UN PASEO POR LA DEEP WEB

Trabajo Fin de Máster - INCIBE

Máster Interuniversitario en Seguridad de las TIC – MISTIC – JUNIO 2018

Autor	Irene Lavín Perrino
Tutor del proyecto	Jorge Chinea López
Profesor responsable asignatura	Víctor García Font

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Un paseo por la Deep Web*
Nombre del autor:	*Irene Lavín Perrino*
Nombre del consultor/a:	Jorge Chinea López
Nombre del PRA:	Víctor García Font
Fecha de entrega (mm/aaaa):	06/2018
Titulación:	*Máster Interuniversitario en Seguridad de las TIC – MISTIC*
Área del Trabajo Final:	*TFM-Ad hoc INCIBE*
Idioma del trabajo:	*Castellano*
Palabras clave	*Deep Web, TOR, cibercrimen*

Resumen del Trabajo:

Se tiene una idea preconcebida, basada muchas veces en lo que dicen los medios de comunicación, sobre lo que es la Deep web, que se relaciona mucho con la ciberdelincuencia, y que no se ajusta mucho a la realidad y para el objetivo que fue diseñada.

Este trabajo final de máster pretende exponer y dar a conocer un poco más y de manera más sincera lo que es realmente la Deep web, explorar y estudiar las diferentes formas de acceso a ella, conocer su estructura, lo que se puede encontrar en la internet profunda y lo que se puede llegar a hacer en las redes existentes. También mencionar las vulnerabilidades y amenazas que existen, los riesgos que puede llegar a tener su uso, así como analizar algunos ataques que se han producido y sus consecuencias.

Abstract:

There is a preconceived idea, often based on what the media say, about what Deep web is, which is very related to cybercrime and that does not fit very well with reality and for the purpose that it was designed.

This master's final work aims to expose and make known a little more and in a sincerely way, what is really the Deep web, explore and study the different forms of access to it, know its structure and what can be done in existing networks. Also, it mentions the vulnerabilities and threats that exist, the risks derivatives from their use, as well as analyze some attacks that have occurred and their consequences.


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Contenido

Índice de ilustraciones

1. Introducción

1.1. Contexto

Este trabajo fin de máster pretende describir la Deep web tal como es, estudiar de manera profunda las características que la conforman, descubrir cuales son los métodos de acceso y probar a instalar y utilizar, el método de acceso más utilizado y popular, Tor, realizando una navegación por la internet profunda para descubrir qué tipo de información y servicios se pueden encontrar y poder realizar una clasificación.

Primero es necesario saber qué es la Deep web. Son los archivos y páginas de internet que no están indexadas por los buscadores. Para *Google, Bing*, etc. Los sitios web que están protegidos por una contraseña, las transacciones realizadas con un banco online, o las series que se ven en *Netflix*, todo ello forma parte de la Deep web. También ocurre con las páginas dinámicas de Internet, cuando se entra en una página de reservas de hotel, por ejemplo, y se realiza una búsqueda de hotel para una fecha concreta, el navegador devuelve una página creada explícitamente para la petición por lo que no se indexa por los buscadores.

Por lo tanto, la Deep web no es algo ilegal. La finalidad de la internet profunda es que los datos considerados como sensibles no estén con acceso público. Este tipo de contenido sensible supone alrededor de 9 de cada 10 contenidos que existen en internet.

Por este motivo, en este trabajo se busca analizar también la Deep web respecto al tema de cibercrimen para desmitificar algunas creencias existentes como que la "*Deep web está hecha por y para criminales"*, que "*la Deep web y la Dark web son lo mismo*" (ver apartado 2.1) o que "*todo lo que hay en la Dark web son drogas y armas*" (ver apartado 2.3 y 4.3). Después de la información y posterior análisis realizado y plasmado a lo largo de los siguientes capítulos, se demuestra que estas afirmaciones son totalmente falsas.

La Dark web forma parte de la Deep web, pero se necesitan navegadores especiales para poder acceder a ella. El objetivo es ofrecer mayor seguridad y privacidad a los contenidos alojados en la misma y los métodos de acceso son softwares legales por lo que, de nuevo no se puede considerar que la Dark web sea algo malo o ilegal.

