Suplantación de DNS

Es el proceso de alterar entradas en un servidor de DNS para redirigir a un usuario especifico a una web malintencionada que está bajo control del atacante. Normalmente ocurre en un entorno de red Wi-Fi pública, pero también puede darse en cualquier situación y que el atacante pueda alterar las tablas de ARP y obligar a los dispositivos del usuario a usar el equipo controlado por el atacante como servidor para una página web especifica.

¿En qué consiste?

Los ciber delincuentes pueden utilizar herramientas para realizar el spoofing de DNS. Por lo general, las redes Wi-Fi publicas suelen ser los principales puntos de ataque, ya que no poseen una buena configuración y suelen tener deficiencias en la protección. Por lo que brinda a los ciberdelincuentes más oportunidades de ejecutar la acción deseada. Por eso se recomienda siempre pensar en la seguridad de las redes Wi-Fi, tanto las privadas como las públicas. Pero es importante entender que no solo se limita exclusivamente a redes publicas y esto puede ocurrir en otros entornos de red si el atacante logra posicionarse en el camino de la comunicación DNS.

¿Por qué es un problema?

Como los usuarios suelen ser víctimas del phishing en los ataques de spoofing de DNS, estos son una amenaza para la privacidad de los datos. La página por suplantar depende de los objetivos del atacante. Por ejemplo, si un atacante quiere robar información bancaria, el primer paso sería hallar una página bancaria popular, descargar el código y archivos de estilo y cargarlos al equipo malintencionado usado para secuestrar conexiones. La mayoría de los atacantes prueban y verifican que la página suplantada esté bien hecha, pero ocasionalmente sucede que hay pequeños errores que revelan que la página está siendo suplantada.