

¿Qué es el TOR?

The Onion Router



DATOS

- TOR es la abreviatura de The Onion Router.
- El software TOR fue desarrollado por el Laboratorio de Investigación Naval de Los Estados Unidos para proteger la comunicación de inteligencia.
- TOR pretende ocultar la actividad e identidad de sus usuarios de la vigilancia y análisis de tráfico en línea.
- TOR tiene usos legítimos para aquellos usuarios que quieren mantener su privacidad; eludir la censura; o protegerse de regímenes represivos o de vigilancia específica.

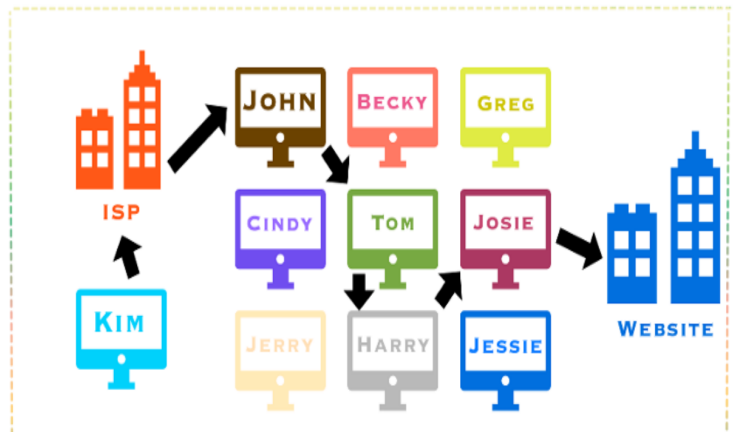
¿Como funciona?

El navegador TOR desvía el tráfico de una red de Internet de manera tal que oculta la ubicación e identidad de un usuario. En lugar de transportar el tráfico en línea a través de una ruta fija predecible [de usuario "Kim" a la Web] tal como lo hacen las visitas a sitios web o mensajes instantáneos, TOR se desplaza a través de una ruta asignada dinámicamente que se vuelve imposible de rastrear.

La conexión TOR está encriptada. Un enlace no cifrado se expone a la vigilancia y rastreando una dirección IP* particular se puede saber que sitios web ha visitado un usuario. Sin embargo, TOR utiliza una conexión cifrada lo que significa que en cualquier punto de ruta, desde el usuario de origen a la ubicación destino del Internet, no está claro de dónde vienen ni a dónde van los datos.

** Una dirección IP refleja la identidad del usuario de un dispositivo (ver ficha técnica ¿Qué es una dirección IP?)*

Cuando "Kim" visita un sitio web utilizando el navegador TOR su tráfico toma un camino al azar a través de la computadora de otras personas hasta llegar a la página web deseada. En cada punto intermedio, la información de origen y destino es eliminada para hacer la identificación del usuario extremadamente difícil. Como resultado, los proveedores de servicios de Internet no pueden realizar un seguimiento de quién es ni que sitios web está visitando el usuario. TOR también puede engañosamente presentar el último nodo de salida ["Josie"] como la información de origen.



TOR aplicado a la Explotación Sexual Infantil en Línea

Los delincentes sexuales con menores usan el navegador TOR para compartir imágenes de abusos sexuales u otros contenidos que facilitan y perpetúan una cultura de abuso sexual con menores. Mas aun, TOR permite que estos delincentes se conecten de forma anónima con víctimas potenciales. Los servicios ocultos de TOR también permiten a delincentes comunicarse en secreto entre sí. Mediante el uso de TOR los delincentes no revelan su ubicación ni identidad, evitando ser detectados por los Proveedores de Servicios de Internet (ISP) y las fuerzas del orden publico. De esta manera TOR complica la identificación de víctimas y delincentes.

TOR es el programa de software más utilizado para acceder a aquellas partes del Internet que fueron construidas deliberadamente para no estar ampliamente disponibles ni ser fácil de usar. Esto también se conoce como el DeepWeb o Darknet (Red Oscura, la cual indica la naturaleza [ilegal] de conductas allí ejecutadas). Esta red "oculta o anónima" de usuarios sólo se puede acceder mediante el uso de una pieza especial de software, tal como TOR, en el ordenador.