La herramienta más utilizada para entrar en la Dark web es Tor. Se analizan las características y funcionalidades de esta herramienta, creada en el año 2002 por *Roger Dingledine*, *Nick Mathewson* y *Paul Syverson* y que a día de hoy es gestionada por *Tor Project*. El propósito de Tor es proporcionar anonimato y privacidad a los usuarios. Como toda herramienta puede contener vulnerabilidades y más aún por la popularidad, uso y gran cantidad de usuarios que tiene. Se han producido numerosos ataques a la red Tor y cada día se descubren más vulnerabilidades. Por esta razón no se puede asegurar al cien por cien el anonimato.

También se quiere analizar y comparar Tor con otras alternativas disponibles actualmente para tener una idea clara de las características de cada una y cuando es mejor utilizar una u otra (ver capítulo 7).

Finalmente, con toda la información recopilada se necesitan extraer las conclusiones finales de este estudio que se encuentran en el capítulo 8 de este trabajo final de máster.

1.2. Objetivos

Para la realización del trabajo fin de máster se plantean los siguientes objetivos:

1) Introducción a la Deep Web y principales métodos de acceso.
2) Descripción de la red Tor y su estructura
3) Descripción de las funcionalidades de Tor
4) Instalación y acceso a la red Tor
5) Descripción de los tipos de servicios e información que se puede encontrar en la red Tor.
6) Cibercrimen, muestra de algunos ejemplos de mal uso de la Deep Web y la lucha contra la ciberdelincuencia.
7) Vulnerabilidades y ataques a Tor.
8) Descripción y comparación de alternativas a Tor: I2P, Freenet, etc.

1.3. Metodología

El método para llevar a cabo este proyecto se puede dividir en las siguientes etapas:

1) **Elaboración del plan de trabajo**: Una primera toma de contacto con el tema del proyecto para decidir los objetivos, el método de trabajo, planificación del tiempo y valorar el alcance que se puede dar al proyecto con arreglo al tiempo que se dispone.
2) **Búsqueda de información**: Esta fase sirve para buscar todo tipo de información sobre el tema a trabajar y su posterior selección.
3) **Análisis de la información**: Se trabaja con los datos obtenidos anteriormente para lograr alcanzar los objetivos formulados y plasmarlos en la memoria del trabajo.
4) **Implementación**: A partir de la información obtenida y su análisis, definir un ejemplo práctico y realizarlo como demostración para el trabajo.
5) **Conclusión**: Con la información recopilada y el ejemplo práctico redactar las conclusiones del trabajo, verificar si se han alcanzado todos los objetivos previstos, así como plantear posibles líneas de trabajo futuro.

1.4. Tareas y planificación

La realización de este proyecto está enmarcada en el espacio temporal de las entregas de la asignatura cuyos plazos se detallan a continuación.

Fase	Tareas	Entregable	Fecha
Elaboración del plan de trabajo	Definir contexto de TFM, objetivos, metodología, listado de tareas, planificación del tiempo y estado arte	PEC1	12/03/2018
Búsqueda de información **Análisis de la información**	Búsqueda información general sobre Deep web y el método de acceso con Tor. Comprender la estructura de la red Tor y sus funcionalidades	PEC2	09/04/2018
Análisis de la información **Implementación**	Realizar una instalación de Tor y acceso para ver tipos de servicios e información disponibles	PEC3	07/05/2018
Conclusión **Memoria final**	Cibercrimen, ataques, posibles riesgos y vulnerabilidades de Tor. Alternativas a Tor y conclusiones finales	PEC4	04/06/2018

1.5. Análisis de riesgos

Se plantean los siguientes riesgos para el proyecto:

1) **Dificultad en el cumplimiento de los plazos**. La dedicación al proyecto puede verse alterada debido a la situación académica y la compaginación con el resto de las tareas del alumno, por lo que existe el riesgo de no cumplir exactamente los plazos para realizar el estudio.
2) Hay una **falta de conocimiento sobre el tema** a tratar. Este riesgo, aunque es menor se debe tener en cuenta ya que necesita un periodo de adaptación y búsqueda de información.
3) **Falta de conocimiento del funcionamiento interno** de la aplicación o tecnología (tipo de comunicación, seguridad, etc.) Se necesita un tiempo para conocer la base tecnológica sobre la que se trabaja.
4) Se pueden producir **fallos en el equipo** de trabajo y requiera reparación.

