Protegernos de Ataques DDoS

¿Por qué protegernos de los ataques DDoS?

Hoy en día es fácil encontrar en las noticias, casi todos los días, referencias de Internet, bancos, foros y webs que han dejado de funcionar durante unas horas para recuperarse al poco tiempo, afirmando que han sufrido un ataque hacker, usualmente el más común de ellos: un ataque DDoS, uno de los más utilizados para detener el funcionamiento de un servicio de Internet y llamar la atención, pero ¿en qué consiste realmente un ataque DDoS? ¿En qué afecta al servidor, y qué efectos puede causar?

Un ataque DoS o DDoS (depende de cómo se lleve a cabo) no es más que un número exageradamente elevado de peticiones a una dirección IP. Tal es así que el servidor es incapaz de gestionar dichas peticiones causando un error en el sistema y la detención o reinicio del servicio, dejando tu web inaccesible al resto de usuarios.

Ahora, un ejemplo más sencillo, imaginemos un hospital, (nuestro servidor) donde cientos de usuarios (solicitudes) llegan a la sala de urgencias, sin embargo el hospital ya no tiene más doctores disponibles y su infraestructura no permite ni un enfermo más. El resultado: el hospital colapsa, no puede brindar un servicio aceptable y cierra sus puertas hasta que pueda reestablecerse y abrirlas de nuevo. Lo mismo ocurre con los ataques DDoS, se crea un enorme flujo de mensajes y solicitudes que se lanzan al objetivo para que este se sobrecargue y sea forzado a cerrase; como resultado, se le niega el servicio a los verdaderos usuarios.

Pero ¿Cómo funcionan los ataques DDoS?

Los **Ataques DDoS** primero infectan con un troyano a otros ordenadores inocentes llamados esclavos, que reciben el troyano a través de spam, emails, visitas a ciertas páginas web poco recomendables, etc. El troyano actúa sin que la víctima se dé cuenta.

Cuando el hacker se lo ordena, esta red de ordenadores esclavos, llamada botnet, realiza un ataque coordinado, todos al mismo tiempo. No es una agresión en sí misma, por eso es difícil de detectar, porque dichos ordenadores piden un acceso de entrada al servicio, o envían un dato, u otra actividad aparentemente inofensiva. Pero al hacerlo todos al mismo tiempo congestionan el sistema y terminan bloqueándolo.

Sea por el motivo que sea: político, económico, o simple un *propósito* personal, **un ataque DDoS puede ser dirigido a cualquier tipo de** *host* **conectado a Internet.** Ya sean los sistemas de un gobierno, los de una empresa, una plataforma de videojuegos, o hasta un simple blog. Los tres ataques más comunes son:

Basados en volumen: en este caso la finalidad del ataque es saturar el ancho de banda de un sitio web que sea el objetivo. La idea es causar congestión.

Ataques de protocolo: este tipo de ataque consume recursos del servidor o algún servicio que funcione de intermediario, como un firewall o el balance de carga. Este ataque puede derribar hasta servicios que son capaces de mantener millones de conexiones activas de forma estable.

Ataques de capa de aplicación: en este se usan peticiones que están disfrazadas como usuarios legítimos o inocentes pero con la finalidad de lograr que el servidor web deje de funcionar.

¿Cómo detectar un ataque inminente?

Si bien hay interrupciones en el servicio que no se producen necesariamente por ataques de hackers, hay algunos síntomas a tener en cuenta para la identificación de un ataque de denegación de servicio. Si la red estuviera funcionando en forma mucho más lenta de lo habitual, los sitios web no estuvieran disponibles, o si recibieras una enorme cantidad de correo no deseado, podrías estar bajo un ataque de denegación de servicio. Debes notificar a tu personal de operaciones de red acerca de tus sospechas.

Pero para evitar estos ataques y seguir brindando el mejor servicio a tus clientes y visitantes, ahora HostDime ofrece hardware DDoS basado en monitoreo premium y mitigación a nuestra base de clientes. El nuevo hardware empresarial de servicios de protección DDoS de HostDime está respaldado por el líder del mercado en seguridad de red, Arbor Networks.

Una vez que te conviertas en nuestro cliente, la protección DDoS de HostDime te proporcionará el tiempo de actividad superior, el acceso ininterrumpido al centro de datos y el aumento de la de retención de clientes.

Visítanos y asegúrate de que tú negocio siempre este protegido con Hostdime.