TRABAJO FIN DE MÁSTER:

RED DE ANONIMINZACIÓN TOR Y CIBERMERCADOS NEGROS

MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

ALUMNO: Ignacio González Muñoz

TUTOR: Ana María Escudero Quesada

Diciembre 2017

Resumen

Con la aparición de las nuevas tecnologías y servicios se ha experimentado un gran cambio en la sociedad haciendo que los usuarios estén constantemente conectados a Internet. Esto nos ha aportado grandes ventajas y agilidad en el día a día, pero también nos encontramos con algunos problemas importantes.

La información que consultamos en Internet está toda indexada en buscadores por lo tanto se está produciendo un seguimiento y análisis de datos. Para evitar esto se buscan algunas alternativas que nos aporte ese anonimato y privacidad que no se tiene en la red, como puede ser la Deep Web o Web Profunda.

El acceso a esta parte de la red no se consigue directamente desde la Web Superficial, sino que es necesario un software específico, como es por ejemplo Tor, que nos da acceso a la red anónima. Tor va a aportar al usuario un anonimato y privacidad en su navegación mediante un enrutamiento especial llamado “enrutamiento cebolla” estructurado en capas de cifrado. Tanto los usuarios como los sevidores de la red van a conseguir anonimidad.

Al surgir esta red anónima también han aparecido algunas nuevas técnicas de criminalidad a través de la red que van a tener que ser estudiadas y solventadas por los agentes de seguridad. Uno de los principales problemas es la expansión internacional que puede llegar a tener estas técnicas llegando a requerir una cooperación internacional para intentar solventarlas.

Summary

With the appearance of new technologies and services society has experimented a big change, making users being constantly connected to the Internet. This has given us great advantages and agility on a daily basis, but it has also introduced some important issues.

The information we find on the Internet is indexed on search engines, therefore data tracking and analysis is taking place. In order to avoid this, we look for some alternatives that provide us with the anonymity and privacy that the web is lacking, such as the Deep Web.

The access to this part of the network can't be achieved directly from the Superficial Web, but a specific software, like Tor, is needed to give us access to anonymity. Tor provides to the user with anonymity and privacy while browsing by using a special routing known as "onion routing", which has multiple layers of encryption. This brings anonymity to both users and servers.

With the emergence of this anonymous network, some new crime techniques have also appeared that will have to be studied and solved by the security agents. One of the main problems is the international expansion that might bring these techniques, requiring international cooperation to try to solve them.

Contenido

1 Introducción

En el Trabajo Fin de Máster *Red de anonimización TOR y cibermercados negros*, se quiere estudiar la red TOR y analizar todo el entorno de anonimato y cibermercados que se alojan en ella.

La red TOR se caracteriza por ser la red anónima donde un individuo puede operar en la red sin ser identificado, debido a que el viaje de la información navega entre servidores para ocultar la dirección IP de origen, cifrando en cada conexión todo el tráfico, haciendo prácticamente imposible conocer el origen de la conexión.

Uno de los objetivos de este trabajo es estudiar y analizar técnicas capaces de desvelar la identidad de un usuario de esta red, haciendo que un individuo anónimo deje de serlo.

La red TOR al aportar anonimato a los usuarios, esto hace que sea utilizada para el desarrollo de actividades comerciales ocultas e incluso actividades o mercados ilegales (armas o drogas). Se analizarán este tipo de actividades, así como los sistemas utilizados para ocultar los mercados alojados en la red.

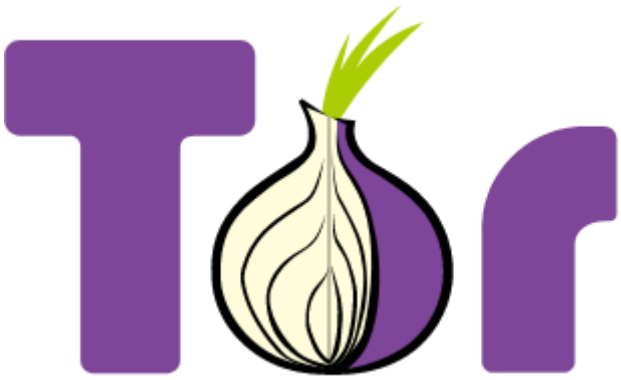
La realización de las transacciones en esta red, para asegurarse de que no se pueden rastrear sus movimientos, se utilizan criptomonedas. La más utilizada es bitcoins, que es comprada y vendida en internet con dinero real. También se estudiarán este tipo de monedas y otros métodos de transacción en la red.

Además, se quiere estudiar cómo las Leyes actuales actúan frente a estos sistemas donde se alojan actividades ilegales y cómo estas actividades intentan evadirlas.

2 QUÉ ES TOR

Tor es el acrónimo de “The Onion Router”, el “Enrutador cebolla”. Esta referencia se debe a la estructura de la red usada por Tor, que consiste en varias capas de cifrado que protegen los datos.

Es un proyecto que tiene como objetivo principal el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela datos de su identidad (anonimato a nivel de red) ni de los datos enviados en la comunicación.



Tor pertenece a la Darknet o también conocida como Deep Web en la que se evita la censura de determinados contenidos alojados. La red Tor es la red distribuida más famosa y utilizada como herramienta para dar solución a la privacidad y anonimato en Internet. Desarrolla una red que permite el acceso a servicios online bloqueados por los proveedores de Internet, manteniendo información confidencial en el anonimato.

Los mensajes realizan el viaje desde el origen hasta el destino a través de varios routers especiales “onion routers” o capas bajo la protección del cifrado, impidiendo que las páginas por las que se navega identifiquen la IP desde la que se accede.

Tor se desarrolló como una red mundial de servidores con la Marina de EEUU con el objetivo de proteger las comunicaciones gubernamentales, permitiendo que se navegara de forma anónima a través de Internet. Actualmente además de objetivos militares, tiene gran variedad de usos ya sean periodísticos, policiacos, activistas, etc.

Los paquetes de datos que se envían a través de la red están compuestos por dos partes: los datos que se quieren enviar y el encabezado que es donde se encuentra mucha información como la fuente, destino, tamaño, tiempo, etc. La persona que recibe el paquete de datos, según la información que recibe por la cabecera puede conocer el originario de la comunicación, además del proveedor de Internet como intermediario autorizado, e incluso algún sujeto no autorizado. Ante este problema se plantea el uso de una red anónima distribuida para estas comunicaciones.

3 COMPONENTES DE LA RED TOR:

La red Tor está compuesta por nodos los cuales se comunican a través del protocolo SSL/TLS, manteniendo cada nodo una conexión TLS con el resto.

El protocolo SSL (Secure Sockets Layer)/TLS es un protocolo cifrado sobre TCP/IP, protocolo con el que funciona Internet. Es un protocolo de seguridad en las comunicaciones, permitiendo que sean confidenciales y autenticadas, a través de algoritmos criptográficos. Su uso en la web se distingue porque la URL empieza en "https://". Para las operaciones de cifrado y hash utiliza algoritmos como el cifrador de llave pública RSA 1024, el cifrador de clave privada AES 128 bits y el algoritmo de hash SHA1.

La utilización de este protocolo garantiza:

- Privacidad: los datos son cifrados antes de enviarse a través de algoritmos criptográficos (criptografía simétrica)
- Autenticación: una de las partes de la comunicación debe autenticarse para el envío de los datos.
- Integridad: los mensajes transmitidos contienen un MAC (identificador único de una pieza de hardware de red) lo que hace posible verificar si la información ha sido modificada o no antes de que el receptor la haya recibido.
- Disponibilidad: es una característica relacionada directamente con la integridad de los datos ya que, de haber un problema con la integridad, la disponibilidad de los datos no se cumpliría.

Los nodos que se pueden encontrar en una red Tor son de dos tipos:

- Los nodos OR (tor-relay): actúan a modo de encaminadores, así como servidores de directorio. Entre los nodos OR se mantiene una conexión, de esta manera no se cierra conscientemente una conexión nunca.
- Nodo OP (Onion Proxy): obtienen información del servicio directorio, crean circuitos aleatorios en la red y controlan las conexiones de las aplicaciones de los usuarios. Las comunicaciones con los nodos OR no son continuas ni permanentes, si no que cuando hay inactividad o se ha cumplido el tiempo de sesión la conexión queda cerrada.

El servicio directorio es una base de datos en la que se registra cada nodo OR con su información. Es una BBDD accesible a todos los nodos OR y usuarios finales para conocer el estado de la red. Hay nodos OR principales y otros que son secundarios que hacen de caché y backup.

Los servidores de directorio son una serie de nodos OR establecidos como nodos confiables. Las entradas a la información del servicio de directorio son protegidas

criptográficamente con firmas. La información para que pueda incluirse en el servicio directorio debe provenir de uno de estos nodos OR confiables.

Los nodos nuevos deben ser aprobados anteriormente, así se evitan ataques de nodos que es dudoso su origen o finalidad. La aprobación de nuevos nodos es realizada desde los servidores de servicios a cargo de los administradores.

El conjunto de datos que describen a un nodo (IP, nombre…), su funcionamiento (versión de Software TOR, SO, claves…) y capacidad es información que se recolecta en el momento que un nodo OR es arrancado.

4 FUNCIONAMIENTO DE LA RED TOR:

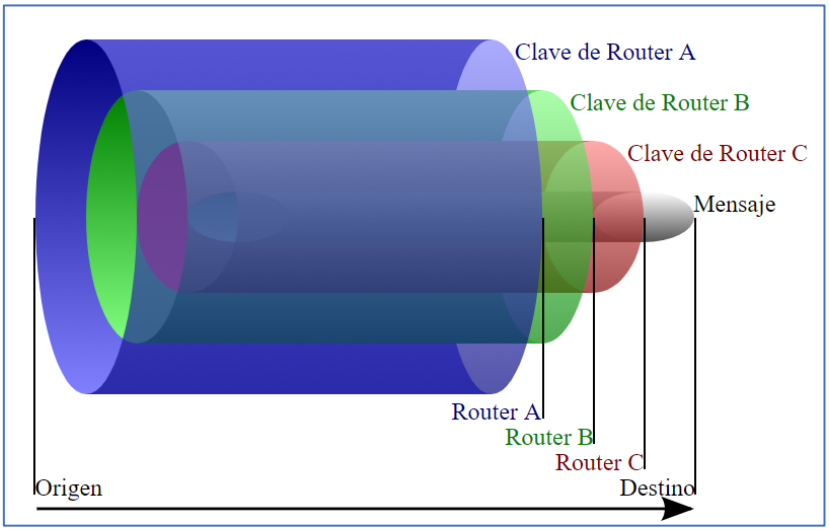
Cuando un usuario intenta conectarse a un sitio web mediante un ordenador o dispositivo móvil, éste intenta conectarse directamente a la máquina de destino por la ruta más directa, obteniendo de esta manera más velocidad y siendo más eficiente.

La red de cualquier usuario está identificada bajo una dirección IP, lo que clasifica a esa red con un identificador único, conociendo de esta manera el punto de partida de la conexión.

Tor es una herramienta para navegar que quiere evitar esa conexión directa entre el servidor remoto y el dispositivo de origen, siendo una red montada dentro de Internet con diferentes elementos por los que viajan los datos.

Para acceder a la red es necesario obtener e instalar el software de Tor en el equipo, el cual utiliza el protocolo proxy SOCKS (Socket Secure) para interconectar el software con la red. El proxy trabaja a más bajo nivel que el proxy HTTP y se inicializa y configura mediante Tor. Es un proxy TCP encargado de encaminar los paquetes de red a través de un servidor proxy entre cliente y servidor. Como se ocupa de las peticiones HTTP y de flujos de datos permite el soporte de las sesiones cifradas extremo-extremo mediante HTTPS

En la red Tor además de garantizar el anonimato al usuario en el momento de la conexión, la estructura de capas creada hace que la información va pasando de un nodo a otro bajo la protección de cifrado, impidiendo que las páginas por las que se navega sean capaces de identificar la IP de origen. De esta manera, los paquetes de datos navegan desde el origen hasta el destino mediante una ruta de caminos aleatorios siguiendo los diferentes nodos para crear el circuito de conexión.



Estructura de la transmisión de los datos con encaminamiento cebolla.

Hay tres partes en este tipo de enrutamiento:

- Establecimiento de la ruta a seguir
- Proceso de cifrado de la información
- Descifrado de la totalidad de la información

El establecimiento de la ruta se va a realizar en el momento que un usuario quiere realizar una conexión con un destino como pudiera ser una página web. La ruta no va a ser directa hacia el servidor, si no que pasará por distintos nodos antes de llegar a su destino. Actualmente la red Tor cuenta con más de 7000 nodos que pueden ser seleccionados de forma aleatoria, cuantos más nodos, más privacidad y mejor navegación.

