Encriptación de peticiones DNS mediante DNSCrypt

Publicado el El Informatico - 20 de noviembre de 2020 -

Usar TOR para encriptar nuestro tráfico es una buena manera de mantener un buen nivel de privacidad en internet, pero no es suficiente. Hay más maneras de controlar tu actividad en la red. Una de ellas es analizando las peticiones que se realizan a los servidores de resolución de dominios (DNS) al conectarnos a una página web.

¿Qué es un nombre de dominio?

Los ordenadores que están conectados a una red se identifican primero por una dirección IP, que es la matrícula de dicho ordenador. Cuando nos queremos conectar a un servicio, lo hacemos (directa o indirectamente) mediante dicha dirección. Las IP son una serie de dígitos, dependiendo de la versión (4 o 6) pueden ser una combinación de 4 bytes con valores del 1 al 255, o una serie de 8 octetos en hexadecimal. Sin embargo, recordar una serie de digitos es muy complicado, y requeriría de mantener un listado de direcciones IP a las que conectarnos.

Para simplificar éste proceso, las direcciones IP se “maquillan” usando **nombres de dominio**.

Los nombres de dominio son nombres descriptivos que se le otorgan a los distintos servicios que se publican en internet, de modo que en lugar de introducir una serie de números, se introduce su nombre (Lo que comúnmente se conoce símplemente como una “dirección” o URL).

Servidores DNS (Domain Name System)

Para saber qué direcciones IP se corresponden con qué nombres, es necesario usar una tabla que relacione cada nombre con las direcciones a las que representa, así como sus propiedades. Esas tablas se encuentran en los **servidores DNS**.

Los servidores DNS utilizan un protocolo que permite a cualquier aplicación conocer la dirección IP que se corresponde con cualquier nombre de dominio. De modo que

cuando introduces una dirección en tu navegador, el navegador manda antes una petición DNS a unos servidores DNS solicitando la dirección IP a la que se corresponde el nombre de dominio. A éste proceso se le denomina **resolución de DNS**.

Ejemplo de resolución DNS para la dirección del buscador de Google

Los servidores DNS a los que se conecta tu ordenador o dispositivo se pueden configurar a mano, o los puede solicitar al servidor DHCP de la red (lo más común), con lo que dependería de la configuración de tu router. Por lo general todos los ISP tienen sus propios servidores DNS (al menos dos, en caso de que uno falle), pero es también una opción popular usar los DNS de Google (8.8.8.8, 8.8.4.4) o Amazon (1.1.1.1, 1.0.0.1).

¿Cuál es el peligro?

El peligro evidentemente radica en que estamos mandando a traves de internet, a un servidor externo, una petición DNS con la dirección a la que nos estamos intentando conectar. Así pues, si intentas conectarte a google.com, el servidor DNS al que intentas conectarte ya sabe a qué página web estás intentando conectarte, y cualquiera que pudiera estar monitorizando tu tráfico podría igualmente saberlo. Entre otros, tu propio ISP.

Para minimizar éste riesgo, algunos servidores pueden encriptar éste tráfico, pero ni todos lo hacen, ni toda la encriptación vale ya que puede no usar un algoritmo criptográficamente seguro.

Si además usamos el navegador TOR, aunque estemos redireccionando las peticiones del navegador a través de TOR, es posible que nuestro sistema todavía pueda mandar peticiones fuera de TOR, hasta el punto de dejarnos al descubierto.

Y no sólo eso, sino que el protocolo DNS es inseguro y susceptible a algunos tipos de ataques.

DNSCrypt-proxy

DNSCrypt es una aplicación open source que añade una capa extra de seguridad asegurándose de que el tráfico DNS quede encriptado de manera segura entre nuestros dispositivos, y los servidores DNS. El trafico requiere ser encriptado entre el DNS y nuestro dispositivo, así que añade un nodo extra además para realizar éste proceso entre nuestro dispositivo y el DNS, y además nos protege frente a algunos de los ataques más comunes.

Podemos usarlo aparte del navegador TOR, de modo que todas las peticiones DNS de nuestro dispositivo, aparte de las del navegador, pasen por DNSCrypt. De modo que será mucho más complicado dejarnos al descubierto, si bien sería necesario conseguir que todo el tráfico pase igualmente por TOR.

Instalarlo es muy sencillo. En linux tenemos el paquete dnscrypt-proxy, que podemos instalar y configurar de manera similar a TOR.

apt install dnscrypt-proxy

O en Arch/Manjaro

pacman -S dnscrypt-proxy

El archivo de configuración se encuentra en */etc/dnscrypt-proxy/dnscrypt-proxy.toml* , del cuál solo configuramos el parámetro server_names con los nombres de los servidores DNS que queramos usar con DNSCrypt. Por ejemplo:

server_names = ['bcn-doh', 'ams-doh-nl', 'brahma-world']

Si necesitas una lista de servidores DNS actualizada, puedes usar ésta lista. De dicha lista, nos interesan los servidores que usen un protocolo DNSCrypt o DoH, que NO hagan "logging", y que además tengan el protocolo DNSSEC activo.

Una vez configurados los servidores, podemos guardar y activar el servicio.

 # systemctl enable dnscrypt-proxy
 # systemctl start dnscrypt-proxy

Y por último, configurar tu sistema para usar el loopback (127.0.0.1) como dirección del servidor DNS de tu sistema. Éste último paso dependerá de tu distribución y versión, con lo que tendrás que buscar información sobre cómo hacerlo en tu sistema. En Ubuntu 20 puedes hacerlo directamente desde las opciones de red de tu entorno de escritorio, o configurando el sistema usando NetworkManager. Este proceso requiere además establecer una dirección IP estática en tu sistema.

En Windows exíste una versión con interfaz gráfica para facilitar el proceso. Podemos descargar el código fuente desde aquí, o simplemente descargar el ejecutable desde aquí, haciendo click en el botón Download.

ANTERIOR

TOR: Encriptación de tráfico (Y por qué deberías de usarlo)

SIGUIENTE

Redes VPN

Buscar ...

Entradas Recientes

- Encriptación LUKS con CRYPTSETUP
- Se acabaron las bromas. A partir de ahora vas a estar constantemente vigilado en todas partes.
- Microsoft anuncia su nueva versión de su sistema operativo: Windows 11
- La historia de Internet en España
- Terminología moderna usada en tecnología digital
- Desactiva la ejecución de JavaScript de los archivos PDF, en Firefox y TOR browser.

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Criptografía | Emulación / Virtualización | FOSS | Hacking | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS