SOTI

Volumen 10, número 01

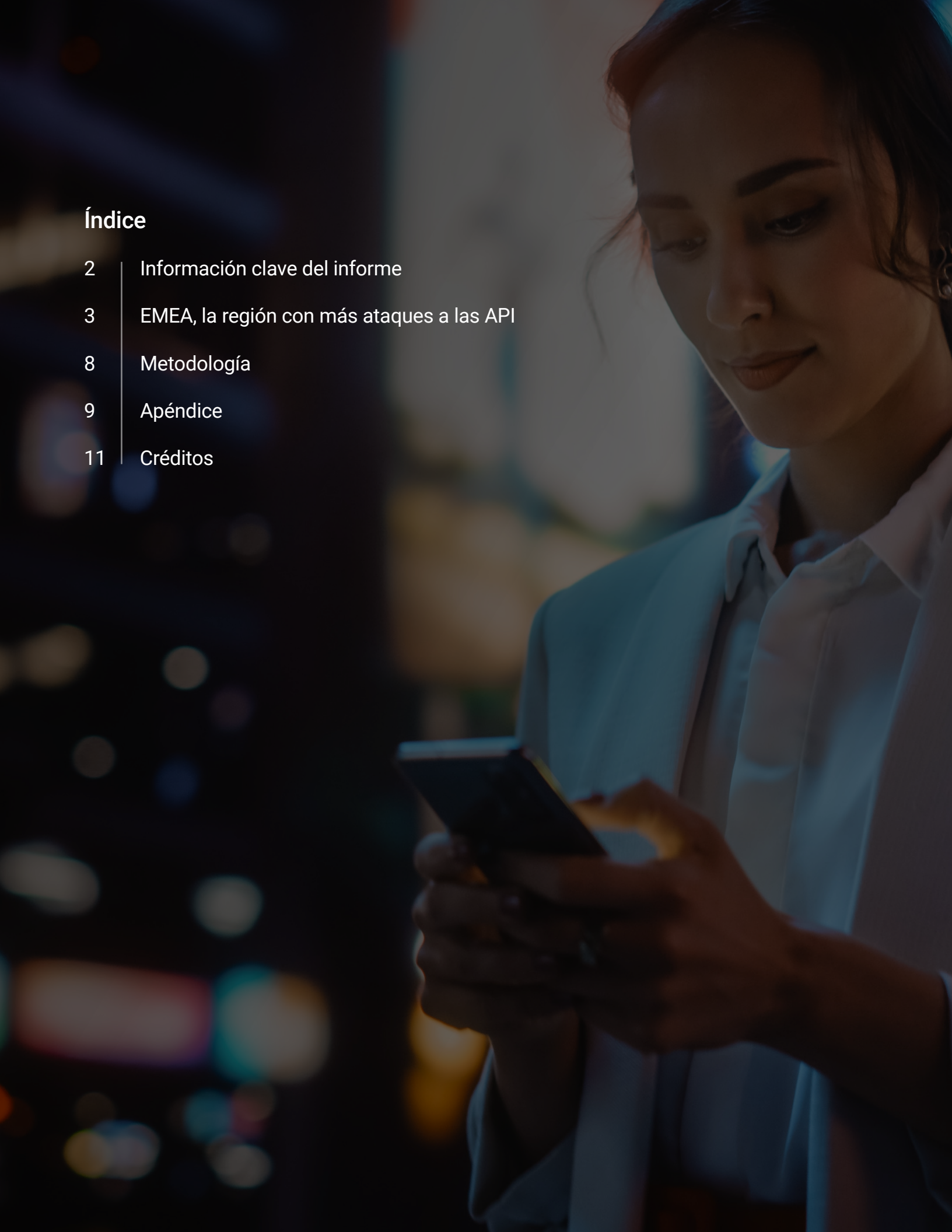
10 YEARS
OF SECURITY INSIGHT

Las tendencias de ataque ponen de relieve las amenazas a las API

Datos de EMEA

Akamai

Estado de Internet en materia de seguridad



Índice

Información clave del informe

Datos de EMEA es un documento complementario a nuestro informe sobre el estado de Internet en materia de seguridad (SOTI) de API Security, más detallado, Al acecho en las sombras: las tendencias de ataque ponen de relieve las amenazas a las API (disponible solo en inglés). En este informe podrá consultar descripciones detalladas de cómo los adversarios aprovechan los vectores de ataque que describimos en él, sugerencias para proteger a su organización, así como una explicación de nuestras metodologías de investigación.

Descripción general

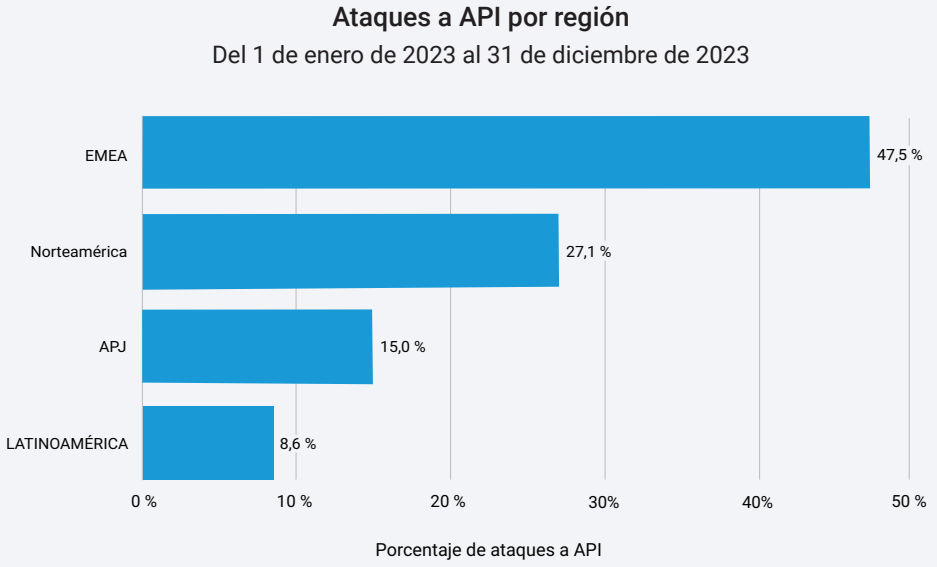
A medida que la innovación digital y la economía de las API mejoran las experiencias de los empleados y los clientes, también representan nuevas oportunidades de explotación para los ciberdelincuentes. Los ataques dirigidos a las API pueden provocar daños financieros, a la marca y a la reputación, así como la pérdida de datos confidenciales y de la confianza de los clientes. Dado el aumento previsto del volumen de ataques a las API y el aumento de las obligaciones de supervisión y notificación de las normativas de ciberseguridad, a medida que las API se utilizan cada vez más para intercambiar información financiera confidencial, la seguridad de estas es más importante que nunca.

Para comprender mejor el panorama de amenazas de las API, en lugar de analizar los ataques a las API y a las aplicaciones web en conjunto, en 2024 utilizamos un nuevo conjunto de datos que permite a los investigadores de Akamai distinguir entre los dos tipos de ataque y centrarse en el porcentaje de ataques dirigidos a las API. En este Datos de EMEA, que abarca los 12 meses desde enero hasta diciembre de 2023, profundizaremos en las tendencias de ataque y cómo pueden afectarle.

- A nivel mundial, la región de Europa, Oriente Medio y África (EMEA) registró el mayor porcentaje de ataques web dirigidos a las API (47,5 %), notablemente superior al de la siguiente región más afectada, Norteamérica (27,1 %).
- En consonancia con la tendencia global, los ataques al protocolo HTTP (HTTP) y de inyección de lenguaje de consulta estructurado (SQLi) han sido los principales vectores en las API de EMEA en los últimos 12 meses.
- Las solicitudes de bots también son motivo de preocupación: el 40 % de los casi cuatro billones de solicitudes sospechosas de bots se dirigió a las API.
- En el sector del comercio, casi tres cuartas partes (74,6 %) de todos los ataques web que afectaron a las organizaciones fueron ataques a las API, más del doble del porcentaje del siguiente sector más afectado, el de la alta tecnología (35,5 %).

EMEA, la región con más ataques a las API

Al aprovechar un nuevo conjunto de datos que realiza un seguimiento específico del tráfico de ataques a las API, la investigación de Akamai reveló que la región de EMEA fue la más afectada. Registró un 47,5 % de todos los ataques dirigidos a las API en todo el mundo, una cifra que supera con creces la de la siguiente región, Norteamérica, con un 27,1 % (EMEA - Figura 1). Estos resultados se basan en el número total de ataques web en cada región y muestran que las API están en mayor peligro en EMEA que en otras regiones.