Así se permite crear una red privada en la que el tráfico circula al menos por tres nodos OR hasta llegar al destinatario. Los dos primeros son nodos intermedios (middle-OR o Bridge-Tor), que son conocidos en la red y cualquiera puede conectar con ellos, y son los encargados de recibir y pasar el tráfico. Los nodos intermedios no se pueden identificar como origen o destino de la comunicación por lo que hay más seguridad. También funcionan como la entrada en la red Tor en los países que los nodos OR están deshabilitados o bloqueados.

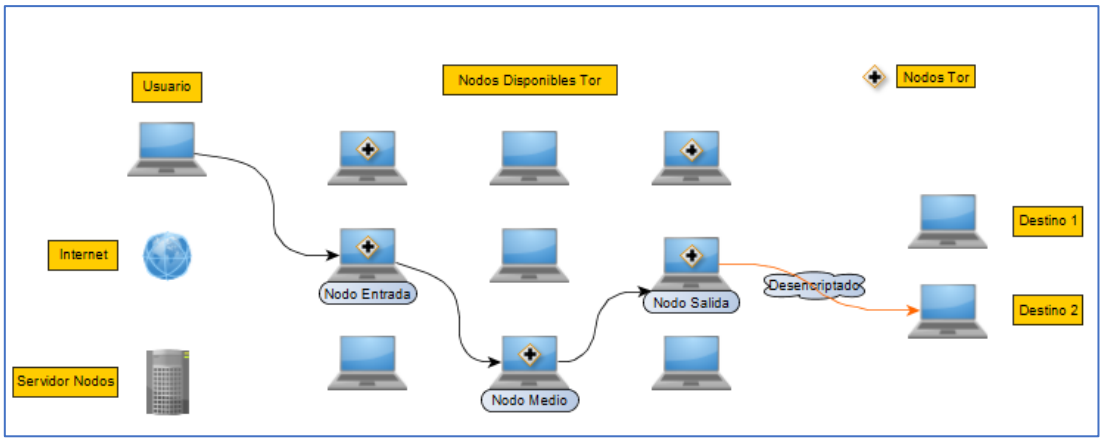
El primer paso que realiza el Software de Tor a la hora de realizar una conexión es conectarse a Internet para obtener el listado de los nodos disponibles y con los que se creará la posterior ruta de conexión aleatoria.

Paso1. El usuario obtiene el listado de nodos Tor del Servidor de Nodos

Una vez obtenido el listado de nodos, Tor seleccionará un nodo de entrada estableciendo con él una conexión segura mediante el protocolo TLS. Cuando la conexión está establecida se crea una clave de sesión entre el Software del equipo y el nodo de entrada.

El software de Tor del equipo usará la clave de sesión para cifrar el mensaje que desea enviar al nodo de entrada. El nodo de entrada recibirá el mensaje y lo descifrará descubriendo el nodo intermedio con el que tiene que contactar. El nodo inicial entonces establece conexión segura con el nodo intermedio mediante TLS. Cuando se

ha establecido la conexión, el nodo de entrada cifra un mensaje con la clave en el que informa a Tor que ya ha establecido conexión con el nodo intermedio. Al recibir Tor el mensaje del nodo de entrada, lo descifra y como se ha confirmado la conexión entre nodos, se asigna una nueva clave de sesión entre Tor y el nodo intermedio.



Paso 2. Tor selecciona los nodos aleatoriamente entre el usuario y el destino

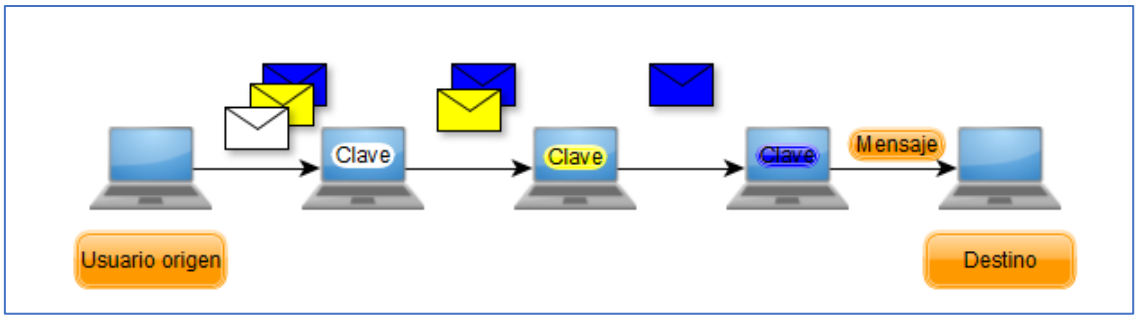
Tor selecciona el nodo de salida, último nodo de la conexión, y genera un mensaje con dicho nodo cifrándolo con la primera y segunda clave de sesión. El mensaje se envía al nodo de entrada, el cual descifra parte del mensaje y luego es enviado al nodo intermedio el cual descifra el mensaje completo con la segunda clave.

El nodo intermedio entonces establece una conexión segura con el nodo de salida, dando a conocer al software Tor que la conexión fue realizada correctamente. En este momento se crea una clave de sesión (tercera) entre Tor y el nodo de salida.

Finalmente, el nodo de salida es el que se encarga de contactar con el destino que había solicitado el usuario. Es un nodo que también se tiene constancia en la red y por lo tanto puede ser utilizado por otros usuarios. Al salir la información por ese último nodo, su IP es interpretada como la originaria del tráfico y los datos son descifrados para que el usuario final pueda utilizarlos, quedando en ese momento desprotegidos.

El enrutamiento de conexión en Tor tiene una duración de 10 minutos, a partir de ese tiempo la ruta se modificará y se establecerá una nueva automáticamente.

La estructura de enrutamiento cebolla de los datos es la que se muestra en la imagen siguiente. A través de un cifrado asimétrico el usuario origen va cifrando el mensaje por capas comenzando por el cifrado del mensaje con la clave pública del último nodo, de este modo sólo él podrá descifrarlo. También se incluyen las instrucciones para que el mensaje llegue a destino. Este paquete se cifra de nuevo añadiendo las instrucciones para llegar al último nodo de la lista para que sólo él lo pueda descifrar y acabe llegando al nodo destino. Mediante la encriptación con clave simétrica se impide que los nodos puedan conocer el resto de nodos con los que se comunican.



Estructura de enrutamiento cebolla de los datos

Todos los nodos de Tor aparecen en un listado público, de esta manera los nodos aumentan la privacidad. Si el equipo de un usuario origen se quiere conectar a un destino mediante la red Tor tiene que conectarse a otro nodo Tor. En el caso de que el equipo origen a su vez sea un nodo Tor para otros equipos origen, también tiene que estar conectado a otro nodo. Esto hace que dificulte mucho saber si las conexiones desde el equipo origen (y además nodo Tor) son iniciadas como usuario o como nodo. Hace que la extracción de información sobre este equipo origen sea mucho más compleja.

Los nodos que hay en la red Tor son equipos de usuarios voluntarios, cualquier persona puede participar en esta red mediante la configuración de su equipo para la donación de ancho de banda y cesión de procesamiento.

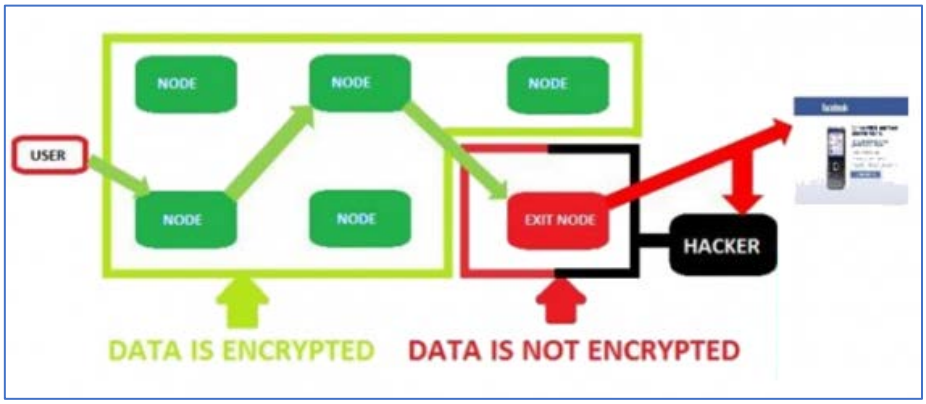
4.1 DESVENTAJAS:

Las principales desventajas que se pueden encontrar al trabajar con la red Tor son:

- La red Tor cifra la información a su entrada y la descifra a la salida, haciendo que sea imposible saber quién envió la información, lo que hace que esta red sea utilizada por muchos usuarios para realizar negocios ilegales.

- El diseño de la red Tor mediante toda esa configuración de nodos hace que la navegación sea más lenta, la información al tener que saltar entre los nodos diseñados, hace que los tiempos de respuesta aumenten y provoque lentitud en la navegación. En Tor, las distancias se amplían entre cliente y servidor, los nodos intermediarios se sitúan dentro del intercambio de datos recibiendo y transmitiendo la información del extremo de entrada al de salida, todo esto con un cifrado en capas para el archivo, así como para las instrucciones hasta el nodo de salida. Por lo tanto, ya no estamos dependiendo de la respuesta y velocidad del servidor, sino también de los diferentes nodos hasta el extremo.

- Cuando la navegación se está utilizando correctamente en Tor, se puede garantizar un grado de anonimato, pero la privacidad puede estar afectada si alguien está a la escucha del tráfico en el nodo punto de salida, donde la información sale descifrada. El propietario de un servidor de salida puede ver toda la información, cuando es descifrada, antes de llegar a Internet. No va a poder conocer el emisor, pero sí podría acceder a la información transmitida.



Encriptación de datos en el circuito de Tor

5 SERVICIOS OCULTOS

Tor nos ofrece, además de la anonimización del cliente y superar censuras gubernamentales, la capacidad de enrutar hacia servicios ocultos internos en su propia red.

Tor ofrece una serie de servicios en máquinas que hace que sea una de las características más interesantes para proporcionar anonimato en la red. Pueden ser servicios de cualquier tipo, siempre que se basen en TCP: SSH, HTTP, IRC, SMB, FTP, etc.

El usuario que desea acceder a un servicio oculto, éste no accede directamente a la máquina si no que accede únicamente al servicio publicado por la máquina. Este tipo de servicios solamente están disponibles en la red Tor, aunque también pueden estar disponibles mediante Tor2web directamente desde Internet. El acceso a estos servicios ocultos desde Tor2web tiene la desventaja de perder el anonimato.

Al conectarse mediante servicios ocultos evitamos conocer la ubicación de la máquina por lo que queda protegida. El acceso siempre se realizará mediante su dirección ".onion", de ahí que su nombre sea servicios ocultos. Se desconoce su existencia siempre que las direcciones no se hagan públicas.

Hay que tener en cuenta que el circuito que se crea para la conexión con servicios ocultos es diferente al circuito que Tor crea cuando enruta a direcciones de internet convencionales. Estos circuitos .onion se componen de 3 o de 6 saltos.

La instalación de un servicio oculto por parte de un usuario es algo sencillo, pero hay que tener en cuenta que están expuestos a ataques. El anonimato no equivale a seguridad

Si un usuario quiere crear un sitio web dentro de la red Tor deberá descargar Tor Browser, instalarlo y comprobar que funciona correctamente. Luego deberá realizar la instalación de un servidor web local y configurarlo para ser accesible desde Tor.

