SOTI

Volumen 10, número 04

10 YEARS
OF SECURITY INSIGHT

Amenazas a las arquitecturas de aplicaciones modernas

Datos de EMEA

Akamai

Estado de Internet / Seguridad

Índice

Información clave del informe

Datos de EMEA es un documento complementario a nuestro informe sobre el estado de Internet (SOTI) en materia de seguridad de las aplicaciones, más detallado, Fortalezas digitales en peligro: amenazas a las arquitecturas de aplicaciones modernas (disponible solo en inglés). En este informe podrá consultar descripciones detalladas de cómo los adversarios explotan una superficie de ataque creciente y sugerencias para proteger su empresa, así como una explicación de nuestras metodologías de investigación.

Descripción general

En las últimas dos décadas, las aplicaciones web han crecido exponencialmente tanto en número como en capacidades, lo que ha agilizado las operaciones empresariales, ha mejorado la experiencia del cliente y ha impulsado el crecimiento a través de funciones como la comunicación en tiempo real, el análisis de datos y la automatización de procesos. Las API, la base de la comunicación entre las aplicaciones, también han proliferado y ahora están preparadas también para dar un gran salto.

Las aplicaciones dirigen casi todos los aspectos de las empresas, facilitando así billones de conexiones, pero también haciéndolas más vulnerables a los ataques. En este Datos de EMEA, que abarca desde enero de 2023 hasta junio de 2024, adoptaremos un enfoque holístico de las amenazas que afectan a las aplicaciones, incluidos los ataques web, los ataques distribuidos de denegación de servicio (DDoS) y las amenazas a cargas de trabajo esenciales, y nos centraremos en cómo pueden afectarle.

El número de ataques DDoS a las capas 3 y 4 creció de forma constante en la región de Europa, Oriente Medio y África (EMEA), y superó la cifra registrada en Norteamérica en cinco de los últimos siete meses. El sector de los servicios financieros se llevó la peor parte en cuanto a estos ataques.

Los ataques mensuales a API y aplicaciones web en EMEA experimentaron una tendencia al alza durante este periodo, con un crecimiento del 21 % entre el primer trimestre de 2023 y el de 2024. Además, los ataques dirigidos a API supusieron de media el 40 % del total de ataques web mensuales.

El comercio fue el sector más afectado por los ataques web en EMEA, con muchos ataques a API, y también por los ataques DDoS a la capa 7.

La preocupación por el ransomware y otros ataques a las aplicaciones y sus cargas de trabajo internas es cada vez mayor. Las empresas están recurriendo a la microsegmentación basada en software con el fin de obtener la visibilidad y los controles detallados necesarios para proteger esta creciente superficie de ataque.

