Akamai

WHITE PAPER

Cómo evitar que le arruinen la fiesta

con la plataforma adecuada para frenar los ataques DDoS a la capa de aplicación

Los ataques DDoS a la capa de aplicación en la actualidad

Los expertos en seguridad de todo el mundo saben demasiado bien que un ataque DDoS, o ataque distribuido de denegación de servicio, es un ciberataque que intenta colapsar un sitio web o recurso de red inundándolo con tráfico malintencionado. Los ataques DDoS siguen siendo la técnica de ataque más popular entre los atacantes y su uso no ha parado de aumentar en los últimos cinco años. A modo de ejemplo, uno de los ataques a gran escala más recientes (en términos de paquetes por segundo [PPS]) alcanzó un máximo de 809 MPPS en unos dos minutos.

Una tendencia que hemos observado al analizar este aumento de los ataques es que cada vez se producen más ataques DDoS a la capa de aplicación. Estos ataques, conocidos también como ataques DDoS de capa 7, se dirigen a aplicaciones web específicas (en lugar de a redes completas). Eso hace que a los defensores les resulte difícil prevenirlos y mitigarlos. Y, por si fuera poco, la extendida adopción de tecnologías como la automatización y los servicios en la nube ha proporcionado a los atacantes un acceso sencillo a las herramientas que necesitan para lanzarlos, por lo que poner en peligro la capa de aplicación es más fácil que nunca.

La realidad es que las solicitudes utilizadas en este tipo de ataques parecen solicitudes normales de usuarios finales, por lo que no hay una forma sencilla de determinar la sofisticación de un ataque. Dado que afectan tanto al servidor atacado como a la red, estos ataques resultan más dañinos con un menor ancho de banda total. En resumen, los ataques a la capa de aplicación son fáciles de implementar, difíciles de frenar o detener, y específicos para un objetivo.

Para comprender de qué forma los ataques DDoS a la capa de aplicación afectan a nuestras organizaciones, debemos conocer las diferentes categorías de estos ataques. Imagine que las categorías de ataques DDoS son cosas que pueden salir mal al organizar una fiesta. Por ejemplo, puede que abra las puertas de su casa a unos cuantos invitados para celebrar una ocasión especial o pasárselo bien un fin de semana. Al hacerlo, pueden pasar varias cosas:

Tipos de ataques DDoS

Escenario 1
Ataque volumétrico

A sus invitados les hace tanta ilusión su fiesta que hablan demasiado sobre ella (quizás en las redes sociales). Se corre la voz de que su fiesta es un evento que nadie querría perderse y, cuando llega el día, incontables extraños se presentan en su puerta. Esto sería un ataque DDoS volumétrico, ya que personas que no ha invitado están consumiendo todos sus recursos.

Escenario 2
Ataque de protocolo

Un invitado en el que creía que podía confiar se ha ido de la lengua. Un grupo de personas que querían asistir a su fiesta (pero que no recibieron invitación) han acorralado a uno de sus invitados y han empezado a pedirle detalles sobre el evento. El invitado ha cedido y un montón de personas que no había invitado han conseguido colarse en su fiesta. Esto sería un ataque DDoS de protocolo, ya que alguien que debía mantener en secreto su fiesta no lo ha hecho.

Escenario 3
Ataque a una aplicación

Una persona con malas intenciones oye hablar de su fiesta, y decide colarse en el evento disfrazado de uno de los invitados para cometer un robo en su casa. Esto sería un ataque DDoS a una aplicación, ya que la persona se está haciendo pasar por un invitado al que conoce.

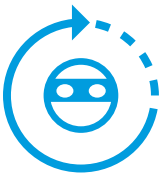
En todos estos escenarios hay una vulnerabilidad común: ha abierto las puertas de su casa con ocasión de un evento. Esta es la vulnerabilidad inevitable de la que se aprovechan los ataques DDoS a la capa de aplicación, ya que se trata de la capa en la que su organización interactúa con el usuario. Además, dado que es una capa sobre la que tiene menos control debido a que atiende directamente las solicitudes de los usuarios, puede ser más complicado mitigar estos ataques.

Y, si alguno de estos escenarios se hace realidad, le supondrá un coste adicional. Cuando alguien arruina su fiesta, la factura nunca es barata. Puede que deba pagar por la comida y bebida de más que han consumido los que se han colado, que algún extraño obtenga información personal sobre usted o que tenga que lidiar con las consecuencias de un robo en su casa.