5.1 Direcciones .onion

Para la construcción de este tipo de direcciones primero se calcula el SHA1 de la clave pública generada. De los 160 bits que forman el hash, se coge la primera mitad y se codifica en Base32, haciendo que todos los nombres de dominio tengan exactamente una longitud de 16 caracteres y solo contengan números de 2-7 y letras de a-z. para finalizar se añade la parte ".onion"

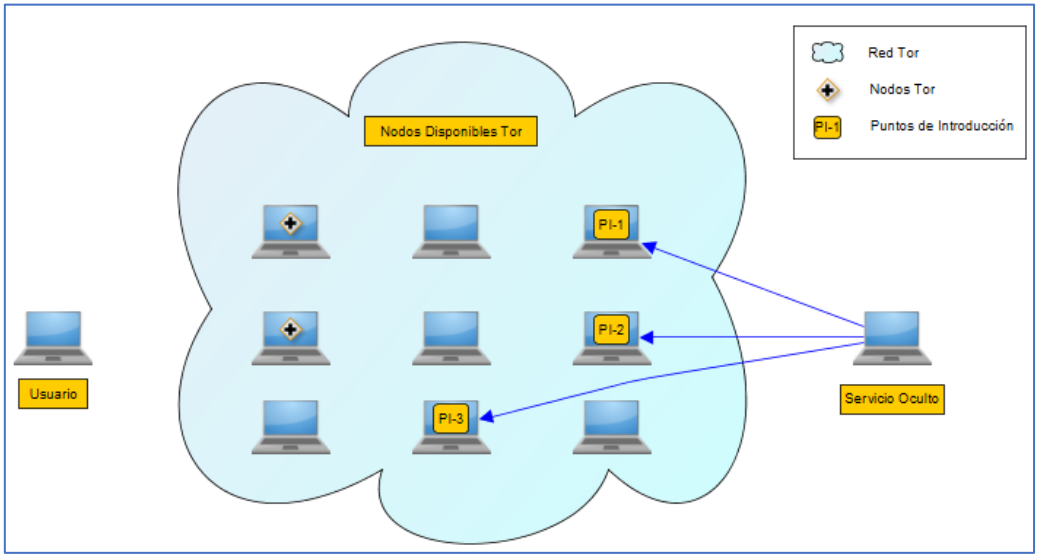
Las direcciones .onion no son tan aleatorias como parece, para la misma página existe un patrón fijo en el nombre que hace que la dirección sea más fácil de recordar. Por ejemplo "https://facebookcorewwwi.onion/"

5.2 Gestión del servicio oculto para constar en la red Tor:

Una vez que se ha montado el servidor, se han añadido las opciones HiddenServiceDir y HiddenServicePort en el archivo torrc y se inicia Tor Browser, el servicio oculto está disponible. El proceso de disponibilidad en la red se divide en dos fases:

1. Elección de los *Puntos de Introducción*:

   El servicio oculto Tor se anuncia en la red Tor y para ello escoge varios nodos aleatoriamente y les entrega su clave pública. Esos nodos son "*Puntos de Introducción*" del servicio oculto.



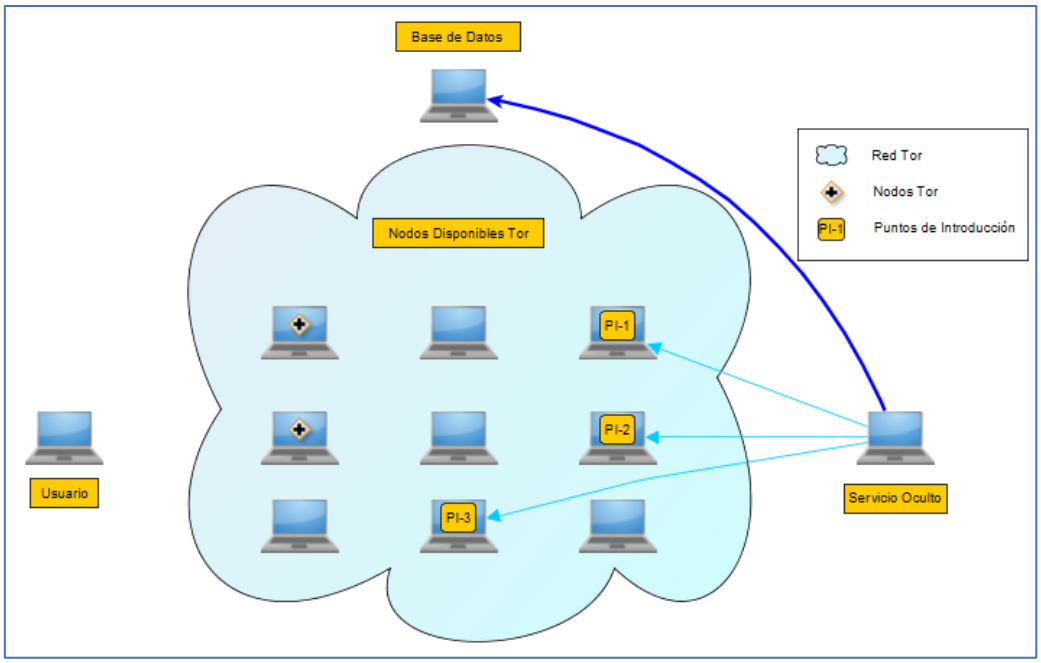
Fase 1. Elección de los Puntos de Introducción

La conexión entre el servicio oculto y los nodos no es directa, ya que si no sería muy fácil desanonimizar al servicio controlando un *Punto de Introducción*. Para evitarlo, la conexión se realiza mediante un circuito Tor compuesto por un nodo de entrada, un nodo intermedio y un nodo de "salida". Así es muy complicado asociar un *Punto de Introducción* con la dirección IP del servicio oculto.

Por defecto se eligen 3 nodos *Punto de Introducción*, pero podrían ser hasta 10.

2. Creación del Hidden Service Descriptor:

   Después de haber elegido los *Puntos de Introducción* el servicio oculto crea el archivo HSD (Hidden Service Descriptor). El HSD contiene información fundamental para la conexión entre clientes y servicios ocultos. Un HSD señala los *Puntos de Introducción* que el servicio oculto eligió en el primer paso.



Fase 2. Creación del Hidden Service Descriptor

Cuando el servicio oculto ha compilado la información necesaria y tiene generado el HSD, es el momento de subir a Tor los datos para que los clientes puedan conectarse a él.

El servicio oculto subirá el descriptor a un conjunto fijo de servidores que harán de servicios directorio si el tipo de descriptor es “v0”. Si el descriptor es tipo “v2” entonces el servicio oculto subirá el archivo a un conjunto no fijo de servidores de directorio ocultos.

Para enviar el descriptor, el servicio oculto generará circuitos de Tor a los nodos correspondientes que cuenten con un flag “HSDir”. El servicio oculto publicará un nuevo descriptor v2 cada hora o cada vez que el contenido sea modificado.

Tras estos dos pasos el HSD ya se ha publicado anónimamente en los servidores de directorio y está disponible para que los usuarios lo obtengan cuando intenten acceder al servicio oculto.

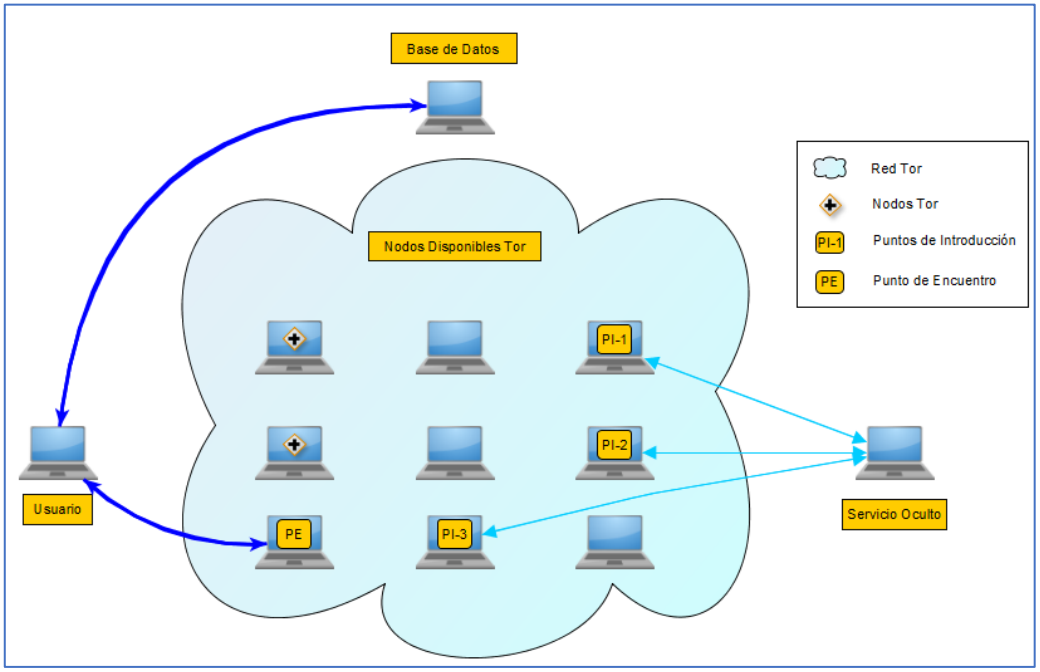
5.3 Conexión a Servicios Ocultos por parte de un cliente

Los pasos que suceden internamente para la conexión de un cliente a un servicio oculto mediante Tor son los siguientes:

1. Conocimiento de la dirección .onion:

   El cliente debe conocer la dirección .onion a la que está asociada el servicio. No existe ningún repositorio oficial donde aparezcan las direcciones .onion disponibles. Esto es así porque si no se consideraría una grave vulnerabilidad.

Existen mercados de direcciones .onion, criptomercados, donde se pueden comprar archivos con direcciones .onion.



Conexión con el Punto de Encuentro

Cuando el usuario introduce una dirección en el navegador, éste deberá obtener el descriptor HSD que el servicio oculto subió a la red Tor. Según la versión, buscará en el conjunto fijo de servidores de directorios v0 o en el conjunto cambiante de servidores oculto de v2.

El cliente también se pondrá en contacto con un nodo aleatorio de Tor y solicitará que actúe como "*Punto de Encuentro*". Le enviará un OTC (one-time secret) que es el identificador único del circuito Tor entre el *Punto de Encuentro* y el cliente.

2. Envío de mensaje de presentación:

   El cliente ya tiene el descriptor y el *Punto de Encuentro* está listo, por lo que generará un mensaje de presentación con la dirección del *Punto de Encuentro* y el OTC. El mensaje está cifrado con la clave pública del servicio oculto, así no podrán ver su contenido los nodos por los que pase. Se enviará a uno de los *Puntos de Introducción* solicitando su entrega al servicio oculto.

   La comunicación con el *Punto de Introducción* se realiza mediante un circuito Tor para no asociar la dirección IP con el mensaje.

   El esquema sería el siguiente:

   Cliente ⇔ Nodo de Entrada ⇔ Nodo Intermedio ⇔ Nodo de "Salida" ⇔ *Punto de Introducción* ⇔ Nodo de "Salida" ⇔ Nodo Intermedio ⇔ Nodo de Entrada ⇔ **Servicio Oculto**

3. Descifrado del mensaje por parte del servicio oculto:

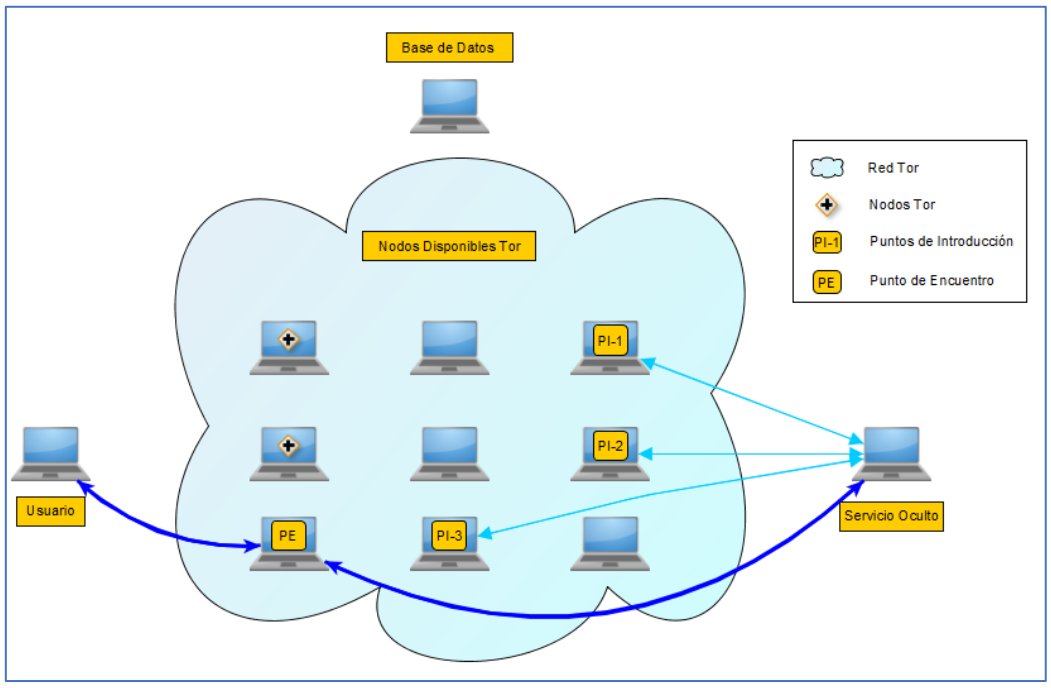
   Cuando el mensaje de presentación llega al servicio oculto, éste lo descifrará con su clave privada y establece la comunicación con el circuito Tor con el *Punto de Encuentro* que eligió el cliente. El servicio oculto enviará el OTC al *Punto de Encuentro.* El *Punto de Encuentro* relacionará la OTC con el circuito Tor creado.

   Es importante que el servicio oculto utilice "entry guards" para evitar elegir un nodo de entrada malicioso que sea capaz de desvelar su IP

4. Notificación al cliente del éxito de la conexión:

   El Punto de Encuentro informará al cliente del éxito de la conexión. A partir de ahora el cliente y el servicio oculto podrán utilizar sus circuitos Tor para comunicarse entre ellos, pasando por el *Punto de Encuentro*. El *Punto de Encuentro* hará la función de retransmitir, con cifrado extremo a extremo, los paquetes de datos del cliente al servidor oculto y viceversa.

