transparent edge

GUÍA PRÁCTICA: Sobrevivir a un ataque DDoS

SOBREVIVIR A UN ATAQUE DDOS

Estrategias de protección, reacción y respuesta

La creciente frecuencia de los ataques DDoS exige desarrollar estrategias integrales para abordar estos potenciales incidentes. En un contexto donde los vectores de ataque evolucionan rápidamente y pueden adaptarse dinámicamente a las defensas implementadas, la preparación y consolidación de planes de contingencia concretos debe ser una prioridad.

En este documento:

- analizamos tácticas de prevención, detección y manejo eficaz de un ataque DDoS;
- valoramos cómo una planificación proactiva y una capacidad de adaptación continua contribuyen a mitigar los riesgos y asegurar la continuidad de las operaciones;
- consideramos la eficiencia de las soluciones integrales de ciberseguridad para proteger entornos web y APIs.

Ataques de denegación de servicio en cifras

Los ataques de denegación de servicio son responsables de más del 50% de los incidentes de caídas de servicios web[1]. Es un patrón predominante que va en aumento año tras año debido a la relación coste-eficacia: implican pocos recursos económicos y tienen grandes posibilidades de éxito.

La mitad de los incidentes críticos comunicados al Instituto Nacional de Ciberseguridad (INCIBE) están relacionados con la disponibilidad del servicio, según los datos del último informe sobre la cibercriminalidad en España.[2]

En el primer semestre de 2024 los ataques DDoS volumétricos se incrementaron en un 30%, en comparación con el mismo periodo de 2023[3]. Solo en la región EMEA, el sector de redes de telecomunicaciones inalámbricas ha experimentado un aumento del 53% en los ataques DDoS[4].

[1] *Verizon, (2024). Data Breach Investigations Report*

[2] *Secretaría de Estado de Seguridad - Ministerio del Interior, (2023). Informe sobre la Cibercriminalidad en España*

[3-4] *NETSCOUT, (2024). DDoS Threat Intelligence Report*

Especialmente destacable es el crecimiento de los incidentes en la capa de aplicación. En particular las inundaciones HTTPS GET y POST, que se han incrementado un 43% en relación al año anterior. Este crecimiento responde, en parte, a la actuación de grupos de cibercriminales como los archiconocidos prorusos NoName057(16), que han realizado diferentes campañas de *hacking* en España. Y es que la situación geopolítica y la ciberseguridad están íntimamente relacionadas.

Respuesta temprana como clave del éxito

La prevención es el punto fundamental para alcanzar la resiliencia. Por eso es clave invertir en un plan de acción que incluya la formación del equipo y fomente la colaboración entre departamentos.

“Contar con un plan de respuesta temprana y que el equipo implicado lo conozca y comprenda es crucial para actuar ante un posible ataque,tomar decisiones proactivas e implementar medidas de seguridad sólidas”.

En el primer semestre de 2024 los ataques DDoS volumétricos se incrementaron en un 30%.

La capacitación se convierte, por tanto, en un aspecto esencial en el plan de respuesta ante ataques DDoS. Es fundamental que el equipo pueda:

- interpretar la analítica web
- identificar anomalías en el tráfico
- diferenciar la legitimidad de las mismas
- responder a las anomalías que no son lícitas

Qué indicadores pueden reflejar que estoy ante un ataque DDoS

El síntoma más evidente de un ataque DDoS es cuando un sitio web o una aplicación se ralentiza o deja de funcionar repentinamente.

Descartados motivos no relacionados con ataques DDoS, como picos de tráfico legítimo o problemas en la infraestructura de *hardware*, entre otros, podemos estudiar estas anomalías:

- Un aumento repentino del tráfico de clientes que comparten características comunes como: versiones de navegadores web similares, país de origen (geolocalización), tipo de dispositivo y perfil de comportamiento.
- Un aumento repentino, sin precedentes e inexplicable de las solicitudes a un *end point* (por ejemplo, una sola página del sitio web).
- Una cantidad masiva de tráfico desde una sola dirección IP (o rango de IP).
- Patrones peculiares en el tráfico, por ejemplo, picos regulares cada diez minutos, picos solo en horas específicas del día, etc.

Cuando se puede identificar un ataque DDoS, el daño ya está hecho y solo queda minimizar sus consecuencias. La prevención y detección temprana será la única formade reducir el daño.