Las aplicaciones web y API: el entorno ideal para los riesgos de seguridad

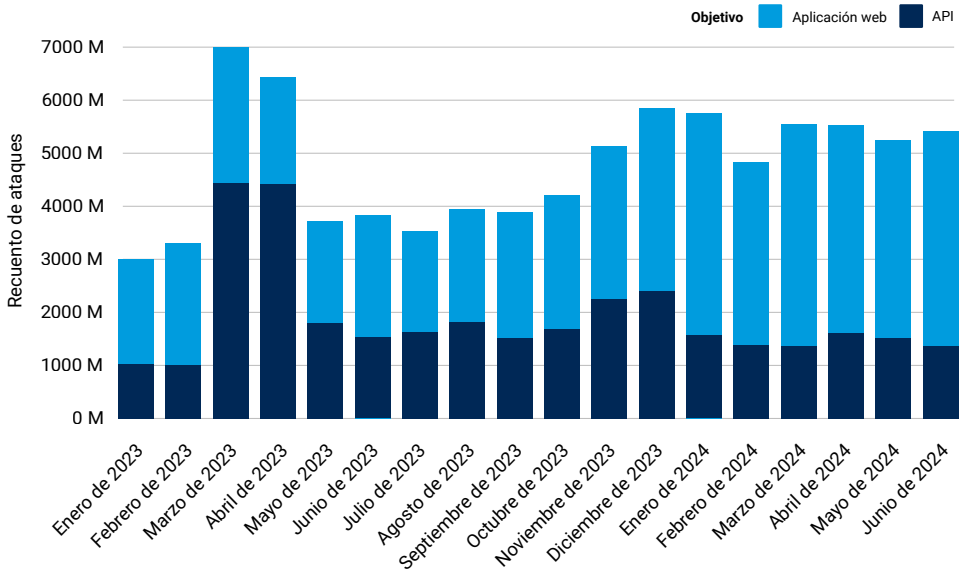
Los ataques a API y aplicaciones web aumentan a medida que las organizaciones se apresuran a implementar aplicaciones con el fin de mejorar la experiencia del cliente e impulsar los resultados empresariales. Los atacantes están aprovechando las vulnerabilidades de esta superficie de ataque (por ejemplo, aplicaciones web con una codificación incorrecta y defectos de diseño, o vulnerabilidades de varios años de antigüedad). Además, la rápida expansión de la economía de las API ha presentado a los ciberdelincuentes nuevas oportunidades de explotación de vulnerabilidades y abuso de la lógica empresarial.

Las tendencias de ataque en cifras

En nuestro primer informe SOTI de 2024, examinamos las tendencias de ataques a API en 2023 en el contexto general de los ataques a aplicaciones web. Al analizar los últimos 18 meses, desde enero de 2023 hasta junio de 2024, los investigadores de Akamai descubrieron que los ataques mensuales a API y aplicaciones web en EMEA crecieron un 21 % desde el primer trimestre de 2023 hasta el de 2024 y que, además, el total de ataques siguió siendo alto durante el segundo trimestre de 2024. Los ataques a las API contribuyeron a mantener ese nivel de actividad, suponiendo de media el 40 % del total de ataques web mensuales durante ese periodo (EMEA - Figura 1).

EMEA: ataques mensuales a las API y aplicaciones web

Del 1 de enero de 2023 al 30 de junio de 2024

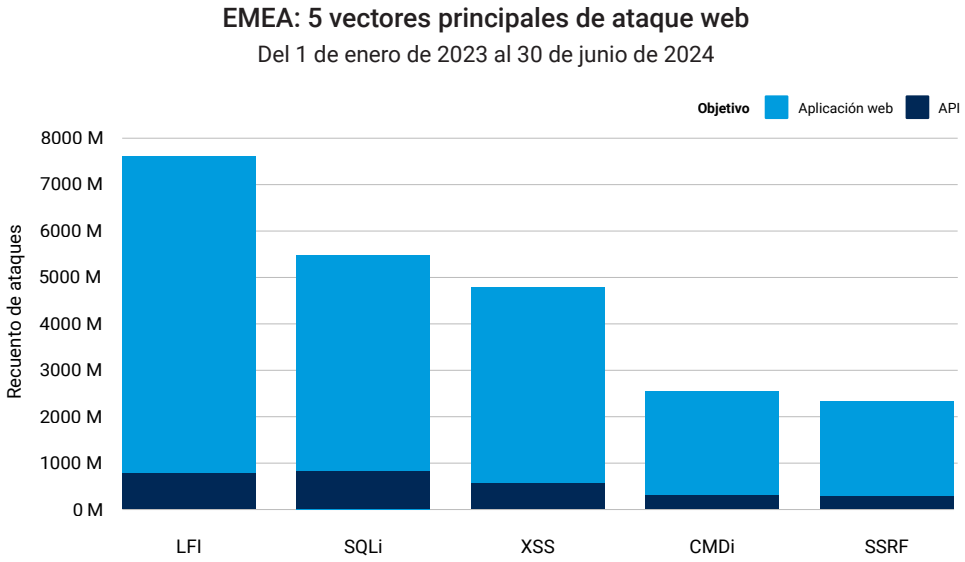


EMEA - Fig. 1: El número de ataques mensuales a API y aplicaciones web sigue siendo alto en 2024 (NOTA: El incremento de los ataques a API está relacionado con el sector del comercio de España, un país que ya cuenta con un gran volumen de ataques a API).

