SOTI

10 YEARS
OF SECURITY INSIGHT

VOLUMEN 10,
NÚMERO 02

Apagando fuegos:

el auge de las amenazas DDoS en EMEA

Akamai

Estado de Internet en materia de seguridad

Índice

Los ataques DDoS son cada vez más frecuentes en EMEA

Los ataques distribuidos de denegación de servicio (DDoS) están aumentando en volumen global y en sofisticación. Este aumento es especialmente evidente en Europa y la región de Oriente Medio y África (EMEA), donde los investigadores de Akamai observaron un aumento drástico en el ritmo de crecimiento de los ataques DDoS; de hecho, el crecimiento de los ataques DDoS en la región es más rápido que en otras áreas geográficas. Los ataques DDoS afectan a objetivos con tráfico malicioso no deseado y obstaculizan las operaciones de redes y sitios web en EMEA.

Nuestra conjetura es que gran parte de este cambio regional se debe a la tensión geopolítica, como las actividades motivadas por ciertos intereses políticos de algunos países y el hacktivismo en respuesta a las guerras actuales, incluidas las guerras entre Rusia y Ucrania e Israel y Hamás. Además, es probable que los próximos eventos más destacados y las elecciones en Europa incrementen aún más el riesgo de ataques DDoS. Aunque la magnitud de los ataques DDoS en EMEA es bastante grande y está creciendo, también hemos sido testigos de un aumento tanto en el número de vectores de ataque DDoS empleados por los ciberdelincuentes como en la duración de dichos ataques.

En este informe sobre el estado de Internet (SOTI), examinamos la naturaleza y la frecuencia de los ataques DDoS en la región de EMEA y analizamos algunos de los principales sectores que se ven afectados por ellos, entre los que se incluyen el de los servicios financieros, el comercio y el sanitario. También analizamos en detalle la nueva legislación de EMEA diseñada para reforzar la protección contra el aumento de las amenazas de ciberseguridad en la región, y proporcionamos técnicas de mitigación y protección que funcionan conjuntamente para luchar contra el fuego que representan las crecientes amenazas DDoS en EMEA.

Información clave del informe

Los investigadores de Akamai han observado que el número de ataques DDoS en EMEA ha aumentado continuamente, con picos más altos, desde principios de 2019.

Más de un tercio de todos los ataques DDoS en todo el mundo se producen en la región de EMEA.

La complejidad y la gravedad de los ataques DDoS en la región de EMEA se han visto transformadas por motivos geopolíticos, como el hacktivismo, con el potencial de tener consecuencias mortales.

De todos los tipos de ataques DDoS, los dirigidos contra el DNS se encuentran entre los más frecuentes, según un estudio de Akamai. Específicamente, observamos que el vector NXDOMAIN (dominio inexistente), también conocido como vector de subdominio pseudoaleatorio, inunda servidores de nombres DNS con solicitudes para dominios inexistentes.

En más de un tercio de los ataques DDoS se utilizan varios vectores de ataque (hasta 12) para ampliar las posibilidades de alcanzar el objetivo.

En EMEA, el sector con el mayor número de ataques de capa 3 y capa 4 es el de los servicios financieros; en el caso de los ataques de capa 7, es el del comercio.

Los gobiernos y las naciones de EMEA se han replanteado el poder de la seguridad de la información mediante la adopción de nuevas medidas legislativas, como NIS2 y DORA, para influir positivamente en las estrategias de TI y ciberseguridad, incluida una resiliencia y protección contra DDoS mejoradas.

El ayer y hoy de los ataques de DDoS

Los ataques DDoS, tanto si los despliegan personas como botnets, inundan los servidores con solicitudes y los saturan con tráfico, lo que hace que los servicios y los sitios alojados no estén disponibles para los usuarios y visitantes.

Los ataques DDoS han evolucionado desde el periodo en el que los atacantes utilizaban herramientas de código abierto para llevarlos a cabo. Para este grupo, la motivación era a menudo simplista: quizás no estaban satisfechos con la nueva función del juego, tenían la esperanza de ganar una ventaja competitiva o simplemente buscaban divertirse. En general, este grupo de atacantes no dominó el panorama de ataques con tendencias de dirigirse a infraestructuras críticas u hospitales, ni con el objetivo de dañar gravemente las redes o poner en peligro la vida humana.

El hacktivismo cambió drásticamente el panorama, tanto en términos de las identidades de los atacantes como de su motivación. Aunque algunos ataques hacktivistas pueden tener un impacto limitado o suponer simplemente una molestia, otros se dirigen al sector comercial para obtener importantes beneficios económicos y pueden provocar interrupciones del servicio que duran días. Los ataques pueden tener consecuencias potencialmente mortales, como se observa en algunos ataques a centros de salud.

La capacidad de llevar a cabo ataques DDoS se ha simplificado en los últimos años, con la aparición de servicios como los DDoS booters, que permiten incluso al adversario menos sofisticado lanzar un ataque con solo hacer clic en un botón y por un precio irrisorio, a veces de tan solo 10 €. Estos sencillos ataques conducen a una gran cantidad de tráfico que obliga a sitios web y redes enteros a desconectarse, perjudicando a las empresas tanto financiera como operativamente, y privando a los clientes y usuarios del uso de servicios esenciales.

Con el foco en la geopolítica

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. Por ejemplo, los ataques DDoS desempeñan un papel importante en la actual guerra cibernética entre Ucrania y Rusia, ya que los hacktivistas han descubierto que son eficaces y rentables.

A principios de 2022, Akamai comenzó a apoyar al Gobierno de Ucrania en la lucha contra la guerra cibernética defendiendo 20 recursos web de entidades gubernamentales diferentes. Esto incluía la URL president.gov.ua, que había sido el sitio más atacado y se observó que tenía un pico de DDoS de gran volumen de 1 millón de solicitudes maliciosas por segundo.

Hacktivistas como Anonymous Sudan, NoName057(16), y Killnet han aparecido en los titulares desde que Rusia invadió Ucrania en febrero de 2022. Killnet fue el primero de estos grupos en aparecer, y comenzó su actividad alrededor de octubre de 2021 ofreciendo servicios de DDoS de alquiler. Killnet ha atacado a agencias gubernamentales, el sector sanitario, las empresas de medios de comunicación y otras organizaciones que consideran aliados de Ucrania.