   Ahora en el esquema del punto 2 quedaría sustituido el *Punto de Introducción* por *Punto de Encuentro*



Notificación al cliente del éxito de la conexión

6 AMENAZAS EN TOR:

En Tor también existen algunos tipos de amenazas que lo pueden poner en peligro, se clasificarían de tres tipos:

- Errores de usuarios: el usuario debe hacer un buen uso del sistema, no accediendo o ejecutando enlaces o direcciones que puedan desviar la comunicación de los nodos del circuito. Esto provocaría que datos del usuario, como la dirección IP, puedan ser desvelados.

  Se debería evitar la navegación por sitios web HTTP, ya que los nodos de salida pueden ser monitorizados y controlado su seguimiento al saberse que son los nodos que pueden ver los paquetes que circulan. En HTTP esto no sucede ya que los nodos de salida no pueden acceder al contenido que transportan.

- Problemas de la propia red Tor: son problemas de diseño que pueden afectar a la privacidad de los usuarios. Al redireccionar a los usuarios a servidores especiales puede facilitar ataques Man in the Middle pudiendo relacionar las direcciones IP con las peticiones enviadas al Servidor. Podrían ser clasificados como los que estudian los patrones de temporización y los que hacen recuento de paquetes por tamaños.

- Problemas indirectos: serían los relacionados con las vulnerabilidades explotables del propio navegador Tor. El nodo de salida es considerado como el más débil debido a la exposición a la que se somete, ya que la información no está cifrada. Este nodo retrasmite directamente a Internet pudiendo conocer lo que se está enviando y recibiendo, por tanto, es fácilmente rastreable.

Algunos expertos opinan que la red Tor cuenta con algunos problemas de configuración y vulnerabilidades que pueden provocar que el anonimato de los usuarios pueda perderse. Parte de estos problemas se encuentran en los navegadores utilizados, ya que mediante exploits se han filtrado documentos con información sensible en la red.

6.1 WebRTC.DLL

Se descubrió hace dos años un método que podía comprometer al navegador web, con el uso de WebRTC.DLL. Esta DLL fue diseñada para organizar un canal de transmisión de flujo de video de apoyo a HTML5, utilizándose para establecer la dirección IP real de la víctima. Las peticiones del llamado STUN de WebRTC se envían en texto plano, evitando Tor y todas las consecuencias que esto conlleva. Este bug rápidamente fue solventado por el sistema Tor y ya bloquea WebRTC por defecto.

Los sistemas de monitorización son otro de los puntos conflictivos del sistema ya que los usuarios pueden compartir sus recursos para configurar un servidor de nodo. Al ser el nodo el elemento intermediario y además el último punto del descifrado del tráfico, puede ser un lugar apto para filtrarse información. Si por ejemplo las direcciones de los

recursos son extraídas de las cabeceras HTTP existe la posibilidad de obtener información del tráfico de modo descifrado.

6.2 TorMoil

Muy recientemente (6 de Noviembre 2017) Tor Project ha lanzado una nueva actualización de seguridad al navegador Tor, un parche para proteger a los usuarios de TorMoil, una vulnerabilidad detectada que podría ser utilizada para mostrar la dirección IP real de los usuarios.

Según se ha visto, cuando un usuario de la red Tor intenta acceder con el navegador web a ficheros a través de un enlace "file://", el navegador establece una conexión directa con el servidor, ignorando Tor Browser, en vez de realizarse mediante los proxies y relés de Tor pudiendo quedar almacenada la IP en el Servidor. Es una vulnerabilidad que afecta a usuarios que utilicen el navegador Tor en sistemas operativos Linux y OS X. Esta vulnerabilidad, al igual que otras que han surgido, ha sido solventada mediante un parche en la nueva versión de Tor Browser 7.0.9.

Algunas de las vulnerabilidades que han sido descubiertas en la red Tor son:

- Las claves RSA-1024 que son utilizadas por los servicios ocultos son consideradas claves débiles. Aunque un ataque a estas claves no es la mejor opción para un atacante, sería recomendable incrementar la longitud de las claves o utilizar otro algoritmo para las claves públicas.
- Facilidad para obtener el flag HSDir y convertirse en un directorio de servicios ocultos. Aunque se han puesto restricciones, sigue siendo viable para un atacante conseguir este flag por lo que habría que tomar medidas para dificultar el acceso.
- Los HSDirs responsables de un servicio oculto son predecibles. Un atacante puede averiguar los nodos responsables de un servicio oculto en un momento determinado de tiempo.

7 DESANONIMIZACIÓN

7.1 Desanonimización de servicios ocultos:

Para realizar la conexión entre un cliente y un servicio oculto es necesario la creación de dos circuitos, con un punto de encuentro intermedio. En el circuito establecido desde el servicio oculto, el primer nodo de entrada es el que conoce la dirección IP de la máquina que ofrece el servicio.

Para poder realizar un ataque y conseguir la dirección IP, sería necesario que el servicio oculto utilizase como nodo de entrada uno de los que tiene el atacante y que el punto de encuentro sea uno de los elegidos por el mismo. Cuando se cumplieran esas condiciones el atacante podría desenmascarar el servicio oculto mediante un ataque de correlación que permitiría al nodo de entrada identificar un patrón de tráfico específico enviado por el punto de encuentro.

7.2 Desanonimización de usuarios:

Este proceso sería similar al de la desanonimización de servicios ocultos, pero en este caso el punto crítico del ataque se encontraría en el nodo que conoce la dirección del usuario, que es el nodo de entrada o el primer nodo utilizado para conectarse al nodo oculto.

Cuando un atacante tiene todos los HSDirs responsables de un servicio oculto podría saber cuándo un cliente quiere conectarse e incluso desvelar su identidad, mediante un ataque de correlación, al reconocer en el nodo de entrada un patrón de tráfico específico enviado desde el HSDir que recibió la petición del cliente.

Este ataque tiene la ventaja de no requerir un nodo de entrada para llevarlo a cabo, ya que al monitorizar la entrada a la red se podría realizar el ataque de correlación y desanonimización del usuario. Incluso se ha advertido, en alguna conferencia de seguridad, del mayor riesgo de desanonimización en usuarios de servicios ocultos que en usuarios de Tor que no utilizan este tipo de servicios.

8 ATAQUES:

Algunos de los ataques que puede sufrir Tor, según sus objetivos, son los siguientes:

8.1 Ataque Sybil:

Tor funciona gracias a todos los usuarios que ceden recursos a la red, por lo que cuenta con nodos en diferentes países, aunque la mayoría están en Europa y América del Norte al ser zonas libres de censura y buena conexión de Internet. Este ataque se centraría en el caso de que un usuario desplegara cientos o miles de nodos y pudiera hacerse con el control.

Aquel usuario que controle mayor número de nodos tiene más posibilidades de formar parte en más circuitos. No es un problema que un usuario u organización cuente con muchos nodos, siempre y cuando su objetivo no sea maligno.

La red Tor cuenta con un sistema (script) que comprueba si ha habido un aumento repentino o anormal de nuevos nodos y además con un contacto para informar de nodos que puedan ser potencialmente dañinos.

8.2 Ataque predecesor:

Tiene como objetivo identificar a los clientes de la red Tor aprovechando la reconstrucción de los circuitos.

Uno o varios nodos hacen un seguimiento de las conexiones. Cada vez que un usuario reconstruye (nuevo circuito aleatorio cada 10min de conexión) un circuito, se vuelve a conectar a nuevos nodos haciendo que el atacante identifique al cliente porque tenderá a conectarse más veces que cualquier otro nodo.

Un atacante que controle muchos nodos podría hacerlos fallar muy habitualmente para obligar a los clientes a reconectarse una y otra vez aumentando el éxito del ataque.

8.3 Ataque de reconstrucción circuital:

se basa en controlar los tres nodos de una conexión. El atacante podría conocer al cliente y al servidor mediante una reconstrucción. Es un ataque muy complejo y complicado, pero es uno de los ataques que aparecen en los documentos filtrados de WikiLeaks.

8.4 Ataque Sniffer:

Debido al funcionamiento de Tor, los nodos de salida podrían realizar ataques “Man in the Middle” para espiar información enviada por el cliente. Es posible sobre todo en conexiones HTTP, por lo que se recomienda usar el protocolo HTTPs. Aun así, hay

herramientas y métodos para atacar conexiones HTTPS. Los nodos que han sido objetivo de intento de espionaje y se ha descubierto se han marcado con un *flag* "BadExit" lo que hace que no puedan volver a ser nodos de salida.

8.5 Ataques derivados de vulnerabilidades presentes en Tor Browser:

El navegador utilizado (Tor Browser) es una modificación de Mozilla Firefox Extend Support Release con modificaciones.

Las extensiones o el mismo navegador pueden presentar vulnerabilidades que pueden ser utilizadas para desanonimizar al cliente.

8.6 Correlación de Flujo:

En este tipo de ataques el usuario que observa dos flujos de paquetes intenta verificar que pertenecen al mismo flujo en diferentes flujos de la red de anonimato. Los flujos en la red Tor tienen cifrado "onion" y no pueden ser comparados directamente, sino que es necesario buscarles una relación mediante otro tipo de información. Algunas técnicas para correlacionar flujos son:

8.6.1 Conteo de Paquetes

Es una de las formas sencillas de correlacionar flujos. Un atacante puede observar los paquetes de entrada y salida del primer Router onion para determinar el siguiente nodo del circuito. Este mismo proceso se repite en otros routers en el circuito hasta que se puede determinar el destinatario. Es una forma sencilla, pero se requiere analizar gran cantidad de datos en la red. Además, asume que no hay variación del número de paquetes entrantes y salientes de un Router en un flujo dado.

8.6.2 Análisis de Sincronización

la sincronización de paquetes es otra parte de los datos que puede ser utilizada para correlacionar flujos. Se puede utilizar una función de correlación para intentar correlacionar flujos basados en su retardo entre paquetes, que es la diferencia de tiempo entre paquetes adyacentes al llegar al flujo. Este método puede tener problemas con paquetes caídos. Una serie de tiempo es una manera de mirar los datos de sincronización de paquetes. Para crear la serie de tiempo se establece una constante de tiempo (T), se divide el flujo de paquetes en ventanas de tamaño T y contabilizar el número de paquetes de cada ventana. La función de correlación es un producto de vector normalizado.

El punto débil de los ataques de sincronización es que dependen de que el atacante controles los routers Tor, y es necesario controlar gran parte de los routers Tor de la red para que sea efectivo. Ha habido también algunos ataques

propuestos sin controlar los routers de la red Tor, en el que los adversarios controlan los Intercambios de internet y así pueden observar el tráfico que entra y sale de los países. Se indicó que se podía rastrear y hacer correlación de un solo paquete de dos mil en un flujo dado.

8.6.3 Correlación Activa de Sincronización

este es un tipo de ataque en el que se quieren hacer correlaciones basadas en el tiempo, pero de forma más fácil y efectiva. Funciona al tener un Router atacante alterando la señal de retraso de un paquete de una conexión al incluir o retrasar paquetes en un flujo. Este tipo de ataques son efectivos contra protocolos altamente interactivos como VoIP.

8.7 Atasco:

Los ataques por atasco fueron presentados con el hecho de que una conexión a través de *n* routers tiene un efecto en las otras conexiones a través de ese mismo Router. El usuario atacante tiene que controlar un Router Tor y ser capaz de observar una conexión intermedia entre la salida del Router y el destino final. Mediante el Router Tor, el atacante, puede crear circuitos en todos los demás routers Tor uno por uno para comprobar la latencia de la conexión si incrementa o no. En el momento que encuentre un Router que sí que lo aumente, entonces ese Router está en el circuito. Es un tipo de ataque que se probó hace tiempo y funcionó, pero actualmente el número de nodos es muy superior y se considera como un ataque no viable.

8.8 Round-Trip Travel Time:

Es un tipo de ataque que depende del tiempo de ida y vuelta de los clientes a los servidores.

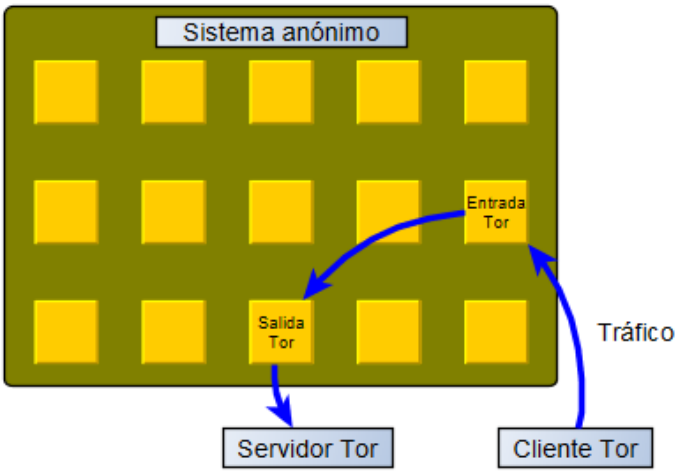
Primeramente, el atacante está en control de los servidores que están recibiendo conexiones del mismo Router de salida. Su objetivo es determinar si las conexiones vienen del mismo circuito.

