¿Se pueden detener los ataques DDoS en cero segundos?

HABLEMOS CLARAMENTE SOBRE EL TIEMPO DE MITIGACIÓN (TTM)

El TTM debería ser limitado, ¿verdad? Se trata del tiempo que transcurre entre el inicio de un ataque DDoS y el momento en que sus activos o aplicaciones están protegidos.

Sin embargo, este no es el significado real en todos los acuerdos de nivel de servicio (SLA) de proveedores. Debe entender exactamente cuándo se inicia y se detiene el reloj.

TENGA CUIDADO CON ESTE TIPO DE SITUACIONES HABITUALES ENTRE LOS PROVEEDORES

PROVEEDOR A

0:10
=
5:10

Los controles del proveedor A deben analizar un pico de tráfico durante más de 5 minutos antes de confirmar un ataque DDoS.

El SLA de tiempo de mitigación de 10 segundos solo comienza después de confirmar el ataque.

PROVEEDOR B

TIEMPO DE MITIGACIÓN
=
TIEMPO DE RESPUESTA

Los términos y condiciones del proveedor B definen el tiempo de mitigación (TTM) como el tiempo necesario para implementar un control de mitigación, es decir, una respuesta.

No existe un acuerdo de nivel de servicio (SLA) comprometido para detener el ataque.

PROVEEDOR C

AUTOMATIZACIÓN
≠
GARANTÍA

El proveedor C se compromete a realizar la detección y mitigación automatizadas durante su TTM.

Técnicas defensivas personalizadas y manuales para detener ataques sofisticados no forman parte de ese SLA.

COMPRENDA LOS TÉRMINOS Y CONDICIONES

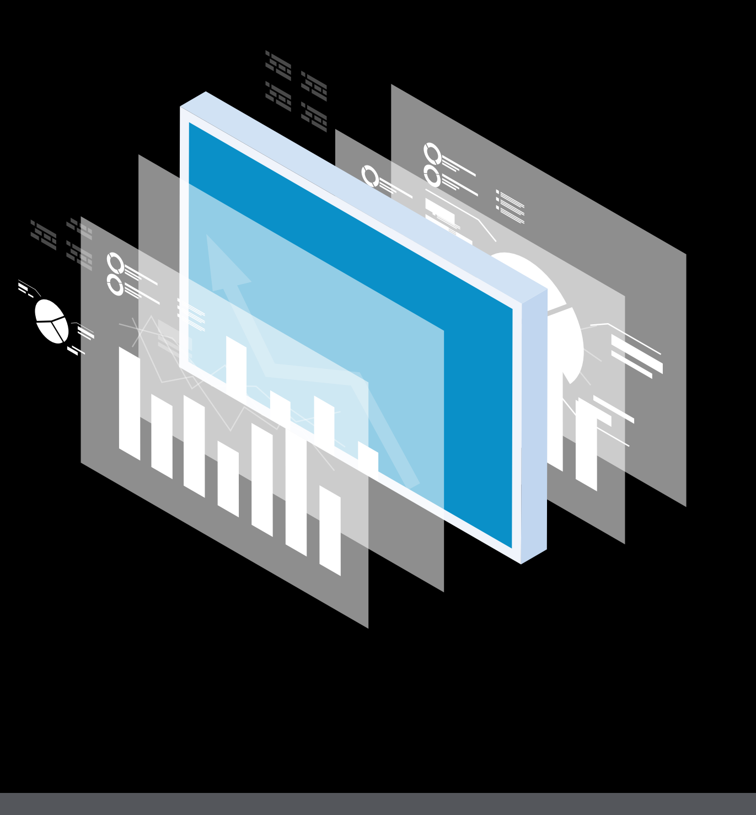
Desconfíe de términos como:

... tiempo de respuesta ...

En caso de un ataque DDoS constante ...

... posdetección ...

EL TIEMPO DE MITIGACIÓN DE AKAMAI



Cuando el **valor cero significa cero** segundos

Nuestros controles de mitigación proactivos están diseñados para eliminar ataques DDoS, al tiempo que le protegen antes incluso de que sepa que está sufriendo un ataque. Descubra la potencia de Akamai Intelligent Edge Platform.