Muchas soluciones de seguridad prometen con cada vez más ímpetu que pueden proteger sus sistemas, recursos e información confidencial frente a los ataques DDoS a la capa de aplicación, que ahora son más comunes y uno de los tipos de ataques ante los que más complicado es defenderse. Y usted confía en esas soluciones para proteger los activos de su empresa. Así que, en última instancia, la eficacia de su protección frente a ataques DDoS depende de lo eficaz que sea la plataforma en la que ha depositado su confianza. Analicemos los cambios y tendencias más recientes que debe tener en cuenta para decidirse por una plataforma de protección frente a ataques DDoS a la capa de aplicación.

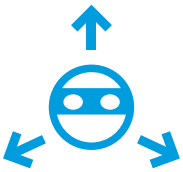
Cambios y tendencias

Como siempre, si diseñamos soluciones para un tipo de ataque concreto, los hackers adaptarán sus estrategias para contrarrestarlas. Pero nosotros les hemos seguido la pista, y estas son las cuatro tendencias y cambios que hemos observado recientemente:



1. Cambio a ataques de corta duración, pero constantes

Los ataques DDoS están dejando de priorizar la duración para dar cada vez más relevancia a su envergadura y frecuencia. Akamai ha observado ataques complejos con más de nueve vectores de ataque diferentes que combinan ARMS, inundación SYN, reflexión de UDP (DNS, WS-Discovery, etc.), inundación HTTP y muchos otros.

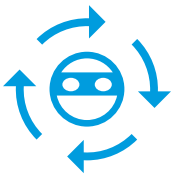


2. Uso más frecuente de ataques multivectoriales

Más del 20 % de los ciberdelincuentes utilizan ataques DDoS multivectoriales, en los que combinan diferentes métodos en un solo ataque de corta duración que repiten poco después. Link11 ha observado un máximo de 18 vectores simultáneos: un aumento del 50 % respecto a las cifras de 2021.

3. Aumento de la capacidad para evitar la detección y la mitigación

Distinguir entre el tráfico de ataque y el tráfico normal es complicado, especialmente cuando se trata de la capa de aplicación. Por ejemplo, una botnet lanza un ataque de inundación HTTP contra el servidor de una víctima. Dado que cada bot de una botnet realiza solicitudes de red aparentemente legítimas, no se detecta que el tráfico esté falsificado y puede parecer "normal" en el origen.



4. Automatización y adaptación de las tácticas

Debido al auge de las plataformas en la nube y las soluciones de IaaS/PaaS, los atacantes pueden automatizar fácilmente sus métodos y disponen de mucha potencia informática, por lo que resulta fácil automatizar los ataques y realizarlos rápidamente y a gran escala. Por tanto, estos ataques no solo son volumétricos, sino que son más distribuidos, aleatorios e inteligentes (utilizan parámetros aleatorios en las solicitudes, entre otras argucias).

Al igual que sucedía en el escenario de la fiesta, su casa podría verse comprometida debido a tres factores: el consumo de recursos, un invitado vulnerable o un delincuente disfrazado. Debido a los cambios y las tendencias de los ataques a la capa de aplicación, alguien podría arruinarle la fiesta sin que se dé cuenta siquiera. De hecho, los hackers tienen todo organizado en torno a estas tres categorías para actuar de manera furtiva. Por ejemplo, puede que echen un vistazo a su casa de antemano para ver cuántas entradas tiene, que averigüen el código de vestimenta de la fiesta con antelación, que creen perfiles falsos en las redes sociales para informarse sobre usted o que engañen a los invitados para hacerles pensar que son amigos íntimos suyos.

Debido a la creciente complejidad de los ataques DDoS a la capa de aplicación, le resultará útil contar con una estrategia de protección más integral que cualquiera que haya tenido en el pasado. Antes, cualquier protección de API y aplicaciones web (WAAP) podía cubrir sus necesidades, incluso las soluciones WAAP diseñadas internamente. Ahora, su solución WAAP debe poder superar la complejidad de los ataques a la capa de aplicación que se producen hoy en día.

Enfoque integral de protección frente a ataques DDoS a la capa de aplicación

Lo que dificulta la detección de los ataques DDoS a la capa de aplicación es que, incluso cuando los de tipo multivectorial presentan patrones obvios, un cibercriminal motivado supervisará la respuesta al ataque y hará los cambios necesarios para neutralizar las defensas. Para abordar este desafío de una forma más precisa y coherente, deberá mejorar sus capacidades WAAP en lo que respecta a las funciones de detección, mitigación y autoservicio.