Identificación	Riesgo	Probabilidad	Impacto	TOTAL
Tiempo limitado	Dada la carga de trabajo actual en otras tareas se plantea la posibilidad de no poder cubrir todos los objetivos marcados	Media/alta (4)	Medio/alto (5)	20
Falta de conocimiento del funcionamiento de la tecnología	Requiere tiempo para aprender la tecnología y puede dificultar la configuración y la prueba de navegación a realizar.	Alta (4)	Medio/alto (5)	20
Fallo en equipo de trabajo	La falta de recursos para el desarrollo conlleva retrasos en el proyecto	Media (3)	Bajo (2)	6

En la tabla se toman los siguientes valores para cuantificar los riesgos y las medidas para paliarlos:

- Muy alto: 5
- Alto 4
- Medio: 3
- Bajo: 2
- Muy Bajo: 1

Sobre los dos riesgos detectados se van a tomar las contramedidas para mitigarlos que se muestran en la siguiente tabla.

Identificación	Acciones de mitigación	Probabilidad	Impacto	TOTAL residual
Tiempo limitado	Trabajo rápido y conciso	Media/alta (4)	Medio/alto (5)	20
Falta de conocimiento del funcionamiento de la tecnología	Obtención de información por internet. Análisis de otros estudios sobre el tema.	Media (4)	Medio/bajo (4)	16

	Acotar la prueba de navegación para no extenderse sin necesidad.			
Fallo en equipo de trabajo	Revisar periódicamente el equipo y disponer de equipo adicional en caso de necesidad.	Bajo (2)	Bajo (2)	4

1.6. Organización de la memoria

En el capítulo 2 expone las capas de la web, los métodos de acceso a la Deep web y un análisis sobre la internet profunda fruto de la búsqueda, selección y posterior análisis de información realizado.

El capítulo 3 está dedicado a la herramienta Tor, se describe qué es, sus características, su estructura, funcionalidades y los servicios más importantes. Los capítulos 2 y 3 cubren las fases de búsqueda y análisis de información.

El capítulo 4 recoge la instalación y prueba del navegador Tor. Se muestra cómo instalar la herramienta tanto en Windows como en Linux, las opciones de seguridad del navegador y se ha dado un paseo por la Deep web en busca de información y tipos de servicios accesibles y disponibles. Se ha conseguido encontrar bastantes servicios ocultos de diferente tipo que permiten una reflexión plasmada en las conclusiones de este trabajo. Este capítulo recoge la fase de implementación del trabajo.

El capítulo 5 abarca el tema del cibercrimen en la Deep web, donde se describe el mundo de los *criptomercados* y las *criptomonedas*.

El capítulo 6 trata sobre las principales vulnerabilidades de Tor y en el capítulo 7 se describen las alternativas más habituales a Tor, sus características más relevantes y una comparativa.

Por último, en el capítulo 8 se encuentran las conclusiones del trabajo con lo que se completa la fase de conclusión y la memoria de este trabajo fin de máster.

2. Descubriendo la Deep web

2.1. Capas del Web

La red está dividida en tres capas tal y como se muestra en la ilustración 1.

