il 40% dei quattromila miliardi circa di richieste di bot sospette ha preso di mira le API.
- Nel settore del commercio, quasi i tre quarti (74,6%) di tutti gli attacchi web sferrati contro le organizzazioni sono stati rappresentati da attacchi alle API, più del doppio rispetto alla percentuale registrata nel settore più vicino, ossia l'high-tech (35,5%).

Gli attacchi alle API prevalenti nell'area EMEA

Dalla ricerca di Akamai, che ha utilizzato un nuovo dataset per monitorare specificamente il traffico degli attacchi alle API, emerge come, nell'area EMEA, si sia registrata la più elevata percentuale di attacchi alle API su base globale con un 47,5%, che ha superato di gran lunga il dato dell'area geografica più vicina, il Nord America, la cui percentuale si è attestata sul 27,1% (EMEA - Figura 1). Questo dato è basato sul numero totale di attacchi web registrati in ciascuna area geografica e mostra come le API siano maggiormente a rischio nell'area EMEA rispetto ad altre regioni.

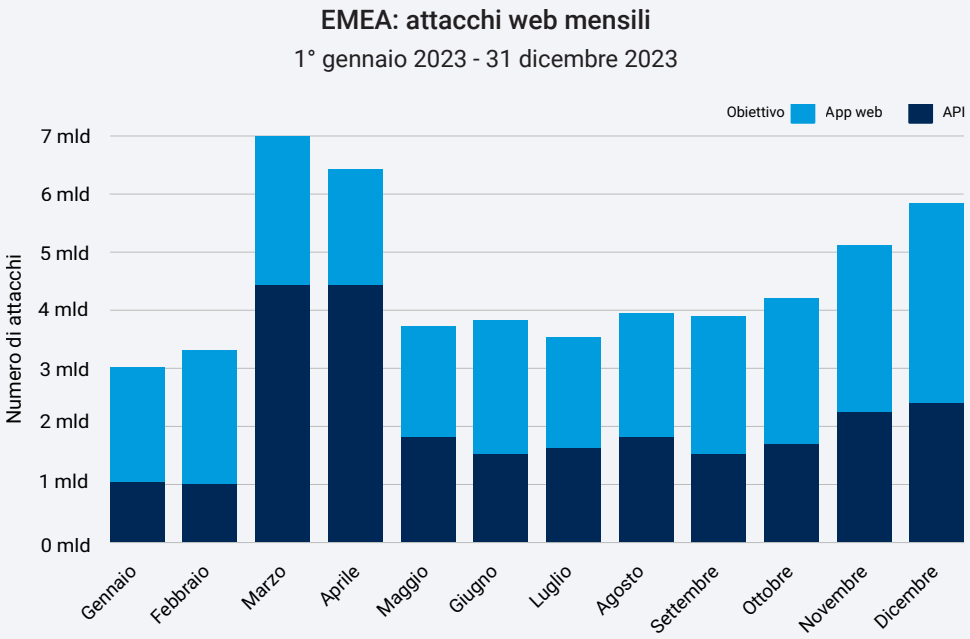


EMEA - Figura 1. Gli attacchi web prendono di mira le API con maggiore probabilità nell'EMEA più che in altre aree geografiche

Possiamo attribuire questa percentuale relativamente alta degli attacchi nell'area EMEA (se confrontata con la percentuale degli attacchi in altre aree geografiche) in parte alle dimensioni alquanto grandi del mercato delle API aperte rispetto al Nord America e all'area Asia-Pacifico, che riflettono i tassi di adozione delle API più elevati nell'area EMEA, nonché all'open banking e al PCI DSS (Payment Card Industry Data Security Standard) v4.0 che stanno favorendo l'utilizzo delle API e possono introdurre i rischi per la sicurezza descritti nel rapporto globale.

Nell'area EMEA, tra i paesi con la più elevata percentuale di attacchi web che hanno preso di mira le API figurano la Spagna (94,8%), il Portogallo (84,5%), i Paesi Bassi (71,9%) e Israele (67,1%). Ciò non vuol dire che il numero di attacchi web nel complesso sia superiore in questi paesi che in altri paesi dell'area EMEA; anzi, questi paesi devono affrontare un rischio di abuso delle API molto più limitato a causa della predilezione di questo vettore da parte dei criminali.