Muchos investigadores de amenazas creen que NoName057(16) apoya a Rusia y este apoyo se ha observado ampliamente mediante ataques DDoS basados en HTTP (capa 7). A principios de 2023, el grupo prorruso Anonymous Sudan comenzó a utilizar ataques DDoS contra entidades de Dinamarca, Suecia, Estados Unidos y otros países. En junio de 2023, muchos grupos de atacantes, entre ellos ReVIL, Killnet y Anonymous Sudan, aprovecharon el caos provocado por la guerra entre Rusia y Ucrania, y centraron su atención en la infraestructura bancaria crítica.

Más recientemente, Anonymous Sudan reivindicó la responsabilidad del ataque a la aplicación de mensajería Telegram de Francia como parte del ataque DDoS sin precedentes a la red interministerial estatal del país, que causó la interrupción de más de 17 000 direcciones IP y dispositivos, y más de 300 dominios. Se cree que este ataque a los sitios web y servicios del gobierno francés se llevó a cabo probablemente en respuesta al anuncio del 26 de febrero de 2024 que hizo el presidente francés Emmanuel Macron sobre la posibilidad de enviar tropas francesas a Ucrania.

El conflicto entre Ucrania y Rusia no es la única batalla que está causando un aumento repentino de ataques DDoS en EMEA. La guerra entre Israel y Hamás también ha provocado un aumento de los ataques. Anonymous Sudan ha reivindicado la responsabilidad de los ataques DDoS contra el Mossad, la agencia de inteligencia nacional de Israel, así como contra el sitio web y las cuentas de Facebook del primer ministro israelí, y contra sitios pro-Israel relacionados con la escalada del conflicto en el Mar Rojo. NoName057(16) también ha atacado sitios web israelíes en respuesta a este conflicto.

Las extorsiones se triplican

Históricamente, los ataques de ransomware cifraban los datos de una víctima, convirtiéndolos en inutilizables a menos que se pagara un rescate. A continuación aparecieron los ataques de doble extorsión, que provocaban mayores daños, ya que los delincuentes hacían una copia de los datos de la víctima antes de cifrar su red y la amenazaban con publicarla o venderla a menos que se pagara el rescate. Poco después surgió un tercer tipo de ataque: la triple extorsión. En estos ataques, el atacante utiliza el DDoS para obstaculizar el negocio de la víctima, además de las otras dos tácticas. Estos ataques de triple extorsión se denominan a menudo DDoS de rescate o RDDoS.

Los ataques DDoS son un elemento común en los ataques de extorsión, ya que se utilizan como una cortina de humo para distraer a los equipos de seguridad en sus tareas de supervisión de la información mientras los hackers intentan infiltrarse en los sistemas o para aumentar la presión sobre la víctima. El uso de varios vectores de ataque aumenta las posibilidades de que una víctima pague un rescate exigido. Uno de los primeros ataques de triple extorsión registrados se produjo en una clínica de psicoterapia finlandesa, Vastaamo, en octubre de 2020, y ocurrió cuando Europa se apresuraba a encontrar formas de compartir mejor los datos sanitarios en toda la Unión Europea.

El sector sanitario sigue siendo el principal objetivo de los atacantes que utilizan ataques de triple extorsión. Un ejemplo es el grupo de ransomware NoEscape, que surgió el año pasado a partir del extinto grupo de habla rusa Avaddon y dirige sus ataques a organizaciones del sector sanitario. Y algunas empresas de ciberseguridad ya se están preparando ante la perspectiva de que más grupos dirijan sus ataques al sector sanitario en el futuro.

Además, se dijo que el grupo de ransomware LockBit, con sede en Rusia, había ejecutado la operación de ransomware más grande y dañina del mundo en febrero de 2024, en una espiral destructiva que provocó pérdidas por valor de miles de millones de euros. Europol y Eurojust se unieron para coordinar un grupo de trabajo internacional conocido como Operación Cronos para acabar con LockBit. La Operación Cronos incluyó arrestos, órdenes judiciales, condenas y la confiscación de 34 servidores en EMEA, Australia y Estados Unidos. LockBit era conocido por experimentar con nuevos métodos para presionar a las víctimas a pagar rescates, como RDDoS.

Aunque hay otros grupos bien conocidos que utilizan RDDoS, como Darkside, Lazarus, AvosLocker y BlackCat, el impacto de la Operación Cronos contra LockBit es significativo porque es la primera vez que la aplicación de la ley cibernética ha sido eficaz hasta este nivel. El alcance y la escala de esta neutralización incluyeron el desmantelamiento y la toma de control total de la infraestructura de un gran grupo de ransomware mientras todavía estaba operativa.

Contrapirateo: cuando el DDoS se combate con DDoS

El concepto de responder a los ciberdelincuentes con ciberataques ha sido objeto de debate durante años. Esta estrategia se basa en la idea de que "la mejor defensa es un buen ataque" (en el sentido de que puede proteger a las empresas de amenazas internacionales), pero también se cree que sentará un precedente peligroso al permitir que las empresas de ciberseguridad lancen ataques DDoS en todo el mundo y desestabilicen así las relaciones estatales y aumenten las tensiones diplomáticas. Además, las ambigüedades normativas relativas a la lucha contra los ciberataques, como los ataques DDoS, plantean cuestiones jurídicas muy complejas.

Como sabemos, LockBit utilizó DDoS como parte de sus ataques de triple extorsión. Irónicamente, su uso de este método se vio influenciado en parte por un ataque DDoS que ellos mismos experimentaron de primera mano. La empresa de ciberseguridad Entrust se añadió a la lista de víctimas de LockBit en julio de 2022. Como respuesta, Entrust lanzó un contraataque DDoS que paralizó eficazmente los sistemas de la Darknet que LockBit utilizaba para publicar datos robados.

Algunos países también están utilizando los contraataques como táctica de guerra. Ucrania ha estado reclutando voluntarios para que formen parte de un "ejército de TI" (IT Army) de hackers de todo el mundo que trabaja para defender las redes mediante contrataques; se considera el primero de su clase.

Análisis de los datos sobre DDoS en EMEA

Los ataques DDoS han ido aumentando a nivel mundial, y esto es especialmente notable en la región de EMEA. Los investigadores de Akamai han analizado los datos de DDoS regionales y están observando cómo las cifras de ataques DDoS de EMEA aumentan de forma más constante que las de cualquier otra región, incluida la de Norteamérica, que lidera la comparación en general (Figuras 1a y 1b).