En EMEA, el Reino Unido (20 500 millones), los Países Bajos (15 600 millones) y España (12 700 millones) fueron los que sufrieron más ataques a aplicaciones web y API, seguidos de Alemania (8700 millones), Austria (7400 millones), Francia (4800 millones), Israel (3000 millones), Italia (2700 millones), Suiza (2500 millones) y Bélgica (2300 millones).

Akamai también realiza un seguimiento de varios vectores de ataque web. En este informe, nos centraremos en los cinco métodos tradicionales de ataque basados en vectores más importantes.

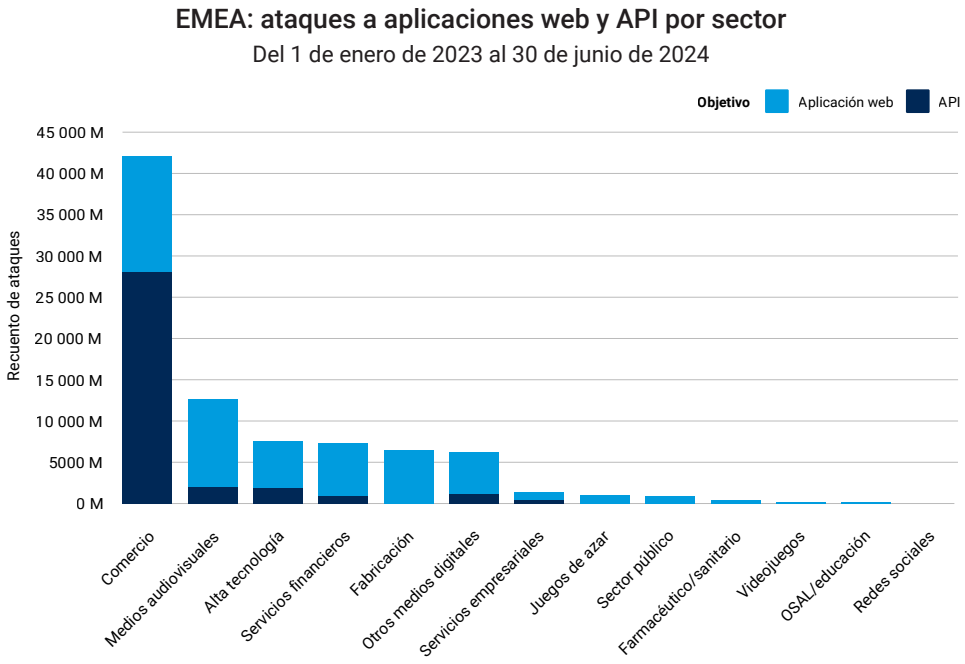
De acuerdo con los informes anteriores, la inclusión de archivos locales (LFI) siguió siendo uno de los principales vectores de ataque, pero otros, como la inyección de lenguaje de consulta estructurado (SQLi) y los scripts entre sitios (XSS), también son motivo de preocupación (EMEA - Figura 2).



EMEA - Fig. 2: LFI, SQLi y XSS están impulsando el crecimiento de los ataques a aplicaciones web y API.

No es raro que los atacantes utilicen tácticas tradicionales como LFI y SQLi para acceder a los datos de sus objetivos. Además, LFI permite a los atacantes abrirse paso y ejecutar código de forma remota, lo que pone en peligro su seguridad.