Utiliza métodos como: forzar al navegador del usuario a descargar miles de pequeñas imágenes secuencialmente, redirecciones HTTP en el navegador del usuario o el uso de un protocolo interactivo como el IRC. Con estos métodos los servidores obtienen gran número de datos del tiempo de ida y vuelta del usuario analizado. Se comparan las frecuencias, y si es similar, entonces las conexiones probablemente sean del mismo circuito.

8.9 Ataque RAPTOR:

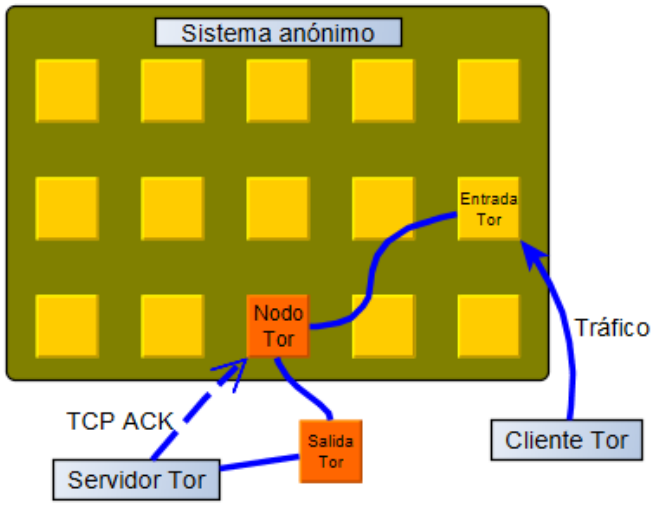
Este tipo de ataques se basan principalmente en tomar el control de un nodo autónomo de la red y aplicar ciertas técnicas de manera que las conexiones y el tráfico de todos los usuarios que se conecten a esta red distribuida a través de este nodo se vean comprometidas, pudiendo obtener la identidad del usuario emisor, así como el contenido de los paquetes enviados. Se podrían encontrar cuatro situaciones diferentes:

- Primer escenario: se aprovecha la escala que hay en el circuito y el hecho de tener acceso al tráfico de datos que se envía desde el cliente al nodo de entrada y desde el nodo de salida al servidor Tor. Se trata de ver las direcciones IP de las conexiones y no el contenido de la conexión.



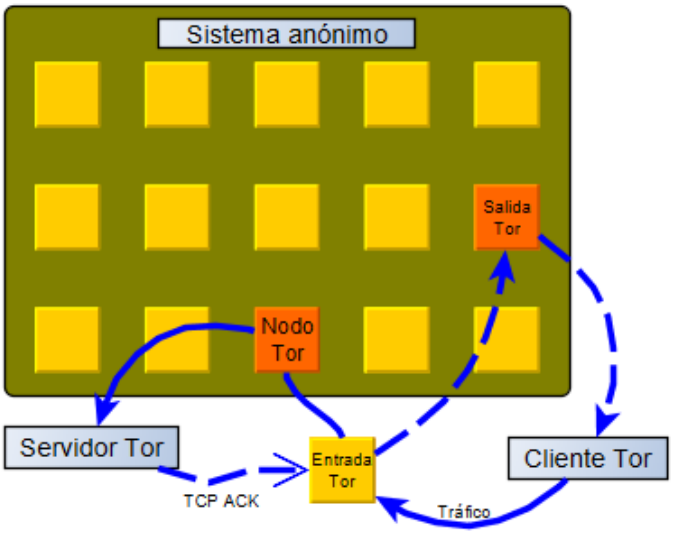
Primer escenario. Tráfico de entrada y salida de los nodos

- Segundo escenario: se consigue romper el anonimato de la conexión al acceder al tráfico de entrada del cliente y a las respuestas TCP ACK enviadas desde el servidor web. De esta manera se va a poder obtener la ruta completa del tráfico e identificar al emisor del tráfico y el contenido de los paquetes.



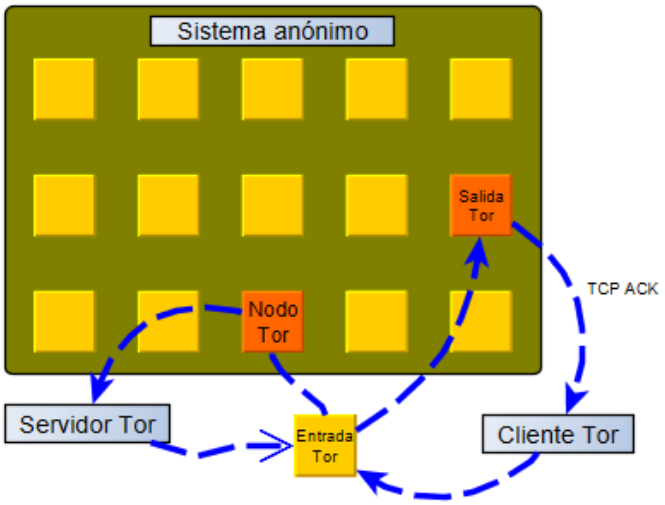
Segundo escenario. Tráfico de la conexión de entrada y las repuestas TCP ACK

- Tercer escenario: Se puede identificar el nodo de salida monitorizando todo el tráfico desde el nodo malicioso y controlando el tráfico que va desde él al servidor de destino, con los paquetes ACK, teniendo bajo control todos los mensajes enviados entre el cliente y el servidor, pudiendo romper así por completo el anonimato de todo el tráfico de la víctima.



Tercer escenario. Se accede a los datos de la conexión de salida y las respuestas TCP ACK al cliente

- Cuarto escenario: se basa solamente en tráfico TCP ACK, permitiendo que se puede acceder a las direcciones IP tanto del servidor como del cliente solo correlacionando los mensajes de *acknowledge* de la comunicación TCP.



Cuarto escenario. Se accede sólo al tráfico de las respuestas TCP ACK

La red Tor, además de los ataques analizados anteriormente, también se expone a dos problemas principalmente:

- Censura gubernamental de carácter mundial: la red Tor puede ser bloqueada de manera sencilla por parte de un Gobierno mediante:
    - Obligar a los ISP a bloquear todos los nodos Tor con la amenaza de no dejarles trabajar en ese país.
    - Los ISP tendrían que bloquear la lista pública de las IPs de los nodos, así impedirían el funcionamiento de Tor.
    - Realización de una potente inspección de paquetes.

  Tor cuenta con herramientas que le podrían evitar, en parte, estas censuras, son los bridges y los Pluggable Trasnports. Los bridges convencionales y los compatibles con Pluggable Transports no podrían absorber el tráfico que se produciría si la censura de nodos es mundial.

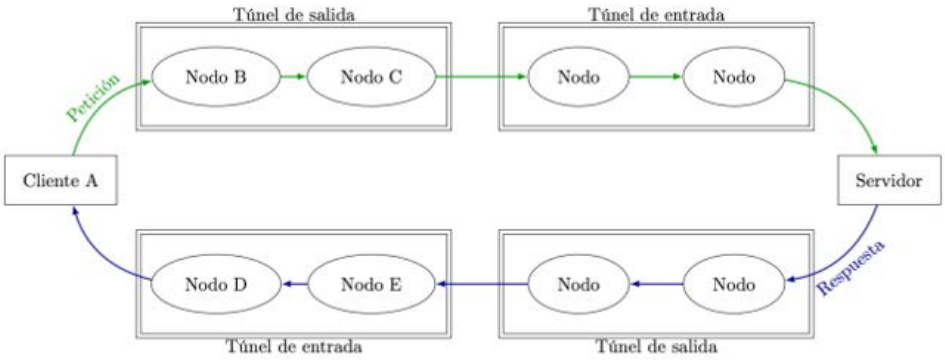
- Bloqueo de nodos de salida por parte de webmasters. Si los sitios web convencionales comenzaran a bloquear conexiones de los nodos de salida, por alguna razón, esto haría que los usuarios no tuvieran acceso a la red Tor.

Tor no tiene como objetivo evitar bloqueos de IPs ya que no oculta el listado de nodos, su estrategia es concienciar a cerca de la importancia de la privacidad y el anonimato en internet.

9 I2P, el Internet invisible

I2P "Invisible Internet Project" es un tipo de red diseñada de forma específica para proteger la información que se transmite por ella, al igual que Tor. Es un protocolo muy parecido al de Tor, aunque tiene sus diferencias:

- El enrutamiento cifra múltiples mensajes juntos para hacer el análisis del tráfico más difícil, al mismo tiempo que aumentar la velocidad de tráfico de red.
- Cada mensaje cifrado tiene su propia instrucción de entrega específica y cada punto final funciona como un identificador de cifrado.
- I2P tiene muchos servicios ocultos y más rápidos que los equivalentes en Tor.
- Funciona junto a la conexión de Internet normal, cifra el tráfico del navegador del equipo. I2P sólo cifra los datos enviados y recibidos a través de un navegador configurado, no cifra actividad de la red para todo el sistema.
- Se usan túneles unidireccionales de salida y entrada (dos nodos en cada uno). El cliente y el servidor construyen su propio túnel, se necesitan dos túneles (entrada y salida) para enviar la información y otros dos para recibirla. Dentro de cada túnel la información se organiza mediante un protocolo de enrutamiento cebolla. Cada mensaje se envía por un túnel paralelo.



Estructura de la Red I2P

I2P añade una capa de seguridad extra, a mayores que Tor, lo que hará más complicado analizar la información teniendo que emplear el doble de tiempo o el análisis del doble de nodos. Su utilización es similar a Tor ya que solamente es necesario la instalación de su cliente.

10 MERCADOS OCULTOS (NEGROS)

El “mercado negro” es aquel en el que se intercambian bienes y servicios cuya procedencia o distribución es ilegal. La prohibición de ciertos productos hace que las personas que los demanden necesiten acceder a este tipo de mercados para conseguirlos.

Los mercados negros varían según los países y sus componentes intentan esconder sus acciones del gobierno, por lo que el tamaño de estos mercados es difícil de calcular. Algunos de los bienes y servicios más habituales que se ofrecen en este tipo de merados son: drogas, armas, medicamentos, órganos, prostitución, divisas…

Los problemas de los mercados negros vienen cuando un consumidor es estafado y este no va a poder reclamar ante la justicia ya que su acción es ilegal. Los riesgos principales con los que cuentan este tipo de mercados son:

- El producto adquirido puede ser peligroso para el consumidor, ya que no existen controles legales sobre los productos que suministran en estos mercados, especialmente medicamentos y drogas. Puede que estos productos supongan un riesgo para la salud.
- El producto adquirido puede ser utilizado para actividades ilegales, como es el caso de las armas. No existe un registro de los propietarios de estos artículos adquiridos en el mercado negro lo que provoca que a la hora de prevenir e investigar delitos no se tenga parte de la información.
- Los productos suelen ser más altos ya que es una actividad ilegal y el vendedor está expuesto a importantes riesgos.
- Aumenta el riesgo de violencia al surgir cualquier problema y el cliente no pueda solucionarlo mediante la justicia, lo cual puede provocar un enfrentamiento.

En la Deep Web existen varios mercados negros en los que se realiza la venta de productos ilícitos por Internet. Estos mercados son accesibles a cualquier usuario que tenga un buscador para navegar por la Deep Web (Tor) y Bitcoins que son las criptomonedas que pueden comprarse de forma sencilla para realizar transacciones de forma anónima.

Las páginas que alojan estos mercados son similares a las que nos podemos encontrar en Internet tipo e-commerce donde se venden productos legales.

Muchos de ellos han sido cerrados por las autoridades, por los propietarios o han cambiado su ubicación. Tras los cierres de un sitio web de estas características rápidamente aparecen otras páginas para cubrir ese mercado.

Algunos ejemplos de mercados negros que fueron desarticulados en la Deep Web:

10.1 Silk Road

Fue el primer gran mercado de compraventa de narcóticos a través de la web profunda. Aquí se podían encontrar armas, drogas, números de tarjetas de crédito robadas, cuentas de PayPal, …

Silk Road llegó a contar con un sistema de puntuaciones en el que se evaluaba el producto que vendían, e incluso hacían llegar muestras de narcóticos a catadores para intentar recibir mejores críticas del producto en venta.

En Octubre 2013 fue clausurada por el FBI y su creador Ross Ulbritch fue condenado a cadena perpetua. Silk Road, ahora tiene su mercado en I2P que tiene mejor seguridad que Tor.

