Por 5 dólares perderías millones en un ciberataque

Si, lo leíste bien. **Por tan sólo cinco dólares la hora**, cualquier ciberdelincuente puede lanzar un **ataque de denegación de servicio distribuido (DDoS)** y causar daños por más de un millón de dólares informó la compañía NETSCOUT Arbor.

Tras dar a conocer que el tamaño y la escala crecen a una velocidad alarmante, impulsados en parte por el **crecimiento de la cantidad de botnets utilizados para desplegar estos ataques,** René Hernández, experto en ciberseguridad de NETSCOUT Arbor, explicó que un ciberataque de tan solo un minuto, **podría generar muchas horas de inactividad imprevista.** "Se estima que **el costo por minuto de tiempo de inactividad de un ataque DDoS es de mil a cinco mil dólares.**

Dijo que el tamaño máximo promedio de **los ataques dirigidos hacia México en los últimos meses** oscila los 30 Gbps, cantidad suficiente para poner la conectividad a internet de una empresa en peligro, tal vez incluso cortarla por completo.

De hecho **un data center con capacidad de ancho de banda de varios Gbps puede verse sobrecargado** por un ataque de ese tamaño, y la magnitud del problema sigue aumentando.

"Hemos llegado a un punto en el que **41% de las organizaciones empresariales y 61% de los operadores de data centers han informado ataques** que superan su capacidad total de Internet. Además, se han reportado múltiples ataques combinados de más de 1 Tbps", agregó.

Según el último Informe de seguridad de infraestructura mundial anual (WISR) de Arbor Networks, 61% de los operadores de data centers hizo referencia acerca de ataques que saturaron por completo el ancho de banda de su data center.

El resultado fue que **no podían garantizar la disponibilidad de todos los servicios** que les brindaban a sus clientes. Esto significa que, incluso si no es el objetivo del ataque, pero depende de un proveedor de servicios que se ve afectado, también podría quedarse sin conexión.

Poca atención

Por otro lado, solo 52% de los proveedores de servicios tienen más de cinco personas dedicadas a la seguridad y solamente 38 % realiza prácticas de ataques DDoS más de una vez al año.

"Los ataques DDoS son originados por diversos motivos, desde competencia comercial, agitación geopolítica, intentos de manipular mercados financieros hasta ex empleados disgustados que buscan causar problemas. Incluso, se sabe que **grupos de cibercriminales han lanzado ataques DDoS para desestabilizar elecciones,** así que existe la posibilidad de que el 1 de julio se busque afectar los Programas de Resultados Electorales Preliminares (PREP)", previó Hernández.

Otras verticales que hoy en día están siendo afectadas por los ataques DDoS son: comercio electrónico, **servicios financieros, gobierno, educación, hosting, fabricación, videojuegos,** juegos de azar, fuerzas policiales, atención médica, energía/servicios públicos y empresas de usuario final/suscriptor.

Hernández insistió en que la frecuencia e intensidad de los ataques está aumentando. "Por tanto,

detener los ataques en su origen no es una opción práctica, por más que quisiéramos que lo fuera. Pero aún existen varias acciones **para mitigar el daño provocado por un ataque DDoS.** Para ser capaz de sobrellevar la amenaza siempre presente de un ataque, se requiere de una estrategia moderna con protección en múltiples capas, desde el borde de la red hasta la nube", agregó.