Ecosistema Tor: anonimato para la militancia

En Internet, todo queda grabado. Desde ese inocente “like” a un post hasta las páginas que se visitan, todas las acciones que se realizan no solo quedan registradas en los servidores de los que se hace uso, sino que, además, el usuario queda identificado como el ejecutor de dichas acciones. Ni siquiera es necesario que una o uno se haya registrado con una cuenta o que se esté usando un nombre real. Basta con la dirección IP, la información que ofrece tu navegador, el sistema operativo del dispositivo, el tamaño del monitor o pantalla, el modelo y marca del smartphone o computadora y una larga lista de variables para poder identificar de forma fácil a un usuario de Internet. Si esto ya es preocupante en actividades “cotidianas”, ni que decir hay sobre los problemas que plantea de cara al uso del ciberespacio por parte de las organizaciones revolucionarias.

Por suerte, hay herramientas que ayudan a mitigar el problema del anonimato de manera efectiva, aunque, como siempre, con limitaciones que hay que conocer. Una de estas herramientas es Tor. En líneas generales, Tor ayuda a sus usuarios a ser anónimos en la red de Internet, aunque, como se verá, también requiere de la parte activa del usuario para evitar filtrar su verdadera identidad. Si bien es cierto que seguramente sea una de las más conocidas herramientas relacionadas con la ciberseguridad, generalmente de Tor solo se suele conocer el navegador web, *Tor Browser*, y poco más. Sin embargo, Tor cubre un gran abanico de posibilidades y de herramientas que se han desarrollado para aprovecharlas. Es por ello que en este artículo se hace un repaso de todas estas posibilidades, que ofrece el Ecosistema Tor: una serie de soluciones técnicas muy potentes e indispensables para la militancia revolucionaria.

¿Debería usar una VPN?

Seguramente **no**.

Una *Virtual Private Network* o VPN, simplificando mucho, implica enviar a un servidor todo el tráfico de red que se haya configurado para que pase por la VPN. Por ejemplo, si se ha configurado la computadora con la VPN de NordVPN (la que, por cierto, no recomendamos en absoluto), esto significa que todo el tráfico irá a parar a un servidor de NordVPN y, después, este servidor lo enviará al servidor que estés deseando acceder. Entonces, siendo las cosas así, ¿confías en darle todo el tráfico de red a un servidor de una empresa privada o de otro tipo de organización capaz de rastrearte? Como respondíamos antes, seguramente no, y mucho menos para actividades militantes.

Como mucho, una VPN debería usarse para conseguir productos (entradas, tickets de viaje, etc.) más baratos, para esquivar el bloqueo de una página web en algún país o para acceder a contenido solo disponible en otro países.

Qué es Tor

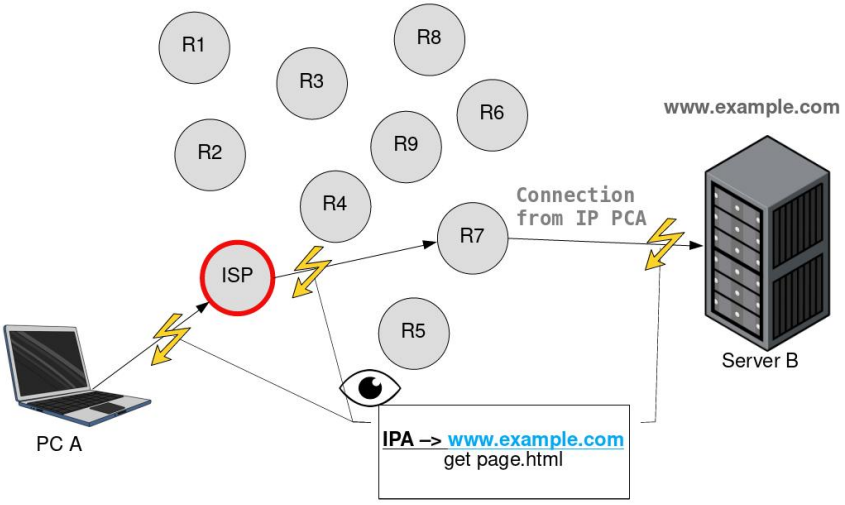
Si se tiene que pensar en Internet, hay que imaginarlo como una gran cantidad de máquinas conectadas unas a otras. Estas máquinas forman redes entre sí e Internet sería la interconexión de estas redes de máquinas. Las máquinas pueden ser de muchos tipos: servidores, computadoras personales, smartphones, tablets, routers, switches, etc. Entre estas máquinas, con fines de simplificación, se diferencian entre máquinas que proveen el servicio de Internet y máquinas finales (*endpoints*) que acceden al servicio. Esto es, una máquina final de un extremo de la conexión se conecta a otra máquina final en el otro extremo a través de las máquinas intermediarias que proveen el servicio a Internet. Éstas últimas suelen ser

