Conviértase en chef de ciberseguridad:

prepare el recetario definitivo para demostrar fortaleza ante DDoS de capa 7

Índice

Introducción

Elaborar una defensa adecuada contra los ataques distribuidos de denegación de servicio (DDoS) actuales puede ser complicado incluso para los profesionales de la seguridad más experimentados. Esto es especialmente aplicable a los ataques DDoS a la capa 7, que plantean otra serie de complicaciones. Un recurso que puede resultar útil sería contar con instrucciones paso a paso con enfoques adaptados a las diferentes amenazas o, dicho de otro modo, con un recetario contra ataques DDoS de capa 7.

Sus adversarios prepararán los ataques DDoS de distintas formas. Los ataques a las capas 3 y 4 son más bien una cuestión de fuerza. ¿Quién tiene más capacidad de red, el atacante o la defensa? Por otro lado, los ataques a la capa 7 se dirigen a la capa de aplicación del modelo de interconexión de sistemas abiertos (OSI), que es el que se encarga de interactuar directamente con las aplicaciones de software. La finalidad de estos ataques es saturar un servidor web, una base de datos o una aplicación aprovechando las asignaciones de memoria o capacidad o los puntos débiles en la forma en que estos sistemas gestionan las solicitudes.

Por lo tanto, los ataques DDoS a la capa 7 plantean problemas específicos en lo que respecta a la mitigación, ya que dichas solicitudes suelen mostrarse como tráfico legítimo, lo que dificulta el poder filtrar las solicitudes maliciosas sin que los usuarios legítimos se vean afectados. Además, la disponibilidad de recursos en la nube y de automatización ha puesto las cosas más fáciles que nunca a los atacantes para lanzar estos ataques de forma rápida y a gran escala.

En este documento, abordamos los problemas relacionados con la mitigación de los ataques DDoS a la capa 7 con recetas detalladas que incluyen las herramientas y técnicas que utilizan los atacantes, tácticas de detección y mitigación para contrarrestarlos, así como sugerencias de análisis y recuperación tras el ataque.

La trayectoria de Akamai en ciberseguridad y distribución de contenido, y una plataforma en la nube distribuida con más de 4200 puntos de presencia en todo el mundo, nos proporciona una perspectiva única respecto a los ataques DDoS actuales. A medida que los ataques DDoS a la capa de aplicación se vuelven más complejos y polifacéticos, resulta importante contar con esa perspectiva y con una estrategia exhaustiva de defensa. Y de eso hablamos aquí.

Tanto si es profesional de seguridad de primera línea que busca ayuda con una amenaza o vulnerabilidad específica, como si es director de seguridad de la información que desea mejorar su estrategia de seguridad, en este recetario encontrará la receta para lograr su objetivo.

Objetivos comunes y ejemplos de los ataques DDoS a la capa 7

Los ataques DDoS a la capa 7 tienen como objetivo la capa superior del modelo OSI, es decir, la capa de aplicación. Estos ataques pretenden saturar los recursos del objetivo, explotando la forma en que las aplicaciones web procesan las solicitudes. Entre los objetivos comunes de los ataques DDoS a la capa 7 se incluyen:

Servidores web: los atacantes tienen en el punto de mira a los servidores web, en los que buscan interrumpir la entrega de contenido a los usuarios legítimos. Este hecho puede hacer que los sitios web tarden demasiado en cargarse o dejen de estar accesibles.

Aplicaciones web: las aplicaciones que utilizan bases de datos o servicios back-end son vulnerables a los ataques DDoS a la capa 7, ya que el ataque puede aprovechar los puntos débiles de las aplicaciones a la hora de analizar las consultas, procesar las solicitudes o gestionar las sesiones.

Interfaces de programación de aplicaciones (API): las API son un componente fundamental de las aplicaciones móviles y los servicios web modernos. Los ataques a las API pretenden interrumpir la interacción entre los diferentes servicios de software, lo que afecta a la funcionalidad de las aplicaciones que utilizan dichas interfaces.

Servicios DNS: aunque los ataques al sistema de nombres de dominio (DNS) también pueden producirse en otras capas, los ataques a la capa 7 pueden conllevar el bombardeo del servicio DNS con solicitudes maliciosas que buscan interrumpir el proceso de resolución de los nombres de dominio, provocando problemas de accesibilidad generalizados. La adopción creciente del DNS a través de HTTP/TLS podría dar lugar a un aumento de dichos ataques.

Servidores de correo electrónico: tener como objetivo a los servidores de correo electrónico puede hacer que se interrumpan las comunicaciones, lo que afecta tanto a los correos electrónicos de entrada como de salida.

Pasarelas de pago y servicios financieros: se trata de objetivos que pueden generar muchos beneficios para los atacantes que desean interrumpir las transacciones y sembrar el caos en las operaciones financieras.

En los informes sobre el estado de Internet (SOTI) y en la información sobre seguridad de Akamai se analiza de forma rutinaria el panorama en constante evolución de los ataques DDoS a la capa 7, y en ellos se destacan la diversidad de vectores de ataque y los sectores más expuestos.

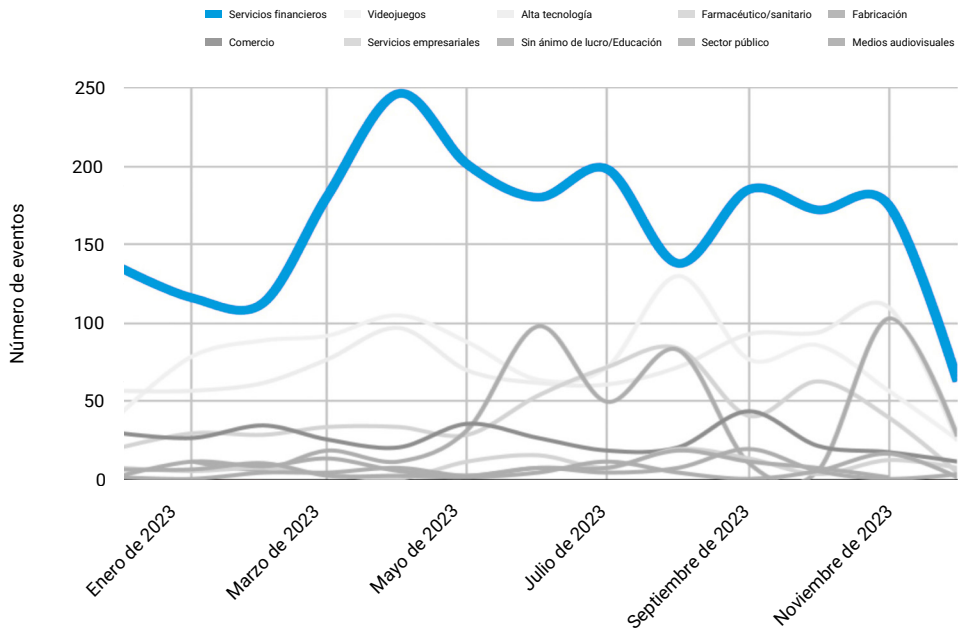
Vectores de ataque

- Ataques a las API y aplicaciones web: los adversarios atacan a menudo los puntos de entrada del sitio web, incluidos los terminales de las API que no se suelen almacenar en caché debido a su contenido o configuración. Algunos ejemplos de rutas que suelen ser objetivos comunes son "/", "/home", "/en-us", "/pricing/", etc.
- Es habitual observar vectores de ataque como:
  • Inundación HTTP GET/POST en las páginas de inicio
  • Inundación HTTPS GET en rutas y cadenas de consulta aleatorias
  • Ataques de lectura lenta
  • Inundaciones con carga de archivos grandes

Además, el número de empresas objeto de un ataque DDoS ha aumentado históricamente año tras año, pero ahora el "cómo" es diferente. En primer lugar, el tipo y el volumen de las propiedades que son víctimas de ataques han cambiado. Por ejemplo, en lugar de 10 ataques contra los mismos terminales o similares, podrían realizarse 100 ataques a diferentes IP en el espacio de red. Esos ataques no solo se dirigen a la capa 3, sino también a la capa 7 al mismo tiempo.

Sectores objetivo

La cifra de ataques distribuidos de denegación de servicio (DDoS) contra los sectores de los servicios financieros, los juegos de apuestas y la fabricación tuvo un repunte en 2023, especialmente en la región de EMEA, donde superó a la del resto de las regiones juntas.