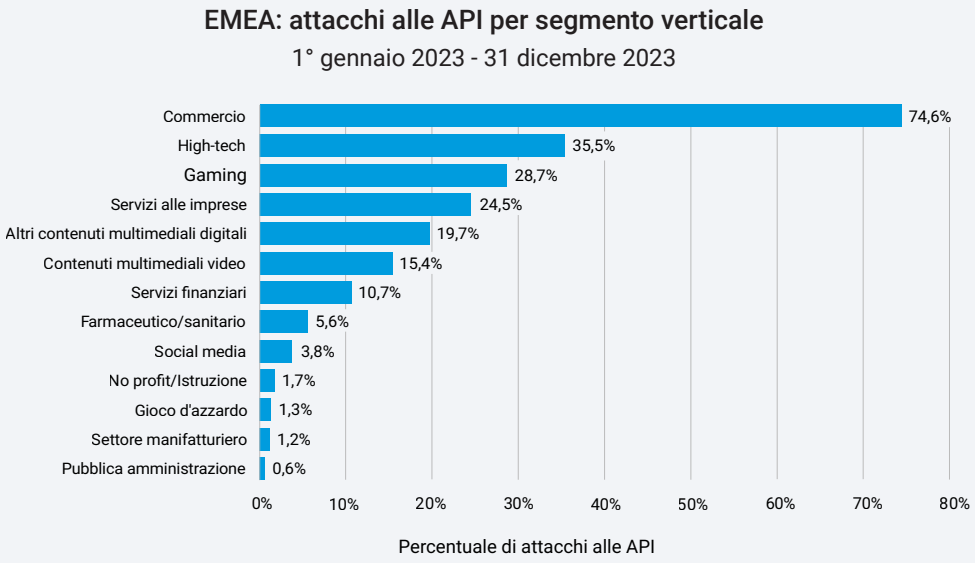
Dalle tendenze mensili osservate durante il periodo esaminato nel rapporto (da gennaio a dicembre 2023), emerge come gli attacchi web che hanno preso di mira le API nell'area EMEA sono aumentati in modo alquanto costante, a partire dal 34% a gennaio fino a salire al 41% alla fine dell'anno (EMEA - Figura 2). Le eccezioni sono state rappresentate dai mesi di marzo e aprile in cui i ricercatori di Akamai hanno osservato un'impennata negli attacchi alle API quando il settore del commercio in Spagna (un paese con una concentrazione di attacchi alle API già enorme) ha subito una serie di attacchi mirati su larga scala. Questo picco mostra come i criminali riescano a spostare rapidamente la loro attenzione da un'area geografica all'altra e da un settore all'altro, quindi è consigliabile monitorare le tendenze in modo più ampio.



EMEA - Figura 2. Ad eccezione dei mesi di marzo e aprile in cui si sono osservati brevi picchi, gli attacchi alle API sono lentamente aumentati nel 2023, arrivando alla fine dell'anno al 41% di tutti gli attacchi sferrati

Gli attacchi alle API nei vari settori

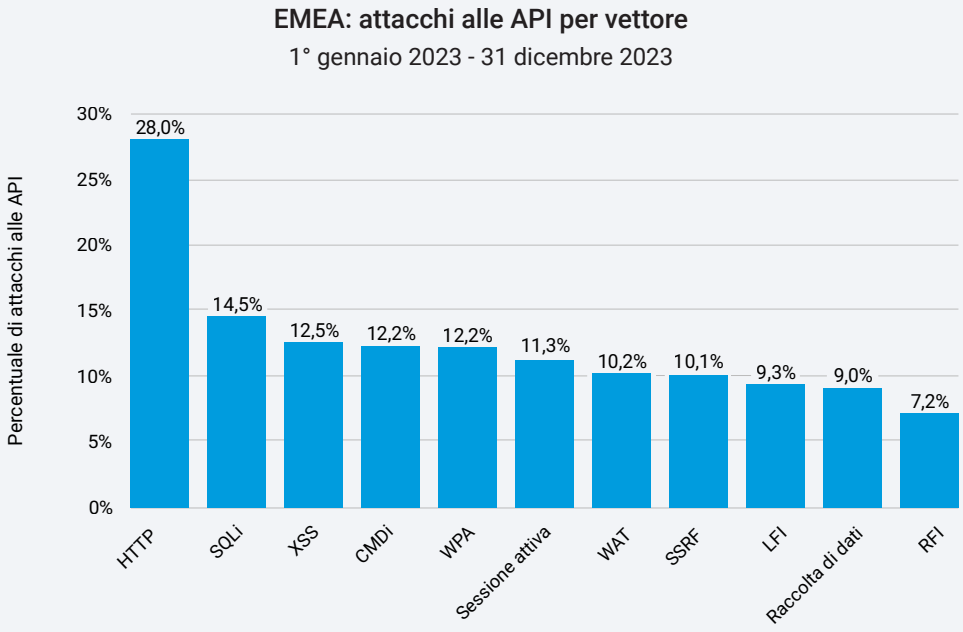
Nel periodo esaminato dal rapporto, i ricercatori di Akamai hanno riscontrato che il settore del commercio ha subito la più elevata percentuale di attacchi web sferrati in totale contro le organizzazioni (74,6%), più del doppio rispetto alla percentuale registrata nel settore più vicino, ossia l'high-tech (35,5%), seguito dal gaming (28,7%), dai servizi alle imprese (24,5%) e dai media digitali (19,7%) (EMEA - Figura 3).