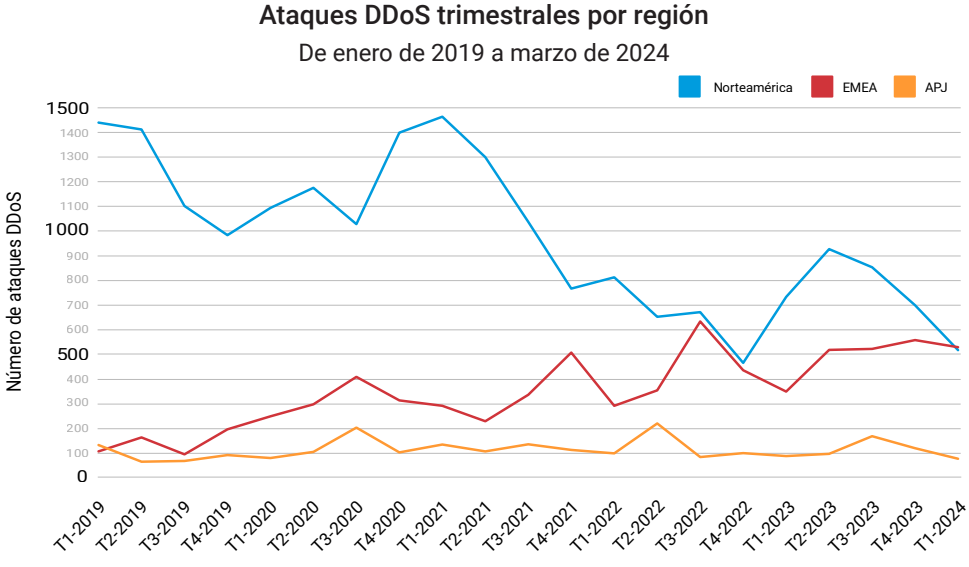


Fig. 1a: Las cifras de ataques DDoS de EMEA están aumentando de forma más constante que las de cualquier otra región, incluida la de Norteamérica.

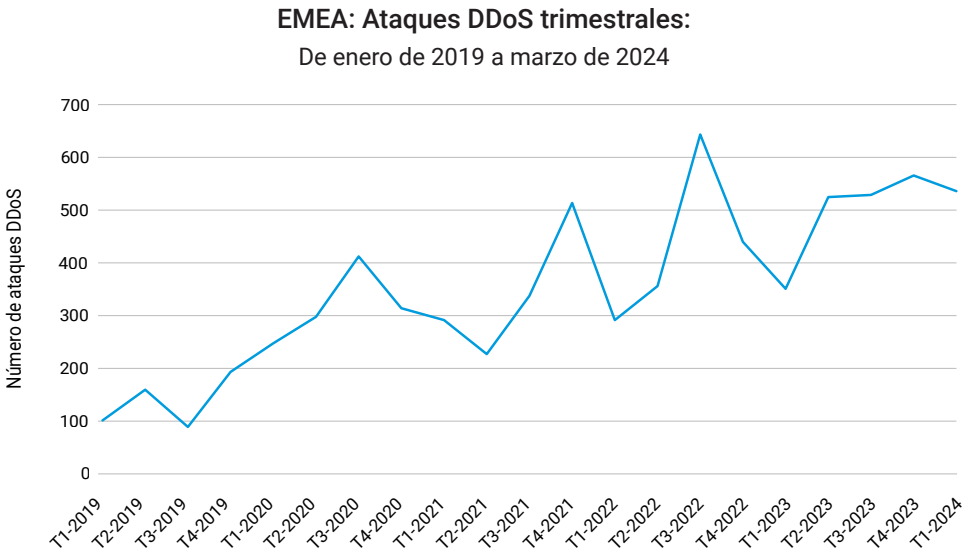


Fig. 1b: El crecimiento de los ataques DDoS en la región de EMEA.

Dentro de la región de EMEA, el Reino Unido (26 %), Arabia Saudí (22,3 %) y Alemania (9,1 %) lideran los países con el mayor número de ataques. Además, el estudio de Akamai muestra que más de un tercio de todos los ataques DDoS en todo el mundo se producen en la región de EMEA (Figura 2).

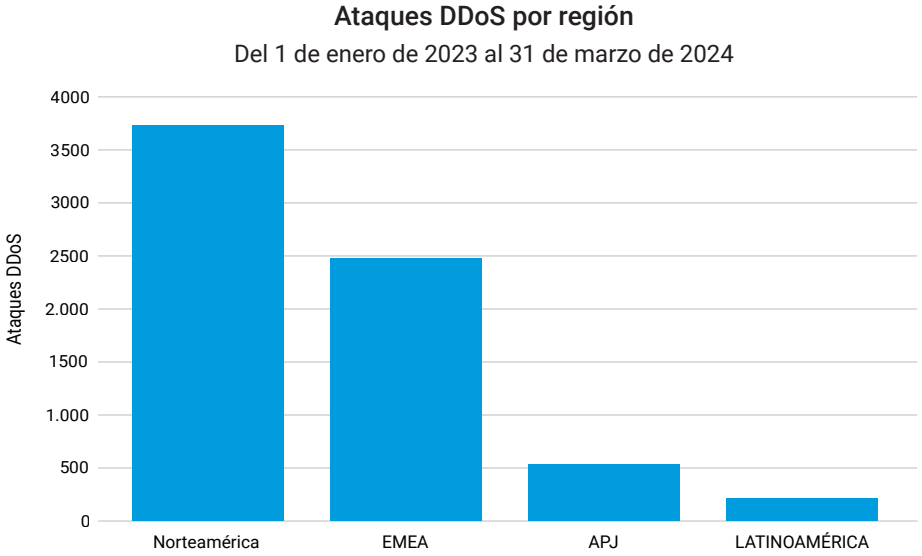


Fig. 2: El número de ataques DDoS en EMEA aumentó a casi 2500 desde principios de 2023 hasta el primer trimestre de 2024, más del triple que en las regiones de Asia-Pacífico y Japón (APJ), y Latinoamérica (LATAM) combinadas.