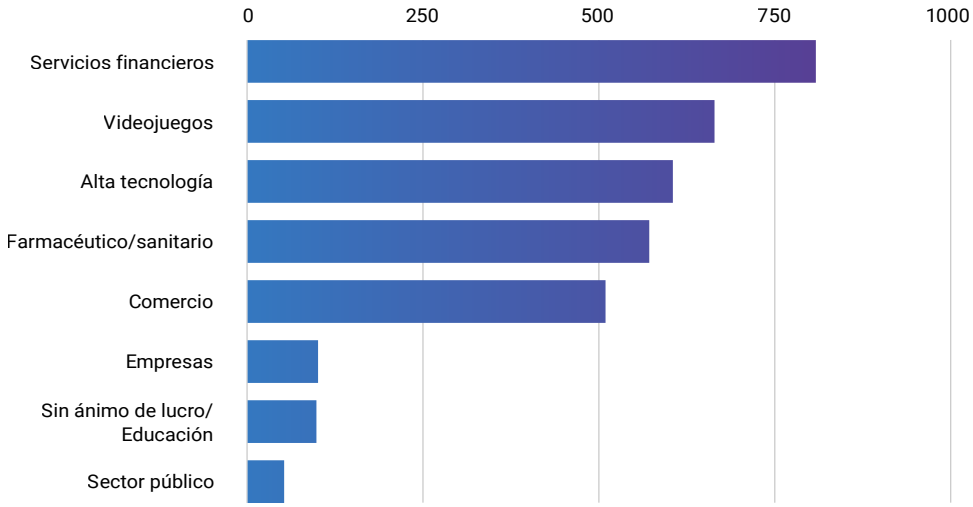


DDoS: Here to Stay, marzo de 2024

En concreto, los servicios financieros se han convertido cada vez más en un objetivo de los ataques DDoS a la capa 7. Desde 2021, Akamai ha observado que se viene produciendo un aumento evidente y notable en el número de ataques DDoS contra empresas de servicios financieros. Más de un tercio (35 %) de los ataques de 2023 a todos los sectores se produjeron contra instituciones de servicios financieros, lo que convirtió al sector en un objetivo más codiciado que el de los videojuegos. Del análisis de Akamai se deduce que la banca fue el objetivo del 63 % de los ataques DDoS en todo el mundo. Casi tres cuartas partes (72 %) de los ataques en la región EMEA y el 91 % en la región APAC se centraron en la banca. En América, sin embargo, los ataques DDoS tuvieron una distribución más uniforme entre las instituciones bancarias, el sector de los seguros y otros servicios financieros.

América: los servicios financieros representan el 28 % de los ataques DDoS

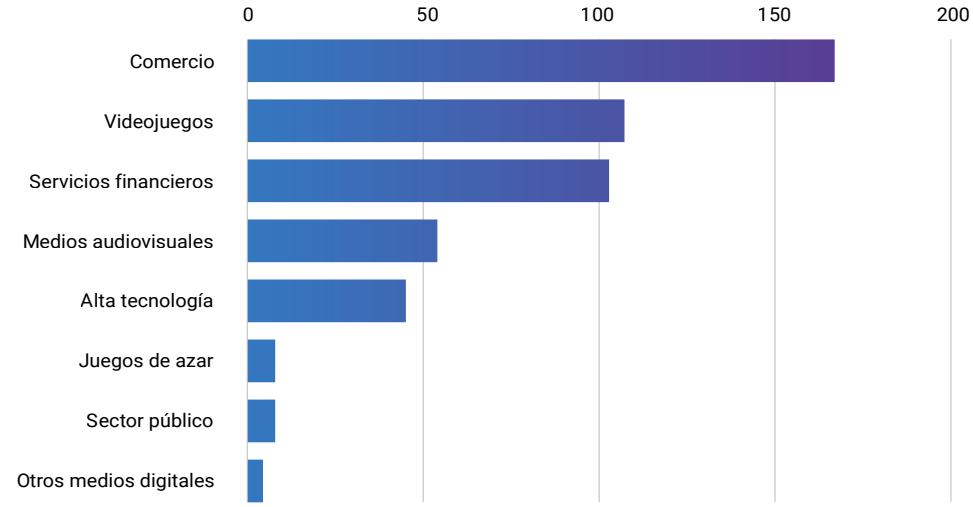
De junio de 2023 a diciembre de 2023



DDoS: Here to Stay, marzo de 2024

APAC: los servicios financieros representan el 11 % de los ataques DDoS

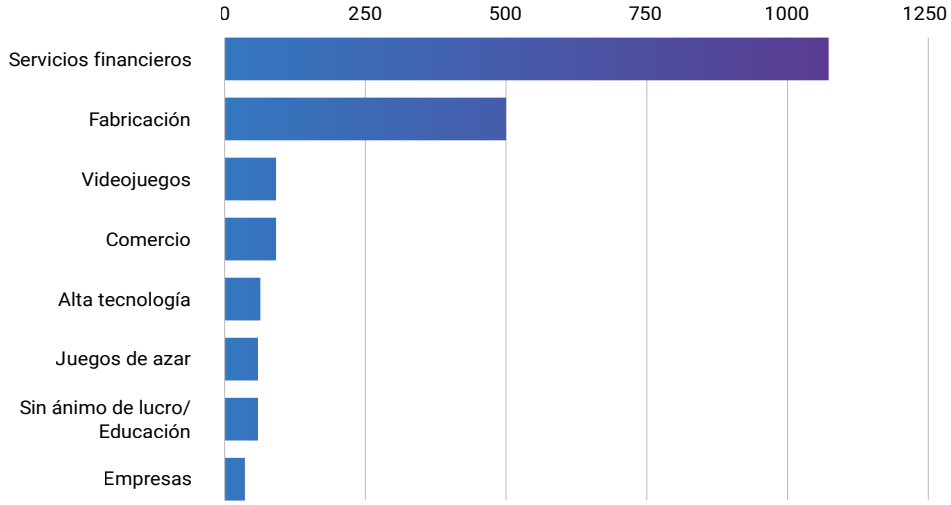
De junio de 2023 a diciembre de 2023



DDoS: Here to Stay, marzo de 2024

EMEA: los servicios financieros representan el 66 % de los ataques DDoS

De junio de 2023 a diciembre de 2023



DDoS: Here to Stay, marzo de 2024

En uno de estos ejemplos recientes de un sofisticado ataque DDoS a la capa 7 dirigido contra uno de los clientes de servicios financieros de Akamai, los ciberadversarios utilizaron la automatización para llevar a cabo un ataque altamente distribuido. En él se utilizó una inundación HTTP GET dirigida principalmente a URL que no se almacenan en caché (como la página de inicio y los terminales de inicio de sesión). Mediante la utilización de varios controles proactivos, se consiguió mitigar este ataque sin que ello afectara al origen del cliente. En este mapa térmico del origen del ataque se revela el creciente uso de proveedores de servicios en la nube, nodos de salida The Onion Router (Tor) y nodos proxy anónimos o abiertos:

Ataques DDoS por sistema autónomo

Visualización de un ataque a la capa de aplicación contra una institución financiera que tuvo lugar en el primer trimestre de 2024 en más de 100 países y que Akamai ayudó a mitigar

Los autores de ataques DDoS tienen la capacidad de crear y coordinar una infraestructura muy dispersa, aprovechando direcciones IP dinámicas en redes extensas, con numerosos países y regiones de todo el mundo.

Herramientas y técnicas utilizadas por los atacantes

Desafortunadamente, los atacantes y sus métodos durante los ataques DDoS no son siempre iguales. A medida que los atacantes siguen encontrando formas de monetizar sus acciones, van adaptando sus técnicas, utilizando las nuevas herramientas disponibles y encontrando nuevos métodos de ataque. Hay varios factores que son reflejo de esta evolución.

Automatización: los atacantes utilizan scripts y bots automatizados para imitar el comportamiento de los usuarios legítimos, lo que hace que la detección sea mucho más complicada. Además, ahora están recurriendo a algoritmos de aprendizaje automático (ML) que se adaptan y evaden la detección tradicional.

Ataques multivectoriales: los adversarios están empleando cada vez más estrategias multivectoriales, combinando diferentes tipos de ataques, como inundaciones de solicitudes GET y POST, así como objetivos de DNS, como ataques de amplificación y fragmentación, con otras combinaciones para saturar tanto a los recursos de red como a los de las aplicaciones.

API como objetivo: conforme las empresas confían cada vez más en las API para impulsar sus aplicaciones, los atacantes están encontrando nuevas oportunidades al aprovechar las vulnerabilidades de las API en sus ataques DDoS. El objetivo de estos ataques es agotar los recursos del servidor y esto lo consiguen solicitando miles de conexiones simultáneamente, o bien aprovechando los defectos lógicos, lo que provoca interrupciones en el servicio.

Explotación de los dispositivos de IoT: la proliferación de dispositivos del Internet de las cosas (IoT) con una seguridad deficiente incluye un enorme ejército de botnets. A menudo, estos dispositivos se secuestran y se utilizan para lanzar ataques DDoS masivos, que aprovechan su conectividad de red y potencia informática.

