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

Publicado el El Informatico - 19 de noviembre de 2020 -

En el artículo anterior he comentado algunas cosas en relación a internet y la privacidad. La preocupación por la privacidad en la red no es algo nuevo. A mediados de la década de los 90 ya había gente empezando a cuestionar la seguridad y la privacidad en la red, a nivel global. Con tan sólo conectarnos a un servidor y realizar una petición ya hemos dado nuestra dirección IP. A través de ella, se pueden obtener muchos datos personales, empezando por el nombre del dueño de la linea, su teléfono y la ciudad de origen o incluso la dirección.

Con el auge de las redes sociales (y nuestra manía de dejar la información personal publicada en ellas) es posible encontrar más información sobre una persona con estos tres datos. Por ejemplo, buscando el número de teléfono en Facebook o Twitter. O incluso buscar en directorios dedicados a éste tipo de información, previo pago de una cuota.

Si gracias a ésto encontramos algún dato extra como, por ejemplo, la dirección de correo electrónico, entonces podríamos hacer muchas más cosas como, por ejemplo, buscar contraseñas filtradas o incluso realizar un intento de ataque *physing* para obtener dinero o contraseñas de acceso.

Y no acaba la cosa ahí. Ya hablé en el artículo mencionado sobre cómo se podía obtener más información sobre la persona en cuestión mediante minería de datos. Por ejemplo, mediante una identificación del navegador por su huella digital.

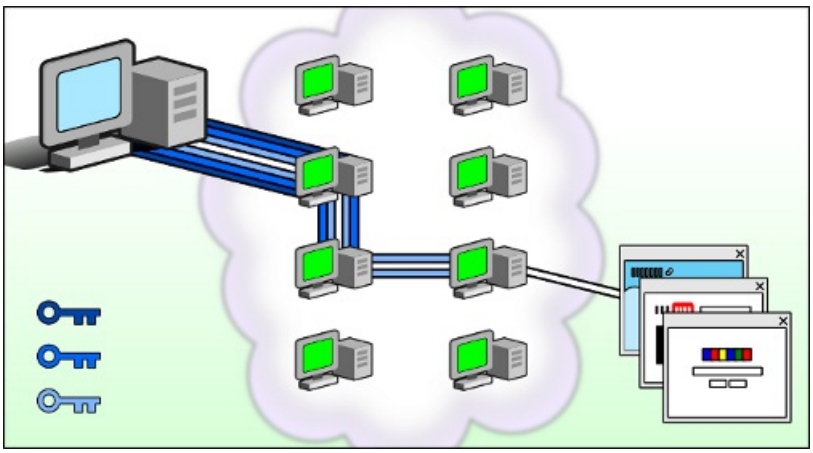
Todo ésto es un simple ejemplo de lo que te puede pasar tan solo navegando por internet o incluso jugando una partida on-line en un juego. No es broma, **ha pasado**. Por eso, ya desde 1995, exísten personas que ya pensaban en un modelo que nos permitiese conectarnos de manera **completamente anónima**. Sin ceder datos personales.

El proyecto TOR

El proyecto TOR nace en 2006 de la idea de una red completamente anónima y privada, con la idea de proteger a los usuarios frente a éste tipo de ataques tan comunes hoy en día.

El funcionamiento es parecido al de un *proxy*. Aunque no es tán sencillo. En lugar de conectarnos tras un nodo adicional, TOR forma un puente entre diferentes ordenadores (llamados 'relays'), concretamente entre tres ordenadores. Cada uno de éstos ordenadores está conectado con el siguiente en la cadena mediante una conexión encriptada con clave pública.

El ordenador con el que se conecta TOR directamente es el 'nodo de entrada', y el último en la cadena es el de salida. Cuando nos conectamos a la red que genera, el tráfico irá encriptado directamente desde el puente hasta nuestro ordenador.