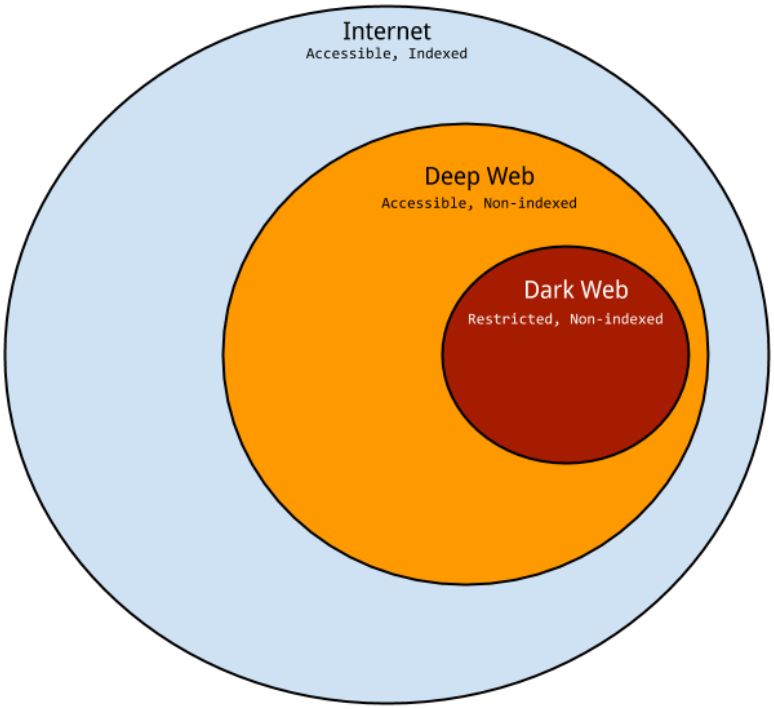


Ilustración 1 Capas en la red

Surface web: Es Internet, se refiere a toda la Web que se conoce y es accesible e indexada por buscadores como *Google*, *Bing*, *Yahoo*, etc.
Deep web: Es accesible pero no indexada por los buscadores. Engloba páginas web con contenido dinámico, sitios privados con acceso por usuarios y contraseña, sitios no linkados o enlazados, páginas que el buscador decidió no indexar, documentos con formato no indexable o indexados pero no accesibles con criterios de búsqueda convencionales y sitios web con nombres de dominio no controlados por *IANA* (*Internet Assigned Numbers Authority*) [1] como por ejemplo *Emercoin* [2], *Namecoin* [3], etc.
Dark web: Es la parte de la red restringida y no indexada. Para acceder a ella se necesitan determinados clientes como *Tor*, *Freenet* o *I2P*. Está formada por el contenido que se puede encontrar en diferentes Dark nets.

2.2. Acceso a la Deep Web

Existen varias herramientas para acceder a la Deep web. Tor [4] es la más conocida y en la que se va a centrar este trabajo, pero también están *I2P* [5] y *Freenet* [6] como sistemas bastante maduros y activos actualmente. En el capítulo 7 se describen con más detalle dichas alternativas y varias adicionales menos populares, pero con sus funcionalidades particulares.

2.3. Investigando la Deep Web

En la Deep web se encuentra el contenido al que no se puede acceder mediante buscadores (*Google*, *Bing*, *Yahoo*, etc.). Los datos son accesibles de forma pública, pero es necesario hacerlo a través de un acceso especial. En la internet profunda se encuentran bases de datos de compañías (bancos, hospitales, etc.), foros privados, carpetas y archivos en *Dropbox*, *Drive*, etc.

En la Dark web, el contenido se oculta de manera intencionada en diferentes Dark nets, utilizando dominios propios (*.onion*, *.i2p*, etc.) y sólo se puede acceder mediante programas como Tor. Además, no puede ser indexado por los buscadores.

La Dark web forma parte de la internet profunda y es donde se encuentran los sitios y servicios ocultos o llamados *hidden services*. El hecho de que estén ocultos no significa que sean sitios dedicados a cometer delitos ni que sea el punto de reunión de criminales, aunque algunas personas se aprovechen de sus cualidades y lo usen con este fin.

Para hacerse una idea de la magnitud de la Dark web y la amplia variedad de páginas y servicios que contiene, se ha creado un mapa (ver ilustración 2), proyecto de la compañía *Hyperion Gray* [7], que recopila casi 7000 páginas web accesibles actualizado a enero de 2018. Los sitios y servicios en la Dark web no tienden a ser muy estables, aparecen y desaparecen rápidamente, por lo que hacer un mapa de toda la Dark web y que esté actualizado es prácticamente imposible, al igual que calcular la totalidad de la extensión de la web oscura. Según las estadísticas que proporciona *Tor Project*, hay más de 60.000 servicios *onion* ejecutándose a fecha abril de 2018 [8].