Su solución WAAP no debería proteger solamente la entrada principal de su casa. Debe proteger cualquier punto de entrada y ser capaz de identificar a los atacantes disfrazados de invitados y adaptarse por si se enfrenta a varios ataques a la vez. La buena noticia es que es posible adoptar la plataforma adecuada para mitigar los ataques DDoS a la capa de aplicación y que su negocio siga operando como de costumbre. Su estrategia de mitigación de DDoS debe ser más integral y centrarse en los siguientes aspectos:

La escalabilidad de la plataforma

No importa si su solución WAAP es muy eficaz en el día a día: si no es capaz de ampliar su capacidad para absorber un ataque volumétrico, esa eficacia durará poco. Por tanto, la plataforma al amparo de la solución WAAP es tan importante como la propia solución WAAP. También debería interesarle saber dónde se ejecuta la plataforma. Por ejemplo, Akamai dispone de ubicaciones en el Edge por todo el mundo, a menudo en las regiones en las que se originan los ataques. Es mucho más fácil detener un ataque DDoS si se puede mitigar en su lugar de origen. Además, la escalabilidad facilitará en gran medida las operaciones esenciales, como la limitación de la velocidad y las reglas personalizadas.

Los recursos de datos y los resultados con los que trabajan sus soluciones de protección

Aunque cualquier solución WAAP puede supervisar el tráfico y generar informes con los datos, busque una solución que sea capaz de agregar los datos desde una perspectiva global. Si su proveedor de soluciones tiene visibilidad del tráfico de miles de empresas, podrá contextualizar los datos que genere comparándolos con los de otras organizaciones que se enfrenten a las mismas amenazas para proporcionar mejores datos a los sistemas de aprendizaje automático de su solución. Y, a partir de esa base, sus propios equipos internos podrán acceder a esos datos y utilizarlos para iterar y personalizar su solución.

Visibilidad y precisión de la solución

Algunos métodos de detección deberían estar incluidos por defecto, como las detecciones conductuales/basadas en anomalías, que no solo se centran en el tráfico entrante del cliente, sino que analizan también la velocidad de la conexión de origen y los parámetros de rendimiento del servidor. Sin embargo, si dispone de una solución escalable con acceso a un robusto conjunto de datos, su solución WAAP será mucho más precisa y selectiva. Además, sabrá mejor qué está sucediendo en su tráfico porque la solución es capaz de adaptarse y puede detectar si un ataque se está ocultando (como los ataques que se ocultan detrás de un proxy abierto en Internet). Todo esto ayudará a garantizar que se notifique a las personas adecuadas y, al mismo tiempo, reducirá considerablemente los falsos positivos.

Por tanto, para continuar con la analogía, si quisiera organizar una fiesta sin miedo de que se la arruinasen, la casa debería ser lo suficientemente grande (escalabilidad) para acoger a otros asistentes a los que tal vez no haya invitado. También le interesaría hablar con otras personas que hayan tenido malas experiencias (recursos de datos) para saber cómo protegerse por adelantado. Por último, querrá compartir la lista de invitados con antelación y saludar a todos los invitados antes de que entren a su casa (visibilidad y precisión) para asegurarse de que todos estén a salvo.

Y, si no quiere hacer todo eso usted mismo, puede contratar a unos refuerzos fiables que lo hagan por usted. Los servicios gestionados pueden prestar atención a todo tipo de señales muy difíciles de detectar para distinguir a un invitado real de uno con malas intenciones. Además, podrá olvidarse del estrés que conlleva tener que dedicar el tiempo y las competencias de su personal a prevenir constantemente este tipo de ataques cada vez más comunes y difíciles de detectar.

La cuestión de los ataques DDoS a la capa de aplicación depende de muchas variables y vulnerabilidades que son una parte inherente de dicha capa. Y se trata de una cuestión muy importante, ya que esos ataques DDoS pueden ser los más perjudiciales para su organización. Sin embargo, la defensa frente a este tipo de ataques no tiene por qué ser compleja o caótica. Todo lo que necesita es una solución estratégica, escalable y basada en datos. Después, la fiesta puede comenzar.

Obtenga más información sobre cómo puede ayudarle Akamai con sus soluciones de protección frente a DDoS de capa 7.