**Guía de Seguridad**

**Fecha de publicación**: 24/06/2022

**Tema**: Guía de Seguridad contra DNS cache poisoning.

**Objetivo:** Proveer una guía para prevenir incidentes de seguridad ocasionados por el DNS cache poisoning.

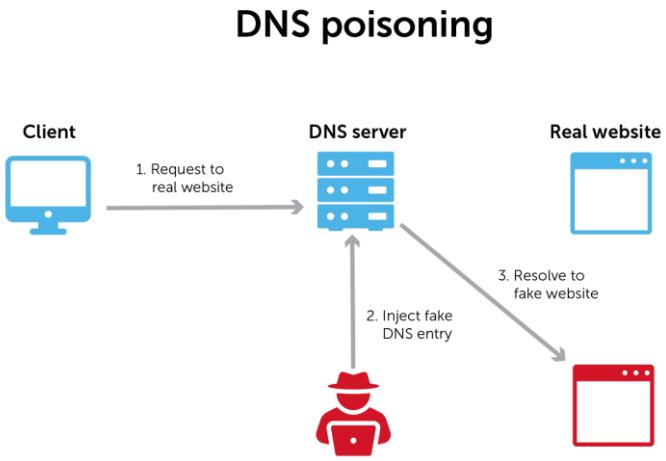
# Índice

## ¿En qué consiste este ataque?

Este ataque conocido como envenenamiento de caché (*cache poisoning*) consiste en el ingreso de información falsa en una caché de DNS correspondiente al servidor DNS por parte de un atacante, de manera a que las consultas realizadas por un usuario a él devuelvan una respuesta incorrecta, haciendo que los usuarios sean redirigidos a una página web malintencionada.

## ¿Qué vulnerabilidad es explotada?

Los ataques de envenenamiento de DNS explotan vulnerabilidades subyacentes en el servicio DNS, es decir, el diseño inseguro de la disposición de la memoria cache utilizada en este protocolo. Sin entrar en los detalles del protocolo DNS, basta con decir que DNS se construyó teniendo en cuenta la escalabilidad, no la seguridad. A continuación se visualiza un gráfico que representa la situación y los detalles del mismo:



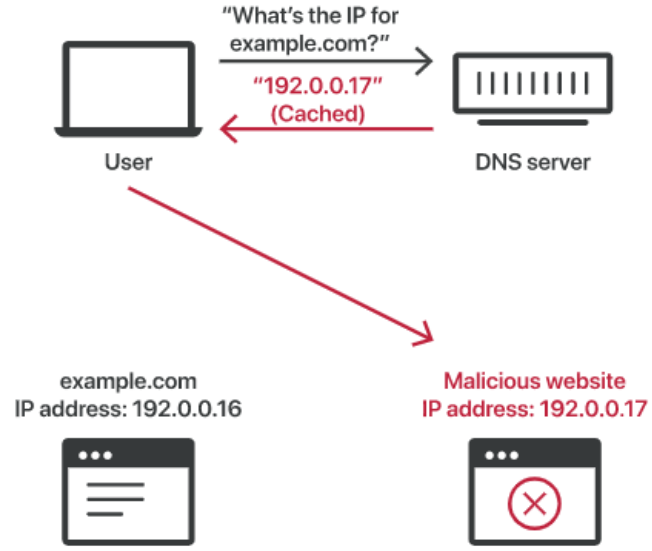

Cuando su navegador o una aplicación sale a Internet, comienza pidiéndole a un servidor DNS local que encuentre la dirección de un nombre (como bluecatnetworks.com). El servidor DNS local preguntará a los servidores raíz que poseen ese dominio y, a continuación, pedirá la dirección al servidor de nombres autoritativo de ese dominio.

El envenenamiento de caché DNS ocurre cuando un actor malicioso interviene en ese proceso y proporciona la respuesta incorrecta.