10.2 AlphaBay y Hansa

Alpha Bay se encargaba del comercio electrónico de un sinfín de productos ilegales como drogas, armas de todo tipo, datos sensibles robados, así como malware para cometer cibercrimen como manuales y herramientas digitales. Era el mayor supermercado de drogas en Deep Web y tenía unos 200.000 usuarios registrados. Esta plataforma cerró el 5 de Julio 2017 y registraba entre 600.000 y 800.000$ diarios en transacciones. Este mercado funcionó desde 2013 coincidiendo con el cierre de Silk Road.

Funcionaba como intermediario (al igual que Hansa) entre compradores y vendedores que cobraban una comisión por transacción. Las operaciones de compra se realizaban con criptodivisas, la más común es el bitcoin.

Su creador fue descubierto por el simple error de utilizar su correo electrónico personal para enviar emails de bienvenida a los nuevos miembros de su sitio web, dirección que lo vinculó con sus redes sociales y de esta manera su identidad y localización.

Hansa era el tercer mercado más grande y llevaba intervenido desde el 20 de Junio 2017 por los agentes holandeses, aunque continuaba operativo.

Con la caída de Alpha Bay muchos clientes se dirigieron a Hansa, pasando de ser 2000 usuarios a 8000 en pocos días. No sabían que se estaba monitorizando esta web, desde las autoridades holandesas, tanto a compradores como vendedores. Hansa fue apagado el 20 de Junio de 2017 tras haber recogido información de perfiles de usuarios que utilizaban estos mercados.

10.3 Agora

Agora fue un mercado que convivió con Silk Road hasta el punto de llegar a eclipsarle antes de que fuera cerrado. Fue un mercado en el que se ofrecían prácticamente los mismos productos que en Silk Road, hasta incluso encargar asesinatos. Tras tener sospechas razonables de actividad policial en sus servidores, Agora, se decidió suspender la actividad.

10.4 Evolution y Sheep

Tras el cierre de Silk Road, Evolution se hizo también hueco en la Deep Web ofreciendo prácticamente los mismos servicios además de un sistema de intercambio de mercancía con fideicomiso. Los administradores huyeron con todo el dinero almacenado en dicho fideicomiso.

En el caso de Sheep también su administrador desapareció con unos 40 millones de dólares (39.918 bitcoins). No era más que una estafa e incluso moderadores de los foros perdieron su dinero.

Otros mercados que también fueron cerrados:

- **Evolution**: el más grande mercado negro de drogas en internet, operaba en Tor y cerró fraudulentamente con millones de dólares en bitcoins.
- **Liberty Reserve:** dedicado al negocio financiero ilegal y cerrado en 2013.
- **Darkode**: venta de servicios hacking, datos de tarjetas de crédito, correo basura… se creó en 2007 y cerrado en julio 2015. Posteriormente reapareció en Tor con mejores controles de seguridad.
- **PedoBook**: dedicado a pornografía infantil ocultado en Tor. Fue cerrado en Diciembre 2012 tras estar varios meses monitorizando desde los servidores a los usuarios que visitaban la página.
- **PlayPen**: ocultado en la red Tor era la mayor web de pornografía infantil. Cerrado en febrero 2015 y mantenido abierto hasta marzo por las autoridades para identificar a 1300 visitantes.
- **Dark Marke*t***: venta de información de tarjetas de crédito, contraseñas robadas, etc. Fue clausurado en 2008

11 CRIPTOMONEDAS

Las criptomonedas o criptodivisas es un método de pago digital usado en los mercados ocultos. La primera criptomoneda que comenzó a usarse fue el Bitcoin, que apareció en 2009 pero después aparecieron otras como Litecoin, Ethereum, Ripple o Dogecoin.

11.1 Bitcoin

Bitcoin es una moneda digital, creada en 2009 bajo el alias de Satoshi Nakamoto, con la finalidad de realizar operaciones dentro de la Red y actualmente es la moneda más usada en todo el mundo.

Algunas de las características de esta moneda son:

- No pertenece a ningún Estado o país y puede usarse en todo el mundo.
- Se pueden comprar bitcoins con dólares u otras monedas y viceversa, al igual que sucede con otras monedas.
- No hay intermediarios, las transacciones se realizan directamente de persona a persona: de comprador a vendedor o de particular a particular. Esto reduce el precio de enviar dinero sustancialmente y permite también vender productos y servicios a un precio más justo.
- Es descentralizada, no está controlada por ningún Estado, banco, institución financiera o empresa.
- Es imposible su falsificación o duplicación gracias al sofisticado sistema criptográfico.
- Las transacciones son irreversibles.
- No es necesario desvelar la identidad del usuario a la hora de hacer negocios y se puede preservar su privacidad. No se revela información sensible como números de tarjeta o números de cuenta.
- El dinero pertenece totalmente al usuario y no puede ser intervenido por nadie ni las cuentas pueden ser congeladas.
- Las propiedades de esta moneda permiten a las páginas establecer un servicio de fideicomiso (escrow), asegurando que el vendedor sólo recibirá el dinero si el producto ha llegado satisfactoriamente a su destino.

Este año su cotización se ha alzado considerablemente pasando de los 731,76 dólares en Enero 2017 hasta llegar a rebasar los 11.000 dólares a finales de Noviembre.

11.2 El funcionamiento de la Red Bitcoin

La red Bitcoin está basado en un sistema P2P “Peer to Peer” o de usuario a usuario. El control es realizado por los usuarios, es la propia red generada por los usuarios (miles de equipos de todo el mundo) que se aseguran de efectuar el seguimiento, control y registro de las transacciones.

La tecnología blockchain está detrás del bitcoin y actúa al mismo tiempo como base de datos y copia de seguirdad del sistema. En una transacción de un sistema financiero tradicional se confía en una tercera persona (banco, tarjeta de crédito, Paypal,…) que es la que da la validez al proceso, en cambio, con esta tecnología de bloques son los propios usuarios quienes realizan esta tarea.

Blockchain es como un gran libro de acontecimientos digitales compartido y distribuido entre muchos equipos, que solamente podrá actualizarse cuando hay consenso de la mayoría de usuarios.

No existe un banco virtual ni físico que respalde esta moneda, solamente existe una red de ordenadores descentralizada que se encarga de su minería y de verificación de operaciones. Al comprar algo con un Bitcoin lo que hace el software es entregar la cantidad a esa red de ordenadores y ésta te verifica la operación. El proceso de verificación lo que hace es indicar que una cuenta tiene una cantidad de Bitcoins y cuando se aprueba la operación se disminuye el número de Bitcoins en la cuenta correspondiente. Se entrega la cantidad a la red y ésta es la que da el OK a la operación, siendo la red la que verifica la transacción y certifica la operación.

Mediante un complejo sistema criptográfico es posible asegurarse de que nadie realice una estafa y que la moneda es segura ante ataques, intentos de duplicación o falsificación. El proceso de recibir o enviar Bitcoins es sencillo y seguro.

Para que el sistema sea fiable existe una tecnología llamada Blockchain o cadena de bloques que, entre otras cosas previene el doble gasto de la moneda, es decir, que alguien pueda gastar de nuevo un mismo bitcoin.

La producción y el valor se basa en la ley de la oferta y la demanda. Se tiene fijado un límite de 21 millones de monedas, que se alcanzará en 2030.

11.3 Valor de Bitcoin

El valor del Bitcoin se basa en la oferta y la demanda y se calcula mediante un algoritmo que mide la cantidad de movimientos y transacciones con Bitcoin en tiempo real. El Bitcoin está catalogado como la moneda más inestable del mercado de divisas.

Este es el valor del Bitcoin en los últimos meses:

La cotización va cambiando, llegando a ser muy fluctuante con subidas y bajadas constantemente.

11.4 Conseguir Bitcoins

La forma de conseguir Bitcoins es básicamente mediante la compra de ellos, la venta de algún artículo en la que se reciban en forma de pago o minando Bitcoins.

11.4.1 Minar Bitcoins

Es una tarea realizada mediante la utilización de potentes equipos informáticos para resolver problemas matemáticos y actuando, a la vez, como guardianes de la seguridad de la moneda.

Las transacciones de envío de dinero, pago, cambio o cobro no serán válidas hasta que se apruebe por la red P2P de Bitcoin, que está compuesta por usuarios y mineros. Cada transacción se agrupa en un bloque que debe sellarse. Es un proceso que requiere complejos cálculos matemáticos, lo cual necesita de mucha potencia de procesamiento. Esta tarea es realizada por los mineros que como recompensa por prestar sus equipos para el procesamiento, la red Bitcoin libera bloques con nuevos bitcoin por los que compiten los mineros.

Para minar bitcoins es necesario un equipo potente y con un software especializado en esta tarea que es el que se encarga de minar. Cuanto mayor potencia de procesamiento menor tiempo en conseguir Bitcoin.

11.4.2 Comprar Bitcoins

Otra manera de conseguir Bitcoins es invertir en monedas virtuales. Para la compra de bitcoins solamente es necesario ir a una plataforma de tradings de bitcoins.

Estas plataformas son los monederos de bitcoins y es el lugar donde se almacenan las monedas virtuales. Existen diferentes tipos de carteras de bitcoins.

11.5 Almacenamiento de Bitcoin:

En Bitcoin se utiliza una dirección de Bitcoin para asociar un saldo a un único usuario, además también cuenta con un identificador de usuario y contraseña (clave privada) que va asociada matemáticamente a la dirección Bitcoin.

La dirección Bitcoin es donde el usuario puede recibir pagos y donde podrá administrarlos mediante el acceso con la contraseña. Las claves privadas se almacenan en programas que actúan como monederos.

Blockchain (cadena de bloques) es un libro de cuentas donde se asocian loa identificadores de los usuarios a los saldos. Los monederos de Bitcoin no almacenan los bitcoins en sí, sino las claves privadas que dan autorización al usuario a realizar operaciones sobre las direcciones bitcoin a las que se asocian. El usuario lo que posee son las claves privadas que gestionan las direcciones que tienen atribuidas una cantidad de bitcoins en la cadena de bloques.

En la cadena de bloques se registra y confirma los cambios de propiedad de las cantidades correspondientes entre diferentes direcciones, lo que son las alteraciones del balance.

Un monedero es un software que simplemente almacenan claves privadas, donde además el usuario puede ver en modo gráfico el estado de sus direcciones asociadas, enviar bitcoins, ….

Existen dos tipos de clientes, en caso de los monederos software:

- Clientes completos (Full Client): descargan toda la cadena de bloques (90 GB). Convierten al usuario en un nodo de la red. Estos clientes pueden revelar la IP del usuario en algunas transacciones.
- Clientes ligeros (Lightweight Clients): almacena las claves privadas de manera local pero no la cadena de bloques, accediendo a estas a través de servidores de terceros, el cual sí que es un nodo con la Blockchain descargada y actualizada. Con estos clientes la IP del usuario queda protegida y es la del servidor tercero la que puede quedar publicada.

Los tipos de monedero que hay actualmente son:

- Ordenador: programas que se instalan en el equipo y permiten controlar el monedero ya que almacena las claves privadas de manera local. Hay algunos que

funcionan como extensiones del navegador. Ejemplos de este tipo de monederos:

  - Bitcoin Core (Full Client)
  - Multibit (Light client)
  - Electrum (Light client)

- Web: es el método más usado y fácil de crear. Es accesible mediante el navegador y las claves se almacenan en los servidores del proveedor. Funciona como un cliente de correo electrónico, pero este tipo de monederos son los más inseguros. Un tercero es el que almacena las claves privadas del usuario. Algún monedero web:

  - Coinbase
  - Blockchain.info
  - Green Address

- Smartphone: programas de clientes ligeros que se almacenan en el teléfono. Suelen utilizar un sistema de verificación de pagos simplificado (SPV) que descarga una pequeña parte de la cadena de bloques y confía en otros nodos de la red para comprobar que la información es real. Algunos ejemplos:

  - Mycelium
  - Bread Wallet
  - Copay

- Hardware: hay dos tipos:

  - Con funcionalidades operativas:

  - Almacenadores seguros de claves privadas: dispositivos físicos que pueden almacenar las claves privadas y hacer operaciones de firmado usando el puerto USB o mediante el OTG del teléfono. Cuando el usuario desde el monedero del ordenador, desde el teléfono o vía web quiera hacer un pago se realizará la transacción mediante el puerto USB/OTG al dispositivo para que la firme. Cuando es firmada se devuelve al software para enviarse a la red Bitcoin.

Son aplicaciones de pago. Alguna de este tipo es Trezor o KeepKey.

El mercado de las carteras de bitcoins es amplio y tipo que escoger dependerá del uso que quieras hacer y la cantidad de bitcoins que se quiera invertir. Los monederos virtuales son indicados para pequeñas cantidades ya que son más rápidos, pero no son recomendables para grandes cantidades. Es imprescindible guardar la clave privada que nos darán ya que será necesaria para recuperar los bitcoins.

