Secuestro de DNS

Es una amenaza grave para el sistema y puede tener consecuencias muy costosas. Como el ataque permite a un ciberdelincuente tomar el control de la configuración del DNS y redirige a los usuarios a sitio web fraudulentos, esto puede afectar a muchos usuarios diferentes. El secuestro de DNS implica el cambio de la propia configuración del DNS, a menudo mediante la instalación de malware en las computadoras víctima. Esto permite que el hacker tome el control de los enrutadores, interceptar señales del DNS o simplemente piratear las comunicaciones del DNS.

¿Cómo funciona?

sistema DNS funciona traduciendo nombres de dominio legibles por humanos a direcciones IP numéricas que los ordenadores utilizan para comunicarse. Cuando un usuario introduce una dirección web, el navegador consulta servidores DNS para obtener la dirección IP correspondiente. El punto vulnerable, es la comunicación no cifrada entre el navegador y el servidor DNS en las consultas DNS tradicionales (sin extensiones de seguridad como DNSSEC).

Tipos de secuestro DNS.

- Secuestro local: El hacker instala un troyano malicioso en el sistema para atacar la configuración de DNS local. Después del ataque, puede cambiar esta configuración local para que apunte directamente a sus propios servidores DNS.
- Secuestro del enrutador: Suele ser el primer punto de ataque para muchos ciberdelincuentes. Esto se debe a que muchos enrutadores tienen contraseñas predeterminadas o vulnerabilidades de firmware existente, que los hackers pueden encontrar fácilmente. Una vez dentro modifican la configuración DNS y especifican un servidor DNS preferido.
- Secuestro fraudulento: Los ciberdelincuentes secuestran el servidor de nombres existente del ISP para cambiar las entradas seleccionadas. Como resultado, las victimas desprevenidas acceden aparentemente al servidor DNS correcto, que en realidad fue infiltrado por los hackers.