# Las vulnerabilidades encontradas en este ataque (DNS Spoofing)

- **Vulnerabilidad de suplantación**

Para casos como el de Windows, esta vulnerabilidad ha sido rastreada como CVE-2020-25705, esta se debe al componente de software Windows DNS Resolver que viene incluido con la pila de Protocolo de control de transmisión de Windows/Protocolo de Internet (TCP/IP). Un atacante podría explotar esta vulnerabilidad para utilizar los registros DNS modificados para redirigir a una víctima a un sitio web malintencionado bajo su control como parte de los ataques de suplantación de DNS.




Estos tipos de ataques *man-in-the-middle* a menudo se denominan ataques de suplantación de DNS. El actor malicioso está, en esencia, engañando al servidor DNS para que piense que ha encontrado el servidor de nombres autorizado cuando, de hecho, no lo ha hecho.

Una vez que ha engañado al navegador o la aplicación para que piense que recibió la respuesta correcta a su consulta, el atacante puede desviar el tráfico. Al hacerlo, podrá alimentar cualquier sitio web falso que desee al dispositivo host. Por lo general, estas son páginas que se parecen al sitio web deseado. En realidad, son sitios web de phishing, que intentan recopilar información valiosa como contraseñas o números de cuenta.

La **mitigación** que se ha proporcionado para esta vulnerabilidad es, modificar el Registro para cambiar el tamaño máximo del paquete UDP a 1.221 bytes, lo que bloquearía cualquier ataque de envenenamiento de caché de DNS que intente explotarlo en dispositivos vulnerables. Para ello se debe **seguir los pasos**:

1. Ejecutar **regedit.exe** como administrador.

2. En el Editor del Registro, desplazar hasta la subclave y establecer los siguientes parámetros:

   - **HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters**
   - **Valor: MaximumUdpPacketSize**
   - **Tipo: DWORD**
   - **Datos: 4C5 hexadecimal o 1221 decimal**
   - **Cierre el Editor del Registro y reinicie el servicio DNS.**

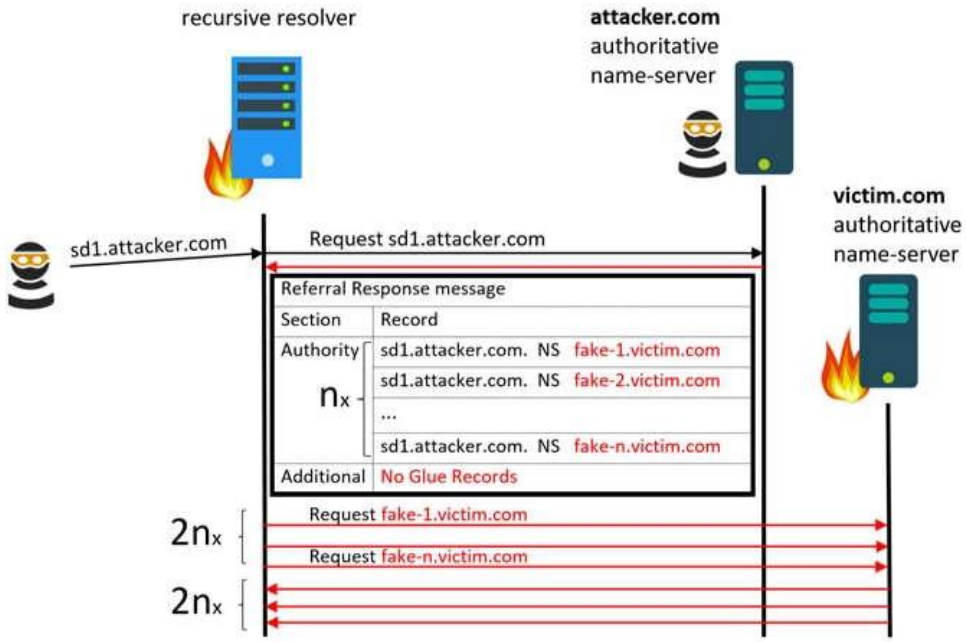
Después de la actualización del Registro, el solucionador de DNS ahora cambiará a TCP para todas las respuestas mayores que 4C5 o 1221, bloqueando automáticamente cualquier ataque CVE-2020-25705.