En el sector de los servicios financieros, EMEA es la región con mayor cantidad de tráfico de ataques DDoS de las capas 3 y 4 (Figura 3). Como se ha mencionado anteriormente, los grupos hacktivistas rusos declararon su intención de lanzar ataques DDoS al sistema bancario europeo, y suponemos que la razón principal del aumento de los ataques DDoS en el sector de los servicios financieros es este hacktivismo geopolítico.

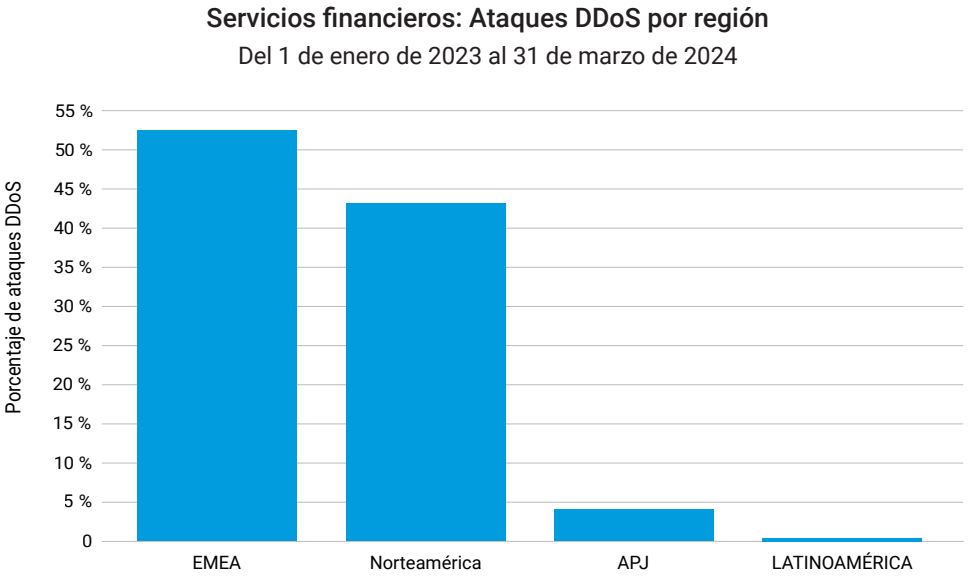


Fig. 3: EMEA experimentó el 52,5 % del tráfico regional de ataques DDoS de las capas 3 y 4 en el sector de servicios financieros.

Además de los ataques de capa 3 y 4, las aplicaciones de servicios financieros están plagadas de ataques DDoS de capa 7. Sin embargo, el sector del comercio está experimentando el mayor aumento de los ataques DDoS de capa 7 en EMEA, con casi el 30 % de todos los ataques en la región (Figura 4).

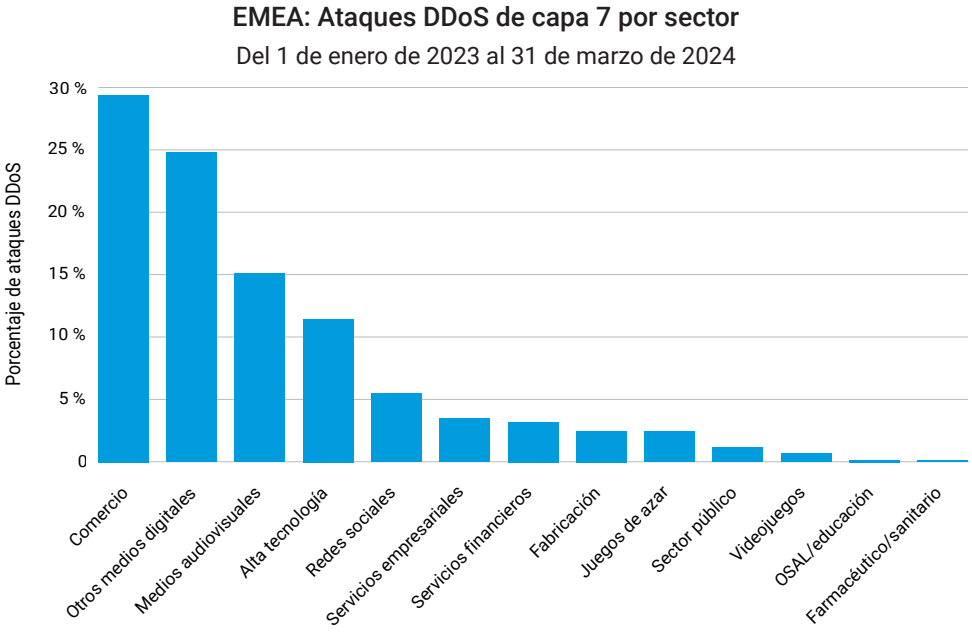
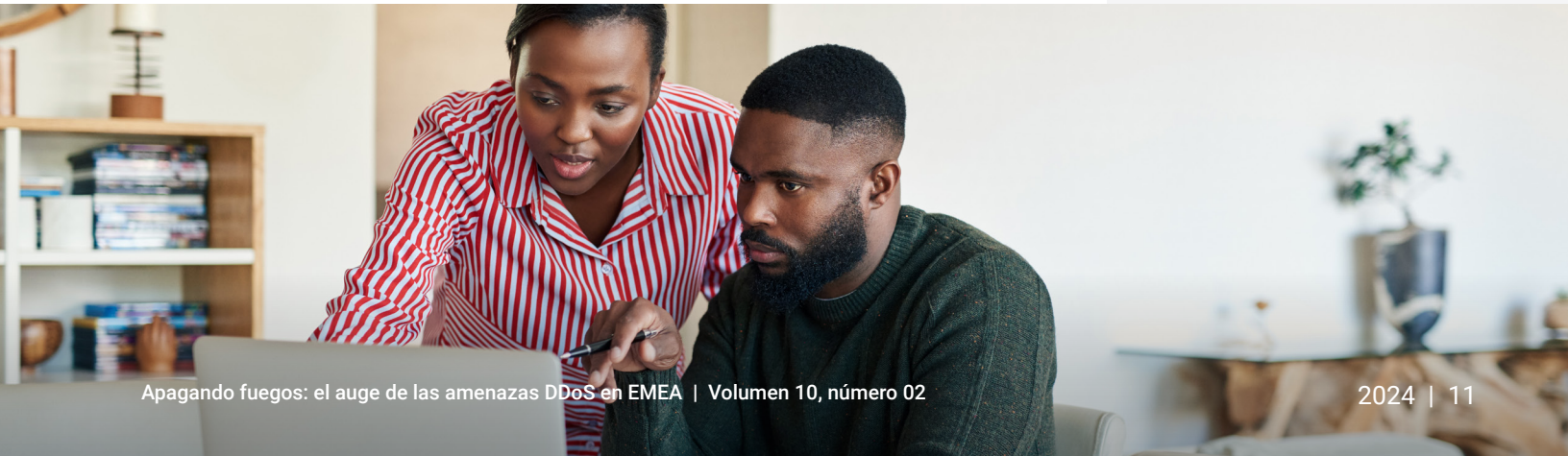


Fig. 4: El sector del comercio experimenta el 29,4 % del tráfico regional de ataques DDoS de capa 7 en EMEA.