Esquema de la red TOR (Fuente: https://tb-manual.torproject.org/about/)

De éste modo, el tráfico queda oculto entre tres puntos. El servidor al que nos conectemos sólo verá el nodo de salida, pero desconoce a donde se dirige el tráfico. Por otro lado, desde el punto de vista de un atacante que intentase monitorizar el tráfico en alguno de los nodos, la información estaría encriptada de manera que será muy complicado obtenerla. Si además hay más personas usando esos nodos, es demasiado complicado saber qué va a quien.

¿Es segura?

La red TOR es segura. Pero NO es infalible, ya que exísten métodos para lograr descubrir quién está detrás de ella. Con lo cuál simplemente se limita a ponérselo muy difícil a cualquiera que pretenda interferir o interceptar las comunicaciones. No obstante, son métodos muy complicados que requieren de tiempo e infraestructuras que no están al alcance de todos. Por ello, **es más sencillo atacar directamente al usuario**.

El método más sencillo sería atacar directamente al usuario mediante alguna táctica que le haga descubrirse. Un ejemplo sería usando un plugin externo, como Flash,

para realizar una conexión descubierta a un servidor fuera de la red o simplemente monitorizando las peticiones a un DNS no seguro, asumiendo que no se estén realizando también a traves de la red TOR a un servidor seguro.

Pero todos éstos ataques requieren de algún fallo por parte del usuario a la hora de conectarse a la red. Asumiendo que el usuario ponga de su parte, es demasiado complicado desenmascarar a un usuario. Con lo que la red en sí es bastante segura.

Usar Microsoft Windows sería uno de los fallos más comunes. Microsoft Windows es conocido por sus puertas traseras y por su peculiar tardanza a la hora de parchear algunos de sus agujeros de seguridad, además de estar en estrecho contacto con la NSA desde al menos los años 90.

¿Es legal?

Depende del país. **En España, actualmente, no está regularizado ni penalizado por ninguna ley**, con lo cuál eres libre de usarlo siempre y cuando lo uses de forma responsable. No obstante, con el nuevo borrador de la ley de telecomunicaciones se garantiza el derecho a la encriptación de las comunicaciones personales. De seguir adelante, aparte de permitirle al gobierno solicitar a tu operador que les permita escuchar en tus comunicaciones (ojo), **tendrás derecho a cifrar tus comunicaciones electrónicas** (Artículo 62 apartado 1 del citado borrador), así como de solicitar los mecanismos de cifrado a entidades públicas (Algo importante ya que he visto páginas de ayuntamientos y entidades estatales sin un mísero certificado SSL). Y ésto evidentemente incluye el uso de la red TOR para cifrar tus comunicaciones, **siempre que sea para proteger la confidencialidad de la información**.

En otros países como China, Corea del Norte, o incluso Reino Unido, puede que no tengas tanta suerte y te expongas a un riesgo a la hora de usar la red TOR. En éstos casos, **ten cuidado**.

En cualquier caso sólo será permitido su uso para garantizar la privacidad del usuario y en ningún caso se exime a nadie de la ley por estar oculto. Todo lo que hagas seguirá siendo amparado por las leyes estatales y si tú decides poner un mercado negro on-line mediante TOR podrás ser arrestado y llevado ante la justicia igual que cualquier otro criminal. O en otras palabras, no hagas el tonto. Usa TOR para el bien, como una herramienta para garantizar tu privacidad en la red.

Servicios ONION (Servicios ocultos, o “Hidden services”)

Los servicios ocultos son servicios similares a los que tenemos en internet (como

por ejemplo, pero no limitado a, páginas web), pero que sólo son accesibles a través de la red TOR. Es decir, no podemos acceder a ellos a través de nuestro navegador de forma normal, pero sí podremos acceder a ellos si estamos conectados a TOR. Por éste motivo a la red de TOR se la conoce como la "deep web" o la "web profunda", o incluso la "web oscura", a modo de calificar a ésta red de servicios que se encuentran ocultos dentro de internet.

Entre las ventajas que presentan éstos servicios es que, como su nombre indica, **están ocultos**. Es decir, su dirección en la red, la dirección física, y su ubicación, están ocultos. Y como la conexión se realiza mediante TOR, no es necesaria ninguna encriptación ya que ésta ya se encuentra presente en la red.