Aumento de la sofisticación

Con estas nuevas herramientas y técnicas, se ha producido un aumento consecuente de la complejidad y frecuencia de los ataques DDoS, pasando ahora los atacantes a utilizar métodos sofisticados para eludir las defensas tradicionales. Algunas de las tendencias destacadas son:

Cifrado: un cambio destacado hacia los ataques DDoS basados en HTTPS ha hecho que mitigar estos ataques sea más difícil. Estos ataques, que están cifrados, se enmascaran como tráfico legítimo, lo que hace que sean más difíciles de detectar y filtrar, ya que las medidas de protección contra DDoS tradicionales tienen limitaciones a la hora de descifrar el tráfico SSL/TLS en la capa de aplicación.

Botnets y proxies: teniendo en cuenta el importante aumento del número de botnets DDoS y el uso mayoritario de proxies anónimos por parte de los atacantes, las solicitudes ahora se envían desde una multitud de direcciones IP (normalmente más de 10 000 IP por ataque). Los atacantes utilizan esta estrategia para eludir las medidas de mitigación que llevan a cabo un recuento de las solicitudes de una única IP. El predominio de plataformas de alojamiento en la nube y la adopción de servicios basados en la nube no hacen sino facilitar la preparación de estos ataques de alta intensidad y altamente distribuidos.

Ataques DDoS por sistema autónomo

Visualización de un reciente ataque DDoS a la capa de aplicación, 650 000 transacciones por segundo (TPS), 20 Gbps, más de 9000 millones de solicitudes en total, contra un cliente financiero de Akamai

Los autores de ataques DDoS son capaces de crear y coordinar una infraestructura con una distribución enorme, principalmente de proveedores de servicios en la nube.

Uno de los enfoques dinámicos que están adoptando los defensores es el seguimiento de solicitudes por huella de TLS, formada por varias señales de la capa de TLS, como los tipos de cifrado y su orden. Aunque este enfoque puede generar falsos positivos, si se utiliza correctamente puede proporcionar una mitigación más eficaz cuando un atacante trabaje desde varias máquinas e IP, ya que los dispositivos afectados tienen instalado el mismo software. Estos dispositivos presentan características similares en cuanto al entorno, una de las cuales es la biblioteca TLS compartida.

Variedad de ingredientes

Aunque las herramientas disponibles en el mercado están en constante cambio, la evolución de las técnicas de ataque hace pensar que se está produciendo una tendencia hacia métodos más sofisticados y menos detectables. Entre ellos se incluyen los siguientes:

- **Dispositivos IoT infectados:** los atacantes siguen utilizando dispositivos del IoT infectados en botnets como método para lanzar ataques DDoS a gran escala, lo que pone de manifiesto la continua vulnerabilidad de estos dispositivos.

- **Servicios de DDoS de alquiler:** la disponibilidad de los servicios de DDoS de alquiler ha bajado la barrera de entrada para lanzar ataques, lo que permite a personas sin muchos conocimientos técnicos llevar a cabo ataques a gran escala.
- **Técnicas de evasión:** las técnicas avanzadas de evasión, como los parámetros de encabezado aleatorios y los argumentos de solicitud dinámicos, se han vuelto habituales. Estas técnicas suponen un reto para los enfoques tradicionales de detección y mitigación, ya que hacen que sea más difícil distinguir el tráfico malicioso de las solicitudes legítimas.

Vulnerabilidades que se suelen aprovechar en estos ataques

Las vulnerabilidades que aprovechan los atacantes en los ataques DDoS a la capa 7 suelen estar relacionadas con la forma en que las aplicaciones web procesan la información introducida por los usuarios y en que gestionan los datos. Para mitigar estas vulnerabilidades, resulta crucial emplear una combinación de medidas de seguridad.

En los últimos años, una de las vulnerabilidades más importantes que los atacantes han aprovechado al llevar a cabo ataques DDoS a la capa de aplicación ha sido Rapid Reset en HTTP/2, del que se habló mucho a finales de 2023. Estos ataques aprovecharon una vulnerabilidad en el protocolo HTTP/2, que es fundamental para el funcionamiento de Internet y de todos los sitios web. Este hecho produjo un aumento general del 65 % en el tráfico de ataques DDoS HTTP en un trimestre en comparación con el anterior, lo que pone de relieve la gravedad y el efecto que tienen los ataques que se valen de esta vulnerabilidad.

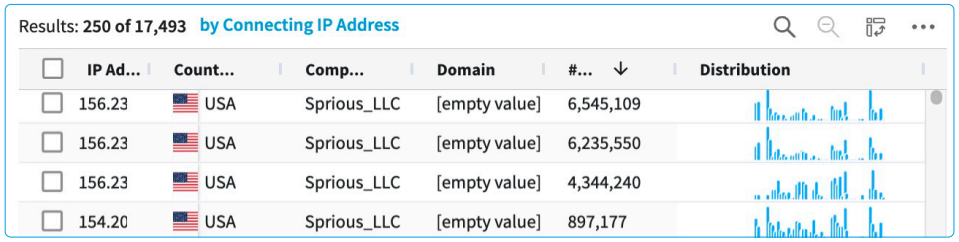
Gracias a esta vulnerabilidad concreta, los atacantes generan un mayor impacto, al aprovechar plataformas de cloud computing y HTTP/2, lo que les ha permitido lanzar ataques DDoS hipervolumétricos con botnets relativamente pequeñas. Entre los sectores más afectados por estos ataques se encontraron el de los videojuegos, el de tecnologías de la información (TI), las criptomonedas, el software informático y las telecomunicaciones, con Estados Unidos, China, Brasil, Alemania e Indonesia como principales orígenes de estos ataques.

Como respuesta, un esfuerzo conjunto de todo el sector reveló la vulnerabilidad HTTP/2 Rapid Reset (CVE-2023-44487) para arrojar luz sobre los ataques DDoS que se sirven de este defecto. El objetivo fueron varios proveedores, incluidos los principales de servicios en la nube y redes de distribución de contenido (CDN), entre otros.

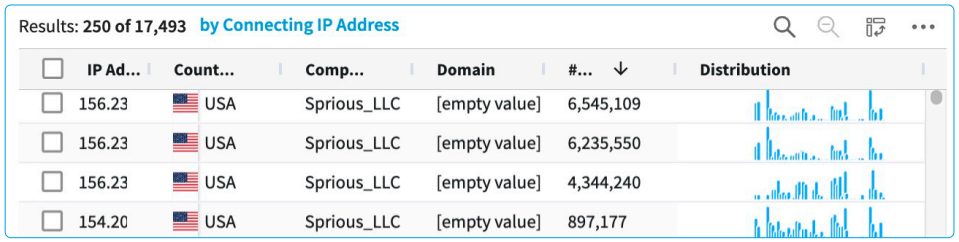
Ejemplos reales: uso de la automatización en un ataque DDoS

Los atacantes a menudo usan varias herramientas DDoS para llevar a cabo sus ataques, y se valen de diferentes técnicas combinadas para eludir los productos de seguridad o, al menos, conseguir que sean menos eficientes. A continuación se describe un ejemplo de ataque documentado con Akamai Web Security Analytics.

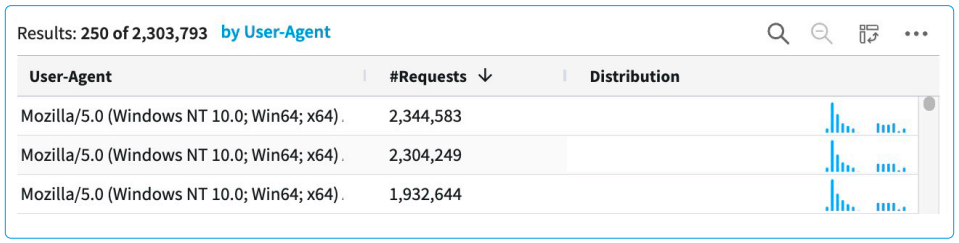
- Ataque observado desde más de 17 000 direcciones IP



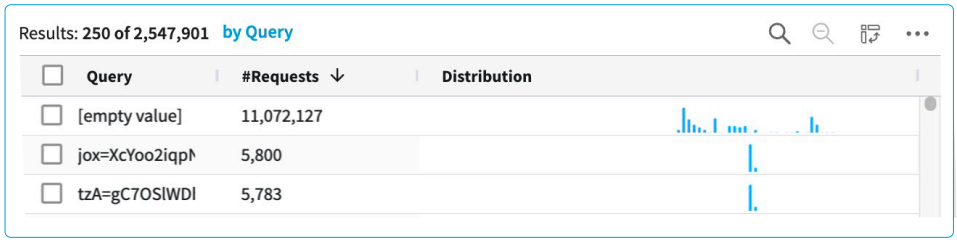
- Orígenes de ataque desde más de 400 redes



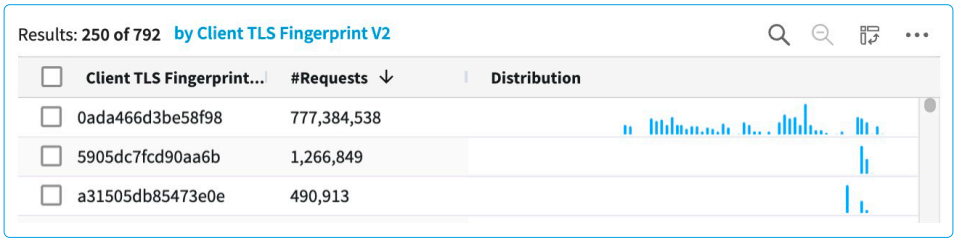
- 2 303 793 agentes de usuario únicos



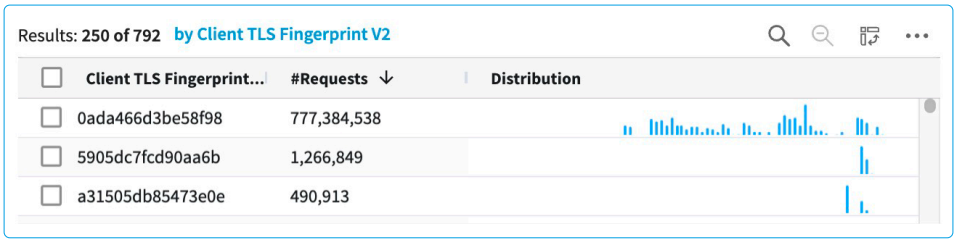
- 2 547 901 cadenas de consulta únicas y aleatorias



- Rotación de encabezados HTTP (por ejemplo, Accept-Language, Referer).



- Rotación de configuración de TLS



Para mitigar estos ataques sofisticados se necesita una estrategia de protección por capas. El uso de controles proactivos y reactivos, como una combinación avanzada de coincidencias de solicitudes y características de tráfico de origen en la limitación de velocidad, o bien de controles de reputación de origen, puede resultar útil.

Evolución de los adversarios: suplantación de la señal TLS

Las observaciones recientes han demostrado que los agentes maliciosos utilizan cada vez más señales TLS como parte de sus herramientas DDoS para eludir las detecciones, lo que hace que dichas conexiones parezcan proceder de navegadores Chrome legítimos. En lugar de utilizar una versión de Chrome sin interfaz que consume muchos recursos, lo que podría ralentizar el ataque, los atacantes podrían haber empleado una versión modificada de la biblioteca TLS, lo que les permitiría establecer e imitar las señales TLS de cualquier navegador auténtico. Aunque existen herramientas diseñadas para replicar las huellas digitales de TLS, no suelen encontrarse en las herramientas de ataques DDoS. El uso de este tipo de ataque sugiere un aumento de la destreza técnica de los atacantes y un amplio conocimiento de las defensas; por eso, las estrategias de defensa contra ataques DDoS a la capa 7 deben incluir investigaciones periódicas sobre las tendencias de ataque más recientes. Esto también parece sugerir que las herramientas DDoS que incluyen la suplantación de TLS son cada vez más habituales.

Akamai

Pasos iniciales antes de preparar su receta de defensa

Eche un vistazo al panorama: evaluación de riesgos e identificación de vulnerabilidades

Al identificar sus activos críticos y decidir cuáles podrían ser sus puntos vulnerables, puede mejorar mucho su estrategia de mitigación de ataques DDoS a la capa 7. Esta evaluación de riesgos permite priorizar qué recursos proteger en función de su importancia y vulnerabilidad. Al conocer los posibles vectores de ataque y sus consecuencias, las organizaciones pueden implementar contramedidas específicas, como la limitación de velocidad, los firewalls de aplicaciones web (WAF) y el análisis del comportamiento, para mitigar los riesgos de forma eficaz. Además, una evaluación continua de riesgos permite una estrategia de defensa que se vaya adaptando a las nuevas amenazas y a los requisitos empresariales en constante cambio.

Los distintos sectores y empresas pueden adoptar otro enfoque para evaluar los riesgos de ataques DDoS a la capa de aplicación. Por ejemplo:

> **Comercio electrónico:** antes de una venta importante, en una evaluación de riesgos se podría identificar el proceso de pago como una vulnerabilidad crítica. Las medidas de mitigación podrían incluir la implementación de un WAF y la limitación de velocidad para proteger el servicio.
>
> **Servicios financieros:** en el caso de una aplicación bancaria, la evaluación de riesgos podría determinar que la página de inicio de sesión es un objetivo principal de los ataques DDoS. El banco podría emplear una combinación de limitación de velocidad adaptada a los terminales y detección conductual para distinguir entre usuarios legítimos y tráfico de ataque.

Conocer las vulnerabilidades concretas permite preparar defensas específicas y mejorar el funcionamiento de los servicios críticos durante un ataque.

Evite que haya demasiados cocineros: roles y responsabilidades

El establecimiento de roles y responsabilidades bien definidos son pasos esenciales para una estrategia eficaz contra ataques DDoS a la capa 7, ya que aumentan las posibilidades de responder de forma coordinada y eficiente en caso de ataque. Sin roles claros, los esfuerzos de respuesta pueden volverse caóticos, con tareas duplicadas y lagunas en la protección. Unas responsabilidades bien definidas ayudan a identificar las tareas específicas de cada uno de los miembros del equipo, desde la supervisión del tráfico y la identificación de anomalías hasta la implementación de estrategias de mitigación y la comunicación con las partes interesadas. Esta coordinación permite minimizar el impacto de los ataques, que se pueda mantener la disponibilidad de los servicios y proteger los activos críticos.

De hecho, que haya demasiadas personas responsables de la toma de decisiones sin roles claros puede hacer que se tarde demasiado en responder a un ataque DDoS. Por ejemplo, si tanto los equipos de operaciones de red como los de ciberseguridad toman decisiones de forma independiente sobre diferentes enfoques de mitigación sin coordinación, podrían neutralizar sin desearlo el trabajo de los demás o no prestar la atención debida a vulnerabilidades críticas. Una estrategia adecuada implica asignar roles predefinidos, como una persona encargada de la respuesta ante incidentes, un encargado de coordinar las comunicaciones y un equipo de respuesta técnica. De esta forma, es posible garantizar acciones rápidas y coordinadas contra los ataques, minimizar el tiempo de inactividad y optimizar el análisis posterior al incidente.

Elija los utensilios adecuados para su cocina

Detectar y mitigar un ataque a la capa de aplicación puede resultar complicado, ya que es muy difícil distinguir entre tráfico legítimo y malicioso. Como respuesta a estas amenazas en constante evolución, recomendamos adoptar un enfoque polifacético de defensa:

- **Adopte soluciones siempre activas y a petición:** asegúrese de que los controles de seguridad de DDoS estén siempre activos, y actualice los planes de respuesta ante incidentes para abordar al instante las amenazas emergentes.
- **Cree una arquitectura flexible y fiable:** anticipe un punto único de fallo, ya que los atacantes probablemente se centrarán en varios servicios, incluyendo el DNS, las aplicaciones web, las API, y la infraestructura del centros de datos y de la red. Usar la arquitectura adecuada será esencial para protegerse contra los ataques DDoS a la capa 7. Estos aspectos que tener en cuenta de la arquitectura pueden incluir la elección de la protección contra DDoS basada en el Edge o en la CDN, que siempre está activada. No sobreestime su fiabilidad. La escala de los ataques DDoS actuales puede saturar fácilmente la mayor parte de la infraestructura.
- **Evalúe los acuerdos de nivel de servicio (SLA) de su proveedor** y adáptelos a su estrategia.
- **Revise el nivel de preparación de su proveedor:** elija uno que garantice la realización de forma periódica de una revisión de sus componentes de red críticos, y que evalúe los diferentes mecanismos de protección contra DDoS para conocer su eficacia a la hora de hacer frente a los métodos de ataque actuales.
- **Consulte su guía de respuesta ante ataques DDoS:** coordine a su personal de TI, operaciones, seguridad y comunicación con el cliente para mejorar su preparación en caso de ataque.
- **Protección contra DDoS de emergencia:** tenga un plan preparado para incorporar un proveedor de soluciones de mitigación de DDoS en caso de crisis. Si cuenta con un partner que le ofrezca protección contra DDoS, llame a su línea directa de asistencia para DDoS.

Recetas para la detección y mitigación

Para una protección eficaz contra ataques DDoS a la capa 7 se necesitan varias estrategias de detección y mitigación. Existen varias metodologías que se pueden aplicar, cada una de las cuales tiene sus puntos fuertes y consideraciones clave.

Detección conductual/basada en anomalías

Puntos fuertes: este enfoque se basa en el uso del aprendizaje automático y el análisis estadístico para conocer sus patrones de tráfico normales y, a continuación, identificar las desviaciones que podrían indicar un ataque DDoS. Es muy eficaz contra ataques complejos, antes nunca vistos.

Aspectos clave: para una detección eficaz se necesita un período de aprendizaje que puede durar varias semanas, en el que se establece una base de tráfico que se considera "normal", durante la que la detección puede que no sea tan eficaz. El modelo puede devolver falsos positivos si no se ha entrenado con precisión.

Detección basada en la velocidad y el rendimiento

Puntos fuertes: este método, que es fácil de aplicar, supervisa la velocidad y el volumen de las solicitudes, activando alertas o procesos de mitigación cuando el tráfico supera unos umbrales predefinidos. Es eficaz para identificar al instante ataques volumétricos a gran escala.

Aspectos clave: los picos de tráfico legítimo, como los que se producen durante eventos promocionales, pueden confundirse con ataques DDoS. Es posible que no detecte ataques de poco volumen y a velocidad lenta que escapan al control del radar.

Detección basada en firmas

Puntos fuertes: mediante la comparación del tráfico con respecto a una base de datos de patrones de ataque conocidos, este método puede identificar y bloquear rápidamente las amenazas reconocidas. Es muy eficaz contra vectores de ataque habituales y previamente identificados.

Aspectos clave: no puede detectar ataques nuevos o modificados que no coincidan con las firmas existentes. Es necesario realizar actualizaciones periódicas para mantener la eficacia.

Pruebas de desafío/respuesta

Puntos fuertes: este enfoque plantea desafíos al tráfico entrante si proviene de personas o bots. Los procesos CAPTCHA o JavaScript pueden conseguir mitigar los bots y las herramientas de ataque automatizadas.

Aspectos clave: los desafíos pueden suponer una interrupción del trabajo del usuario si se implementan de forma agresiva. Los bots más sofisticados pueden superar algunas pruebas de desafío/respuesta, lo que obliga a actualizar de forma periódica sus mecanismos de defensa.

Enfoques híbridos

La combinación de varias estrategias de detección y mitigación puede ofrecer una protección más completa. Por ejemplo, el uso de la detección basada en anomalías para detectar posibles ataques, junto con métodos basados en la velocidad y en la firma para conseguir una mayor cobertura, permite mecanismos de defensa más sólidos. Las pruebas de desafío/respuesta pueden ayudar a distinguir entre bots sofisticados y usuarios legítimos.

Métodos convencionales

Filtrado de IP y geográfico: bloquear o limitar el tráfico de determinados rangos de IP o CIDR y regiones geográficas que no son relevantes para su empresa puede reducir su exposición a ataques procedentes de esas áreas. Aunque este método puede ser útil cuando el origen de los usuarios de la empresa es conocido y limitado, a menudo puede plantear desafíos para el mantenimiento rutinario y la actualización de la lista de fuentes autorizadas. Además, los hackers experimentados pueden utilizar proxies para evitar el bloqueo geográfico. Sin embargo, sigue siendo un método habitual y una estrategia de defensa inicial contra los ataques DDoS a la capa 7.

Análisis de protocolos de la capa de aplicación: con este método se pueden mitigar los ataques DDoS a la capa 7 mediante el análisis de los datos de sus protocolos para detectar anomalías o patrones maliciosos, lo que permite adoptar mecanismos de defensa proactivos. Con este método pueden evitarse ataques DDoS sofisticados que eludan las medidas de seguridad convencionales, pero puede generar un consumo de recursos elevado para realizar una inspección exhaustiva de los paquetes, así como más posibilidades de falsos positivos, lo que podría bloquear, de forma no intencionada, el tráfico legítimo.

Cómo encontrar la receta correcta y equilibrada para una estrategia de defensa contra DDoS multicapa

La elaboración de una estrategia de defensa contra DDoS multicapa implica un enfoque diferenciado, adaptado al perfil de riesgo específico de una organización y al panorama de ciberamenazas en constante cambio. En esencia, para esta estrategia es necesario realizar una evaluación inicial que identifique los activos críticos y los posibles vectores de ataque, a lo que seguirá la implantación de protecciones básicas, como la limitación de velocidad y los firewalls. Las medidas avanzadas requieren una combinación de detección basada en anomalías en el caso de nuevas amenazas, detección basada en firmas para ataques conocidos y mecanismos de desafío/respuesta para el filtrado de bots.

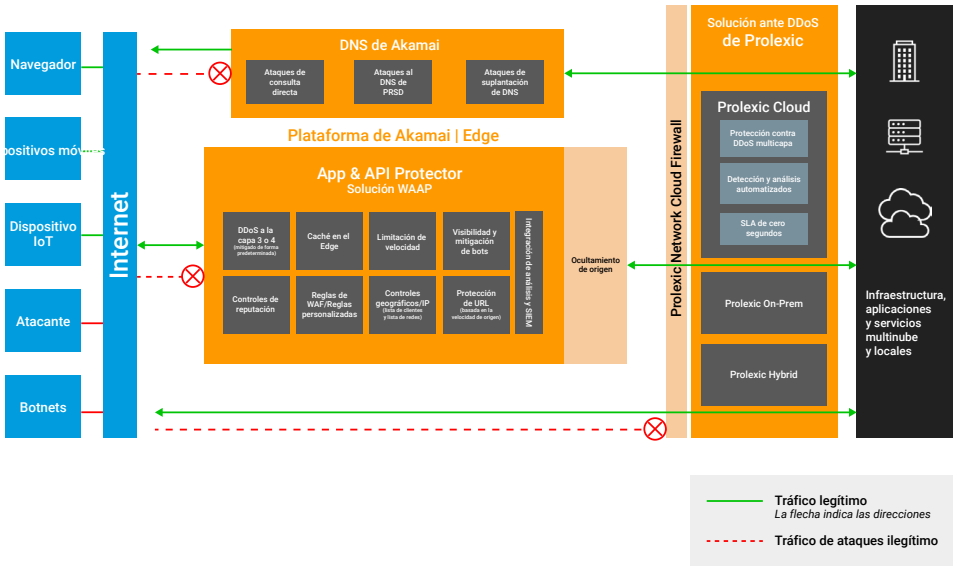
Mediante la incorporación de inteligencia adaptativa frente a amenazas, como algoritmos que determinan los patrones de huella digital de TLS de fuentes de ataques DDoS conocidas y emergentes, el sistema de seguridad puede adaptar automáticamente sus mecanismos de mitigación para bloquear o desafiar el tráfico que muestra esa huella digital y neutralizar eficazmente el ataque. Un plan completo de respuesta ante incidentes y recuperación es crucial para minimizar los daños y mantener la confianza durante y después de un ataque. El aprendizaje continuo y los ajustes basados en ataques anteriores y tendencias emergentes consiguen que la estrategia de defensa sea eficaz y flexible en todo momento.

Una institución financiera que sufre sofisticados ataques DDoS multivectoriales es un claro ejemplo de la importancia de contar con una estrategia de defensa equilibrada y multicapa. El efecto que el tiempo de inactividad puede tener en sus operaciones y en la confianza de los clientes convierte a estas instituciones en los principales objetivos.

Mediante la integración de una combinación de métodos de detección y mitigación, como la detección de anomalías de tráfico, el uso de métodos convencionales, como la limitación de velocidad, el filtrado de IP/ubicaciones geográficas, la reputación de las IP y la inteligencia ante amenazas en tiempo real, junto con un sólido plan de respuesta ante incidentes, pueden proteger sus activos críticos contra interrupciones, al tiempo que se garantiza la continuidad del servicio a sus clientes. Este enfoque integral es una muestra de cómo las organizaciones pueden defenderse de la naturaleza polifacética de los ataques DDoS en el panorama digital actual.

Preparación: estrategia de defensa en profundidad con la arquitectura en el Edge de Akamai

El enfoque de Akamai ante la protección contra DDoS a la capa de aplicación tiene un carácter multicapa, exhaustivo y adaptable, diseñado para proteger los sitios web, las aplicaciones y las API contra los ataques más sofisticados. App & API Protector utiliza varias funciones clave que proporcionan una protección completa, al combinar un firewall de aplicaciones web, visibilidad y mitigación de bots, seguridad de API y protecciones contra DDoS de capa 7 en un único producto. De esta forma, es capaz de ofrecer una protección completa.



Arquitectura de referencia para la protección integral contra DDoS mediante las soluciones Edge DNS, App & API Protector y Prolexic

La estrategia de protección contra DDoS de Akamai se basa en una arquitectura de defensa del Edge que enruta el tráfico a través de una plataforma ampliamente distribuida, donde se revisa cada una de las solicitudes en tiempo real. Esta configuración protege contra ataques DDoS a las aplicaciones web y API, así como contra bots maliciosos en el Edge, evitando que lleguen a las aplicaciones o a la infraestructura. De esta forma, se mejora la continuidad empresarial, al mantener una arquitectura rápida, muy segura y disponible en todo momento que cambia conforme lo hacen los ataques.