- **Vulnerabilidad de consulta DNS recursivo**

La vulnerabilidad recursiva denominado NXNSAttack, se debe al fallo del mecanismo de delegación de DNS que obliga a los dominios a generar más consultas a los servidores autorizados de elección del atacante, permitiendo causar una interrupción a escala de *botnet* en los servicios en línea.

Una búsqueda DNS recursiva ocurre cuando un servidor DNS se comunica con varios servidores DNS autorizados en una secuencia jerárquica para ubicar una dirección IP asociada con un dominio (por ejemplo, www.google.com) y devolverla al cliente. Esta resolución generalmente comienza con la resolución DNS controlada por sus ISP o servidores DNS públicos, como Cloudflare (1.1.1.1) o Google (8.8.8.8), lo que esté configurado con su sistema.

La resolución pasa la solicitud a un servidor de nombres DNS autorizado si no puede localizar la dirección IP de un nombre de dominio determinado. Pero si el primer servidor de nombres DNS autorizado tampoco contiene los registros deseados, devuelve el mensaje de delegación con direcciones a los siguientes servidores autorizados a los que puede consultar el solucionador DNS. Un atacante podría aprovechar esta vulnerabilidad para realizar denegación de servicios (DoS). El ataque se visualiza a continuación:




Varias compañías a cargo de la infraestructura de Internet, como PowerDNS (CVE-2020-10995), CZ.NIC (CVE-2020-12667), Cloudflare, Google, Amazon, Microsoft, Dyn, propiedad de Oracle, Verisign e IBM Quad, han parchado su software para solucionar el problema.

## ¿Cuáles son algunas recomendaciones de uso para el DNS?

Por más que el envenenamiento de DNS suena bastante perturbador, existen maneras internas de prevenirlas:

- Contar con un antivirus/antimalware, que se encuentre actualizado.
- Prevenir la descarga de archivos relativamente sospechosos, de sitios que no sean confiables.
- Utilizar un servidor DNS respetado y un ISP de buena reputación.
- Verificar si los sitios web que visita utiliza encriptación HTTPS.
- Vaciar el caché de DNS de la computadora, como el caché de DNS almacenado en el enrutador.
- Utilizar el cifrado de DNS o protocolo DNSSEC.
- Actualizar periódicamente los servidores DNS.
- Hay que asegurar que los servidores DNS tengan acceso restringido solo para los recursos de su organización que lo requieran. Mantener servidores DNS distintos para la resolución interna y de Internet con el servidor interno detrás de las defensas de la red para que el acceso a los atacantes externos esté restringido.

- Desactive las consultas recursivas
- Almacene únicamente información relacionada con el dominio solicitado en los servicios de cache dns
- Asegúrese de que el servicio de dns cache provea solo respuestas sobre el dominio solicitado por el cliente

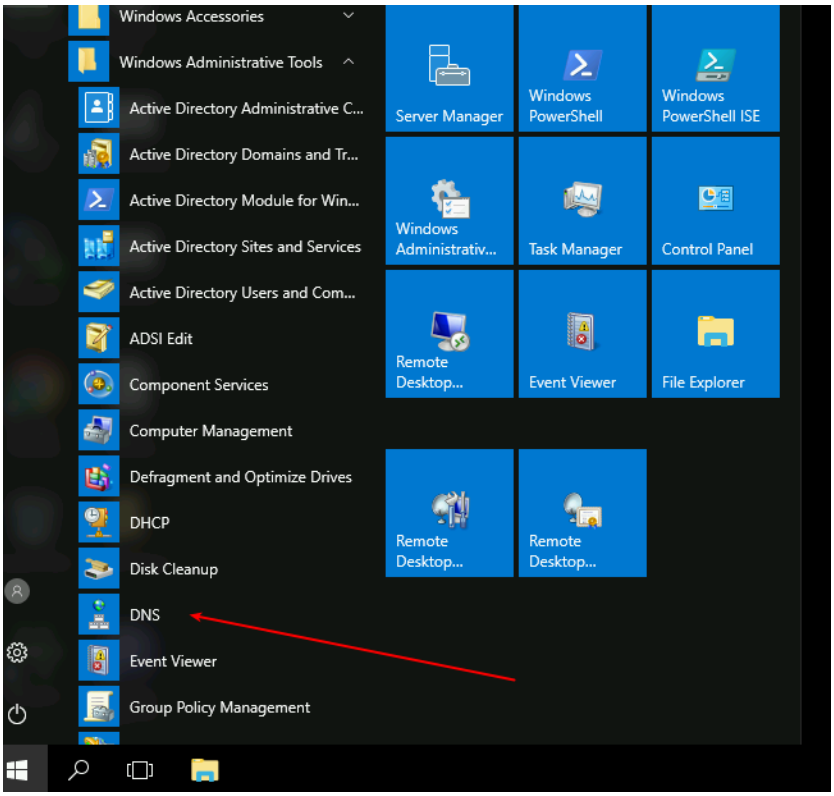
Cuando el servidor DNS de Windows es instalado, viene consigo la recursividad activada. Es decir, trabaja no solo como DNS autoritativo si no como DNS no-autoritativo a la misma vez.