Las fases de respuesta ante un ataque DDoS

A continuación detallamos los diez pasos clave para enfrentar y mitigar un ataque DDoS con éxito, permitiendo responder de forma efectiva y minimizando el impacto de este sobre las operaciones. La velocidad de respuesta marca la diferencia entre la continuidad y la interrupción del servicio.

01. Preparación

Incorporar herramientas de detección a los sitios web y API, establecer procedimientos, formar al equipo y practicar con simulaciones de ataque es el primer paso para una buena estrategia anti DDoS. Es fundamental implementar tecnologías de prevención y captura de trazas, además de brindar al equipo los conocimientos necesarios para operar estas herramientas con confianza.

02. Definición de responsabilidades

Resolver los roles del equipo con sus responsabilidades claramente definidas. Esto favorece la agilidad y la asertividad a la hora de enfrentar un incidente.

03. Monitorización

Analizar el tráfico constantemente y valorar si hay patrones de tráfico amplificado. La detección de anomalías permite estar atentos a un potencial ataque DDoS.

04. Capacidad de detección

¿A qué tipo de ataque nos enfrentamos?¿Qué sabemos del atacante?

05. ¿Cuál de las herramientas de mitigación debemos aplicar? ¿Necesitamos soporte externo?

Estas preguntas orientan una detección rápida y precisa, clave para elegir la respuesta más adecuada.

06. Reacción

Una vez hemos confirmado que el tráfico no es legítimo o es dudoso, conviene colocar los sitios en modo "bajo ataque" y notificar a los *stakeholders* correspondientes para alertarlos. Esto activa protocolos de defensa y asegura que los equipos estén preparados para contrarrestar el ataque.

07. Exploración

Identificar la fuente del ataque y entender dónde y cómo afecta a los sitios para reducir las zonas vulnerables. Este rastreo permite centrar los esfuerzos de mitigación en los puntos críticos y detener los intentos del atacante.

08. Bloquear el tráfico malicioso

Supervisar patrones específicos que desencadenan tráfico amplificado y utilizar fuentes de inteligencia sobre amenazas facilita la identificación y bloqueo del tráfico procedente de *bots* conocidos.

09. Limitar la velocidad para el tráfico no deseado

Implementar limitaciones de velocidad (*rate limit*) para prevenir el abuso de protocolos. Establecer alertas para cuando estos límites se superan ayuda a reaccionar rápidamente ante anomalías.

10. Utilizar listas de filtros por IP

Las bases de datos de reputación y filtros personalizados ayudan a restringir el acceso de IP maliciosas.

11. Registro

Tanto para controles propios como para cumplir con la legislación vigente es fundamental documentar la información detallada del ataque y realizar las notificaciones pertinentes a las autoridades. Este proceso es interesante para aplicar lecciones en el siguiente incidente.

Qué tecnologías de protección son efectivas ante un ataque DDoS

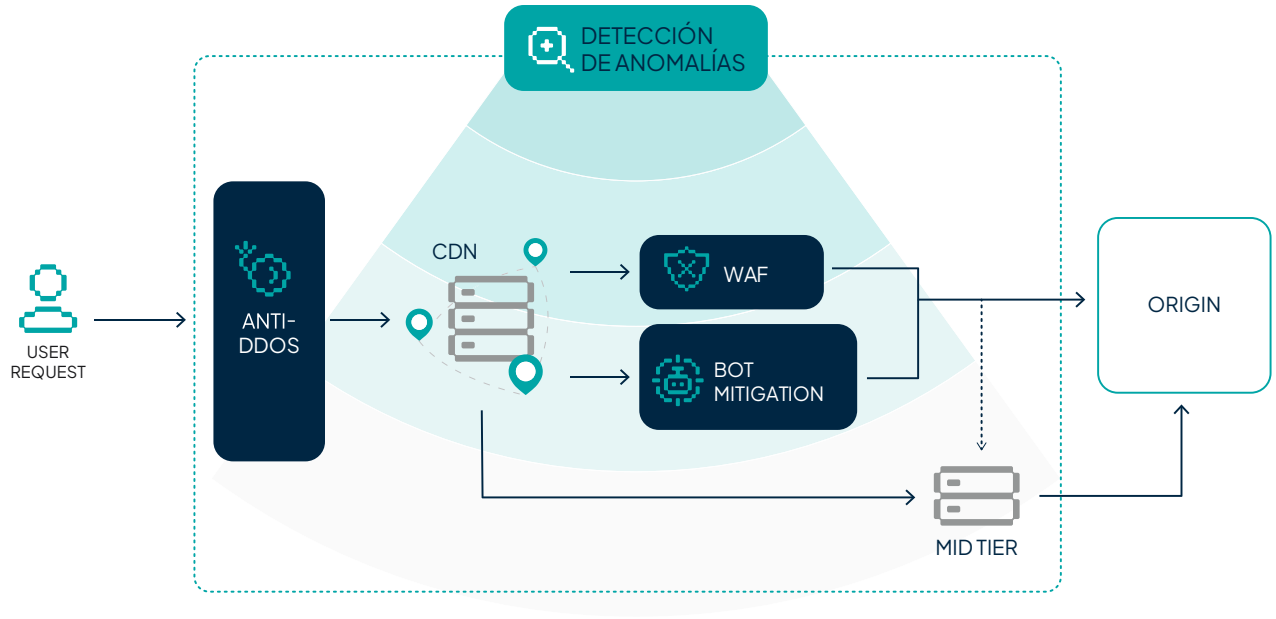
A mayor resistencia, mayor eficiencia en la protección:

Funcionalidad	Efectividad	Detalles
Firewall	0–20%	Los *firewalls* no son efectivos para detener un ataque DDoS multivector.
Anti-DDoS+WAF	80–100%	Al activar el Under Attack Mode (UAM) se puede frenar rápidamente un incidente. Ataques de altísima intensidad requieren medidas manuales ejecutadas por el equipo de soporte.
Perimetrical+CDN	100%	El ataque nunca llega al origen. *Suites* de ciberseguridad integral, como Perimetrical -que combina Anti-DDoS y WAF- detiene las amenazas en capas 3,4 y 7.

Qué puede hacer Perimetrical por mí

Debido al impacto que pueden causar los ataques en aplicaciones y servicios críticos para el negocio, así como la necesidad de mitigar estos incidentes casi en tiempo real, contar con una solución de respuesta siempre activa y ubicada lejos del origen es esencial para una defensa DDoS integral.

perimetrical



La tecnología de última generación de **Perimetrical** depura el tráfico malicioso en el *edge*, impidiendo que se acerque al origen y garantizando que el tráfico legítimo no se vea afectado. Perimetrical mitiga de forma eficiente los DDoS de interrupción del servicio web en las capas 3 y 4, mientras que las funcionalidades especializadas de protección en capa 7 frenan los ataques de volumetría de alto nivel dirigidos a la aplicación.

Perimetrical ofrece visibilidad en tiempo real, controles precisos y la capacidad de detener las amenazas desde una única plataforma. Esta tecnología avanzada desarrollada por **Transparent Edge** libera a tu equipo de las tareas más ejecutivas, al tiempo que blinda la seguridad de tu ecosistema digital.

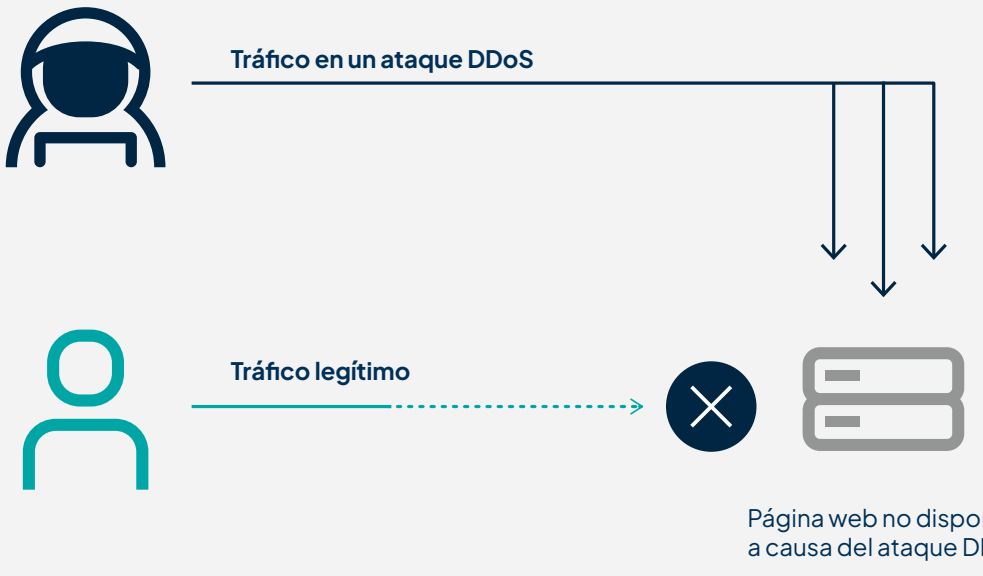
La mitad de los incidentes cítricos comunicados al INCIBE están relacionados con la disponibilidad del servicio.