Estos servicios no se identifican mediante dominios normales como en la red normal, sino que las direcciones se generan de forma automática, mediante un código hash muy largo que acaba en un dominio *.onion*. Son nombres en apariencia muy feos, como por ejemplo:

jzrxewwairq4j3eru3xlkb2fkjalgx4usabg8eurilboka7sasv2ognd.onion

Esto es una ventaja y un inconveniente al mismo tiempo. Una de las ventajas de usar dominios con nombres descriptivos es que son fáciles de memorizar y la gente los puede memorizar y compartir fácilmente, incluso boca a boca. Por contra, hay que pagar por ellos y no garantizan tu privacidad si lo que quieres es, por ejemplo, conectarte con el ordenador de tu casa sin usar una dirección física (IP), además de necesitar una dirección estática para tu servidor, realizar una configuración en tu red, etc.

Los nombres de éstos servicios ocultos no son nada bonitos ni fáciles de recordar (casi que asustan), y probablemente preferirías usar direcciones físicas. Pero son gratis, mantienen la privacidad de tu servicio, y encima van siempre contigo aunque no dispongas de una dirección IP estática. De hecho, no tienes que hacer absolutamente nada para conseguir una, ya que se generan y se asignan automáticamente al poner tu servicio on-line en la red TOR.

Acceder a un servicio es igual de sencillo. Sólo tenemos que introducir dicha dirección en un navegador, igual que cualquier otra dirección. Con la limitación de que sólo podremos acceder si estamos conectados a través de la red TOR.

Limitaciones

Todo lo que se expone en éste artículo es muy bonito, pero naturalmente todo tiene una cierta letra pequeña. TOR no está exenta de algunas limitaciones en su tecnología.

Una de las quejas más comunes de la gente que usa TOR es la velocidad de conexión. O mejor dicho, **el ancho de banda**. Los nodos de conexión limitan el ancho de banda a cada conexión, y ésto es por un buen motivo: para que todo el tráfico tenga el mismo peso y no haya ningún usuario que llame más la atención que otro. De éste modo se garantiza que un tercero no pueda identificar una conexión midiendo el exceso de ancho de banda utilizado si, por ejemplo, decide ver videos en Youtube.

Las limitaciones dependerán de cada nodo y obviamente se utilizará el ancho de banda más bajo. Es decir, que si esperas que tu conexión siga funcionando a 20Mbps de bajada, me temo que no va a ser el caso.

Por otro lado, **TOR sólo encripta las comunicaciones que utilicen el protocolo TCP**. Es decir, no sirve como proxy para UDP. Si un servicio o un juego decide utilizar el protocolo UDP, tendrás que pasarlo por fuera de TOR (y, por tanto, exponerte) o no pasa. Existen formas de redireccionar las conexiones UDP a TCP mediante TOR, pero son algo más complejas.

Muchas páginas bloquean el acceso a sus servicios mediante TOR. En especial, las que peor lo llevan son las que utilizan **Cloudflare**, un servicio de distribución de tráfico y entrega de contenidos (CDN) bastante popular hoy en día. Google a veces tampoco está muy contento con éstas conexiones, y en ocasiones te ofrecerá un *captcha* para verificar que no eres un programa automatizado. Si bien ésto puede ser un inconveniente o una ventaja dependiendo de tu filosofía con respecto a la privacidad y tus preferencias de uso, ya que son servicios bastante infames por minar datos de sus usuarios sin su consentimiento y, en ocasiones, sin su conocimiento.

Por último, cabe recordar que TOR sólo protege las comunicaciones entre el cliente y el servidor de destino. Ésto quiere decir que tu navegador sigue expuesto a posibles ataques y pueden seguir obteniendo la huella digital de tu navegador. Para minimizar éstos riesgos, es recomendable usar el navegador **Tor Browser**, que viene configurado para camuflar tu huella digital y con los últimos parches de seguridad.

Cómo se usa TOR

La manera más sencilla de usar TOR es mediante el uso de su navegador Tor browser. Este navegador es una versión modificada de Mozilla Firefox unida a un proxy SOCKS5 que se conecta automáticamente a la red TOR. Existen versiones para todos los sistemas operativos populares, incluido **android**. Así que podrás usarlo en prácticamente cualquier dispositivo (salvo en un iPhone). Puedes ver cómo haciendo click aquí.