Mantener el DNS recursivo activo representará un riesgo de seguridad para tu servidor, por lo que, se recomienda desactivarlo.

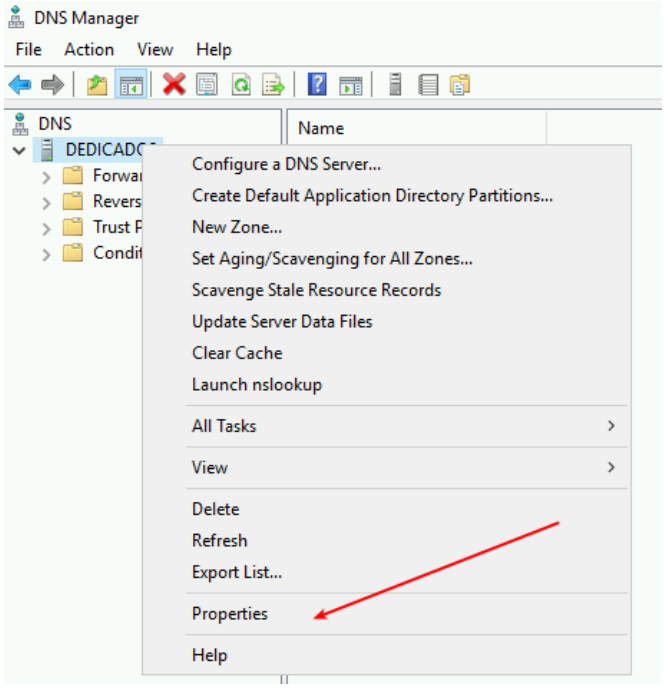
## Desactivar recursividad

### Para Windows server:

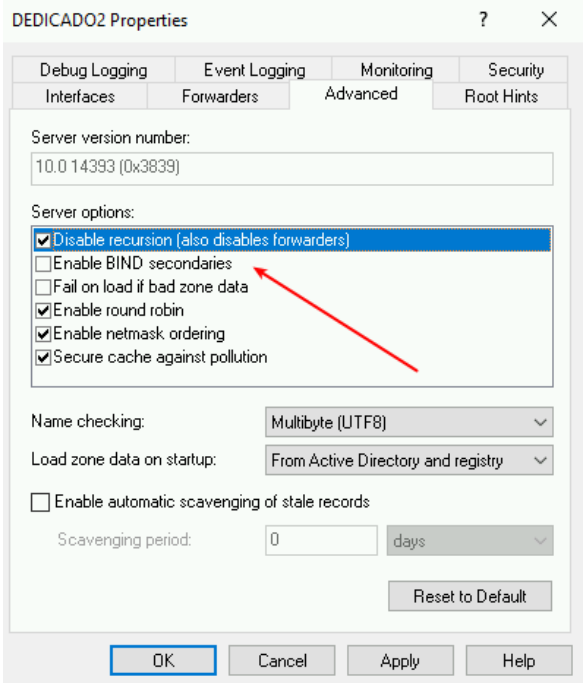
1. Ir a **Inicio**, buscar la herramienta **DNS**. En caso de no aparecer entre las opciones, buscar en la barra de búsqueda junto al botón de **Inicio**.