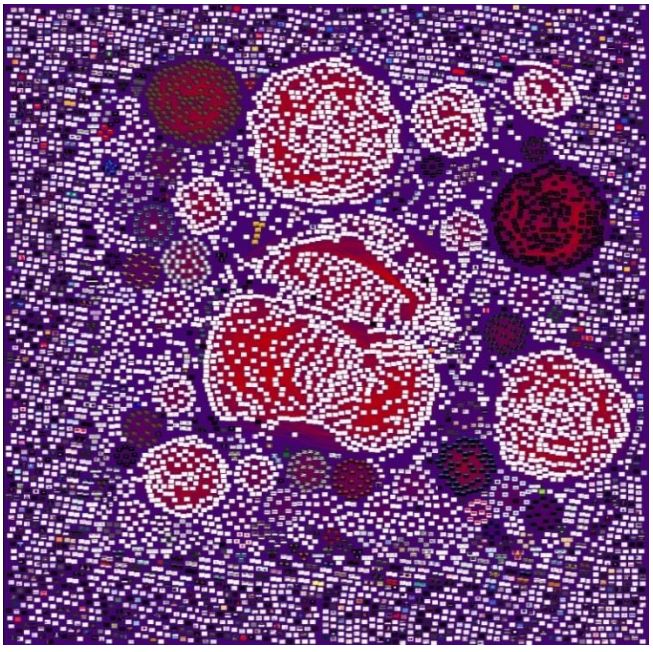


Ilustración 2 Mapa Dark web de Hyperion Gray

En el mapa se pueden encontrar sitios de todo tipo y algunos contienen material ofensivo y/o ilegal que se muestra sin censurar. Cada sitio está representado en el mapa por una captura de pantalla y los sitios con estructura similar están conectados por líneas. Los sitios con temática parecida están agrupados por zonas en el mapa. Hay varios niveles de zoom que permiten leer claramente el contenido del sitio web. En la ilustración 3 se puede ver un ejemplo de una página que parece un servidor de correo encontrado en el mapa y en la ilustración 4 el grupo de páginas que tienen el mismo aspecto que ella conectadas por líneas.

Ilustración 3 Ejemplo servidor correo en mapa Dark web

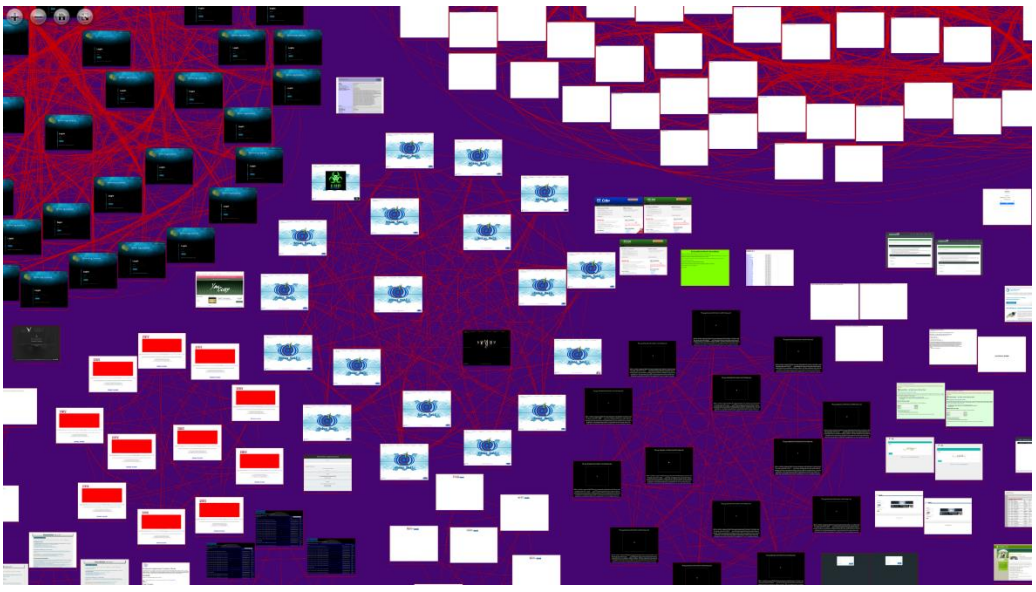


Ilustración 4 Ejemplo grupo páginas en mapa Dark web

El mapa permite hacerse una idea de lo que hay en la Dark web y la proporcionalidad entre los sitios inofensivos y los dedicados a actividades ilegales, gracias a la agrupación que muestra. Hay unos pocos grupos grandes y bastantes grupos de pequeño tamaño. Tras una inspección por el mapa se puede concluir que los grandes grupos se trata mayoritariamente de páginas en blanco con mensajes del tipo *504 Time-out Gateway*, *Page not found*, *403 Forbidden*, etc. En los grupos pequeños hay variedad de temas, desde copia de tarjetas VISA, tráfico de *Bitcoins* o simples servidores de correo. En la ilustración 5 se muestra un ejemplo y en la ilustración 6 el grupo marcado en rojo dentro del mapa.