routers ofrecidos por los proveedores de Internet (en adelante ISP, *Internet Service Provider*) que se encargan de gestionar el tráfico, es decir, de generar las vías para que la comunicación entre máquinas finales sea posible. Así, por ejemplo, cuando se abre el navegador en la computadora y se conecta a una página web, lo que se está haciendo es pasar por una serie de routers hasta llegar al servidor. En este caso, la computadora y el servidor serían las máquinas finales, y los routers las máquinas intermedias.

Para que esto suceda así, las máquinas necesitan establecer los caminos que van a seguir para llevar información desde un origen a un destino. Para ello, utilizan el protocolo IP (*Internet Protocol*) que, resumidamente, asigna a cada máquina una dirección, de tal modo que las máquinas especifiquen entre ellas adónde quieren enviar la información, como si de una dirección de correo postal se tratara.

Teniendo en cuenta esto, si cada vez que una máquina se conecta a Internet, el resto de máquinas de las que hace uso conocen su dirección IP (sumado a que las direcciones IP llevan asociadas unas coordenadas geográficas), está claro que en Internet nadie es anónimo. Desde el momento en que alguien accede a una determinada página web, tanto el servidor de la página como el ISP saben quién se está conectando y desde dónde se está conectando. Este es el primer problema que presenta Internet de cara al anonimato, pero no el único, como veremos más adelante.

Para superar este problema, en 2002 nació Tor (*The Onion Router*), un software desarrollado para habilitar comunicaciones anónimas. Tor es un protocolo de comunicación que ofrece un servicio de anonimato sobre una red ya existente, habitualmente Internet. Su funcionamiento es bastante simple de explicar. En el siguiente diagrama podemos ver cómo se conecta de normal un usuario de Internet a un servidor (en el ejemplo www.example.com):



En este caso, para acceder al servidor web (Server B), el usuario (con dirección IP del PC A) primero se conecta al ISP (proveedor de Internet) y este se encarga de gestionar la ruta y envío de la información hasta el servidor (www.example.com). Durante toda esta conexión, el ISP conoce la IP del usuario y el servidor al que está accediendo. Por su parte, el servidor (www.example.com) conoce la dirección del usuario (IP PCA). Por tanto, cuando se navega por Internet de forma normal, se está continuamente ofreciendo al ISP y al servidor la identidad (a través de la dirección IP) del usuario que navega. Así, vemos que usando Internet de forma normal, el anonimato es prácticamente inexistente.

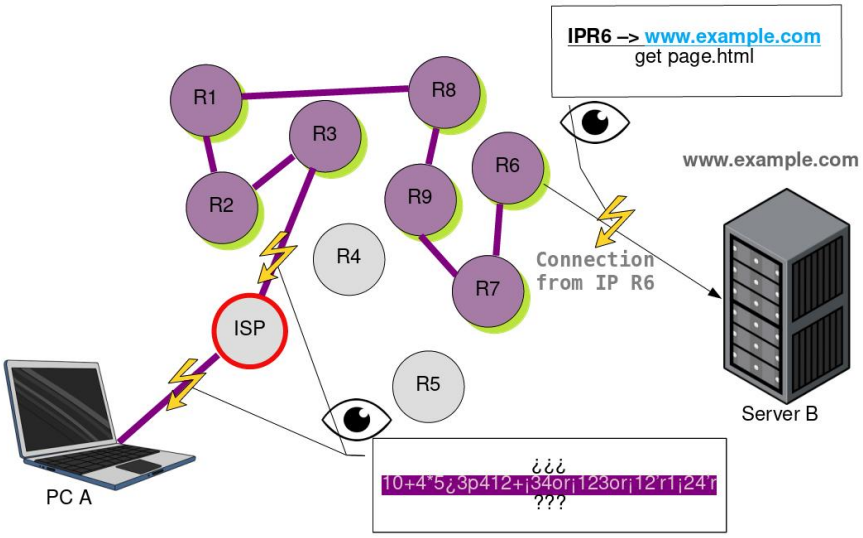
Efectivamente, por un lado, que el ISP sepa qué servidores visitas y con qué frecuencia, es problemático, sobre todo si el contenido de los servidores no le gusta al ISP o al gobierno de turno (porque, sí, los ISP colaboran con las agencias de inteligencia gubernamentales o son obligados a colaborar por orden legal). Además, si la conexión no va cifrada