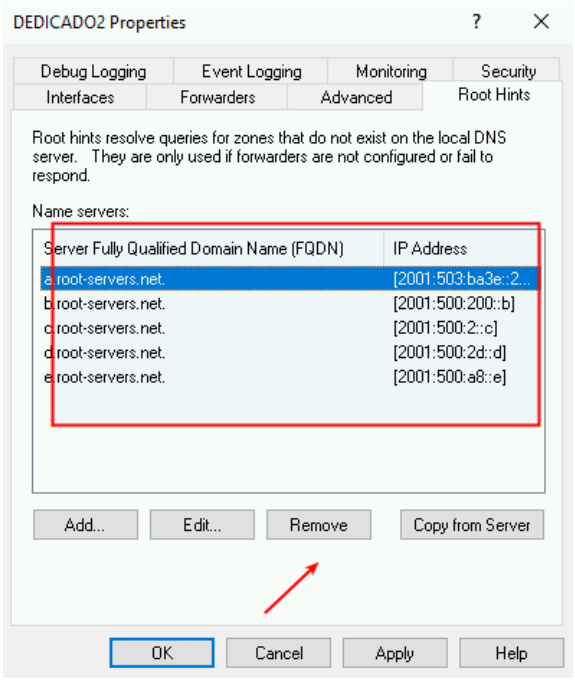
2. Hacer clic derecho en el nombre del servidor y luego ir a **Propiedades**.



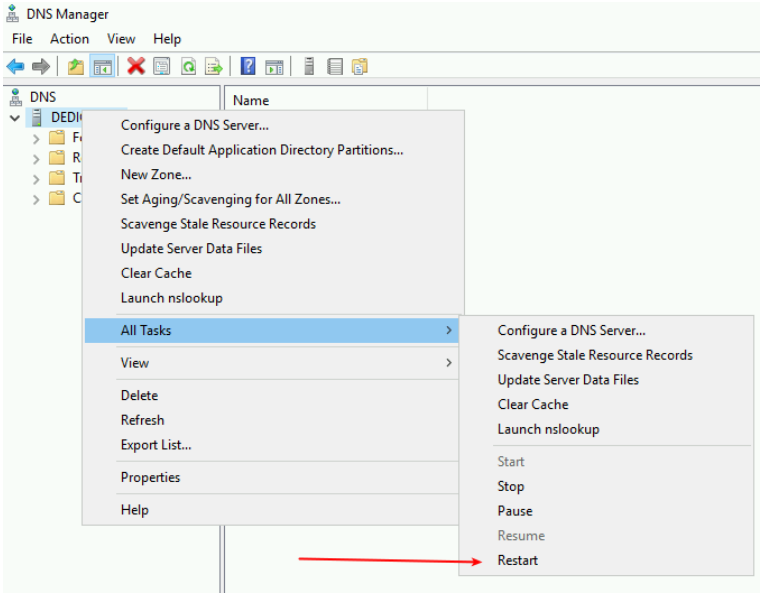

3. Ir a la solapa **Avanzada** y marcar la opción **Deshabilitar recursión** o **Disable recursion**. Al finalizar hacer clic en **OK**.



4. Ir a la pestaña **Root hints** y eliminar todos los servidores vistos en la lista. Luego hacer clic en **OK**.




5. Ahora, nuevamente hacer clic derecho en el servidor, ir a **All tasks** y hacer clic en **Restart** para aplicar la nueva configuración.




**DNS recursivo desactivado**

### Para Linux/Unix:

1. Buscar el archivo de configuración de **BIND** en el sistema operativo. El archivo de configuración BIND normalmente se encuentra en una de las siguientes rutas:
   - **/etc/bind/named.conf**
   - **/etc/named.conf**
2. Abrir el archivo named.conf en su editor de preferencia.
3. Agregar los siguientes datos para la sección de Opciones:
   - **allow-transfer {"ninguno";};**
   - **allow-recursion {"ninguno";};**
   - **recursion no;**
4. Reinicie el servicio.