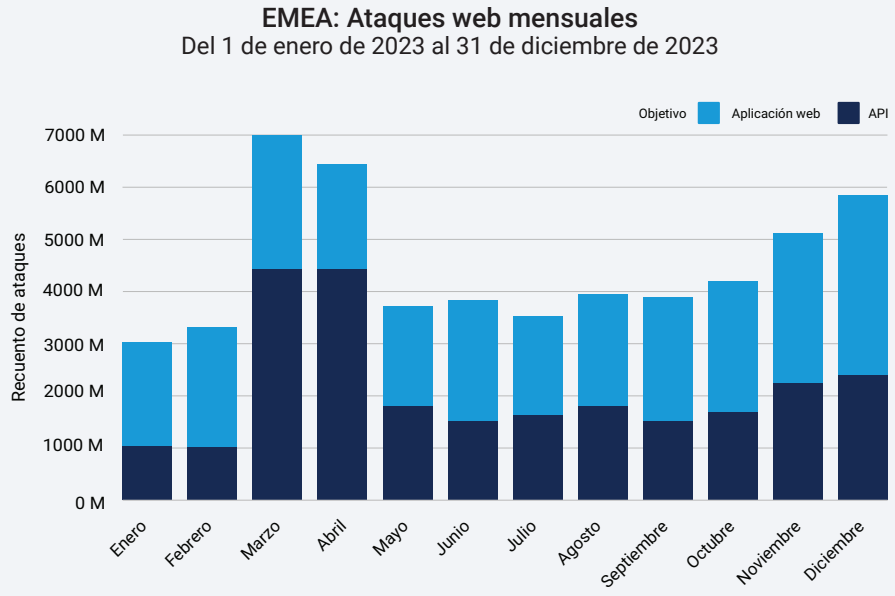


EMEA - Fig. 1: EMEA es la región con más probabilidad de sufrir un ataque web dirigido a las API

Es posible que, en parte, podamos atribuir este porcentaje relativamente alto de ataques en EMEA (en comparación con el porcentaje de ataques en otras regiones) al tamaño relativamente grande del mercado de API abiertas que tiene en comparación con Norteamérica y Asia-Pacífico, lo que refleja unas tasas de adopción de API más altas en EMEA, además de la banca abierta y la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) v4.0 que favorecen el uso de API y pueden introducir los riesgos de seguridad que se analizan en el informe global.

En EMEA, las áreas con el mayor porcentaje de ataques web dirigidos a las API han sido España (94,8 %), Portugal (84,5 %), Países Bajos (71,9 %) e Israel (67,1 %). Esto no quiere decir que el número de ataques web en general sea mayor en estos países que en otros de la región EMEA, sino que estos países se enfrentan a un riesgo mucho más centrado en el abuso de las API debido al interés de los atacantes en ese vector.

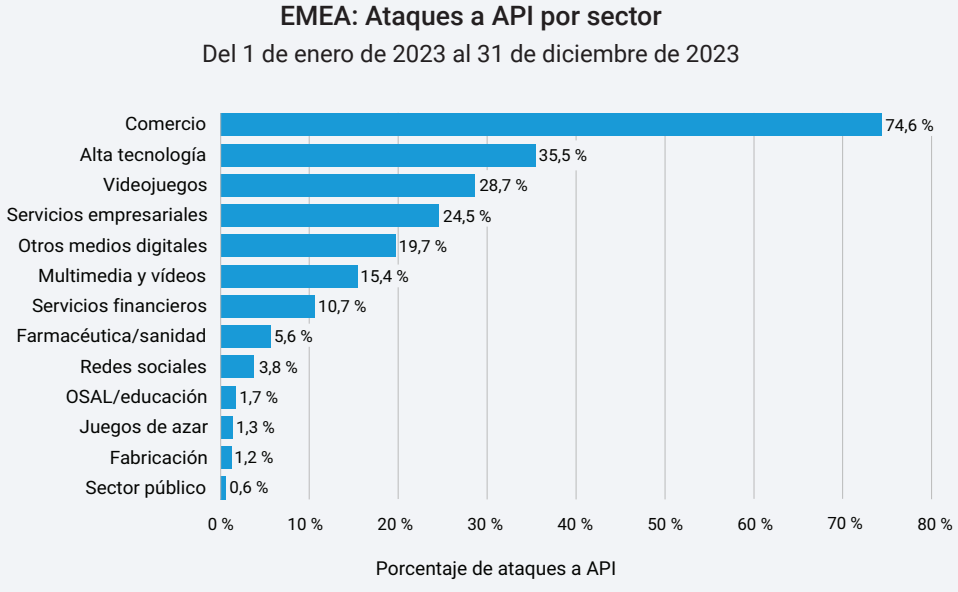
Las tendencias mensuales durante el periodo analizado entre enero y diciembre de 2023 muestran que los ataques web dirigidos a las API en EMEA aumentaron de forma bastante constante, ya que comenzaron con un 34 % en enero y aumentaron al 41 % a finales de año (EMEA - Figura 2). Las excepciones tuvieron lugar en marzo y abril, los meses en los que los investigadores de Akamai observaron un aumento en los ataques a las API, ya que el sector del comercio en España, un país con una concentración ya enorme de ataques a las API, experimentó ataques centrados a gran escala. Este aumento muestra la rapidez con la que los atacantes pueden cambiar su interés entre regiones y sectores, por lo que merece la pena realizar un seguimiento de las tendencias más amplias.



