Como Funciona El Ataque De Envenenamiento De Caché DNS

El **envenenamiento de caché DNS**, también conocida como ***suplantación de DNS***, es un tipo de ataque que explota vulnerabilidades en el sistema de nombres de dominio (DNS) para desviar el tráfico de Internet de los servidores confiables, a servidores falsos.

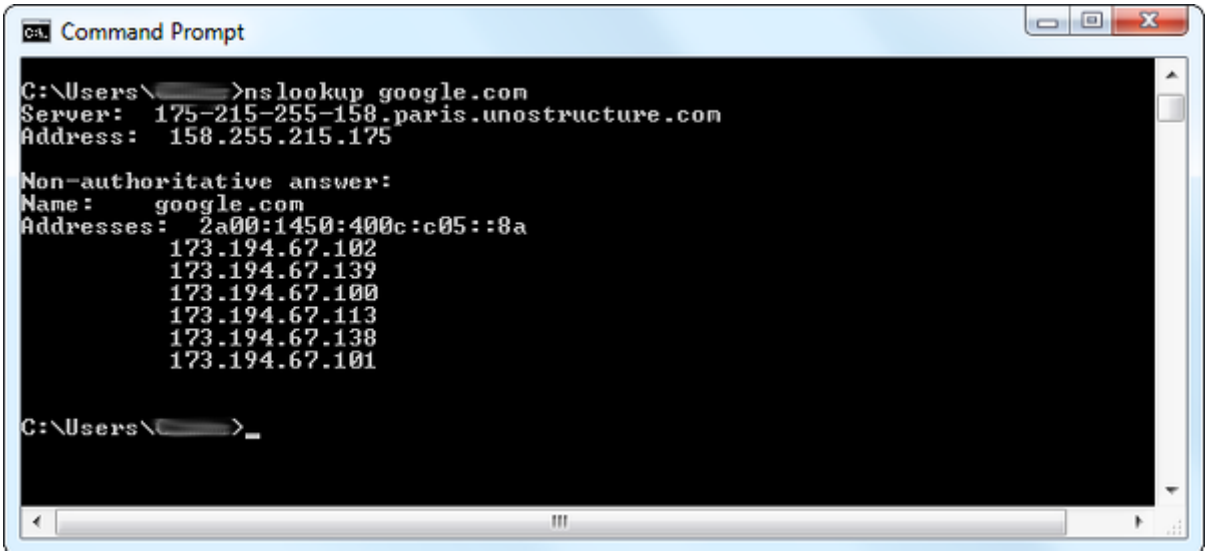
Una de las razones de que el **envenenamiento DNS es tan peligroso,** es porque puede propagarse de **servidor DNS a servidor DNS**. En 2010, un ataque de envenenamiento de DNS, tuvo como resultado la filtración del Gran Cortafuegos de China, pasando temporalmente las fronteras nacionales de China, y llevando censura de Internet a algunos usuarios en los EE.UU. hasta que se solucionó el problema.

¿Cómo Funciona El DNS?

Cada vez que busca el nombre de un dominio, como «**hostdime.com.co**«, la primer petición se envía al ***servidor DNS***. El servidor DNS responde con una o más direcciones IP en las que el equipo puede llegar a la direccion indicada, en nuestro ejemplo a **hostdime.com.co**. Su equipo se conecta directamente a esa dirección IP. El DNS convierte direcciones legibles como «google.com» en direcciones IP legibles por el ordenador como «173.194.67.102».

Almacenamiento En Caché Del DNS

Internet no sólo cuenta con un ***servidor DNS***, ya que sería algo ineficiente. Tu proveedor de servicios de Internet, ejecuta sus propios servidores DNS, este almacena información de otros servidores DNS. El router de tu hogar funciona como un servidor DNS, que almacena información de los servidores DNS de tu ISP. El equipo tiene una ***memoria caché de DNS local***, por lo que puede hacer referencia rápidamente a las búsquedas de DNS que han sido realizadas con anterioridad, en lugar de realizar una búsqueda de DNS varias veces.