## ¿Qué buenas prácticas se recomienda?

- **UDP Source Port Randomization (UDP SPR)**

Este método consiste en configurar el puerto UDP de origen de forma aleatoria, previniendo así que el atacante pudiese adivinar el ID de manera sencilla.

**Configurar para Windows:**

En los sistemas de servidor DNS de Windows pueden visualizar un aumento en la memoria y el consumo de recursos de controladores de archivos para los sistemas en los que está instalada la actualización de seguridad que se describe en **MS08-037**. Este es el comportamiento esperado debido a la característica de aleatorización SocketPool que se implementó para abordar esta vulnerabilidad de seguridad en servidores basados en Windows. La implementación de la actualización de seguridad del servidor DNS reserva un conjunto de puertos. Uno de los puertos se selecciona aleatoriamente para cada consulta DNS saliente. Esta decisión de diseño se tomó para abordar los problemas de rendimiento de los servidores DNS que manejan y originan un número significativamente mayor de consultas que los clientes basados en Windows. El conjunto de puertos reservados que reserva el servidor DNS se conoce como "grupo de sockets".

De forma predeterminada, el tamaño del grupo de sockets en servidores basados en Windows es de 2.500 sockets. El tamaño se podrá configurar, cambiando la entrada del Registro SocketPoolSize en la siguiente subclave del Registro:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\SocketPoolSize**

Se debe de tener en cuenta que el 956188 experimenta problemas con los servicios de red dependientes de UDP después de instalar la actualización de seguridad del servidor DNS 953230 (MS08-037). Mientras que el 977512 es el servidor DNS enlazado a todos los puertos del intervalo de puertos de Servicios de implementación de Windows en un servidor que ejecuta Windows Server 2008 R2 o Windows Server 2008

**Configurar para BIND:**

1. Instalar la actualización de BIND 9, utilizando los siguientes comandos

**Resultado de ejemplo:**

```
# apt-get update
# apt-get install bind9
Do you want to continue [Y/n]? y
*** db.root (Y/I/N/O/D/Z) [default=N] ? y
```

2. Comprobar que la aleatorización del puerto de origen esté activa. Comprobar que el archivo **/var/log/daemon.log** no contiene mensajes de la siguiente forma:

```
named[6106]: /etc/bind/named.conf.options:28: using specific
query-source port suppresses port randomization and can be insecure.
```

3. En caso de ver el mensaje desplegado arriba, proceda a reemplazar los números de puerto contenidos en ellos con el signo "*****" (por ejemplo, reemplazar "puerto 53" por "puerto *") en el archivo **/etc/bind/named.conf.option.**

**Referencias:**

- https://help.wnpower.com/hc/es/articles/360051879351-C%C3%B3mo-desactivar-el-DNS-recursivo-en-tu-servidor-Windows#:~:text=C%C3%B3mo%20desactivar%20el%20DNS%20recursivo%20en%20Windows%201,seguridad%20que%20genera%20que%20tu%20DNS%20sea%20recursivo.
- https://nethostingperu.com/blog/deshabilitar-recursividad-para-dns/
- https://www.bleepingcomputer.com/news/security/microsoft-issues-guidance-for-dns-cache-poisoning-vulnerability/#:~:text=%22Microsoft%20is%20aware%20of%20a,of%20this%20month's%20Patch%20Tuesday
- https://www.redeszone.net/2018/02/04/riesgos-la-seguridad-del-dns-evitarlos/
- https://www.muyseguridad.net/2020/05/22/vulnerabilidad-del-protocolo-dns/#:~:text=Vulnerabilidad%20del%20protocolo%20DNS%3A%20NXNSAttack,com)%20y%20devolverla%20al%20cliente.
- https://newhelptech.wordpress.com/2017/07/02/step-by-step-implementing-dns-security-in-windows-server-2016/