En sintonía con la tendencia observada en los informes anteriores, los sectores del comercio y de medios audiovisuales fueron los más afectados por los ataques a aplicaciones web y API en EMEA. Además, como comentamos en nuestro informe SOTI de seguridad de las API, el comercio siguió experimentando el porcentaje de ataques a API más alto en comparación con los otros sectores de la región (EMEA - Figura 3).



EMEA - Fig. 3: Debido al elevado porcentaje de ataques a API, el comercio fue el sector más afectado por los ataques web, seguido por el de medios audiovisuales, la alta tecnología y los servicios financieros.

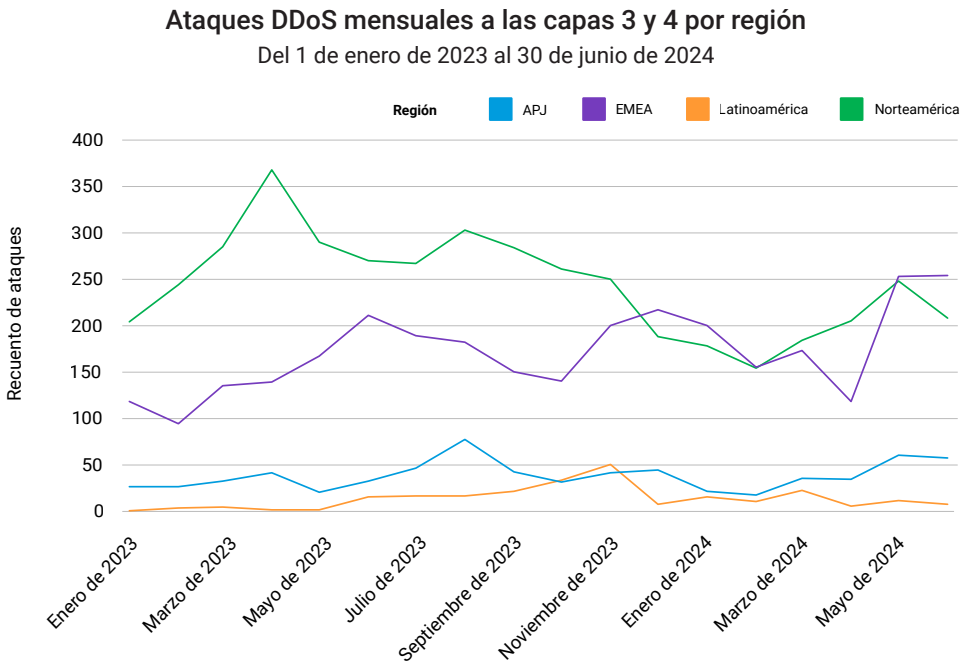
Los ataques DDoS comprometen el tiempo de actividad de las aplicaciones

A medida que la superficie de ataque continúa creciendo, también lo hacen los tipos de ataque DDoS que afectan a las aplicaciones. Como se explica en mayor detalle en el informe SOTI global, los ataques DDoS a la infraestructura tradicional (capa 3 y capa 4) son los más antiguos y tienen como objetivo saturar la capacidad de la red o del servidor de aplicaciones. Los ataques DDoS a la capa de aplicación (capa 7) explotan las vulnerabilidades, las brechas y los defectos de la lógica empresarial de dicha capa. Pueden causar daños importantes incluso con una cantidad relativamente pequeña de tráfico malicioso. Independientemente del vector de ataque, el impacto de un ataque DDoS es el tiempo de inactividad de las aplicaciones.

En el último informe SOTI de EMEA en 2024, se investigaron a fondo los tipos de ataques DDoS y las tendencias de la región. En este, incluimos algunos datos actualizados que demuestran el continuo aumento de las amenazas DDoS en las capas 3, 4 y 7, a la infraestructura que sirve de base a las aplicaciones, así como a las propias aplicaciones.