EMEA - Figura 3. Il segmento verticale del commercio ha registrato la più elevata percentuale di attacchi alle API , in parte a causa della natura complessa del suo ecosistema, alla sua elevata dipendenza dalle API e ai dati preziosi di cui dispongono le organizzazioni che operano in questo settore

API sotto attacco: analisi del traffico

Coerentemente con la tendenza globale, l'HTTP e l'SQLi sono stati i vettori di attacco predominanti per le API nell'area EMEA negli scorsi 12 mesi, mentre l'LFI (Local File Inclusion) è sceso in basso nella classifica pur rimanendo predominante negli attacchi alle applicazioni web (EMEA - Figura 4).



EMEA - Figura 4. L'HTTP, l'SQLi e l'XSS sono i vettori di attacco predominanti negli attacchi alle API, mentre l'LFI è meno prevalente negli attacchi alle API, ma ancora attivamente usato negli attacchi contro le applicazioni web

Nell'area EMEA, l'XSS (Cross-Site Scripting) rimane la tecnica preferita negli attacchi alle API e risulta prevalente anche il CMDi (Command injection). Questo nuovo dataset ci consente di monitorare ulteriori vettori di attacco nelle API. Ad esempio, l'SSRF (Server-Side Request Forgery), di cui abbiamo discusso nel nostro rapporto del 2023), è ora un nuovo vettore emergente. Un elenco completo delle definizioni dei vettori di attacco è disponibile nell'appendice.

Dalla nostra ricerca, è emerso anche che le richieste di bot creano motivo di preoccupazione. Nello stesso periodo di 12 mesi osservati nel rapporto, il 40% dei quattromila miliardi circa di richieste di bot sospette ha preso di mira le API.

Conclusione

Difendere le API è un chiaro imperativo dal punto di vista della gestione dei rischi e della sicurezza. Inoltre, le leggi e le normative esistenti, insieme alle riforme emergenti, che tengono la legislazione in materia di cybersicurezza al passo con l'attuale scenario delle minacce, rendono ugualmente fondamentale proteggere le API.

Ad esempio, il Regolamento generale per la protezione dei dati dell'Unione europea (GDPR) è focalizzato sulla protezione dei dati personali e le API sono ora all'avanguardia nel modo con cui questi dati vengono utilizzati e condivisi. Inoltre, la nuova direttiva NIS2 (Network and Information Security) richiede di stabilire nello specifico un solido programma per la sicurezza delle API. Al di fuori dell'UE, paesi come l'Arabia Saudita hanno introdotto leggi per la protezione dei dati simili al GDPR, che introduce obblighi da rispettare per gli enti che si occupano del trattamento di dati personali. Inoltre, nella sezione 6 del nuovo PCI DSS (Payment Card Industry Data Security Standard) v4.0 sono inclusi specificamente nuovi standard sull'utilizzo delle API per lo sviluppo e la manutenzione di sistemi e software al fine di ridurre il rischio di incorrere in problemi di violazione di dati.

Poiché le autorità di regolamentazione governative hanno messo in atto iniziative e policy per rafforzare gli standard in materia di cybersicurezza per le API, è importante comprendere le best practice e le linee guida in modo da poter integrare le API nel proprio programma di sicurezza per migliorare la visibilità, rafforzare i sistemi di difesa e soddisfare i requisiti di conformità.

Per maggiori informazioni, potete consultare il rapporto SOTI globale sulla sicurezza delle API dal titolo Minacce in agguato: le tendenze degli attacchi fanno luce sulle minacce delle API.

Metodologia

Attacchi alle applicazioni web e attacchi bot

Questi dati descrivono gli avvisi a livello di applicazione relativi al traffico osservato tramite la nostra soluzione WAF (Web Application Firewall) e lo strumento di gestione dei bot. Gli avvisi sugli attacchi alle applicazioni web vengono attivati quando si rileva un payload dannoso all'interno di una richiesta a un sito web, un'applicazione o un'API protetta. Gli avvisi sui bot vengono attivati quando si rileva un payload bot all'interno di una richiesta a un sito web, un'applicazione o un'API protetta. Questi avvisi possono essere attivati sia da bot dannosi che non dannosi, e non indicano la corretta riuscita della violazione. Sebbene questi prodotti consentano un alto livello di personalizzazione, i dati qui presentati sono stati raccolti senza prendere in considerazione le configurazioni personalizzate delle proprietà protette. I dati sono stati ricavati da uno strumento interno per l'analisi degli eventi di sicurezza rilevati sull'Akamai Connected Cloud, una rete globale di oltre 4.000 punti di presenza (PoP) sull'edge in più di 130 paesi. I nostri team addetti alla sicurezza utilizzano questi dati, misurati in petabyte al mese, per effettuare ricerche sugli attacchi, segnalare comportamenti dannosi e includere ulteriori informazioni nelle soluzioni Akamai.