Es posible que los ataques DDoS a la capa de aplicación, como los que emplean inundaciones HTTP, sean más frecuentes en el sector del comercio, debido a la gran oportunidad de interrupción de los ingresos que estos ataques ofrecen a los atacantes. Estos tipos de ataques son especialmente devastadores para las organizaciones del sector del comercio, ya que pueden hacer que no se pueda acceder a una tienda online o que un sistema de reservas no esté disponible, lo que provoca una importante pérdida de ingresos para la empresa víctima. Además, se pueden desplegar como una táctica de distracción para consumir recursos de respuesta a incidentes mientras que los atacantes pretenden robar datos lucrativos de los clientes (como información de las tarjetas de pago) de otras áreas de la red de la víctima.



Aunque el número de ataques DDoS ha ido en aumento, también hemos observado que el número de vectores utilizados para desplegar ataques DDoS ha aumentado considerablemente (Figura 5a). Estos tipos de ataques incluyen inundación DNS, fragmento UDP y reflexión NTP (Figura 5b). Los ataques también han durado más.

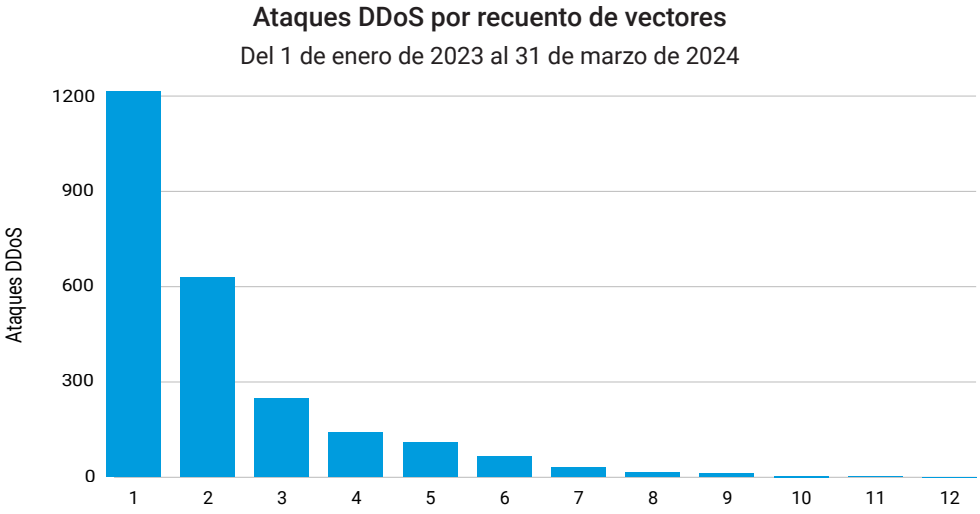


Fig. 5a: El número de vectores utilizados para desplegar ataques DDoS ha aumentado considerablemente.

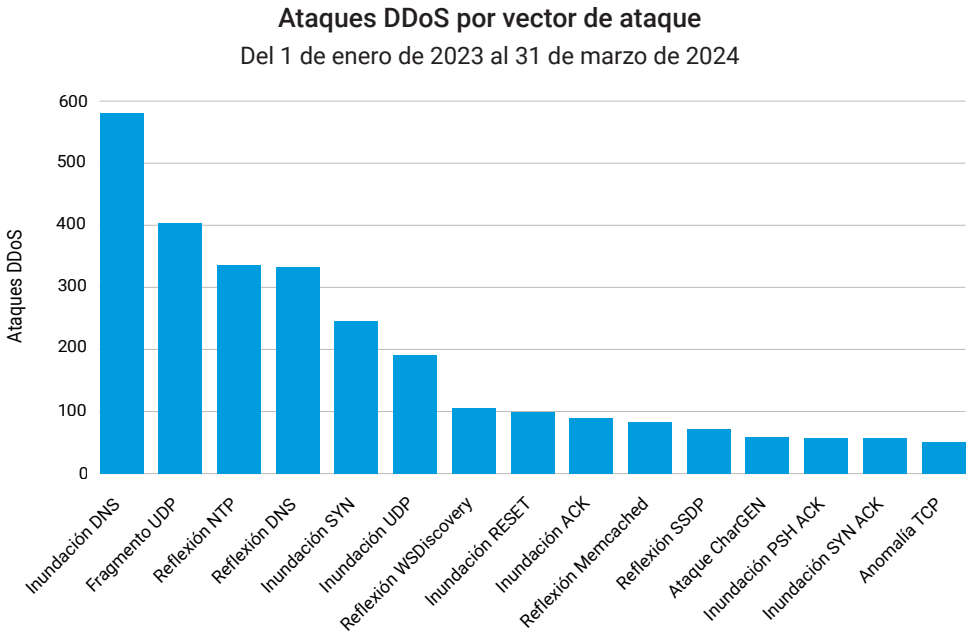


Fig. 5b: Los tipos de ataques DDoS de EMEA incluyen inundación DNS, fragmento UDP y reflexión NTP.

Los ataques prolongados obstaculizan la productividad y la capacidad de mantener la continuidad de las operaciones cuando se detectan otras amenazas y se requieren acciones de respuesta. Las técnicas DDoS que implican ataques de larga duración y el uso de más vectores de ataque son estrategias eficaces para los atacantes, ya que les permiten agotar mejor los recursos y saturar a los equipos encargados de la seguridad de las redes empresariales.