Los ataques DDoS a la infraestructura

Durante el periodo de 18 meses que abarca el informe, desde enero de 2023 hasta junio de 2024, los investigadores de Akamai descubrieron que el número de ataques DDoS a las capas 3 y 4 creció de forma constante en EMEA, superando el total de ataques DDoS mensuales en Norteamérica en cinco de los últimos siete meses (EMEA - Figura 4).



EMEA - Fig. 4: Las cifras mensuales de ataques DDoS a las capas 3 y 4 en EMEA superaron a las de Norteamérica durante cinco de los últimos siete meses.

Dentro de EMEA, los países más afectados por los ataques DDoS a las capas 3 y 4 fueron Arabia Saudita (957) y el Reino Unido (576), seguidos por Suiza (240), Turquía (205), Italia (203), Alemania (189) y Polonia (115).

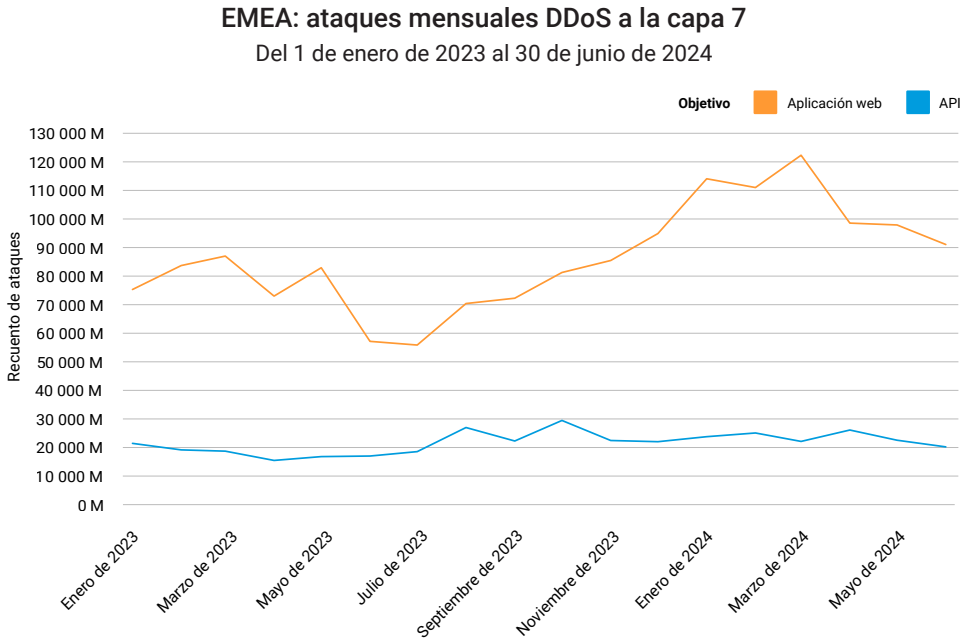
Como se describe en nuestro informe SOTI de EMEA, los ataques DDoS son una estrategia recurrente de los hacktivistas y los atacantes que cuentan con el respaldo financiero de los gobiernos, todos ellos motivados por ciertos intereses políticos. Además, las guerras entre Rusia y Ucrania e Israel y Hamás han provocado un aumento de los ataques.

Al analizar por sectores, descubrimos que las empresas que pertenecen al ámbito de los servicios financieros (1523) y la fabricación (890) experimentaron el mayor número de ataques DDoS a las capas 3 y 4, seguidas de las de la industria de los videojuegos (189), el comercio (151), los juegos de apuestas (105) y la alta tecnología (95).

Ataques DDoS a la capa de aplicación

Además de los ataques DDoS a las capas 3 y 4, la región también sufrió ataques DDoS a la capa de aplicación (capa 7). Durante los 18 meses comprendidos entre enero de 2023 y junio de 2024, nuestros investigadores descubrieron que EMEA fue la tercera región más afectada por los ataques DDoS a la capa 7, con 1,9 billones frente a 8,7 billones en Norteamérica y 5,1 billones en APJ.