El sólido conjunto de herramientas e ingredientes de Akamai proporciona controles proactivos y reactivos, cada uno de los cuales cumple un objetivo distinto en la estrategia de defensa general.

Controles proactivos

Los controles proactivos ayudan a prevenir los ataques antes de que se produzcan, centrándose en reforzar la estrategia de seguridad para minimizar las vulnerabilidades. Entre ellos, se incluyen:

- **Controles de IP (bloqueo de rangos de IP, de CIDR y ASN):** estos controles, capa fundamental de defensa, bloquean direcciones IP maliciosas conocidas o rangos identificados a través de la inteligencia contra amenazas.
- **Controles geográficos (bloqueo de determinadas zonas geográficas):** al permitir o restringir el tráfico de regiones concretas, las organizaciones pueden limitar de forma preventiva la exposición a ataques procedentes de zonas de alto riesgo.
- **Reglas de firewall de aplicaciones web (WAF):** la aplicación de reglas contra vulnerabilidades y vectores de ataque conocidos, por ejemplo herramientas DDoS como FiberFox, ofrece una sólida primera línea de defensa.
- **Controles de reputación de IP:** el uso de la inteligencia a través de heurística de recursos maliciosos conocidos de DDoS, scraping web y otras actividades maliciosas permite el bloqueo preventivo o el escrutinio del tráfico sospechoso.
- **Inteligencia sobre DDoS de la plataforma:** la información sobre ataques DDoS de la plataforma en el Edge de Akamai distribuida a nivel mundial puede permitir la creación de una estrategia de mitigación proactiva en la lucha contra los ataques DDoS a la capa de aplicación.
- **Almacenamiento en caché:** la optimización del almacenamiento en caché de contenido puede reducir en gran medida la carga en los servidores de origen, mitigando de forma indirecta el impacto de los ataques DDoS mediante el envío de solicitudes desde la caché en el Edge.
- **Site Shield:** la ocultación del origen, al permitir solo solicitudes a orígenes a través de la red Edge de Akamai, puede reducir aún más las cargas del servidor.

Controles reactivos

Los controles reactivos son respuestas ante un ataque detectado, cuyo objetivo es mitigar su impacto y conseguir que el servicio siga estando disponible.

- **Limitación de velocidad (políticas de velocidad):** resulta esencial para mitigar los picos de tráfico repentinos que pueden ser indicativo de un ataque DDoS. Las opciones se pueden configurar y adaptar a los perfiles de tráfico específicos del cliente. La limitación de velocidad suele ser la primera línea de defensa a la hora de proteger el origen del cliente frente a ataques DDoS volumétricos y distribuidos.
- **Protección frente a POST lento:** este control se centra específicamente en los ataques HTTP POST lentos y reacciona ante patrones de tráfico anómalos que pretenden agotar los recursos del servidor.

- **Reglas personalizadas en el WAF:** debería poder adaptar las reglas rápidamente como respuesta a las amenazas emergentes, ofreciendo mecanismos de defensa flexibles y dinámicos.
- **Visibilidad y mitigación de bots:** el aprendizaje automático para detectar la suplantación de los navegadores le permite identificar y bloquear sofisticados ataques DDoS que se originan mediante la automatización.
- **Protección de URL con deslastre de carga inteligente:** los controles que limitan el exceso de solicitudes al origen y priorizan a los usuarios legítimos sobre el tráfico malicioso pueden ayudarle a mantener el tiempo de actividad del servicio durante un ataque DDoS.
- **Inteligencia sobre DDoS de la plataforma:** el deslastre de carga es una categoría de protección de URL que utiliza la información sobre ataques DDoS de la plataforma global de Akamai, y permite a nuestros clientes crear una estrategia de mitigación proactiva para combatir los ataques DDoS al nivel de aplicación.

Combinación de ingredientes para conseguir una receta equilibrada

- **Ejemplo:** una importante empresa de servicios financieros desarrolla una estrategia de defensa en profundidad con la solución WAAP de Akamai

Es posible que algunas organizaciones se encuentren como objetivo frecuente de los ataques DDoS. Por ejemplo, según la investigación de Akamai, más de un tercio de los ataques DDoS en 2023 tuvieron en el punto de mira a instituciones de servicios financieros. Una importante empresa de servicios financieros, cliente de Akamai, fue objeto de un ataque a su página de inicio de sesión. Fue capaz de seguir los pasos de una receta con resultados demostrados para la defensa. Usted también puede hacer lo mismo.


Perfil del atacante: hacktivista


Objetivo: terminal de inicio de sesión


Método: inundación HTTP POST


Orígenes de ataques: ~66 000 direcciones IP y ~140 países

Akamai

Receta
mitigación de un ataque de inundación HTTP POST

Ingredientes:

Controles proactivos:

- **Controles de IP**: utilice la inteligencia contra amenazas para bloquear direcciones IP o rangos de CIDR asociados a entidades maliciosas conocidas.
- **Controles geográficos**: bloquee tráfico de zonas geográficas conocidas por albergar a grupos hacktivistas, como regiones asociadas a "Anonymous Sudan".
- **Reglas de firewall de aplicaciones web (WAF)**: implemente reglas diseñadas específicamente para contrarrestar las herramientas y tácticas DDoS conocidas, incluidos los patrones típicos de las inundaciones HTTP GET.
- **Controles de reputación de IP**: supervise exhaustivamente o bloquee activamente (en tiempo real) el tráfico de fuentes con puntuaciones de reputación bajas.
- **Inteligencia sobre DDoS de la plataforma**: aplique la información obtenida de los datos de ataques DDoS a nivel mundial de Akamai para anticiparse a los vectores de amenazas emergentes y contrarrestarlos.
- **Site Shield**: habilite listas de control de acceso (ACL) del firewall para permitir solo el tráfico procedente de la red del Edge de Akamai y bloquear el resto.

Controles reactivos:

- **Limitación de velocidad**: establezca políticas de velocidad para mitigar los picos repentinos de tráfico, definiendo umbrales adecuados para las solicitudes por segundo en la página de inicio. Optimice la limitación de velocidad (1) reduciendo los intervalos de tiempo para medir la velocidad de las solicitudes a una solicitud por segundo, y (2) aplicando la limitación de velocidad en función de la puntuación de la zona geográfica y de reputación de las fuentes de IP conectadas, al tiempo que se autorizan las fuentes, como las direcciones IP corporativas y los partners de la institución financiera.
- **Reglas personalizadas en WAF**: cree reglas personalizadas como respuesta a las características específicas del ataque una vez detectado. Utilizar controles de muestreo de tráfico en sus reglas personalizadas facilitará el análisis del tráfico, para buscar de manera más eficiente las principales fuentes de ataques, mientras que el uso de controles geográficos/IP en las reglas personalizadas puede ayudar en el proceso de mitigación instantánea.
- **Visibilidad y mitigación de bots**: utilice la detección de suplantación del navegador para identificar y bloquear las solicitudes que imitan el comportamiento del usuario legítimo, pero que forman parte de la inundación.
- **Protección de URL**: aplique controles para limitar los índices de solicitudes específicamente a la URL de inicio de sesión, conservando el ancho de banda para los usuarios legítimos. Configurar el deslastre de carga inteligente con categorías como proxies, nodos de salida Tor, bots básicos, IP de baja reputación, etc., permitirá priorizar el tráfico de usuarios reales por encima de esas posibles fuentes maliciosas.

Método de preparación:

Fase de revisión:

- **Revise la configuración**: lleve a cabo una revisión exhaustiva de su estrategia de seguridad actual. Configure sus controles proactivos en función de lo que encuentre, asegurándose de que todos los controles geográficos y de IP relevantes se gestionen de la forma adecuada.
- **Optimización de la configuración**: ajuste la configuración para reconocer y mitigar patrones de tráfico inusuales, incluidas las características de los ataques de inundación HTTP POST.

Fase de detección y mitigación:

- **Supervisión y alertas**: la arquitectura de defensa en el Edge de Akamai puede supervisar el tráfico entrante en busca de patrones que podrían indicar un ataque DDoS. Así, le permite configurar alertas para picos de tráfico o patrones anómalos asociados a los métodos DDoS conocidos, como una inundación HTTP POST.
- **Detección y mitigación**: varios controles proactivos, como la reputación de IP, el almacenamiento en caché y los controles de IP/ubicación geográfica, proporcionan automáticamente funciones de detección y mitigación si se configuran correctamente.