La nueva tendencia en objetivos de los DDoS: el DNS

De todos los tipos de ataques DDoS, los dirigidos al sistema de nombres de dominio (DNS) se encuentran entre los más frecuentes (Figura 6). El DNS es un objetivo habitual de los ataques DDoS debido al impacto que el tráfico malicioso puede tener en este servicio tan fundamental. Un ataque con éxito al DNS tiene el potencial de borrar literalmente la presencia de una empresa en Internet.

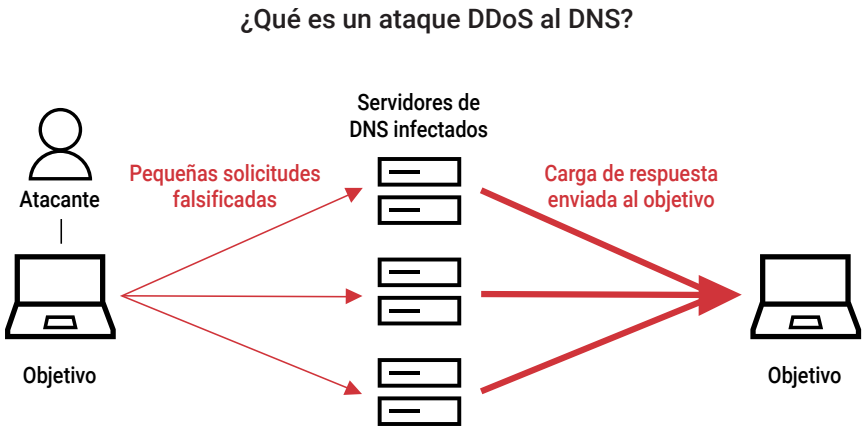


Fig. 6: Un ataque DDoS al DNS satura los servidores del DNS con solicitudes falsificadas que provocan una abrumadora respuesta de cargas útiles al objetivo.

En concreto, se ha observado que los ataques NXDOMAIN (dominio inexistente), también denominados ataques de subdominio pseudoaleatorio (PRSD) o "DNS Water Torture", inundan la infraestructura del DNS con solicitudes para dominios inexistentes. Este tipo de ataque tiene como objetivo llegar a los servidores de nombres de origen y provocar una alta carga en los sistemas. Procesar una solicitud para un dominio inexistente es una tarea complicada que consume muchos ciclos de procesamiento, lo que en última instancia agota la capacidad de respuesta de los sistemas. Hemos visto muchos ataques cortos de este tipo, que normalmente se utilizan para sondear la configuración de la infraestructura del DNS de la víctima, solo para volver más tarde con un ataque perfeccionado en toda regla. Según los resultados del estudio de nuestros 50 principales clientes financieros que utilizan Akamai Edge DNS, las solicitudes hacia dominios inexistentes representaron casi el 60 % de su tráfico de Internet en marzo de 2024 (Figura 7).

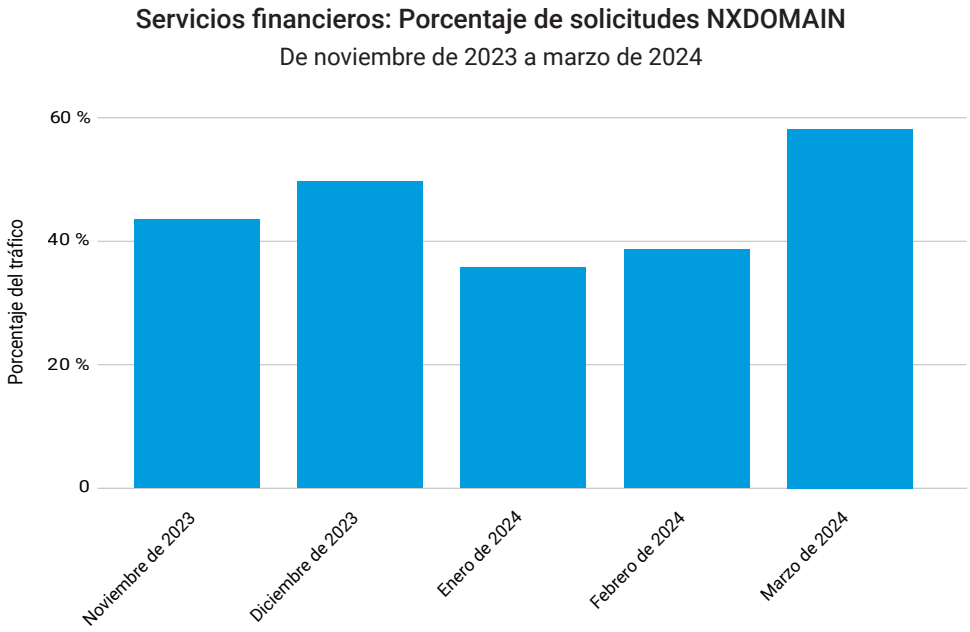


Fig. 7: Desde finales de 2023, las solicitudes NXDOMAIN alcanzaron un pico en marzo de 2024 con un porcentaje del 58 %.

Los ataques de inundación DNS son uno de los dos grupos principales de ataques DDoS al DNS. El otro son los ataques por amplificación de DNS, que incluyen ataques de reflexión, e implican la falsificación de direcciones IP creadas por el atacante para enviar un número considerable de solicitudes de DNS en un intento de paralizar los recursos del equipo objetivo. Otro incentivo para que el atacante seleccione ataques DDoS al DNS es la facilidad para ejecutarlos, ya que la mayor parte del tráfico se ejecuta sobre el protocolo de datagramas del usuario (UDP), que permite IP falsificadas.

Combatir los ataques replanteando el poder de la seguridad de la información

Para combatir y prevenir el aumento de las amenazas de ciberseguridad (incluidos los DDoS) en la región, los gobiernos y las naciones de EMEA se han replanteado el poder de la seguridad de la información. El panorama cambiante incluye la nueva directiva relativa a la seguridad de las redes y sistemas de información (NIS2) y la Ley de Resiliencia Operativa Digital (DORA), entre otras nuevas medidas legislativas, por ejemplo, el Reglamento General de Protección de Datos (RGPD), la Ley de Ciberresiliencia (CRA), el Programa europeo para la protección de las infraestructuras críticas, etc.