EMEA - Fig. 2: Con la excepción de marzo y abril, cuando los ataques a las API aumentaron, los ataques a las API aumentaron lentamente a lo largo de 2023, representando el 41 % de todos los ataques a finales de año.

Ataques a las API en distintos sectores

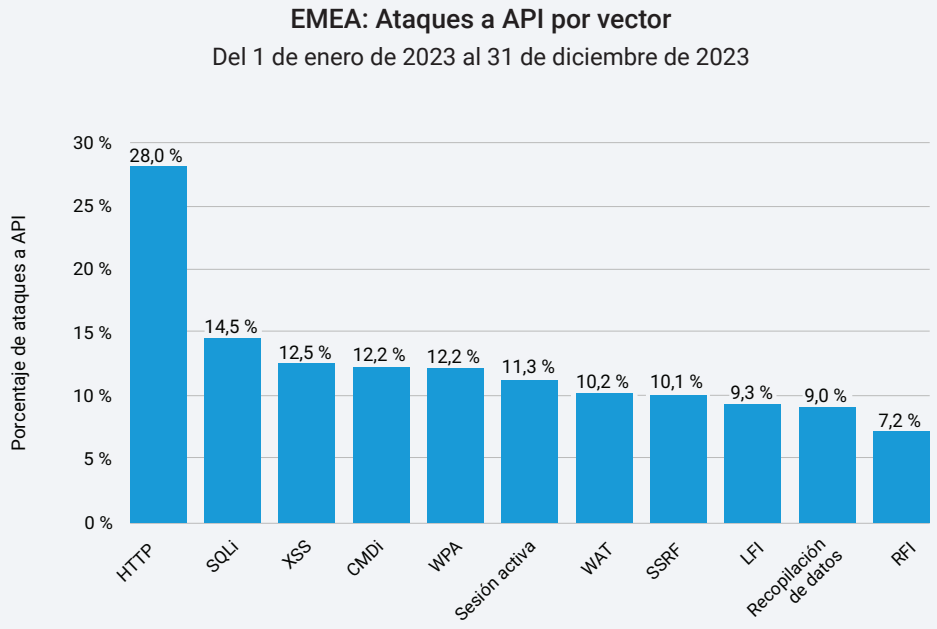
Durante el periodo analizado, los investigadores de Akamai observaron los mayores picos en el comercio, que asumió el 74,6 % de ataques web en general, más del doble que el siguiente sector más afectado, el de la alta tecnología, con un 35,5 %. Les siguieron los sectores de los videojuegos con un 28,7 %, el de los servicios empresariales con un 24,5 % y el de otros medios digitales con un 19,7 % (EMEA - Figura 3).



EMEA - Fig. 3: El sector del comercio tuvo el mayor porcentaje de ataques a las API, en parte por la compleja naturaleza de su ecosistema, por su gran dependencia de las API y por los valiosos datos que poseen estas organizaciones.

API atacadas: análisis del tráfico

En consonancia con la tendencia global, los ataques de HTTP y SQLi han sido las formas predominantes en las que los adversarios se han dirigido a las API en EMEA durante los últimos 12 meses, y la inclusión de archivos locales (LFI) ha descendido más en la lista en comparación con su predominio en los ataques a aplicaciones web (EMEA - Figura 4).