Ilustración 5 Ejemplo página en Dark web

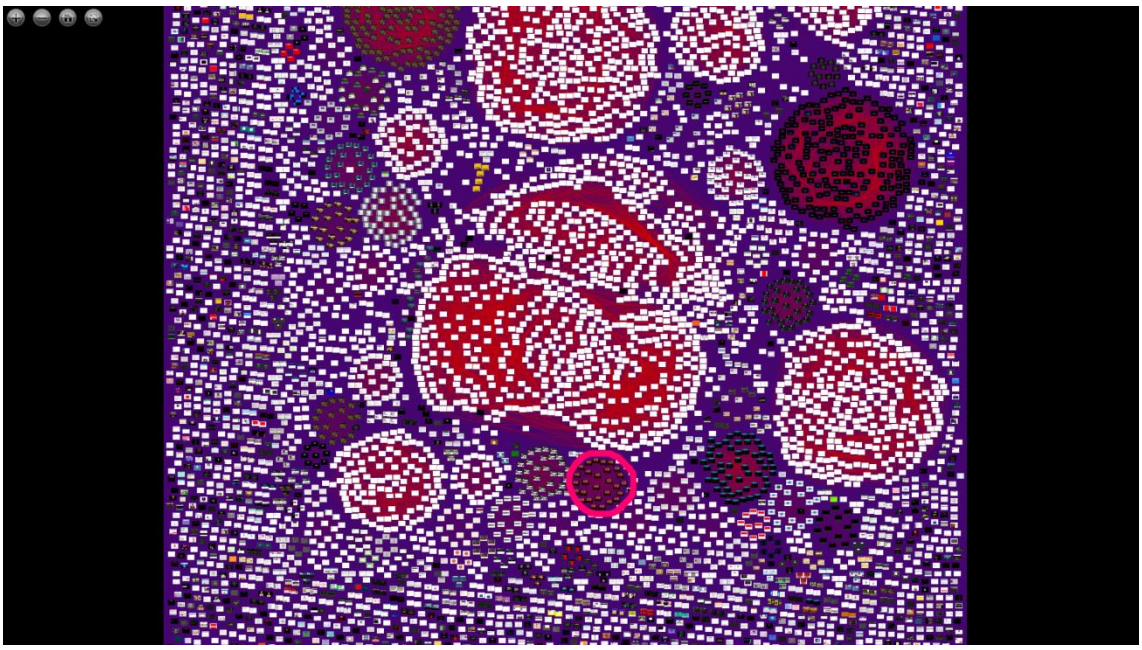


Ilustración 6 Vista grupal en mapa Dark web

3. Características de Tor

3.1. ¿Qué es TOR?

Es un servicio online que mediante un software específico permite conectarse a una red de comunicaciones de baja latencia que brinda anonimato a sus usuarios. Se creó en el año 2003 con este objetivo de proporcionar privacidad y anonimato. Está basado en el proyecto *OR* del *Laboratorio de Investigación Naval de los Estados Unidos* [9], quien lo financió hasta que en el año 2004 pasó a manos de la *EFF* [10].

En la actualidad y desde el año 2005 el proyecto pertenece a *Tor Project* [4], una entidad sin ánimo de lucro dedicada a la investigación. Es de código abierto y en permanente evolución. Se estima que Tor es utilizado diariamente por cientos de miles de usuarios en todo el mundo. En la ilustración 7 se puede ver el tráfico en la red Tor el 13 de enero de 2016 por la herramienta *TorFlow* [11].