Es fundamental que las empresas implementen medidas de seguridad sólidas y evalúen de forma rutinaria sus aplicaciones y redes para evitar y mitigar los ciberataques. Esta estrategia es especialmente importante para protegerse contra los ataques DDoS, ya que no hay mucho tiempo para reaccionar ante ellos. Además, los ataques DDoS tienden a dirigirse a entidades menos protegidas, que los atacantes identifican mediante un reconocimiento y pruebas precisos. Por lo tanto, es importante que las organizaciones establezcan procedimientos de seguridad eficaces y que dispongan de planes de continuidad del negocio y recuperación ante desastres. Combinadas, las nuevas medidas legislativas y las directivas pueden proporcionar ciertos mecanismos de seguridad para las organizaciones.

La directiva NIS2, que se adoptó en diciembre de 2022 y deroga y sustituye a la directiva NIS1, tiene por objeto ampliar, reforzar y armonizar la aplicación del marco de ciberseguridad existente en la Unión Europea para responder al aumento de la exposición de Europa a las ciberamenazas. Los Estados miembros de la UE tienen hasta el 17 de octubre de 2024 para trasladar la directiva.

Los procedimientos para la gestión de proveedores, como terceros, también son importantes. DORA se centra en la normativa de los servicios financieros de la UE y será aplicable a partir del 17 de enero de 2025. Además de promover la ciberresiliencia y ayudar a las entidades de servicios financieros de la UE a lidiar con incidentes de ciberseguridad, DORA proporciona orientación para los procedimientos de gestión de proveedores externos. Esto ayuda a las entidades financieras al garantizar que los proveedores de tecnologías de la información y la comunicación (TIC) que contratan cumplan con los estándares de seguridad de la información adecuados. Estos son componentes clave del modelo de los cinco pilares de DORA, que está diseñado para mejorar la ciberresiliencia de las entidades en el sector de los servicios financieros. Los cinco pilares son la gestión de riesgos, la generación de informes de incidentes, las pruebas de resiliencia operativa digital, el riesgo de terceros de TIC y el intercambio de información e inteligencia.

Tanto NIS2 como DORA incluyen orientación sobre estrategias que aprovechan el enfoque Zero Trust como método de resiliencia. La confianza y la disponibilidad son cruciales, especialmente en el universo online, y un ataque DDoS puede erosionar la confianza de forma crítica. Por lo tanto, es importante que las empresas sigan los procedimientos de protección adecuados, como la ciberhigiene básica. Este concepto incluye el uso de principios Zero Trust, que aplican un mecanismo de control de acceso más detallado y con reconocimiento teniendo en cuenta el contexto que verifica continuamente la identidad, el nivel de seguridad del dispositivo y el comportamiento del usuario antes de otorgar acceso a recursos confidenciales. Además, el concepto de privilegio mínimo es una parte clave de las prácticas de seguridad Zero Trust y segmenta a los usuarios aprobados para el acceso. Las soluciones Zero Trust también ayudan a proteger los activos críticos de las organizaciones frente a ataques RDDoS.

Además de la legislación relacionada con los DDoS, también es importante que las organizaciones estén familiarizadas con otras leyes existentes en la región de EMEA que tienen como objetivo hacer frente a las ciberamenazas. Por ejemplo, la nueva CRA de la Unión Europea está diseñada para las vulnerabilidades de software y hardware que los atacantes aprovechan cada vez más para infiltrarse en las organizaciones y lanzar ataques de ransomware. Además, el RGPD creó obligaciones para todas las organizaciones que tratan datos personales relacionados con empresas y clientes europeos.

Y fuera de la Unión Europea, otros países están creando y aplicando sus propios controles. La Autoridad Nacional de Ciberseguridad de Arabia Saudí ha introducido leyes de protección de datos similares al RGPD, y la Oficina de Operaciones contra la Ciberdelincuencia en África de Interpol ha establecido programas como el Africa Cyber Surge.

Caso real: Una organización de comercio electrónico europea experimenta un ataque DDoS a la capa de red

Mantener el tiempo de actividad y la resiliencia del sitio web es fundamental para que cualquier organización de comercio electrónico pueda generar ingresos por ventas. Por eso, la protección de los activos y las aplicaciones en entornos web contra los DDoS para evitar ataques que afecten a su negocio y a sus clientes es una prioridad para los responsables de la seguridad. Pero ¿qué pasaría si la infraestructura subyacente o los sistemas back-end en los que se apoya el procesamiento de los pedidos se interrumpieran o se desconectaran completamente? Por ejemplo, si un cliente hace un pedido, pero este no se puede procesar o completar, la actividad se detiene. Eso es lo que le sucedió a una organización de comercio electrónico en Europa cuando un ataque DDoS a la capa de red afectó a los servicios del centro de datos, en el que no se habían implementado controles suficientes.

Muchos atacantes suelen lanzar campañas de ataque los fines de semana y festivos, cuando hay menos personal de seguridad y recursos de respuesta a incidentes disponibles para neutralizar una amenaza. En el caso de esta organización europea de comercio electrónico, los cibercriminales utilizaron una combinación de vectores de ataque de inundación SYN y UDP para golpear el centro de datos de la organización un viernes por la tarde y colapsar recursos corporativos vulnerables, como el correo electrónico de la empresa. Esto impidió la transmisión de datos importantes a otras partes de la organización, incluidos los almacenes de aprovisionamiento.

Como resultado, la infraestructura logística no pudo llevar a cabo las operaciones y procesar los pedidos recibidos de la plataforma de comercio electrónico, aunque la infraestructura logística en sí no se viera afectada. Debido a que la organización no era capaz de defenderse del nivel sostenido de ataques DDoS volumétricos, se recurrió a Akamai para ayudar con una integración de emergencia con el fin de proteger los centros de datos corporativos del retailer. En 24 horas, el cliente se encontraba en la plataforma Prolexic de Akamai y se restauró su conectividad a los servicios corporativos esenciales.

Conclusión: las organizaciones de comercio electrónico deben adoptar un enfoque integral frente a los ataques DDoS que incluya la mitigación de los ataques de capa 7 (aplicaciones) y los ataques de capa 3 (red) y capa 4 (transporte) para evitar el tiempo de inactividad y garantizar la resiliencia durante todo el ciclo de vida de los pedidos.