Una vez detectado un ataque, controles como la limitación de velocidad, la protección de URL y la detección de la suplantación del navegador se activan automáticamente sin la intervención del usuario.

- **Análisis y adaptación**: analice de forma continua los patrones de ataque y adapte sus medidas defensivas en tiempo real para hacer frente a la evolución de las tácticas. Por ejemplo, cree reglas personalizadas o políticas de limitación de velocidad basadas en el análisis del tráfico de ataques recientes.

Recuperación y análisis después del ataque:

- **Análisis de registros**: después del ataque, haga un análisis detallado del registro de tráfico para identificar los vectores empleados y la eficacia de los controles implementados.
- **Adaptaciones**: realice las adaptaciones necesarias en los controles proactivos y reactivos en función de la información obtenida del análisis de ataques.

Sugerencias de presentación:

- Revise y actualice periódicamente su estrategia de defensa para adaptarse a las tácticas de DDoS en constante evolución. Estas revisiones pueden variar mucho en función de la organización, como reflejo de sus necesidades específicas, la exposición a las amenazas y las prácticas recomendadas del sector. Una organización de servicios financieros puede necesitar dichas revisiones cada trimestre, mientras que una plataforma de comercio electrónico podría llevar a cabo revisiones semestrales como preparación para los picos de determinadas temporadas de compras.
- Establezca un plan de formación continua para que el equipo de seguridad se capaz de reconocer y responder a los nuevos vectores de ataque DDoS.
- Ponga en práctica simulacros de ataque para probar la eficacia de las medidas desplegadas y establecer el nivel de preparación del equipo para los incidentes reales.

Recuperación y análisis después del ataque

En la defensa contra los ataques DDoS a la capa de aplicación (capa 7), la fase posterior al ataque es esencial para reforzar las defensas futuras y conocer a su adversario. Esto implica dos pasos esenciales: analizar el patrón de ataque y mejorar sus defensas en función del análisis. Estos pasos son fundamentales para elaborar una estrategia de defensa flexible y garantizar la continuidad e integridad de los servicios online.

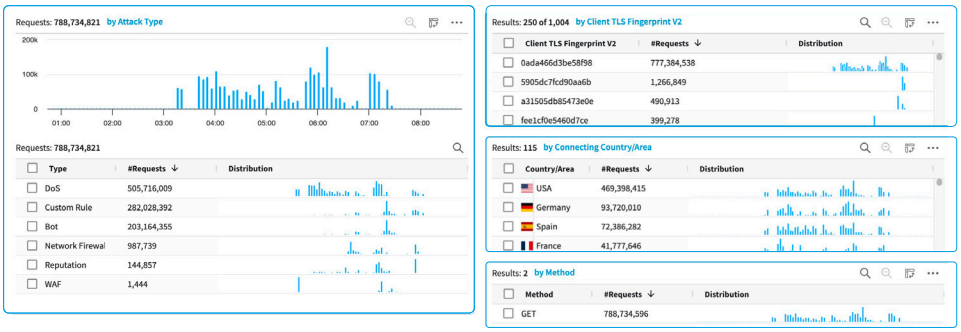
Análisis del tráfico y del patrón de ataque

El siguiente paso después de gestionar un ataque consiste en analizar el incidente para saber qué estrategia funcionó y cuál no funcionó según lo previsto. En esta evaluación se incluyen factores a largo plazo, como el impacto en la confianza del cliente, la integridad de los datos y las posibles pérdidas financieras. Los sistemas de análisis de seguridad integrales, como Web Security Analytics de Akamai, son herramientas indispensables en esta fase, que permiten a las organizaciones conocer el tráfico de los ataques y sus consecuencias.

Este análisis implica examinar al milímetro las tácticas, las técnicas y los procedimientos (TTP) que utilizan los atacantes. Algunas de las preguntas clave que se deben abordar son:

- ¿Qué tipo de pico de tráfico se produjo?
- ¿Fueron objetivo del ataque determinadas funcionalidades de la aplicación?
- ¿Aprovechó el ataque alguna vulnerabilidad conocida?

Akamai Web Security Analytics identifica anomalías en los patrones de tráfico, detecta el origen geográfico del ataque y clasifica el tipo de ataque en función de los comportamientos observados. En el siguiente ejemplo se muestran algunas de las características o dimensiones del tráfico que se pueden aplicar para investigar un ataque DDoS.



Las imágenes que se muestran proceden de Web Security Analytics, que ofrece una visibilidad sin precedentes y un análisis proactivo de los eventos de seguridad

Revisión y actualización de las estrategias de defensa según lo observado en el análisis del ataque

La revisión y actualización de las estrategias de defensa tras el análisis de los ataques es un componente fundamental para reforzar la estrategia de ciberseguridad de una organización. Al analizar los detalles concretos de un ataque anterior, las organizaciones pueden identificar vulnerabilidades en sus defensas actuales y hacer los ajustes necesarios. A continuación se detallan algunos ejemplos de cómo se puede aplicar este proceso con ayuda de Akamai Web Security Analytics.

Ejemplo 1: Actualización de las reglas del WAF en función de los patrones de ataque

Escenario: Una organización es objeto de un ataque DDoS a la capa 7 contra su aplicación web con un aluvión de solicitudes maliciosas a la página de inicio de la aplicación.

Revisión: El análisis de los ataques revela que las reglas de firewall de aplicaciones web (WAF) existentes consiguieron detectar y bloquear más del 90 % del tráfico de ataque, pero que el aproximadamente 10 % restante se filtró porque había una lista explícita de ubicaciones geográficas autorizadas que permitía que las fuentes de ataque de esa ubicación saturaran la aplicación.

Actualización: Tomando como base este análisis, la organización actualizó sus configuraciones de WAF con una regla personalizada adaptada a las características específicas del tráfico de ataque de esa zona geográfica concreta. Las excepciones pueden hacer que la ubicación geográfica siga estando autorizada, pero bloquear los atributos concretos del tráfico de ataque. Además, se han aplicado ajustes de limitación de velocidad más estrictos para esa zona geográfica concreta.

Ejemplo 2: Mejora de la protección del origen

Escenario: El proceso de inicio de sesión de un sitio web de retail es objeto de un sofisticado y altamente distribuido ataque DDoS a la capa 7 donde se utilizan bots automatizados.

Revisión: El análisis posterior indica que el tráfico durante el ataque estaba altamente distribuido, con origen en más de 150 países y con cientos de huellas digitales de TLS que parecían ser navegadores legítimos. Una buena parte del tráfico procedía de proveedores de servicios en la nube, algunos de los cuales estaban autorizados como fuentes de partners de confianza. Aunque el ataque se consiguió mitigar, el análisis reveló la necesidad de más medidas de defensa.

Actualización: Para proteger las URL donde se usan muchos recursos informáticos, como un proceso de pago, esta organización implementó protección de URL, una función diseñada específicamente para proteger las URL y los terminales de API que hacen un uso elevado de recursos informáticos frente a ataques DDoS a la capa de aplicación altamente distribuidos. Un arquitecto de seguridad también permitió el deslastre inteligente de cargas para bots, proxies, reputación de IP, etc. Esta función secundaria de la protección de las URL permite priorizar el tráfico de usuarios reales, al rechazar en primer lugar las solicitudes de fuentes posiblemente maliciosas.

La organización también decidió habilitar la funcionalidad integrada de protección contra bots en el WAF, a que la empresa no había prestado anteriormente la suficiente atención debido a la presencia de una solución de bots local que no pudo escalarse durante este ataque de gran velocidad.

Ejemplo 3: Implementación de la limitación de velocidad para terminales de API

Escenario: Un terminal de API de una aplicación de servicios financieros se ve saturado por una avalancha de solicitudes de transacciones fraudulentas, lo que es un indicativo de un ataque DDoS a la capa 7 cuyo objetivo es agotar los recursos del servidor.

Revisión: El análisis del patrón de ataque muestra que el objetivo concreto de los atacantes eran los terminales de API con un menor nivel de protección, que no eran capaces de procesar un volumen muy elevado de solicitudes.

Actualización: Como respuesta, la organización implementó una limitación de velocidad estricta en todos los terminales de API, especialmente en aquellos identificados como vulnerables. También adoptó un complemento de seguridad de API específico que ofrece capas avanzadas para la seguridad de API, incluido el abuso de la lógica de API, la amenaza de API en la sombra y la supervisión de vulnerabilidades de las API.

Conclusiones estratégicas

- **Supervisión y registros continuos:** cree sistemas sólidos de supervisión y registro para detectar lo antes posible anomalías y evaluar con precisión los daños durante y después de un ataque.
- **Gestión de vulnerabilidades:** actualice y aplique los parches necesarios a los sistemas con regularidad para mitigar las vulnerabilidades conocidas, con lo que se reducirá el riesgo de sufrir un ataque.
- **Análisis del patrón de ataque:** utilice herramientas de visibilidad adecuadas para analizar en profundidad los patrones de ataque y conocer las metodologías y la intención de los atacantes.