(por ejemplo, que en vez de HTTPS se use HTTP), le da al ISP acceso a toda la información que intercambias con el servidor, incluídas contraseñas, datos personales y conversaciones. Por ello, siempre es importante utilizar protocolos cifrados como HTTPS, tanto para evitar el posible espionaje del ISP, como el de otros agentes intermedios.

Por otro lado, también es problemático que el servidor que visitas sepa quién eres. Porque si habitualmente visitas cierto tipo de contenido dentro del servidor (por ejemplo, que veas vídeos de determinada temática asociada con lo políticamente radical) tal vez llames la atención de los administradores del servidor o de las agencias gubernamentales.

En resumen, que tanto el ISP como el servidor sepan quién eres y qué visitas, es un problema. Y no tanto por ejemplos tan “inocentes” como ver vídeos de determinado género o consultar páginas web de alguna organización política, sino que pueden saber fácilmente qué dices en Internet (por ejemplo, qué tweets publicas) o, peor aún, que accedes a determinados servicios de correo, artículos privados, inicios de sesión y, en general, que interaccionas con servicios fuertemente relacionados con una organización política. O sea, que fácilmente se puede determinar tu pertenencia a una organización solo por las conexiones que realizas a través de Internet.

En cambio, cuando utilizas un servicio de anonimato como Tor, las cosas son diferentes, debido a que tu conexión rebota por varias máquinas que dan servicio a la red Tor. Estas máquinas se llaman nodos de Tor (*Tor nodes* o *relays*) y funcionan como routers que cifran y reenvían tus peticiones a través de ellos para hacerte anónimo. En el diagrama de abajo, podemos ver cómo funcionaría una conexión a través de Tor:



A diferencia del primer diagrama, ahora observamos cómo primero se conecta al ISP y a través de él a un nodo de entrada (*entry node*) de la red Tor. Este nodo pasa la conexión por varios nodos de Tor elegidos aleatoriamente hasta que uno de ellos, el nodo de salida (*exit node*) de la red, accede al servidor (www.example.com).

Ahora, a diferencia de una conexión de Tor, han cambiado varias cosas. En primer lugar, la IP mediante la que accedes al servidor (www.example.com) no es tu IP (del PC A), sino la IP del nodo de salida (IP de R6). En segundo lugar, ahora, cada nodo de Tor que se atraviesa cifra la conexión con una capa adicional de cifrado; de ahí que se llame *The Onion Router*, porque va añadiendo y quitando capas de cifrado como si fuera una cebolla. Finalmente, a diferencia de lo que mucha gente piensa sobre el funcionamiento de Tor, el ISP ya no conoce qué estamos visitando, sino que

solamente sabe que estamos conectándonos a la red Tor, ya que, como hemos dicho, Tor cifra la conexión.

Entonces, resumiendo, cuando haces uso de Tor, el ISP no sabe qué estás visitando (solo sabe que estás usando Tor) y el servidor sabe qué estás visitando, pero no sabe quién eres, porque la IP de la que dispone es la de un nodo de salida de la red Tor y no tu IP. Y, así, se logra el anonimato que estábamos buscando.

Limitaciones de Tor y responsabilidades del usuario

Si bien Tor es una herramienta técnica que en condiciones ideales funciona bien, es cierto que tiene algunas limitaciones importantes de señalar. Estas se dividen en dos: limitaciones técnicas y limitaciones humanas.

Las limitaciones técnicas son difíciles de evitar por parte de un usuario estándar de Tor y son en gran parte responsabilidad de los desarrolladores de Tor. La principal de estas limitaciones tiene que ver con los nodos de Tor.