Protección y mitigación

Ahora que hemos hablado de las principales tendencias y legislación de DDoS en EMEA, y hemos proporcionado algunos ejemplos de ataques, veamos qué puede hacer para proteger su organización. Además de seguir las medidas legislativas mencionadas anteriormente, incluidas las normativas NIS2, DORA, RGPD y CRA, y utilizar las soluciones Zero Trust, los investigadores de Akamai recomiendan tres estrategias prácticas para ayudar a combatir el panorama de DDoS en constante evolución.

1. **Prepárese de forma proactiva con una estrategia de protección frente a DDoS para sus activos digitales.**
   Esto incluye:
   - Garantizar que se aplican controles de mitigación para todas las direcciones IP expuestas y subredes esenciales.
   - Implementar controles de seguridad frente a DDoS dentro de una estrategia de protección en línea.
   - Garantizar que los planes y equipos de respuesta a incidentes estén actualizados y designados.
   - Reforzar su protección frente a DDoS local con una plataforma de protección híbrida para defenderse de los ataques que sobrecargan los dispositivos en el entorno local.
   - Establecer controles de seguridad proactivos a través de un firewall de nube de red, así como un firewall de aplicaciones web.
   - Configurar la limitación de velocidad.
   - Almacenar el contenido en caché en una red de distribución de contenido (CDN).
   - Utilizar un equipo del centro de control de operaciones de seguridad para aliviar la presión sobre los recursos internos esenciales.

2. **Proteja su infraestructura de DNS.** Si el DNS de una entidad cae, también lo hace su presencia online. Es posible que un firewall de DNS tradicional no proporcione la protección adecuada si la configuración gestiona zonas tanto en el entorno local como en la nube. En este caso, una plataforma híbrida podría ser la solución óptima. Por lo general, para lograr una estrategia de seguridad ante DDoS suficiente, se debe examinar cualquier tráfico entrante de Internet a la red, y se debe mitigar y filtrar el tráfico de ataque antes de que llegue a sus aplicaciones, API e infraestructura reales, incluido el DNS.

3. **No confíe en soluciones que sean "suficientemente buenas".** Puede parecer más sencillo utilizar solo las protecciones mínimas básicas en función de los requisitos y el presupuesto. Sin embargo, las empresas a menudo descubren que este "ahorro" inicial conduce a una pérdida posterior que conlleva más gastos y daños, y que superan drásticamente las ventajas del plan original. Por lo tanto, es importante someter sus defensas a una prueba de estrés desde la perspectiva tanto de las prácticas recomendadas como de las soluciones técnicas. Estas pruebas deben incluir documentación de incidentes, procesos, runbooks y mucho más para garantizar que sus soluciones proporcionan un nivel sólido de ciberseguridad.

Conclusión

Los ataques DDoS han observado importantes transformaciones, tanto en su naturaleza como en su impacto, y se han vuelto cada vez más graves y complejos.

La región de EMEA se ha visto especialmente afectada por este panorama de aumento de ataques DDoS. Los sectores gubernamentales, de servicios financieros, del comercio y sanitario han experimentado un número cada vez mayor de estos tipos de ataques. Este cambio regional se puede atribuir, en parte, a las tensiones geopolíticas y los conflictos que están teniendo lugar en el área de EMEA, que han impulsado un aumento del hacktivismo y de sus actividades DDoS asociadas.

Además, es probable que los próximos eventos más destacados y las elecciones en Europa, incluidas las elecciones al Parlamento Europeo, las elecciones en el Reino Unido y los Juegos Olímpicos de Verano en Francia, incrementen aún más el riesgo de ataques DDoS. Estos ataques, que tienen una importancia política y económica significativa, pueden servir como motivaciones principales para los ciberdelincuentes que desean interrumpir e influir en los procedimientos mediante el uso de tácticas DDoS.

Los legisladores de EMEA se han replanteado el poder de la seguridad de la información y han reforzado las medidas de seguridad con nuevas directivas y normativas. Por lo general, las empresas y organizaciones que cumplen con estas normativas y tienen implementadas medidas de protección son menos propensas a ser consideradas por los ciberdelincuentes como presa fácil. Los autores de ataques DDoS tienden a dirigirse a objetivos que no están bien protegidos, y efectúan continuamente operaciones de reconocimiento para descubrir los más vulnerables. Debido a la multitud de vectores de ataque DDoS y a las numerosas rutas disponibles entre las capas de red, transporte y aplicación, es fundamental utilizar una combinación de soluciones para proporcionar una protección completa contra DDoS. Este tipo de defensa es esencial para tener las mejores posibilidades de éxito en la lucha contra el calor de las crecientes amenazas DDoS en EMEA.

Metodología

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.

Los datos de este informe cubren el periodo de 15 meses que abarca desde el 1 de enero de 2023 hasta el 31 de marzo de 2024, a menos que se indique lo contrario.

DDoS (capa 7)

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 DDoS de 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 para este informe 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.

Los datos de este informe cubren el periodo de 15 meses que abarca desde el 1 de enero de 2023 hasta el 31 de marzo de 2024.

DDoS (NXDOMAIN)

Estos datos describen el tráfico observado a través de nuestra red en el Edge para 50 de nuestros principales clientes de servicios financieros. Se realiza un seguimiento y se documentan las solicitudes dirigidas a los NXDOMAIN. Estas solicitudes se pueden realizar con intenciones maliciosas o legítimas. En general, un aumento de las solicitudes NXDOMAIN observadas dentro de un periodo de tiempo o geografía específicos indica un comportamiento malicioso. Nuestros equipos de seguridad utilizan estos datos para investigar ataques, detectar comportamientos maliciosos y proporcionar información adicional a las soluciones de Akamai.

Estos datos cubren el periodo de cinco meses que abarca desde noviembre de 2023 hasta marzo de 2024.

Créditos

Editorial y redacción

Lance Rhodes – Editor jefe
Susan McReynolds – Escritora de casos reales
Maria Vlasak – Corrección de textos

Revisión y expertos en la materia

Christian Borggreen
Cheryl Chiodi
Sven Dummer
Jim Gilbert
Mitch Mayne
Richard Meeus
Craig Sparling
Carley Thornell

Análisis de datos

Chelsea Tuttle

Materiales promocionales

Annie Brunholzl

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 los ataques DDoS, visite nuestras **soluciones Prolexic** y las páginas de **seguridad de API y de aplicaciones**.