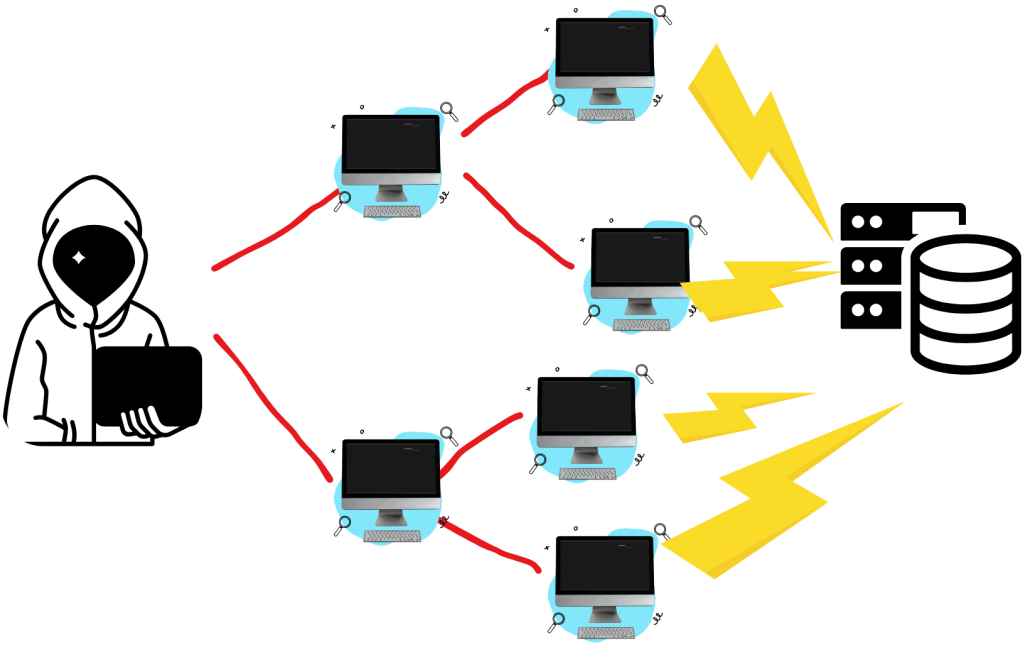
FICHA TÉCNICA: PROTECCIÓN TÉCNICA DE DATOS

EL ATAQUE DE DENEGACIÓN DE SERVICIOS (O DDoS)



Autor: Miracle Malaquias -Consultor en Protección de datos
Diseño Gráfico: Miracle Malaquias

INDICE

1) **¿DE QUÉ SE TRATA?**
2) **¿QUÉ LOGRA EL ATACANTE CON ESTO?**
3) **¿QUÉ HAY QUE HACER PARA CONFRONTAR ESTE TIPO DE ATAQUES?**

DESARROLLO

1) ¿DE QUÉ SE TRATA?

Un ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés) consiste en un tipo de ataque cibernético mediante el cual varios sistemas informáticos, a veces controlados por bots a veces infectados por malware, son utilizados para atacar un solo sistema como un servidor web, una red o incluso toda una infraestructura de TI. El objetivo de un ataque DDoS es inundar el sistema objetivo con una cantidad abrumadora de tráfico de internet, lo cual sobrecarga los recursos y la capacidad de respuesta del sistema atacado, haciéndolo inaccesible a los usuarios legítimos.

Explicado de una forma más accesible, un ataque de DDoS es algo así como si una sola persona reservarse (sin todavía comprar nada) todas las entradas de butaca para ver *Men*

in Black. Y, además, lo hiciese con cientos de identidades falsas. Lo cual ya señala una mala fe. De modo que, si cualquier otra persona quisiera realmente comprar entradas,y no solo reservar, no podría comprar nada. E incluso aquellos que pagasen mensualmente cuotas premium para ir al cine, se verían con la problemática de no poder reservar ni comprar nada. En esto consiste un DDoS. La diferencia es que se obstruyen servidores web, redes de internet e infraestructuras de TI o TO.

2) ¿QUÉ LOGRA EL ATACANTE CON ESTO?

Para responder a esta pregunta basta con imaginar qué es lo que pasaría si los usuarios legítimos de un servicio (como el cine CINESA) no logran acceder al cine al que están suscritos: se darían de baja y la empresa perdería dinero. Por no hablar del coste de oportunidad derivado de perder potenciales clientes. La pérdida no solo sería de dinero, sino también de confianza y reputación.

3) ¿QUÉ HAY QUE HACER PARA CONFRONTAR ESTE TIPO DE ATAQUES?

Habría que realizar un análisis forense del tráfico para identificar el origen de un ataque DDoS El análisis forense del tráfico de red implica examinar los logs de red y el flujo de datos para identificar patrones de tráfico inusuales, como múltiples solicitudes desde la misma dirección IP. Esto ayuda a rastrear el origen del ataque y a implementar medidas preventivas para mitigar su impacto. Esto complementa la configuración de defensa, ayudando a comprender cómo se originan y se distribuyen estos ataques.

Abordaje paso a paso:

1. Identificar el tráfico anómalo: ○ Consultar el mapa de redes y las notificaciones de tráfico anómalo en el panel de control. Analiza los gráficos de flujo de tráfico para observar picos, lo cual es un indicio de trráfico anómalo: estos picos indican que se produce un volúmen mucho mayor de tráfico de lo habitual.

2. Analizar los logs de red: ○ Examinar los logs de red para encontrar patrones de tráfico inusuales y múltiples solicitudes desde la misma dirección IP.

3. Rastrear el origen del ataque: ○ Utilizar la información de los logs para identificar la IP fuente del ataque.

4. Implementar medidas preventivas: ○ Aislar la IP maliciosa y actualizar las reglas del firewall para bloquear el tráfico hacia y desde esa dirección.