EMEA - Fig. 4: HTTP, SQLi y XSS son los vectores más relevantes para los ataques a las API; LFI es menos frecuente para los ataques a las API, pero se sigue utilizando activamente para los ataques contra aplicaciones web.

En la región de EMEA, los scripts entre sitios (XSS) siguen siendo la técnica preferida, incluso para lanzar ataques a las API, y la inyección de comandos (CMDi) también es frecuente. El nuevo conjunto de datos nos permite supervisar vectores de ataque adicionales en las API. Por ejemplo, la falsificación de solicitudes del lado del servidor (SSRF, de la que hablamos en nuestro informe de 2023) es ahora un vector emergente. (Consulte el apéndice para obtener una lista completa de definiciones de vectores de ataque).

Nuestra investigación también reveló que las solicitudes de bots son un área de preocupación. Durante el periodo analizado de 12 meses, el 40 % de los casi cuatro billones de solicitudes sospechosas de bots se dirigió a API.

Conclusión

La defensa de las API es fundamental desde el punto de vista de la seguridad y la gestión de riesgos. Además, las leyes y normativas existentes, y las reformas emergentes para que la legislación sobre ciberseguridad se mantenga al día con el panorama de amenazas también hacen que sea imprescindible proteger las API.

Por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea se centra en la protección de los datos personales, y las API están ahora a la vanguardia de la forma en que se utilizan y comparten estos datos. Además, la nueva Directiva sobre Seguridad de las Redes y los Sistemas Informáticos (NIS2) exige específicamente el establecimiento de un programa de seguridad de las API sólido. Fuera de la UE, países como Arabia Saudí han adoptado leyes de protección de datos similares al RGPD de la UE, que imponen obligaciones para las entidades que gestionan datos personales. Además, la sección 6 de la próxima norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) v4.0 incluye específicamente nuevos estándares sobre el uso de las API en el desarrollo y mantenimiento de sistemas y software para reducir el riesgo de vulneración de los datos.

A medida que los reguladores ponen en práctica iniciativas y políticas para reforzar los estándares en materia de ciberseguridad, es importante que sepa cuáles son las prácticas recomendadas y las directrices para que pueda integrar las API en su programa de seguridad con el fin de mejorar la visibilidad, reforzar las defensas y adaptarse a los requisitos de cumplimiento.

Para obtener más información, consulte el informe SOTI de seguridad de las API, Al acecho en las sombras: las tendencias de ataque ponen de relieve las amenazas a las API.

Metodología

Ataques a aplicaciones web y ataques de bots

Estos datos describen las alertas en la capa de aplicación sobre el tráfico observado a través de nuestro firewall de aplicaciones web (WAF) y la herramienta de gestión de bots. Las alertas de ataques contra aplicaciones web se activan cuando detectamos una carga maliciosa en una solicitud a un sitio web, una aplicación o una API protegidos. Las alertas de bots se activan cuando detectamos una carga de bots en una solicitud a un sitio web, una aplicación o una API protegidos. Estas alertas de bots las pueden activar tanto bots maliciosos como bots legítimos. Las alertas no indican que un ataque haya conseguido su objetivo. Aunque estos productos permiten un alto nivel de personalización, recopilamos los datos presentados aquí de una manera que no tiene en cuenta las configuraciones personalizadas de las propiedades protegidas. Los datos se extrajeron de una herramienta interna de análisis de eventos de seguridad detectados en Akamai Connected Cloud, una red de más de 4000 puntos de presencia en el Edge en más de 130 países. Nuestros equipos de seguridad utilizan estos datos, medidos en petabytes mensuales, para investigar ataques, detectar comportamientos maliciosos y proporcionar información adicional a las soluciones de Akamai.

Los datos de este informe cubren el periodo de 12 meses que abarca desde el 1 de enero de 2023 hasta el 31 de diciembre de 2023.

Actualización de datos de 2024

Nos complace anunciar algunas actualizaciones de nuestros conjuntos de datos para nuestro décimo aniversario. Nuestros conjuntos de datos de ataques a aplicaciones web y ataques de bots han recibido algunas actualizaciones. El método de recopilación de cada uno de ellos se ha transformado, agilizado y optimizado. Se ha ampliado el alcance y el nivel de detalle de nuestra perspectiva. Se han agregado clasificaciones para vectores de ataque adicionales, como SSRF. También se ha agregado a cada conjunto de datos la identificación de los ataques dirigidos a los terminales de API. Hemos disfrutado describiendo algunas de estas nuevas mejoras en este informe y nos complace seguir compartiendo estas actualizaciones a lo largo del año (y más adelante) al tiempo que celebramos este hito sobre el estado de Internet en materia de seguridad con nuestros lectores.