11.6 Monederos SPV (Simplified Payment Verification)

Son monederos intermedios entre el cliente ligero y el pesado ya que ocupan poco, pero realizan una verificación criptográfica de los datos recibidos para evitar mostrar información falsa al usuario en caso de un ataque en el servidor.

Este tipo de monederos realizan la descarga de una copia completa de las cabeceras de todos los bloques disponibles en la cadena de bloques y así saber si una transacción pertenece a un bloque de cadena sin tener descargado completo la cadena de bloque. Contiene la información necesaria para no depender de un tercero en una transacción.

El proceso de validación cuenta con tres pasos:

1. Cada transacción tiene un hash
2. Cada bloque tiene un hash
3. El hash de una transacción y el de un bloque pueden relacionarse mediante una prueba de Merkle tree (modelo matemático dónde el bloque es la cúspide y la transacción se colocaría en una estructura similar a un árbol).

Con la prueba del Merkle tree obtenemos una lista de todos los hashes entre el bloque y la transacción. Lo más importante de esta verificación es que tan sólo necesitamos una pequeña parte del bloque para probar que la transacción en concreto está en él. Por lo tanto y antes de confiar en una transacción, las SPV wallets siempre verifican:

- Realizan la prueba Merkel tree para comprobar la existencia de una transacción en un bloque
- Verifican el bloque para validar que se encuentra en la cadena principal.

Una vez ambas respondan satisfactoriamente, estamos hablando de una transacción correcta y será añadida en nuestro monedero en forma de ingreso o gasto. BitCoinJ (Hive, Multibit, Schildbach wallet, biteasy…), picocoin con su librería libccoin y Electrum son algunos ejemplos de implementación de este modo.

11.7 Impuestos sobre bitcoins

La inversión en bitcoins no está exenta de pago de impuestos por lo que hay que añadirlo en la declaración de la renta y en el impuesto sobre el Patrimonio.

A partir de 2017 si se ha realizado una compra de bitcoins es necesario incluirlo en la renta 2017 en el apartado de ganancias o pérdidas patrimoniales indicando el resultado de la operación (positivo o negativo en caso de ganancia o pérdida). Los tipos de ahorro del IRPF 2017 son:

- Ganancias inferiores a 6000€ -- 19%
- Ganancias entre 6000€ y 50000€ -- 21%
- Ganancias superiores a 50000€ -- 23%

Mientras el usuario tenga bitcoins en su Bitcoin Wallet no tendrá que declararlos en la Renta, pero sí que tendrá que hacerlo en el Impuesto sobre el Patrimonio al igual que ocurre con las acciones, fondos de inversión y demás ahorros.

11.8 Criptomonedas alternativas al Bitcoin:

Tras el auge de Bitcoin, surgieron numerosas criptodivisas alternativas basadas en los conceptos del protocolo original de Bitcoin. La mayoría de ellas se basan en cambiar algunos de los parámetros de diseño de Bitcoin (parámetros por defecto) y utilizar el código base del cliente Bitcoin para generar y validar transacciones. Algunas de estas monedas son:

- Ethereum: es una de las criptomonedas que más ha crecido y que tiene un gran potencial como medio de pago y divisa electrónica. Las monedas de la red ethereum se denominan ether. Las transacciones de esta red son más rápidas, de apenas 15 segundos y según las técnicas de encriptación que utiliza se pueden minar ether con un ordenador normal.
- Litecoin: surgió en 2011 con un límite de 84 millones de monedas. Se creó a partir de una mejora del Bitcoin y lo hizo en tiempo de generación de bloques para grandes transacciones. Utiliza un algoritmo de minado diferente y que no está al alcance de un ordenador al uso.
- Dash o Darkcoin: se caracteriza por el anonimato de sus transacciones ya que elimina, dentro de sus posibilidades, el origen de las transacciones.
- Ripple: es la moneda virtual de la banca, por lo que lucha en contra del concepto que subyace en el bitcoin. El Banco Santander UK lo usa en tecnología blockchain en alianza con la start up Ripple. Es uso limitado de los clientes del Banco Santander.
- Algunas otras son: Namecoin, Devcoin, Dogecoin, Terracoin, Megacoin,…

Las características del Bitcoin que suelen ser modificadas por las diferentes criptomonedas alternativas son:

- El algoritmo de hashing SHA-256 de Bitcoin se sustituye por el algoritmo scrypt. La diferencia fundamental entre los dos algoritmos es que la eficiencia de cálculo de SHA-256 es proporcional a la capacidad del procesador (CPU-intensive) mientras que scrypt no depende tanto de la capacidad de cálculo sino en mayor medida de la memoria disponible (RAM-intensive). Al ser la memoria mucho más cara que los procesadores, hace que la tasa de aumento en la potencia de cálculo de las diferentes redes sea más constante y plana.
- El número de hashes iterativos que realizan hasta llegar al resultado final. Bitcoin siempre aplica dos veces la función de hash para aumentar la seguridad y disminuir

la probabilidad de colisión. En otras monedas alternativas, este parámetro puede ser diferente.

- El tiempo de confirmación de una transacción. El tiempo de confirmación para una transacción está relacionado con el tiempo entre dos bloques consecutivos. Existen criptomonedas que definen un tiempo entre bloques de 10 minutos (Freicoin o Namecoin), 2 minutos (Terracoin), 1 minuto (Dogecoin) o 12 segundos (Fastcoin).
- El número máximo de monedas en circulación. Si para Bitcoin el número máximo de monedas en circulación es de 21 millones, para otras monedas alternativas este valor puede ser mayor, menor o incluso no tener límite.
- El número de monedas como recompensa a la generación de un bloque. Al solucionar un bloque, Bitcoin actualmente entrega 25 bitcoins, mientras que otras monedas cambian este parámetro para recompensar con más o menos monedas.
- Reducción de la recompensa a lo largo del tiempo. En Bitcoin, cada 210.000 bloques la recompensa se divide por dos, mientras que en monedas alternativas ambos parámetros varían sustancialmente.
- Número de bloques antes de cambiar el target. El ajuste de la dificultad mediante el cambio del target en Bitcoin se hace cada 2.016 bloques, mientras que en otras monedas este parámetro se ajusta para que sea más rápido, más lento o inexistente.

12 Delitos en Tor

Como ya se ha estado comentando, la red Tor ofrece anonimato a sus usuarios y estos utilizan esta propiedad para realizar acciones ilegales sabiendo lo difícil que es rastrearles. Algunos de los delitos más comunes que ocurren en la red son:

12.1 Tráfico de drogas

Dentro de los market place alojados en Tor se puede encontrar todo tipo de productos, aunque uno de los más solicitados es la droga, siendo para compradores y vendedores el lugar idóneo para realizar sus actividades. Se ofrece gran cantidad de sustancias y estupefacientes ilegales clasificados incluso por categorías.

En este tipo de portales también se ofrecen medicamentos como “oxidocona” o “xanax”, además de herramientas y utensilios para la fabricación de drogas.

Silk Road, indicado anteriormente, fue cerrado en 2013 en su versión 2.0 y fue el mercado más popular, aunque ha resurgido este año con su versión 3.0.

Son mercados que están en continua aparición y desaparición, pero hay repositorios de sitios web que se actualizan con las nuevas direcciones de estas páginas. Algunas webs requieren de invitación para poder acceder y realizar transacciones, teniendo así más control sobre las acciones y quien las realizan.

12.2 Pedofilia y pornografía infantil

Internet se ha convertido en un lugar de fácil y rápido acceso a este tipo de contenido, especialmente en la darknet debido al carácter anónimo que tienen los usuarios. En ella se encuentran criminales de todo el mundo con contenido listo para ser difundido bajo seudónimos.

12.3 Venta ilegal de armas

Muchos de los market de venta y tráfico de drogas cuentan también con este tipo de actividad. En la darknet se pueden encontrar compradores y vendedores de una gran cantidad de armas ilegales, desde pistolas, granadas, fusiles o impresoras 3D para la fabricación de armas.

12.4 Sicarios

Los sicarios ofrecen sus servicios también en esta red. Dependiendo del servicio a realizar estos aplicarán una tarifa u otra. Algunos de los factores que influyen son el país

de residencia tanto del objetivo como del sicario, importancia del objetivo, desplazamientos que hay que realizar, tiempo de realización, edad, etc.

Algunos tienen sus excepciones a la hora de la realización de estos "trabajos", como no matar a menores o cargos importantes. También ofrecen una demostración gráfica del objetivo cumplido con un sobre coste. Hay bastantes ofertas falsas de esta actividad, aunque tampoco es difícil conseguirlo.

12.5 Falsificación de documentos

Se pueden conseguir pasaportes falsos en la darknet de manera fácil, aunque no a un precio barato dependiendo del país del que se quiera el pasaporte. También puede influir en el precio el tipo de falsificación ya que el país para el que se emite puede tener mejores o peores técnicas de comprobación de su autenticidad. Además de pasaportes se pueden encontrar carnets de conducir o incluso falsificaciones de dinero.

12.6 Extorsión y localización

Uno de los servicios ofrecidos en la red es la localización de personas mediante el teléfono móvil o a través de otros medios que desvelen su ubicación.

Esta actividad puede tener finalidades diversas y pueden ser desde la localización de un familiar desaparecido hasta localización de una persona para un posible acoso o ser víctima de un ataque.

La acción de utilizar Internet u otra tecnología para la localización, persecución o amenazar a una persona se llama "cyberstalking", y gracias al anonimato de la darknet alojan ahí sus actividades sin temor a ser descubiertos.

También se realizan otro tipo de acosos como es el cyberbullying, siendo uno de los tipos más comunes de agresiones entre menores. Otros fenómenos con menores también suceden, como es online grooming, en el que pederastas y pedófilos contactan con sus víctimas a través de falsos usuarios consiguiendo su confianza. Una vez que consiguen su confianza se hacen con material digital de las víctimas que ellas mismas les envían. Posteriormente son chantajeadas amenazándolas con difundir el material, y así conseguir algunas peticiones que les proponen. Estas técnicas también son utilizadas fuera de la darknet ya que las víctimas no suelen tener conocimientos informáticos amplios y no acceden a esta red.

12.7 Terrorismo

Aquí se congregan grupos terroristas (yihadistas) para realizar comunicaciones con sus militares. Hay sitios dedicados a la divulgación de la ideología yihadista, incluso

incitando al alistamiento en el ejército de la guerra santa, recaudación de fondos (bitcoins) o explicaciones para el proceso de compra de armas.

Los grupos terroristas poseen webs en Internet con contenidos sin importancia, aunque sus auténticas páginas para reclutar se encuentran en la Darknet y de esta manera intentar despistar a las autoridades de sus actos ilícitos.

12.8 Hacktivismo

Los denominados hackers crean grupos (por ejemplo, Anonymous) para operar y se alojan dentro de este tipo de redes. Su filosofía es siempre hacer el bien o lo correcto según su moral, aunque no siempre lo correcto es legal.

Las comunicaciones entre los grupos de hackers suelen realizarse mediante foros con acceso restringido mediante invitaciones.

12.9 Malware

Son programas maliciosos que se instalan en los equipos de las víctimas sin que estas den su consentimiento. Cualquier dispositivo con conexión a Internet puede ser objetivo de este tipo de ataques.

Uno de los principales problemas de esto es que, aunque el tráfico generado por el software malicioso, desde el equipo de la víctima, sea interceptado por las autoridades es muy difícil rastrear o descubrir al ciberdelincuente.

Ransomware es un malware muy utilizado en estos últimos años. Su función es infectar un PC pudiendo bloquearle remotamente o encriptar sus archivos. Para volver a recuperar el control el equipo el usuario deberá pagar una cantidad de dinero (moneda virtual).

12.10 Piratería

Con el endurecimiento de las leyes para perseguir las descargas ilegales y piratería en la Web superficial, ahora se alojan en lugares más escondidos de la Darknet. Hay gran cantidad de contenidos disponibles para su descarga ilegal, ya sean libros, películas, música, software o programas de pago.

12.11 Revelación de documentación confidencial

Los grupos de hackers que han realizado robos de información confidencial y posteriormente su revelación a los diferentes gobiernos y empresas han hecho que la darknet sea aún más conocida en estos últimos años.

Uno de los casos más sonados de esto fue Wikileaks, cuando Snowden desveló información secreta a través de periódicos incluyendo datos de programas con las que había trabajado o colaborado. Otro caso fue el del robo de datos a Sony en el que muchos usuarios vieron como la información de sus cuentas de PlaySatation eran publicados en Internet.

13 Aspectos legales

13.1 Legislación en la red Tor

La red Tor se concibe como una amenaza importante para los gobiernos a nivel internacional debido a que es considerado como refugio de la criminalidad. La regulación legal en esta materia determinará la posición de los gobiernos en acciones en Internet, el uso y derecho a la privacidad y el proceso criminal.