Análisis posterior al ataque

La evaluación de las consecuencias y el análisis del patrón de ataque son componentes fundamentales de una estrategia sólida de defensa contra DDoS a la capa 7. Estos pasos no solo ayudan a comprender y mitigar los efectos inmediatos de un ataque, sino que también sirven de base para la mejora continua de los mecanismos de defensa, garantizando una mejor preparación ante futuras amenazas.

Mantenimiento y actualización de sus recetas

Mantener una sólida defensa contra ataques DDoS a la capa 7 exige una supervisión constante de las últimas tendencias y técnicas.

Los atacantes combinan de forma constante patrones de ataque y utilizan nuevas herramientas y vulnerabilidades. Para contrarrestar de forma proactiva estas amenazas, las organizaciones deben invertir tiempo y esfuerzo en investigar, supervisar, evaluar las defensas, automatizar las protecciones y colaborar con la comunidad de inteligencia contra amenazas.

Echar un vistazo a los principales foros de ciberseguridad es un buen punto de partida, pero recomendamos una estrategia más prescriptiva:

Realice supervisiones y evaluaciones periódicas: supervise con regularidad el rendimiento de la red y las aplicaciones para detectar nuevos patrones o anomalías que indiquen amenazas emergentes. Utilice estos datos para evaluar la eficacia de sus mecanismos de defensa existentes, identificando áreas que se deben mejorar o ajustar.

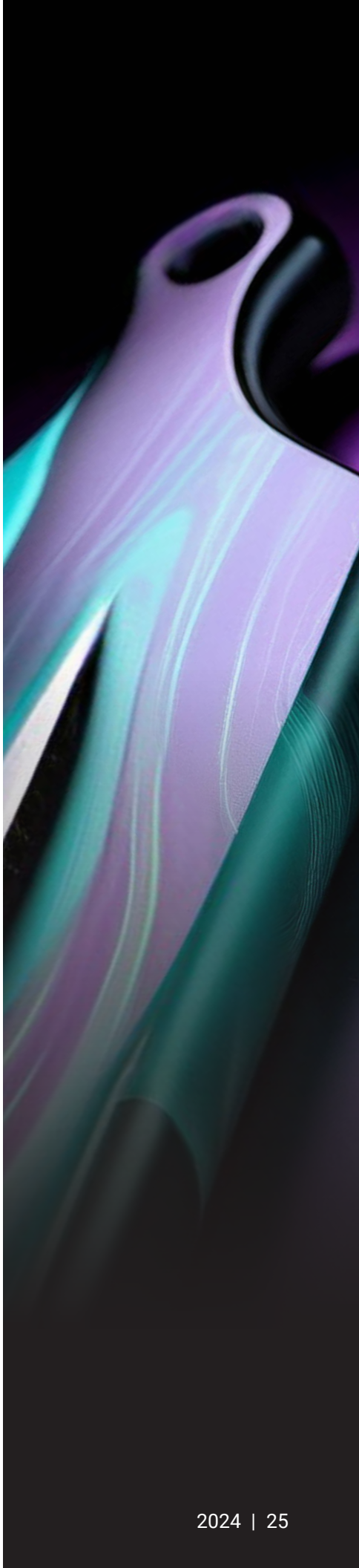
Cree un equipo antiDDoS: designe a su persona de referencia o cree un equipo dentro de la organización encargado de investigar y supervisar el panorama de ataques DDoS, así como de informar a toda la organización, al menos de forma trimestral, sobre cualquier conclusión y recomendación clave.

Trabaje con la comunidad de inteligencia frente a amenazas: los atacantes se comunican entre sí sobre cuáles son los métodos más efectivos y recientes. No hay ninguna razón por la que no debería hablar con colegas de otras empresas y sectores sobre cuáles son las mejores defensas. Manténgase al día de cuál es la inteligencia contra amenazas más reciente. Suscríbase a fuentes de seguridad, participe en foros de ciberseguridad y colabore con colegas del sector. Esta información le ayudará a anticipar nuevos vectores de ataque y adaptar sus defensas de la forma necesaria.

Confíe en su proveedor de ciberseguridad: los proveedores de tecnología suelen tener grupos de investigación de amenazas específicos, y los que tienen una red de distribución de contenido pueden proporcionar información que no se encuentra en ningún otro lugar. Aproveche estas oportunidades para aprender cuando y donde pueda. También podría ser útil recurrir periódicamente a expertos en consultoría en materia de seguridad.

Ponga a prueba sus propias defensas: aquellos que no se preparan se están preparando para fallar; la práctica hace al maestro… Sea cual sea su tópico favorito, el mensaje es el mismo: realizar pruebas y simulacros con regularidad tiene sus recompensas.

Haga revisiones periódicas y cree escenarios de ataque simulados (ejercicios de equipo rojo) para probar la resiliencia de sus estrategias de defensa. Estos ejercicios pueden sacar a la luz puntos débiles en su configuración actual y proporcionar información sobre cómo los atacantes podrían dañar su sistema.



Realice una prueba a su red al menos una vez al año. Los perfiles de ataque recientes también pueden ser una buena referencia para un caso de prueba, especialmente uno que le haya ocurrido a una empresa de su sector.

Cuente a la comunidad lo que ha aprendido. Merece la pena repetirlo: de la misma forma que los atacantes comparten sus herramientas y tácticas, las organizaciones también deberían intercambiar información sobre estrategias de defensa eficaces.

Al documentar tanto los éxitos como los fracasos, los profesionales de la ciberseguridad pueden proporcionar información real que se incorporará a la base de conocimientos colectiva. Participar en foros del sector, ofrecer asesoramiento a aquellos que están empezando en el campo y formar parte de proyectos colaborativos son medidas esenciales para conseguir un ecosistema de defensa sólido. Estas iniciativas no solo contribuyen al desarrollo de estrategias y herramientas más eficaces, sino que también constituyen un conjunto diverso de experiencias y conocimientos que permiten adaptarse a las cambiantes tácticas de los atacantes. Este espíritu de colaboración es fundamental para mantenerse a la vanguardia en el panorama de la ciberseguridad, donde cada aportación contribuya a crear un mundo digital más flexible y resiliente.

Puntos clave

El panorama de las amenazas DDoS es dinámico, con unos atacantes que buscan constantemente nuevos métodos para eludir las defensas. El mantenimiento y la actualización de sus estrategias de protección contra DDoS a la capa 7 es un proceso continuo que exige vigilancia, capacidad de adaptación y una actitud proactiva. Si se mantiene informado, lleva a cabo pruebas y revisiones periódicas y fomenta una cultura de mejora continua, podrá mantener una defensa sólida contra las amenazas presentes y futuras.

Conclusión

Está claro que los ataques DDoS a la capa 7 no solo se han vuelto más sofisticados, sino que también es más fácil iniciarlos gracias a los avances en la automatización y coordinación entre los atacantes. Por su parte, las organizaciones deben defender un panorama más amplio y complejo donde los costes de los fallos no paran de crecer.

De hecho, elaborar una receta de defensa no es una tarea sencilla. Ningún método concreto ofrece una panacea para los ataques DDoS a la capa 7. Como hemos demostrado, un enfoque polifacético, donde se combinan varias estrategias de detección y mitigación, proporciona la defensa más sólida.

Además, la elección de los métodos debe guiarse por las necesidades específicas, los patrones de tráfico y el perfil de riesgo de la aplicación o el servicio que se está protegiendo. No puede crear una defensa sin conocer su empresa, su tráfico y sus vulnerabilidades. Las actualizaciones y los ajustes constantes de estas estrategias son esenciales para adaptarse al panorama de las amenazas DDoS en constante cambio.

Por último, también queda claro que su trabajo no termina una vez que termina un ataque. El análisis y los ajustes posteriores al ataque son esenciales para garantizar el éxito continuo y pueden desempeñar un papel importante en el intercambio de conocimientos y el desarrollo profesional.

Afortunadamente, Akamai es la mejor opción para brindar ayuda en cada una de las etapas del proceso. Desde la protección de aplicaciones y API, pasando por la obtención de información muy valiosa sobre el tráfico global, hasta el análisis por parte de expertos posterior al ataque, muchas empresas aprovechan la oportunidad de obtener todas las protecciones DDoS de capa 7 que necesitan de un único proveedor.

Vea cómo funcionan las protecciones de Akamai contra DDoS a la capa 7.
Comience una prueba gratuita de App & API Protector.

Créditos

Editorial y redacción

Aseem Ahmed
Barney Beal

Revisión y expertos en la materia

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing y publicación

Georgina Morales Hampe
Shivangi Sahu

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. 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 octubre.