La red Tor se sostiene gracias a que hay personas y organizaciones que levantan o activan nodos de Tor. Un nodo de Tor no es más que una máquina (por ejemplo, un portátil, una computadora vieja que no se use, servidores profesionales, etc.) que ejecuta el software de nodo de Tor. Así, hay miles de voluntarios que con una computadora vieja, su portátil u otro tipo de máquinas levantan nodos de Tor para sostener la red. Pero, desde el momento en que esto es así, existe la posibilidad de que actores maliciosos levanten nodos con funcionalidades maliciosas, encaminadas deanonimizar al usuario o a inspeccionar el tráfico de red en busca de información valiosa. Pero, incluso siendo esto así, para la actividad política revolucionaria es mejor usar Tor que no usarlo, ya que, si no se usa, se está renunciando de facto a un anonimato muy beneficioso para dicha actividad. Es decir, es mejor usar una red que cifra el tráfico y lo hace anónimo, con el eventual peligro de toparse con un nodo malicioso, que

usar una red que, directamente, le ofrece toda la información de tus sesiones en Internet al ISP, al servidor que visitas y a las fuerzas represivas del Estado.

Existe otra limitación muy a tener en cuenta que consiste en que hay Estados que censuran el uso de Tor, para evitar que se esquive el control social. A veces esto ocurre en momentos de crisis políticas, aunque también hay Estados que censuran Tor continuamente. Este problema es habitualmente resoluble utilizando puentes o *bridges* que permiten acceder a Tor desde entradas que quedan fuera del alcance del Estado censurador.

En cuanto a las limitaciones humanas, estas son triviales, pero no por ello menos importantes. El ejemplo más claro para ilustrar una limitación humana de cara al uso de Tor sería estar navegando una web a través de Tor y hacerlo habiendo iniciado sesión con una cuenta con nombre y apellidos reales, o con una cuenta que previamente estuviese siendo utilizada sin Tor. El servidor que visites no conocerá la IP real (sino la del nodo de salida), pero sabrá que eres tú. Por ello decimos que la responsabilidad activa del usuario es importante: en todo momento tiene que tomar acciones para no revelar su identidad, pese a estar usando Tor. Estas posibles acciones son muchas y dependen del caso, pero no son difíciles de realizar. Es más una cuestión de sentido común: no usar datos reales, no usar correos que se usan para otras actividades no anónimas, no descargar archivos sospechosos, no dar información personal, no usar siempre los mismos nombres de usuario, etc. La lista es larga, pero fácil de intuir. Lo más importante es tener en cuenta una máxima: Tor te hace anónimo, pero solo si colaboras.

Cúando usar Tor y cúando no usarlo

Es relativamente fácil determinarlo. Si vas a realizar actividades en Internet que no te gustaría que ni el ISP, ni el gobierno ni los servidores que visitas

lo sepan, entonces utiliza Tor. En cambio, si vas a realizar actividades como utilizar una cuenta personal en las redes sociales que no tenga que ver con tu actividad militante o política, acceder a la cuenta del banco, utilizar el correo personal y todo tipo de actividad cotidiana, entonces mejor no usar Tor.

En el ámbito militante, es recomendable, si no necesario, utilizar siempre Tor, desde el acceso al correo de la organización, hasta el uso de servicios relacionados con la organización como una nube propia, un chat, la página web, el blog o las cuentas en redes sociales. El uso de redes de anonimato es indispensable y una necesidad que las organizaciones revolucionarias deben promover, junto con el uso de otras herramientas seguras propuestas por nuestro colectivo, de cara a enfrentar la investigación y persecución políticas.

Sin embargo, hay situaciones en las que es problemático usar Tor. Uno de los mejores ejemplos es el uso de cuentas en las redes sociales. Es bien sabido que, por ejemplo, Twitter o Instagram no permiten crear ni utilizar cuentas desde Tor, al menos de forma sencilla. Existen métodos, y algún día los explicaremos, para crear cuentas en este tipo de redes sociales de forma anónima y superando los obstáculos que ponen al registro y uso anónimo. Pero lo cierto es que hay muchos servicios en Internet que impiden u obstaculizan las conexiones desde Tor. Ahora bien, una vez más, los militantes políticos deben esforzarse por utilizar estas herramientas pese a saber que muchas veces se van a encontrar con dificultades. Si no somos capaces de esforzarnos en tareas tan simples ¿en qué lo seremos?