Este navegador funciona como un navegador firefox normal y corriente, con la peculiaridad de que la conexión va tunelada por defecto mediante un proxy SOCKS5 a TOR.

Para usuarios más avanzados, o si quieres crear un servicio oculto, necesitarás instalar el paquete de Tor. Para ésto se utiliza Linux o BSD, aunque supongo que se podrá compilar y usar en Windows usando Cygwin o incluso un subsistema Linux si lo que quieres es un poco de privacidad pero sin dejar de concederle tu información a la NSA.

Instalarlo en Linux es muy sencillo, y la mayoría de distribuciones lo tienen en sus repositorios. Por ejemplo, en Debian y Ubuntu, se puede instalar desde aptitiude con un simple:

 # apt install tor

O en arch/manjaro:

 # pacman -S tor

La configuración se realiza en el archivo *torrc*, que normalmente se encuentra en */etc/tor*. En este archivo, podemos establecer la dirección y el puerto de escucha del proxy mediante el parámetro *SocksPort*. Por defecto deberá ser 127.0.0.1:9100, salvo que queramos exponerlo a la red (por lo general no será el caso).

SocksPort 127.0.0.1:9100

Una vez configurado ésto, guardamos y activamos el servicio.

 # systemctl enable tor
 # systemctl start tor

Y comprobamos su estado:

 # systemctl status tor

Si se encuentra **activo** (active), desde éste momento podremos redireccionar cualquier conexión mediante éste proxy. Por ejemplo, podemos configurar Firefox para usar un proxy SOCKS5 (Opciones > Configuración de red > Configuración > Configuración manual del proxy). En dirección SOCKS ponemos 127.0.0.1 y en el puerto ponemos 9100. En los selectores de abajo, seleccionamos la versión SOCKS5.

Un poco más abajo encontraremos una opción que dice “Redireccionar peticiones DNS cuando se use SOCKS v5”, esa opción debe estar activa. Pulsamos sobre Ok y reiniciamos el navegador. Desde éste momento, nuestro navegador utilizará la red TOR para realizar las conexiones.

TORSOCKS

Existe un paquete en Linux llamado torsocks, que no es más que un script que nos permite redireccionar la conexión de cualquier aplicación a traves de TOR. Para instalarlo en Debian/Ubuntu lo podemos hacer también desde aptitude

 # apt install torsocks

O en Arch/Manjaro:

 # pacman -S torsocks

Podemos activarlo mediante el comando:

$. torsocks on

A partir de éste momento, todos los comandos que se conecten a internet irán redireccionados por TOR. Para desactivarlo, basta con usar el comando

$. torsocks off

Crear un servicio oculto

Para crear un servicio oculto, como por ejemplo una página web, basta con configurar un servidor web de la misma manera que lo configurarías normalmente, pero escuchando en local solamente (127.0.0.1:80). Una vez configurado, sólo hay que decirle a TOR que tenemos un servicio en esa dirección, editando el archivo de configuración de TOR (/etc/tor/torrc):

HiddenServiceDir /var/lib/tor/hidden_service
HiddenServicePort 80 127.0.0.1:80

Podemos añadir tantos servicios como queramos de ésta misma manera. Una vez configurado, guardamos y reiniciamos el servicio.

 # systemctl restart tor

Y comprobamos que se encuentre activo:

 # systemctl status tor

Una vez activo, TOR colocará el nombre del servicio en un archivo 'hostname' dentro del directorio especificado en HiddenServiceDir.

$ cat /var/lib/tor/hidden_service/hostname

Abre un navegador conectado a TOR y escribe la dirección especificada en éste archivo para comprobar que se encuentra en funcionamiento.

ANTERIOR

Internet y la privacidad en 2020 (Y en el futuro)

SIGUIENTE

Encriptación de peticiones DNS mediante DNSCrypt

Entradas Recientes

Categorías

RSS

Subscribirse al feed RSS