Para conocer más sobre los ataques DDoS

Los ataques DDoS tienen como propósito interrumpir la disponibilidad de un sitio web o aplicación, generando confusión, afectando la operatividad y provocando posibles pérdidas de negocio.

Aunque las motivaciones detrás de estos ataques son múltiples y no se cubren en este documento, los ataques DDoS se dividen principalmente en dos grupos: aquellos dirigidos a la capa de aplicación y aquellos dirigidos a la capa de red. Ambos tipos buscan saturar el ancho de banda y reducir el rendimiento del servicio, llegando incluso a interrumpirlo por completo.

Ataque DDoS

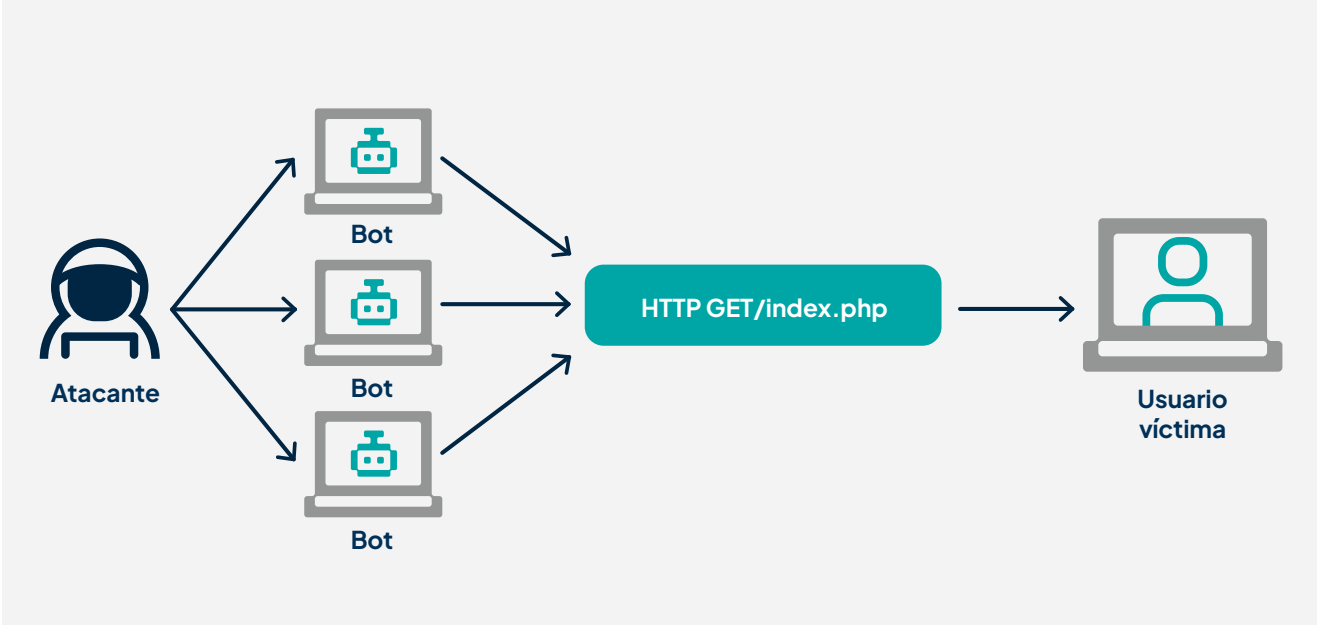


01.
Ataques a la capa de aplicación

Estos ataques se centran en parámetros específicos de los protocolos o servicio con el fin de agotar los recursos disponibles. Ejemplos comunes de ataques a la capa de aplicación incluyen inundaciones HTTP/SGET o POST e inundaciones de consultas DNS.

Los ataques a la capa de aplicación afectan directamente las métricas del servicio atacado, lo que puede generar un impacto económico significativo en servicios en la nube al incrementar sus costes. La efectividad de estos ataques depende de los límites del servidor, como los ciclos de CPU, la memoria RAM y/o el ancho de banda para transacciones simultáneas, lo que hace esencial contar con capacidades de defensa bien planificadas.

La velocidad de respuesta marca la diferencia entre la continuidad y la interrupción del servicio.

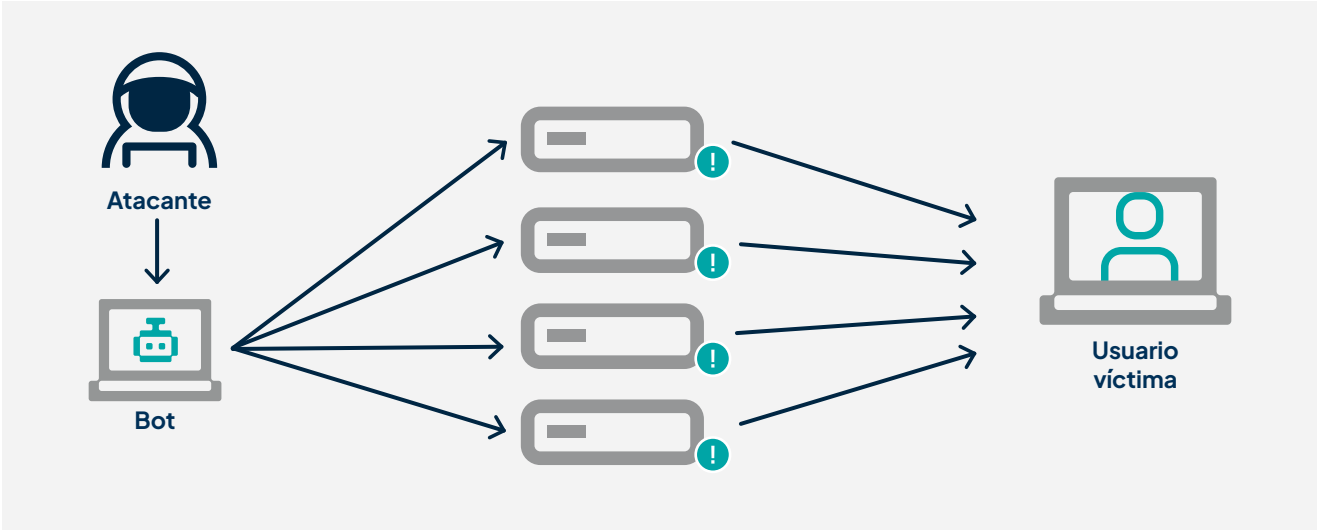


02.
Ataques a la capa de red

Un ataque volumétrico tiene como objetivo saturar por completo la capacidad de la red, anulando la capacidad de enviar o recibir tráfico legítimo. Esto provoca que los paquetes se acumulen en la caché y se descarten, agotando los recursos.

- **Ataques de reflexión/amplificación:** estos ataques emplean dispositivos de miles de usuarios desprevenidos para reflejar y amplificar grandes cantidades de tráfico hacia el objetivo. Aprovechan vulnerabilidades en protocolos y servicios, como DNS, NTP o SSDP, para multiplicar el volumen de datos enviados al objetivo. Esta estrategia permite a los atacantes generar volúmenes de tráfico muy superiores a la capacidad de los sistemas atacantes originales, lo que hace que sean altamente efectivos para saturar los recursos del objetivo a un coste mucho menor que los de ruta directa.

- **Ataques de ruta directa:** implican el envío de tráfico directamente desde los sistemas atacantes al objetivo sin intermediarios. Estos ataques generalmente recurren a una red de *bots* que genera grandes volúmenes de tráfico. Aunque no cuentan con el beneficio de la amplificación, los ataques de ruta directa pueden ser igualmente eficaces cuando la red de *bots* es lo suficientemente grande y el ataque se coordina adecuadamente.



transparent edge

Jump to the edge!

Protege tus sitios web y API y detén ataques avanzados sin interrumpir tus servicios.

Habla hoy con uno de nuestros expertos y solicita una demo.

#secureYourSite

www.transparentedge.eu