Ahora bien, existe una consideración importante que no debe olvidarse: cuando se usa Tor, el ISP y, en caso de quererlo, el Estado sabrá que lo estás usando. Esto podría levantar sospechas, pero, y aquí entra el dilema de siempre: ¿qué es mejor, que el Estado sepa que usas Tor y sospeche, pero que no sepa qué estás haciendo o que el Estado pueda saber, directamente, qué estás haciendo?

Herramientas del ecosistema Tor

Tor Browser

El Navegador Tor o *Tor Browser* (en iOS se llama *Onion Browser*) es la herramienta desarrollada por el Proyecto Tor para navegar anónimamente, tanto para espacios alojados en la red Tor (conocida como *Dark Net* o *Dark Web*), como para aquellos alojados en la web clara (*Clear Web*, la web habitual), que protege anonimizando y estableciendo unos ajustes de privacidad que otros buscadores de Internet no llegan a considerar. Los buscadores de Internet como *Google Chrome*, *Firefox*, *Safari*, *Vivaldi*, *Opera*, etc. no llegan a poder acceder a la red de Tor por defecto, exceptuando el caso de *Brave* que da la opción de hacerlo, pero no lo recomendamos por razones entre las que se encuentra la ausencia de protección en el resto de situaciones en el que *Tor Browser* sí protege.

En general, si se realiza una serie de configuraciones, puede utilizarse Tor con cualquier navegador, pero la ventaja principal de Tor Browser es que está configurado para conectarse automáticamente a Tor y que está ajustado para evitar la filtración de datos que puedan identificar al usuario. Entre estas medidas se encuentran:

- El ajuste de tamaño de la pantalla de navegación para evitar que el servidor conozca el tamaño del monitor.
- La desactivación de código Javascript, muy útil para rastrear a los usuarios.
- El uso de HTTPS por defecto, para cifrar las comunicaciones.
- Otros ajustes más técnicos, para evitar el filtrado de información y el *fingerprinting*.

En lo que se refiere a las limitaciones de *Tor Browser*, una de ellas es técnica y está relacionada con la seguridad de Firefox. Se ha criticado en varias ocasiones (1, 2 y 3) la seguridad de *Firefox* y se han puesto sobre la mesa desventajas de este navegador en materia de seguridad frente a *Chrome* (y *Chromium*). Es por ello que creemos, junto a la comunidad de expertos en la materia, que *Tor Browser* debería desarrollarse basado en *Chromium*, ya que este navegador provee mejores características de seguridad.

Sobre las limitaciones humanas, básicamente son las que se han mencionado más arriba. El factor humano es muy importante para preservar el anonimato. Por ello, hay que tener cuidado de no filtrar información personal, pero también de descargar archivos que pudieran comprometer el anonimato y la seguridad del usuario. Por ello, solo hay que descargar archivos en los que se confíe plenamente.

El Navegador Tor es una gran herramienta que debería usarse siempre que se vaya a leer, escribir y consultar contenido web que pudiera comprometer al militante y su organización.

Qué es un *Hidden Service*

Cuando haces uso de Internet de forma normal, utilizas nombres de dominio para conectarte a páginas web o, en general, a servidores. Por ejemplo, un nombre de dominio sería *example.com* y estaría asociado a un servidor web. Entonces, cuando a través del navegador u otro tipo de herramienta te conectas a *example.com*, te estás conectando a una máquina (servidor) con una determinada dirección IP relacionada con dicho nombre de dominio.

Un *Hidden Service* o Servicio Oculto es un servidor accesible desde la red Tor y dispone de una dirección con extensión ".onion" para acceder al mismo. Por ejemplo, la dirección ".onion" actual de la página oficial de Tor

(torproject.org) sería:

2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion

De esta forma, puede accederse a un servicio sin salir de la red Tor, preservando el anonimato del usuario, el anonimato del servidor y el cifrado de la red.