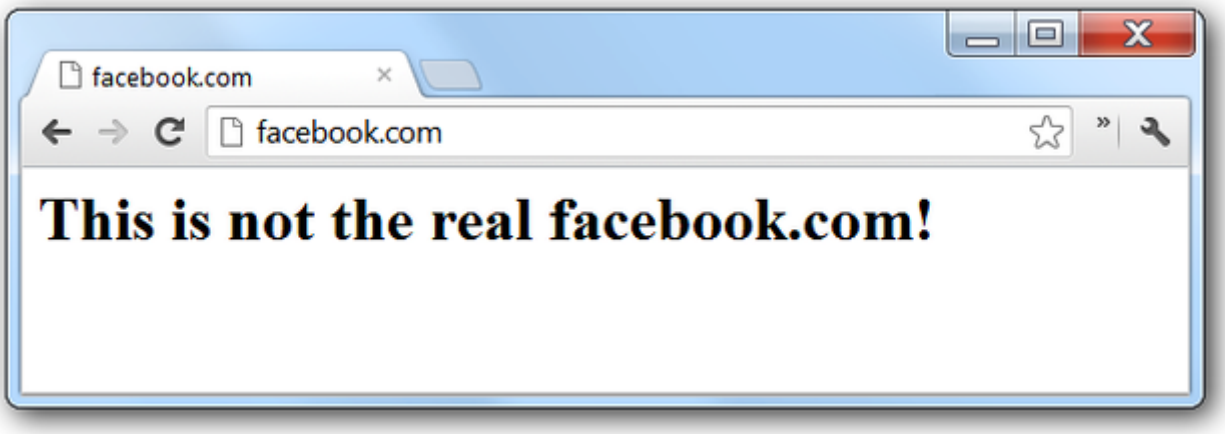


Técnica Envenenamiento Caché De DNS

Una **caché DNS puede llegar a ser envenenada** si contiene una entrada incorrecta. Por ejemplo, si un atacante obtiene el control de un servidor DNS y cambia alguna de la información que exista en él, por ejemplo, podrían modificar la IP de alguna pagina en especifica y redireccionar la IP a la

dirección que desee el atacante. La IP del atacante podría contener algún **tipo de sitio web de phishing** malicioso.

El envenenamiento de DNS también se puede propagar. Por ejemplo, si varios proveedores de servicios de Internet están recibiendo su información de DNS desde un servidor comprometido, las entradas DNS envenenadas, se extenderán a los proveedores de servicios de Internet y luego serán almacenadas en caché. Luego se extenderán a los routers domésticos y las cachés DNS en los equipos, con esto el atacante ya podría asegurar la infección de una gran variedad de usuarios.



Las Historia Del Gran Cortafuegos De China

Esto no es sólo un problema teórico, esto sucedió y a una escala de nivel mundial. Uno de los **métodos de protección Firewall** en China, es por medio del bloqueo de DNS. Por ejemplo, un sitio web bloqueado en China, como twitter.com, puede tener sus registros DNS apuntando a una dirección incorrecta en los servidores DNS en China. El resultado seria que ningún usuario de China que use este servidor puedan acceder a este sitio web.

En 2010, un proveedor de servicios de Internet fuera de China,

por error configuró sus servidores DNS para buscar información en los ***servidores DNS en China***. Con esto, buscaría los registros DNS incorrectos de China y los almacenaba en caché en sus propios servidores DNS. Otros proveedores de **servicios de Internet usaban la información DNS** de ese proveedor de servicios de Internet y la utilizaron en sus servidores DNS. Las entradas DNS envenenados continuaron extendiéndose hasta llegar a algunas personas en los EE.UU., estos registros bloquearon el acceso a Twitter, Facebook y YouTube. En esencia, este fue un ataque de envenenamiento de DNS a gran escala, claro esta, sin tener la intención de hacerlo. (Fuente).

La Solución

Realmente no se puede conocer si la respuesta a la URL que pedimos es la correcta o es manipulada. La solución a largo plazo para el envenenamiento de caché DNS es DNSSEC. **DNSSEC** permitirá a las organizaciones firmar sus registros DNS, usando criptografía de clave pública, asegurando que su equipo sabrá si un registro DNS debe ser de confianza o si ha sido envenenado y redirige a una ubicación incorrecta.