I dati inclusi in questo rapporto hanno riguardato un periodo di 12 mesi, dal 1° gennaio al 31 dicembre 2023.

Aggiornamento dei dati nel 2024

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

Informazioni su Akamai API Security

Desideriamo rivolgere un ringraziamento speciale al nostro team di progettazione della soluzione Akamai API Security per il contributo apportato con informazioni reali sui rischi per le API e sul loro potenziale impatto in base ai nostri avvisi sulla sicurezza delle API.

Appendice

Vettore di attacco	Definizione
Sessione attiva	Il traffico degli attacchi è stato recentemente segnalato al client e le richieste ripetute vengono bloccate per tutta la durata della sessione
CMDi (Command injection)	Un criminale inietta nuovi elementi in un comando esistente per modificare l'interpretazione allontanandola dal suo significato originale e rivolgendola verso le azioni desiderate
XSS (Cross-Site Scripting)	Un criminale incorpora script dannosi nei contenuti in modo da farli eseguire al software preso di mira con i privilegi degli utenti quando i contenuti vengono distribuiti ai browser web
Raccolta di dati	Un criminale sfrutta le vulnerabilità di progettazione o configurazione del sistema preso di mira e le sue comunicazioni per rivelare una quantità di informazioni maggiore del previsto; questa operazione viene spesso eseguita per raccogliere i dati in vista di un altro tipo di attacco, ma ottenere l'accesso alle informazioni può essere anche l'obiettivo finale del criminale
Protocollo HTTP	Un criminale sfrutta le vulnerabilità presenti nel protocollo con cui comunicano il client e il server per eseguire azioni impreviste; lo sfruttamento di altri tipi di protocolli può condurre a diversi obiettivi finali degli attacchi
LFI (Local File Inclusion)	Un criminale manipola gli input immessi nel software preso di mira per ottenere l'accesso (ed eventualmente modificare) ad alcune aree del file system che non dovrebbero essere accessibili

Vettore di attacco	Definizione
RFI (Remote File Inclusion)	Un criminale carica ed esegue codice arbitrario remoto, "dirottando" successivamente l'applicazione presa di mira e forzandola ad eseguire le proprie istruzioni
SSRF (Server-Side Request Forgery)	Un criminale abusa della funzionalità del server di leggere o aggiornare le risorse interne
SQLi (Structured Query Language injection)	Un criminale crea stringhe di input in modo che, quando il software preso di mira intende creare affermazioni SQL basate sull'input dell'utente, l'affermazione SQL risultante esegue invece le azioni desiderate dal criminale; i comandi "iniettati" possono causare la divulgazione di informazioni, nonché la possibilità di aggiungere o modificare i dati presenti nel database
WAT (Web Attack Tool)	Un criminale esamina attivamente il sistema preso di mira in modo da ricavare informazioni da poter sfruttare per scopi dannosi; di conseguenza, il criminale riesce ad ottenere informazioni dal sistema preso di mira che lo aiutano a trarre conclusioni sul suo livello di sicurezza e configurazione o sulle potenziali vulnerabilità
WPA (Web Platform Attack)	Un attacco sferrato contro una piattaforma software (cloud, web o applicazione) che non è classificato in un altro gruppo di attacchi

Riconoscimenti

Editoria e stesura

Badette Tribbey - Editor-in-Chief
Charlotte Pelliccia - Lead Writer (regionali)

Collaboratori editoriali

James Casey
Edward Roberts
Steve Winterfeld

Revisione e contributi di esperti del settore

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

Analisi dei dati

Chelsea Tuttle

Marketing ed editoria

Georgina Morales Hampe
Emily Spinks

Altri rapporti sullo stato di Internet - Security

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

Ulteriori informazioni sulla ricerca delle minacce Akamai

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

Accesso ai dati del rapporto

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

Ulteriori informazioni sulle soluzioni Akamai

Per ulteriori informazioni sulle soluzioni Akamai per gli attacchi alle API, visitate la nostra **pagina sulla sicurezza di app e API.**

Data di pubblicazione: 03/24.