Los servicios ocultos disponen de muchas ventajas:

- A diferencia de los nombres de dominio de la web normal (por ejemplo, torproject.org), un dominio ".onion" es gratuito y no requiere de ningún dato personal para obtenerlo y registrarlo.
- Permiten crear servidores "invisibles", ya que no se revela la IP real del servidor, los nombres de dominio son aleatorios y solo se puede acceder al *Hidden Service* si se conoce su dirección.
- Toda la conexión al *Hidden Service* ocurre dentro de la red Tor, preservando así el cifrado de la red y el anonimato.
- No es necesario abrir los puertos del router ni hacer configuraciones especiales de red para proveer acceso a un *Hidden Service*.

La principal posibilidad que ofrece es la de levantar servidores web, de chat, de videollamadas, de correo, etc. de forma fácil, segura, anónima y resistente a la censura y la persecución política.

Creemos que todos los servicios propios de una organización deberían consistir en *Hidden Services*, es decir, servidores dentro de la red Tor, y, por ello, en un futuro explicaremos cómo activar un *Hidden Service*, de tal forma que las organizaciones revolucionarias puedan generar de forma anónima, segura y gratuita sus propias infraestructuras. Por ahora, sirva esta guía para levantar una página web en la red Tor en un sistema

operativo GNU/Linux. Si bien, normalmente, como sugiere la guía, los *Hidden Services* suelen ser páginas web, no solo se limitan a ello, pues un *Hidden Service* no es más que una dirección asociada a una máquina, con unos puertos abiertos. Bastaría con abrir los puertos asociados al tipo de servicio (chat, conferencia, web, etc.) que se quiera proveer, para poder ser accedido desde la red anónima de Tor.

Orbot y el proxy Tor

Además de utilizarse para navegar la web, hemos dicho que Tor es una red y, como tal, permite anonimizar casi todo tipo de tráfico de red. Esto quiere decir que, por ejemplo, podríamos configurar una aplicación de chat cualquiera (Molly, Signal, Element, Telegram,…) para que pase todo su tráfico por Tor.

Pasar el tráfico de las aplicaciones por Tor solo es recomendable en algunos casos. Por un lado, puede ser que queramos utilizar una cuenta anónima, tanto en el registro como en el uso normal. Este caso solo es posible si no se pide ningún dato personal, como, por ejemplo, el número de teléfono, cuenta del banco, etc. Por otro lado, puede ser que haya servicios en los que ya tengan algún dato personal. Por ejemplo, en Signal hay que introducir el número de teléfono para registrarse. Entonces, en el primer caso, pasar el tráfico por nos Tor haría totalmente anónimos mientras que, en el segundo caso, el de Signal, solo serviría para ocultar al ISP que estamos utilizando Signal o cualquier otro servicio. Para ambos casos, es muy útil pasar el tráfico por Tor.

Sin embargo, para usar servicios como Whatsapp, Instagram o redes sociales en los que se nos puede identificar, no es recomendable pasar el tráfico por Tor y tampoco lo es utilizarlo en servicios en los que vayan a bloquear por usar Tor (por ejemplo, en Instagram).

Para pasar el tráfico de una aplicación por Tor existen diferentes maneras.

En Android, existe la aplicación Orbot, que permite pasar el tráfico de las aplicaciones seleccionadas a través de Tor. Para ello, la mejor opción es seleccionar el modo VPN y luego escoger qué aplicaciones pasar por Tor. Las más recomendables serían las aplicaciones utilizadas para actividades de militancia y aquellas relacionadas con la política capaces de despertar la atención de las fuerzas represivas del Estado.

También existe la posibilidad de activar un proxy para conectar programas a la red Tor en Windows, en MacOS y en Linux. No obstante, si lo único que se desea es navegar, es mejor utilizar únicamente Tor Browser sin configurar ningún proxy o el sistema operativo Tails que estudiaremos más adelante.

Para usuarios de iPhone no existen actualmente aplicaciones que permitan aprovechar características de este tipo.

OnionShare

OnionShare consiste en un programa que nos permite compartir archivos, levantar una página web en la red Tor y chatear de forma anónima. Es una especie de navaja suiza de Tor y, por tanto, muy útil para la militancia.