Aunque este número sea menor que en otras regiones, cabe destacar que los ataques DDoS a la capa 7 están aumentando en EMEA. Tras descender en mayo de 2023 hasta los 74 000 millones, los ataques DDoS mensuales a la capa 7 adoptaron una tendencia ascendente destacable, hasta casi duplicarse en marzo de 2024, antes de finalizar el segundo trimestre de 2024, con una media mensual de 119 000 millones de ataques dirigidos a aplicaciones web y API (EMEA - Figura 5).

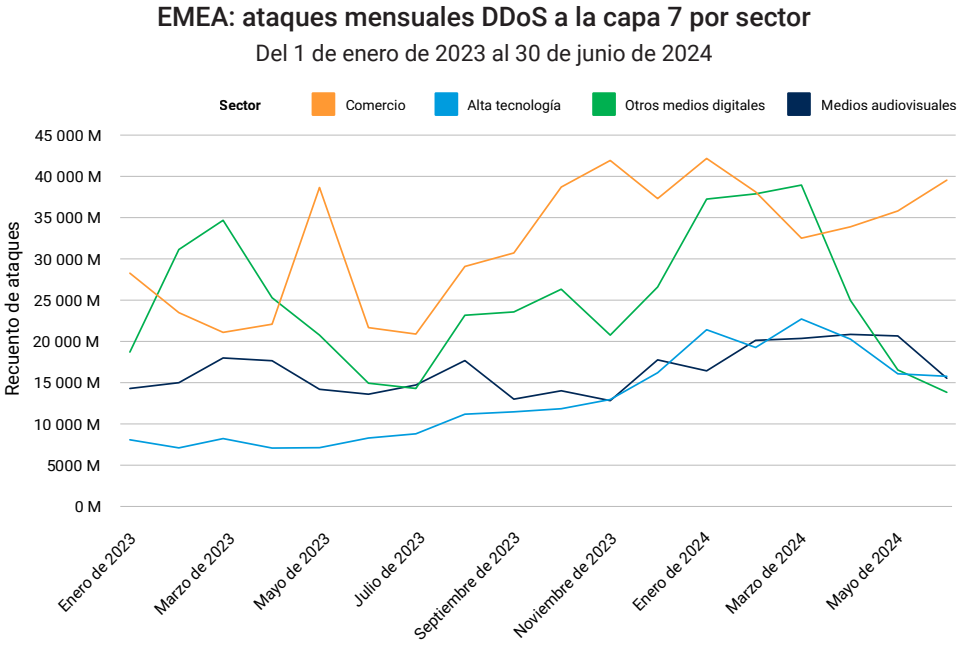


EMEA - Fig. 5: Desde junio de 2023, los ataques DDoS a la capa 7 han aumentado significativamente, llegando a una media mensual de 119 000 millones de ataques al final del segundo trimestre de 2024.

Durante este periodo, los ataques DDoS dirigidos a API se mantuvieron bastante estables y representaron el 25 % del total de ataques. Por lo tanto, además de tener que defenderse de los vectores de ataque mencionados anteriormente con respecto a los ataques a aplicaciones web y API (consulte EMEA - Figura 2), proteger las API frente a los ataques DDoS es esencial, sobre todo porque las directivas y las normativas siguen fomentando su uso.

En EMEA, las áreas con el mayor número de ataques DDoS a la capa 7 fueron Alemania (461 000 millones) y el Reino Unido (366 000 millones), seguidas por Suecia (167 000 millones), Israel (151 000 millones), Italia (125 000 millones), Malta (113 000 millones), Suiza (112 000 millones), Francia (90 000 millones), Países Bajos (79 000 millones) y España (77 000 millones).

Al analizar los sectores, observamos que el comercio fue el más afectado por los ataques DDoS de capa 7 al inicio y al final del periodo, seguido de otros medios digitales, los medios audiovisuales y la alta tecnología (EMEA - Figura 6).



EMEA - Fig. 6: El sector del comercio fue el más afectado por los ataques DDoS a la capa 7.