Información sobre API Security de Akamai

Queremos mostrar nuestro agradecimiento especial a nuestro equipo de ingeniería de soluciones de API Security de Akamai por sus aportaciones de información del mundo real centradas en los riesgos de las API y el posible impacto que tienen según nuestras alertas de API Security.

Apéndice

Vector de ataque	Definición
Sesión activa	El tráfico de ataque se ha marcado recientemente para el cliente y las solicitudes repetidas se bloquearán durante el tiempo que dure la sesión.
Inyección de comandos (CMDi)	Un adversario inyecta nuevos elementos en un comando existente para modificar la interpretación con el fin de alejarla de su significado original y hacia acciones de su elección.
Scripts entre sitios (XSS)	Un adversario incrusta scripts maliciosos en el contenido para que el software al que va dirigido el ataque ejecute los scripts con los niveles de privilegios de los usuarios cuando el contenido se envía a los navegadores web.
Recopilación de datos	Un adversario aprovecha las debilidades en el diseño o configuración del objetivo del ataque y sus comunicaciones para conseguir que revele más información de la prevista; este ataque a menudo se ejecuta para recopilar datos en preparación para otro tipo de ataque, pero obtener acceso a la información también puede ser el objetivo final del adversario.
Protocolo HTTP (HTTP)	Un adversario aprovecha las debilidades del protocolo mediante el cual un cliente y un servidor se comunican para realizar acciones inesperadas; la explotación de diferentes tipos de protocolos puede conducir a diferentes objetivos finales de los ataques.
Inclusión de archivos locales (LFI)	Un atacante manipula las entradas en el software al que va dirigido el ataque para obtener acceso a áreas del sistema de archivos que no estaban destinadas a que fueran accesibles, y tal vez modificarlas.

Vector de ataque	Definición
Inclusión remota de archivos (RFI)	El adversario carga y ejecuta código arbitrario remoto, secuestrando posteriormente la aplicación a la que va dirigido el ataque y forzándola a ejecutar sus propias instrucciones.
Falsificación de solicitudes del lado del servidor (SSRF)	El atacante abusa de la funcionalidad del servidor para leer o actualizar recursos internos.
Inyección de lenguaje de consulta estructurado (SQLi)	Un atacante diseña las cadenas de entrada para que cuando el software al que va dirigido el ataque intente crear instrucciones SQL basadas en la entrada del usuario, la instrucción SQL resultante realice en su lugar las acciones que el atacante pretendía; las inyecciones correctas pueden provocar la divulgación de información, así como la capacidad de agregar o modificar datos en la base de datos.
Herramienta de ataques web (WAT)	Un adversario rastrea activamente el objetivo del ataque de una manera diseñada para solicitar información que podría aprovecharse con fines maliciosos; como resultado de estos rastreos, el adversario puede obtener información del objetivo del ataque que ayuda al atacante a hacer inferencias sobre su seguridad, configuración o posibles vulnerabilidades.
Ataque de plataforma web (WPA)	Un ataque contra una plataforma de software (nube, web o capa de aplicación) que no está clasificado en ningún otro grupo de ataques.

Créditos

Editorial y redacción

Badette Tribbey – Editora jefe
Charlotte Pelliccia – Redactora principal (regional)

Colaboradores editoriales

James Casey
Edward Roberts
Steve Winterfeld

Revisión y expertos en la materia

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

Análisis de datos

Chelsea Tuttle

Marketing y publicación

Georgina Morales Hampe
Emily Spinks

Más información sobre el estado de Internet en materia de seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai y entérese de cuándo se publican los siguientes números. **akamai.com/soti**

Más información acerca de la investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad. **akamai.com/security-research**

Acceda a los datos de este informe

Vea versiones de alta calidad de los gráficos a los que se hace referencia en este informe. Puede usar estas imágenes y hacer referencia a ellas libremente, siempre que se cite debidamente a Akamai como fuente y que se conserve el logotipo de Akamai. **akamai.com/sotidata**

Más información sobre las soluciones de Akamai

Para obtener más información sobre las soluciones de Akamai para combatir los ataques a las API, visite nuestra **página de seguridad de aplicaciones y API**.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn.
Publicado el 24 de marzo.