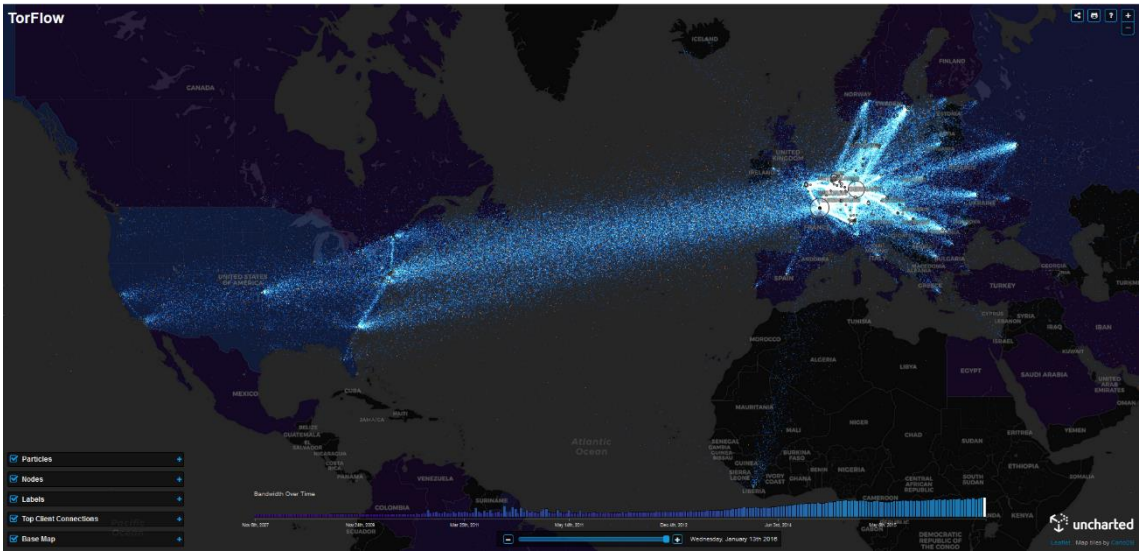


Ilustración 7 Tráfico red Tor el 13 enero de 2016

Tor también se creó para evitar las censuras de ciertos proveedores de servicios y de ciertos países. Como cualquier herramienta o tecnología, se puede utilizar para hacer el bien y para hacer el mal. Los ciberdelincuentes han aprovechado las características de anonimato de la red para cometer delitos y por este motivo, se tiende a relacionar las redes Tor con ciberdelincuencia. Por ejemplo, un informe del FinCEN (Financial Crimes Enforcement Network) [12] del departamento de Estado de EE. UU afirma que entre un total de 6048 acciones sospechosas reportadas por bancos entre 2001 y 2014, al menos 975 involucraban nodos Tor. También la denominada Operación Onymous [13], ejecutada por varias organizaciones de seguridad internacionales como Europol y FBI entre otras, detuvieron a 17 personas responsables de más de 400 direcciones .onion asociadas a 27 sitios web con servicios ocultos.

Estos hechos no deberían prevalecer sobre el verdadero fin para el que se creó Tor y habría que conocer mejor y dar más importancia a las cualidades y servicios que ofrece la red, así como educar a los usuarios en las buenas prácticas para poder protegerse mejor y sacar el mejor provecho posible tanto de la red Tor como de Internet.

La red Tor es outproxy e inproxy. Outproxy porque permite salir a internet la surface web a través del nodo de salida e Inproxy porque permite navegar a través de los servicios ocultos de la propia red navegando a páginas ".onion". Estas páginas están formadas por un conjunto de 16 caracteres alfanuméricos y terminados en ".onion". Un ejemplo de dirección sería:

http://eqt5g4fuenphqinx.onion/

En Tor el anonimato se logra a través de distintas capas como las que tiene una cebolla. Cuando un cliente quiere conectarse a un sitio web primero se consigue un listado de directorio del servidor central. La conexión hasta el destino se realizará a través de un nodo de entrada, uno o más nodos intermedios y finalmente un nodo de salida. Todas las conexiones serán encriptadas salvo la que se produce desde el nodo de salida hasta el destino. Ninguno de los nodos puede descifrar el mensaje y solo conoce el siguiente nodo al que pasar el mensaje. Visto desde el exterior, lo único que se ve es una serie de conversaciones fragmentadas y cifradas saltando a un lado y otro. Pero el sistema no es perfecto y los mismos desarrolladores lo advierten en su página web. No se proporciona protección frente a un ataque "extremo a extremo" lo que permite a un atacante interceptar las conexiones de salida del cliente o bien el tráfico que llega y sale desde un destino concreto pudiendo llegar a identificarlo utilizando distintas técnicas de análisis estadístico de conexiones. En la ilustración 8 se muestra cómo funcionan las conexiones dentro de la red Tor.