Los atacantes se centran en las cargas de trabajo de las aplicaciones

Normalmente, se habla de Zero Trust en el contexto de la seguridad de red. Sin embargo, las aplicaciones web y sus cargas de trabajo internas también pueden verse expuestas a amenazas como el ransomware, que busca la forma de infiltrarse y alcanzar a sus objetivos.

Como se explica en detalle en el informe global, para que las aplicaciones funcionen, ya sea en la nube, de forma local o en un entorno híbrido, todas las cargas de trabajo individuales deben funcionar de forma fluida. Las cargas de trabajo atraviesan diferentes jurisdicciones de seguridad a medida que se mueven por la red, por lo que cualquiera de ellas podría abrir la puerta a un intruso. Proteger esta creciente superficie de ataque es fundamental para reforzar la estrategia de seguridad general, pero complica aún más el trabajo de los equipos de seguridad, ya de por sí muy difícil.

La implementación de un marco Zero Trust a partir de un enfoque tradicional definido por hardware requiere mucho tiempo y recursos, además de un tiempo de inactividad. Es más, también es necesario tener una estrategia de microsegmentación para protegerse ante el ransomware o ataques contra las propias cargas de trabajo.

La microsegmentación definida por software es fácil y rápida de implementar y utilizar, por lo que puede incluso servir como medida de respuesta ante incidentes y como punto de control para aislar los sistemas esenciales de acuerdo con las normativas. Además. proporciona una imagen exhaustiva de la red y controles de gestión extremadamente detallados. Teniendo en cuenta estas ventajas, las empresas están recurriendo cada vez más a este enfoque para detectar cargas de trabajo o contenedores en peligro en sus entornos de centros de datos dinámicos, nube y nube híbrida, y mitigar esas amenazas.

Ejemplos reales sobre la protección de cargas de trabajo de aplicaciones

En esta sección, presentaremos dos casos prácticos de la región de EMEA que ejemplifican cómo las empresas protegen las cargas de trabajo esenciales y avanzan hacia el modelo Zero Trust.

Caso práctico de EMEA n.º 1: Para proteger los sistemas más importantes y los datos confidenciales relacionados con las operaciones comerciales y los pagos, el director de seguridad de la información (CISO) de un banco de inversión líder revisa periódicamente su infraestructura tecnológica para reforzar la estrategia de seguridad de todos sus dominios. La detención de los ataques de ransomware es primordial, al igual que la escalabilidad y la cobertura de los diferentes sistemas operativos y entornos de nube. Además, el CISO quería reducir la superficie de ataque sin incurrir en los costes y retrasos relacionados con la actualización de los firewalls heredados. Las cargas de trabajo de aplicaciones se acordonaron individualmente al aplicar una estrategia de microsegmentación basada en software, que crea zonas seguras en los entornos de los centros de datos. Si una carga de trabajo sufre un ataque, esta se puede aislar, lo que evita que el software malicioso se extienda a través de la red.

Caso práctico de EMEA n.º 2: Un proveedor de software y medios necesitaba una forma más sencilla de fortalecer su marco Zero Trust para proteger mejor las cargas de trabajo básicas y los datos de los clientes. Para lograr esta mejora, era imprescindible separar los componentes de gran valor, como los sistemas de gestión de identidades y planificación de recursos empresariales, mediante políticas de segmentación precisas. El objetivo era minimizar el tráfico entrante y saliente, y reforzar las políticas de acceso en cientos de servidores empresariales. Al mismo tiempo, la empresa quería evitar realizar cambios importantes en el ecosistema que pudieran causar interrupciones y aumentar el riesgo de seguridad. Adoptar un enfoque de microsegmentación basado en software con una visibilidad detallada de los patrones de interacción y las alertas permitió al equipo al equipo contar con funciones para evitar el movimiento lateral malicioso en toda la red.