El hecho de que Tor reserva el anonimato de sus usuarios beneficia también para la comisión de delitos, aumentando la problemática existente del creciente uso del ciberespacio. Algunos países apoyan desde sus gobiernos a la red, incluso llegando a aportar sugerencias de desarrollo e incluso contribución financiera.

El desconocimiento de los elementos básicos de las amenazas contra las que actúan y la falta de formación de todos los agentes y personal en material tecnológico hace que dificulte la actuación contra estas acciones. La lucha en la red requiere del uso de los mismos medios usados para cometer el delito, por eso la importancia de que los países usen la red Tor para la investigación de la cibercriminalidad, siempre respetando los límites legales y no llegando a vulnerar derechos.

Algunos países (Holanda, Alemania, EEUU, Noruega o Bélgica) han formado a sus policías y FBI en la red Tor para poder realizar investigaciones criminales. Las funciones principales que realizan los cuerpos de seguridad en la red son:

- Vigilancia online: navegación por sitios web y servicios sin dejar rastro.
- Sting Operations: operaciones de picadura, que aprovechando el anonimato realizan operaciones encubiertas.
- Líneas de sugerencias anónimas: la ocultación de identidad garantiza acceso y uso de sitios web por usuarios que temen su identificación.

La aplicación de la Ley frente al uso de la red Tor va a depender mucho de la legislación nacional donde se aplique. El registro de pruebas digitales supone importantes retos desde el punto de vista procesal, incluso algunos sistemas jurídicos pueden cuestionar su fiabilidad ante los tribunales. También se estudia el tratamiento de los datos de carácter personal que se encuentran en las BBDD de los servicios ocultos.

Por lo tanto, se considera a Tor como la herramienta que garantiza libertad virtual y permite eludir la censura y restricciones impuestas en el entorno electrónico. La privacidad es una propiedad que se pretende proteger y garantizar en el entorno cibernético y Tor es una herramienta que lo ofrece. Desde los gobiernos se pretende anteponer la seguridad colectiva y el orden público ante cualquier amenaza, llegando a requerir el desarrollo de herramientas y medidas que resuelvan el conflicto entre la libertad virtual y la seguridad

La comunidad pide tener mayor seguridad y una mayor libertad ya que consideran que el control ejercido supera los límites que garantizan la seguridad buscada. La

consecuencia de esto es que tras continuas regulaciones y leyes algunos sectores y miembros de la sociedad han acudido a medidas como Tor para conseguir el anonimato.

Uno de los problemas a destacar en el ámbito tecnológico se encuentra en el momento que un Estado interviene servidores localizados en un país extranjero, el cual necesita un consentimiento del Estado extranjero de acuerdo con la normativa internacional. Como consecuencia de esto hay importantes problemas legales dificultando la regulación y penalidad.

El castigo a aplicar en caso de intervenir servidores, se rige por la legislación del Estado donde se alojan dichos servidores. Se entiende que no se puede conocer el ámbito de actuación en base a la jurisdicción sobre el territorio donde se tiene competencia, mientras no se conozca el lugar donde están físicamente los servidores, aplicando entonces la legislación del Estado correspondiente.

La legislación en España sí que permite el cifrado en las comunicaciones mantenidas en la red por un usuario según el art.36.1 de la Ley 32/2003, de 3 de noviembre, General de telecomunicaciones, cualquier tipo de información transmitida en redes de carácter electrónico pueden protegerse mediante procedimientos de cifrado.

Una variante de ese artículo comentado anteriormente sería cuando el usuario instalase un nodo Tor, en cuyo momento, se le trataría como un operador al tener el equipo encendido y estar haciendo función de enrutador de tráfico. Estos usuarios deberían cumplir las obligaciones previstas para los operadores.

Las investigaciones podrían estar limitadas por las legislaciones en materia de tratamiento de los datos de carácter personal. La aplicación Tor también requiere aceptación de requisitos y recursos legales, establecidos por el Reglamento de Protección de Datos, para realizar investigaciones.

En el estado español se consideran las direcciones IP como datos de carácter personal. Las actuaciones policiales, como comentábamos anteriormente, pueden descubrir datos personales como es la IP de personas que no tienen que ver con ninguna pesquisa policial produciéndose entonces la vulneración de su privacidad.

En la lucha contra las actividades ilegales en internet (en especial, el tráfico de seres humanos), la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos está desarrollando un rastreador de páginas web al que ha denominado Memex. Su objetivo es indexar y organizar el contenido de millones de páginas de la web profunda, con base en la relación existente entre las páginas, a partir de un tema particular, lo que puede ser aprovechado por militares, gobierno y empresas. La agencia expresa que el propósito de Memex no es vulnerar el anonimato de la red ni acceder a información privada.

Hay múltiples dificultades que tienen que ser tratadas como el desconocimiento del impacto y el alcance producido, dificultad de obtención de pruebas, falta de formación de las autoridades o problemas jurisdiccionales.

14 Conclusión

Tor es un servicio específico que fue desarrollado por el gobierno estadounidense siendo actualmente el servicio de privacidad y seguridad mejor reconocido en internet aportando anonimato a los usuarios y servidores que participan en su red. Para conseguir este nivel de anonimidad es necesario crear un circuito complejo entre el cliente y el servidor, aunque no está exento de ataques de otros usuarios. El anonimato en la red, por lo tanto, no es absoluto ya que el tráfico puede ser monitorizado. Cuantos más usuarios formen la red mayor seguridad se obtiene al ofrecer más nodos disponibles de conexión.

Los principales buscadores de Internet tienen todo su contenido indexado llegando a poder analizarlo y conocer el comportamiento de los usuarios en la red. Esto es algo que a la sociedad no le gusta y piden una mayor privacidad en sus acciones, lo que provoca que la red Tor cada vez tenga más asiduos. Tor ofrece al usuario el acceso a la web profunda y a la web superficial con un alto nivel de anonimato. Muchos usuarios no han llegado a conocer o acceder a la Deep Web por miedo o desconocimiento. El usuario común prefiere limitarse a la navegar por la parte más superficial antes de arriesgarse a entrar en esta parte de la web.

Gracias a la existencia de este tipo de redes anónimas ha crecido también la cibercriminalidad ofreciendo en sus portales todo tipo de productos, servicios o elementos ilegales. El método de pago en la red es mediante monedas virtuales difíciles de rastrear, especialmente se utiliza el Bitcoin.

El uso de estas herramientas dificulta el rastreo y conocimiento del origen y destino de la información y de sus posibles consecuencias. Se intenta buscar, a nivel internacional, alguna solución para aplicar una cobertura legal a las actuaciones ocurridas en Internet. Las autoridades necesitan infiltrarse en la red Tor, utilizando las mismas herramientas que los criminales, y desde dentro de la misma intentar averiguar delitos. Es necesaria la cooperación entre gobiernos internacionales para poder analizar estas actividades criminales ya que muchas de ellas suceden en distintas regiones del mundo.

El intento de acabar con el anonimato e identificar al criminal de los actos conlleva un desafío entre los límites de lo público y lo privado de los usuarios. El derecho tiene que decidir entre la vulneración de los derechos fundamentales de libertad de expresión y derecho de la información o la intromisión a los datos sensibles del usuario, pudiendo suponer una violación del derecho a la intimidad.

No se debe tener un concepto de Internet como un medio de propagación del crimen, sino como un método de comunicación, ágil para realizar trámites, facilidad de conexiones intergubernamentales, traspaso de información y conocimientos actualizados instantáneamente e incluso la formación de la sociedad.

15 Bibliografía

Agudo, S. (s.f.). *Mercado negro en Internet: auge y caída de los grandes de Tor.* http://www.malavida.com/es/analisis/mercado-negro-en-internet-auge-y-caida-de-los-grandes-de-tor-005781#gref.

BIT2ME. (s.f.). *Cómo almacenar bitcoins.* http://blog.bit2me.com/es/como-almacenar-bitcoins/.

Castillo, P. (s.f.). *Servicios ocultos en Tor, ¿cómo consiguen pasar desapercibidos? .* https://securityinside.info/servicios-ocultos-en-tor-como-pasan-desapercibidos/.

Castillo, P. (s.f.). *Vulnerabilidades en Tor ponen en peligro el anonimato en los servicios ocultos .* https://securityinside.info/vulnerabilidades-en-tor-anonimato-servicios-ocultos/.

Cebolla, R. (s.f.). *Enfoque en Tor.* https://redescebolla.wordpress.com/2010/02/07/tor/.

CERTSI. (s.f.). *Vulnerabilidad en TOR capaz de revelar la IP de los usuarios.* https://www.certsi.es/alerta-temprana/bitacora-ciberseguridad/vulnerabilidad-tor-capaz-revelar-ip-los-usuarios.

Díaz, J. (s.f.). *Tor, servicios ocultos y desanonimización.* https://www.certsi.es/blog/tor-servicios-ocultos-desanonimizacion.

Dorado, J. G. (s.f.). *La web profunda y sus desafíos legales.* https://www.eltribuno.com/salta/nota/2016-4-3-1-30-0-la-web-profunda-y-sus-desafios-legales.

ESTESO, M. P. (s.f.). *¿QUÉ ES Y CÓMO FUNCIONA LA RED TOR?* https://geekytheory.com/que-es-y-como-funciona-la-red-tor.

FERRI-BENEDETTI, F. (s.f.). *Qué es Tor y cómo funciona.* https://www.softonic.com/articulos/que-es-tor-uso-seguridad-y-alternativas?ex=DSK-309.2 .

García, A. (s.f.). *¿Es CG-NAT el nuevo Tor? La Europol no puede identificar a los delincuentes.* https://www.adslzone.net/2017/10/17/cg-nat-tor-europol/.

Gomez, B. A. (s.f.). *Privacidad y Seguridad en Internet: La Web Oscura (DeepWeb).* http://hackeruna.com/2017/02/02/privacidad-y-seguridad-en-internet-la-web-oscura-deepweb/.

JULIÁN, G. (s.f.). *Cómo espía la NSA a los usuarios de Tor.* https://www.genbeta.com/actualidad/como-espia-la-nsa-a-los-usuarios-de-tor.

Luz, S. D. (s.f.). *Así se puede descubrir tu dirección IP real cuando estás dentro de Tor.* https://www.redeszone.net/2015/06/21/asi-se-puede-descubrir-tu-direccion-ip-real-cuando-estas-dentro-de-tor/.

Merino, M. (s.f.). *¿Qué es y cómo funciona Tor?* http://www.ticbeat.com/seguridad/que-es-y-como-funciona-tor/.

OLLERO, D. J. (s.f.). *Así funciona el mercado de la droga en Internet.* http://www.elmundo.es/tecnologia/2017/07/21/5970fab5268e3e5c3d8b471b.html.

PAGNOTTA, S. (s.f.). *Navegación anónima en Tor: ¿herramienta para cuidadosos o para cibercriminales?* https://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/.

PRESS, E. (s.f.). *Clausuran dos de los mercados negros más importantes de la 'dark web'.* http://www.excelsior.com.mx/hacker/2017/07/21/1177095.

Rodríguez, P. O. (s.f.). *Web profunda, Darknet, Tor.* http://crimina.es/crimipedia/topics/web-profunda-darnet-tor/.

RUS, C. (s.f.). *Los principales mercados de la Dark Web llevan horas offline, y los usuarios se temen lo peor.* https://www.xataka.com/seguridad/los-principales-mercados-de-la-dark-web-llevan-horas-offline-y-los-usuarios-se-temen-lo-peor.

Sánchez, R. A. (s.f.). *Darknet de Tor: ¿Útil para los periodistas? ¿Peligrosa para los Estados?* https://ramonalarconsanchez.com/2017/07/31/darknet-de-tor-util-para-los-periodistas-peligrosa-para-los-estados/#losservocultdetor.

Sánchez, R. A. (s.f.). *Las principales vulnerabilidades de Tor.* https://periodismoactual.com/tecnologia/2017/08/17/las-principales-vulnerabilidades-de-tor/.

Sarabia, D. (s.f.). *Alpha Bay, el mayor supermercado de drogas en Internet ha caído: ¿y ahora qué?* http://www.eldiario.es/cultura/privacidad/Alpha-Bay-supermercado-drogas-Internet_0_668433415.html.

TORPROJECT. (s.f.). *Tor: Overview.* https://www.torproject.org/about/overview.html.en.

UNOCERO. (s.f.). *Dos de los sitios más importantes de mercado negro en la Deep web fueron cerrados por las autoridades.* https://www.unocero.com/noticias/dos-los-sitios-mas-importantes-mercado-negro-la-deep-web-fueron-cerrados-las-autoridades/.

VALLE, M. (s.f.). *GLOBB SECURITY.* http://globbsecurity.com/vulnerabilidades-tor-35381/.