TIEMPO PARA **detectar el ataque** + TIEMPO PARA **aplicar controles de mitigación** + TIEMPO PARA **bloquear el ataque** = **El mejor tiempo de mitigación**

8 PASOS PARA LA MITIGACIÓN DE DDOS

Akamai tiene el TTM más rápido del sector, con una potente combinación de investigadores en seguridad, gestores de incidencias, responsables de arquitectura de seguridad e innovadoras tecnologías de protección. El centro de control de operaciones de seguridad (SOCC) de Akamai ejecuta los siguientes pasos:

1. **Detectar** un ataque a tiempo mediante un control de DDoS ininterrumpido.
2. **Alertar** al cliente mediante el uso de un "runbook" establecido.
3. **Gestionar** el tráfico de clientes con un enrutamiento siempre disponible.
4. **Analizar** el tráfico e identificar vectores para aplicar la mitigación.
5. **Ajustar** las medidas de mitigación aplicadas para optimizar entre falsos positivos y falsos negativos.
6. **Identificar** nuevos vectores de ataque.
7. **Analizar** el tráfico e identificar vectores emergentes para aplicar la mitigación de forma continua.
8. **Optimizar** las medidas de mitigación aplicadas para neutralizar los ataques cambiantes.

LOS RIESGOS DE TTM DILATADOS

¿Cuáles son las **consecuencias** del tiempo de inactividad?

0:01

En 1 segundo, sus activos o aplicaciones orientados a la web dejarán de estar disponibles.

0:10

A los 10 segundos, aumenta la fricción para el cliente y disminuye la productividad de los empleados.

5:00

A los 5 minutos, la reputación de su marca está dañada y se produce la pérdida de ingresos.

EVALÚE SU ESTRATEGIA FRENTE A LOS ATAQUES DDOS

¿Con qué rapidez puede detectar su proveedor un ataque?	¿Sus aplicaciones principales estarían disponibles?
¿Sufriría daños colaterales?	¿Afectaría a los usuarios legítimos?
¿Con qué rapidez puede aplicar su proveedor medidas de mitigación?	¿Con qué rapidez puede empezar su proveedor a analizar el tráfico?

INFORMACIÓN DE AKAMAI SOBRE AMENAZAS

Mayor, más **complejo** y más **peligroso**

Los ataques DDoS aumentan y alcanzan niveles históricos. En 2020 hemos observado una actividad DDoS cada vez más grande y compleja; ya que la cantidad y las combinaciones de vectores de ataque no tienen precedentes.

18 de febrero de 2018	16 de junio de 2020	21 de junio de 2020
1,3 Tbps (terabits por segundo) Este ataque fue dos veces mayor que el más grande registrado anteriormente. Utilizó un nuevo vector de ataque de reflexión DDoS: tráfico en Memcached basado en UDP.	**1,44 Tbps/385 Mpps** (millones de paquetes por segundo) Este ataque utilizó nueve vectores diferentes y varias herramientas de ataque de la botnet. Duró casi 2 horas y mantuvo una velocidad de 1,3 Tbps.	**809 Mpps** (millones de paquetes por segundo) Este fue el mayor ataque en paquetes por segundo jamás registrado en Akamai Intelligent Edge Platform. Utilizó varias IP de origen distribuidas globalmente sin registrar hasta la fecha, lo que implica una botnet emergente.

Una buena defensa requiere la combinación de una plataforma de eficacia probada, profesionales experimentados y procesos y técnicas perfeccionados.

El **tiempo de mitigación** debe hacer referencia a la rapidez con la que se identifica y bloquea el tráfico malicioso, sin que esto afecte al tráfico legítimo ni a los usuarios.

En definitiva, la protección de las aplicaciones clave, la infraestructura y la reputación de la marca es la verdadera medida del éxito.

REFUERCE SU PROTECCIÓN CONTRA DDOS HOY

Descubra cómo puede ayudarle Akamai con la mitigación de cero segundos.

Más información

Publicado en noviembre de 2020