Conclusión

En este Datos de EMEA, hemos tratado de dar una visión general de cómo los atacantes pueden comprometer sus aplicaciones y API. Desde el punto de vista de la seguridad y la gestión de riesgos, es imprescindible que las empresas comprendan las amenazas a las aplicaciones, las API, la infraestructura y las cargas de trabajo esenciales, y se defiendan ante ellas. Además, estamos obligados a proteger las aplicaciones por ley.

Dentro de EMEA, en la Unión Europea, las principales legislaciones relacionadas con este tema son la Directiva actualizada relativa a la Seguridad de las Redes y Sistemas de Información (NIS2), la Ley de Resiliencia Operativa Digital, la Ley de Resiliencia Cibernética, el Programa Europeo para la Protección de las Infraestructuras Críticas, la nueva Norma de Seguridad de Datos del Sector de las Tarjetas de Pago v4.0 y la segunda Directiva sobre Servicios de Pago de la UE (PSD3).

Las aplicaciones son más importantes que nunca para las empresas, pero también son más vulnerables a los ataques. Con las funciones y las prácticas recomendadas para abordar los retos que supone una superficie de ataque en constante expansión, las empresas pueden proteger las aplicaciones que desarrollan en cualquier lugar y en todo momento, sin comprometer el rendimiento ni la experiencia del cliente.

Para obtener más información, consulte el informe SOTI global sobre la seguridad de las aplicaciones, "Fortalezas digitales en peligro: amenazas a las arquitecturas de aplicaciones modernas".

Metodología

Ataques DDoS a la capa 7 y a aplicaciones web

Estos datos describen las alertas en la capa de aplicación sobre el tráfico observado a través de nuestro firewall de aplicaciones web (WAF). 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 DDoS a la capa 7 se activan cuando detectamos anomalías volumétricas en el número de solicitudes a un sitio web, una aplicación o una API protegidos. Estas alertas las pueden activar tanto bots maliciosos como bots legítimos. Normalmente, las solicitudes son legítimas, pero el gran volumen de solicitudes indica intenciones maliciosas. 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 aproximadamente 340 000 servidores repartidos entre más de 4000 centros, casi 1300 redes y 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.

Estos datos cubren el periodo de 18 meses que abarca desde el 1 de enero de 2023 hasta el 30 de junio de 2024.

Actualización de datos de 2024

Nos complace anunciar algunas actualizaciones de nuestros conjuntos de datos para nuestro décimo aniversario. Hemos mejorado nuestro conjunto de datos de ataques a aplicaciones web y el método de recopilación se ha transformado, agilizado y optimizado. Además, 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 al 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.

DDoS (capas 3 y 4)

Akamai Prolexic Routed defiende a las organizaciones de los ataques DDoS y otro tipo de tráfico no deseado o malicioso deteniéndolos antes de que lleguen a las aplicaciones, los centros de datos y las infraestructuras de Internet en la nube o híbridas (públicas o privadas), incluidos todos los puertos y protocolos. Los expertos del centro de control de operaciones de seguridad (SOCC) de Akamai pueden adaptar los controles de mitigación proactivos para detectar y detener los ataques al instante, y realizan análisis en tiempo real del tráfico restante para implementar medidas de mitigación adicionales si es necesario. Estos ataques mitigados se organizan y agrupan en eventos de ataques, y el SOCC registra todos los datos asociados para analizarlos.

Estos datos cubren el periodo de 18 meses que abarca desde el 1 de enero de 2023 hasta el 30 de junio de 2024.

Créditos

Director de investigación

Mitch Mayne

Editorial y redacción

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Revisión y expertos en la materia

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

Análisis de datos

Chelsea Tuttle

Materiales promocionales

Barney Beal

Marketing y publicación

Georgina Morales
Emily Spinks

Más informes SOTI/ 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 investigaciones 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 y las aplicaciones, visite nuestra página de seguridad de aplicaciones y API.