Como hemos dicho, OnionShare nos permite compartir archivos a través de la red Tor. Esto lo hace levantando un *Hidden Service* temporal, para el que se genera una dirección ".onion" que hay que compartir con quien quieras transferir archivos. Y viceversa, pueden recibirse archivos. Que se haga a través de Tor implica que es una transferencia anónima y cifrada con varias capas, por lo que lo hace, a nuestro juicio, uno de los mejores programas para compartir archivos en el ámbito militante.

También nos permite levantar una página web de forma rápida y fácil en la red Tor. Comunmente esto se conoce como una paǵina de la *Dark Web* y se accedería a ella a través del Navegador Tor, conociendo su dirección

“.onion” asociada. La utilidad de levantar una página web en la red Tor radica en que es resistente a la censura, gratuita y anónima, por lo que animamos a todas las organizaciones a disponer de su página web también en la red Tor.

Finalmente, en las últimas versiones han introducido la capacidad de levantar una web de chat en vivo, de gran utilidad para mantener conversaciones de forma anónima, cifrada y temporal.

Para más información sobre las utilidades de OnionShare y cómo utilizarlas, recomendamos encarecidamente consultar su documentación oficial.

Sistema operativo Tails

Tails es un sistema operativo GNU/Linux configurado por defecto para hacer anónimo al usuario, a través de la red Tor. Sin embargo, Tails dispone de muchas más características que lo hacen indispensable para la militancia revolucionaria. Hagamos un breve repaso por ellas.

Tails está pensado principalmente para ser instalado en una unidad de almacenamiento extraíble (como USB) y ser cargado en una computadora, tanto PC como en Apple Mac. De este modo, sin necesidad de cambiar el sistema operativo habitual de la computadora, Tails se ejecuta en vivo (live), sin instalarse y sin interactuar con el SO original. Y así, se introduce una de las mejores características de Tails: la amnesia. Efectivamente, una vez terminada una sesión en Tails y apagada la computadora, se borra todo lo que se haya hecho durante dicha sesión, de tal forma que no quede rastro de las actividades que se han realizado. Tails, como sistema operativo, no se borrará y podrá inciarse de nuevo, pero sin ningún dato de la anterior sesión.

Si Tails aparece en el ecosistema de Tor es por una razón: todas las

conexiones a Internet dentro de Tails se hacen a través de Tor. Es decir, no solo el navegador por defecto es Tor Browser, sino que, además, todos los programas que se ejecuten en Tails pasarán sus conexiones a través de la red Tor. De este modo, la sesión es anónima y segura. Además, para evitar la filtración de la identidad del usuario por otras vías, Tails viene configurado de tal modo que *dificulta* la identificación incluso si la computadora es comprometida a través de una descarga maliciosa u otro tipo de amenaza.

Añadido a esto, Tails trae consigo una serie de herramientas útiles para la gestión segura de la información, como el gestor de contraseñas KeePassXC, OnionShare para compartir ficheros, herramientas de ofimática como LibreOffice, editores de imágenes y audio, cliente de correo electrónico, algunos sistemas de mensajería instantánea, etc.

En resumen, Tails es una herramienta muy útil para la militancia. En primer lugar, anonimiza todas las conexiones de red que se hagan mientras se use. En segundo lugar, es portátil, se puede llevar en una unidad de almacenamiento externa y no se instala en la computadora, por lo que no afectará al sistema operativo que se use de normal. En tercer lugar, es amnésico, es decir, que una vez se apaga la computadora, en el sistema operativo no se guarda nada de lo que se haya hecho: todos los archivos que no se hayan sacado del sistema operativo a través de Internet o a través de, por ejemplo, una unidad de almacenamiento USB, no se guardarán; en el próximo inicio de sesión, Tails se iniciará como si nada hubiese pasado. Por último, dispone de muchas herramientas para realizar actividades militantes, como abrir archivos cifrados, enviar correos, compartir archivos de forma segura, navegar de forma anónima, redactar artículos y otras muchas posibilidades que no podemos explorar aquí, por cuestiones de brevedad.

Puesto que Tails es relativamente fácil de instalar y muy popular, dejamos un enlace a la guía oficial de instalación y animamos a buscar por Internet tutoriales más detallados de cómo instalarlo y usarlo. Conocemos las

dificultades que puede causar la instalación de Tails, por lo que ofrecemos nuestra ayuda a los colectivos u organizaciones que estuvieran interesados en implementarlo como herramienta de uso militante.

Colectivo 406