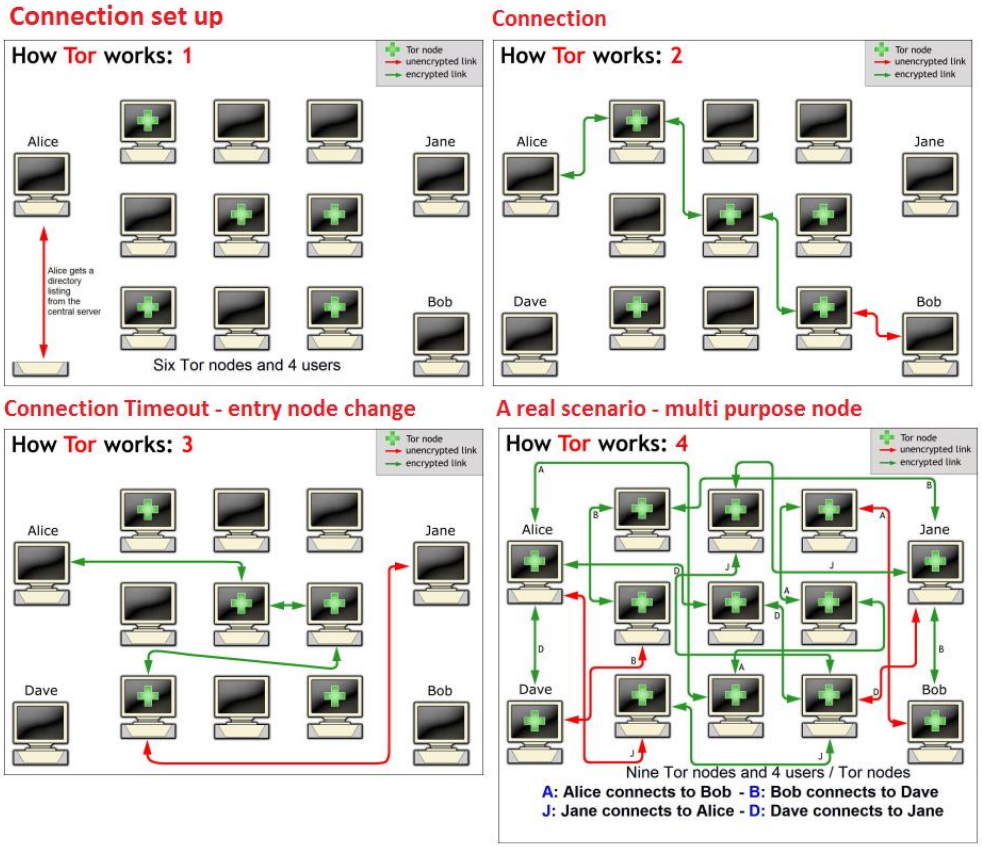


Ilustración 8 Conexiones en red Tor

Tor tiene numerosas vulnerabilidades. Un ejemplo es la detectada en noviembre de 2017 [14] por un investigador italiano y que revela la dirección IP de los usuarios que intentan acceder con el navegador web a ficheros a través de direcciones *file://* al realizar una conexión directa al host remoto sin utilizar el navegador Tor. La vulnerabilidad afecta a los sistemas operativos Linux y OS X y en este caso ha sido corregida por los desarrolladores de TOR en la actualización a la versión 7.0.9.

El uso de Tor y el acceso a la Deep web conlleva un riesgo que el usuario debe conocer y asumir. Además, es responsabilidad de cada uno las acciones que lleve a cabo y el nivel de confianza otorgado en los nodos por los que se conecta en la red. Tor hace más complejo el rastreo en la web y aporta privacidad, pero las actividades delictivas siguen siendo ilícitas.

3.2. Onion Routing y Onion Services

Tor es una tecnología para preservar la privacidad con dos objetivos principales. El primero es esconder la localización de los usuarios que navegan por la web. Cuando se utiliza un navegador convencional, los sitios web que se visitan conocen la dirección IP del usuario. Esta dirección puede ser rastreada hasta localizar al usuario, a través del proveedor de servicios (ISP), que sabe los sitios web que el usuario visita. Tor mediante ***Onion Routing*** encripta el tráfico durante la navegación, se mezcla con el tráfico de otros usuarios y oculta la dirección IP a los sitios web visitados. También evita que el ISP pueda ver el tráfico, es decir dónde está navegando el usuario, y sólo puede ver que está conectado a la red de Tor.

El segundo objetivo es ocultar la localización de los sitios web. Cuando se navega a un sitio con un navegador convencional, lo primero que se hace es determinar la dirección IP del sitio. La dirección se puede rastrear hasta dar con la localización del negocio o individuo que ha montado el sitio web. Con Tor, mediante los ***Onion Services*** o *hidden services*, se puede ocultar la dirección IP del sitio a los usuarios que lo visitan. Un servicio crea varios puntos de introducción en ciertos nodos de la red y notifica a una base de datos qué nodos son. En el momento que un cliente quiere conectarse con el servicio, enviará a uno de los nodos la dirección de un punto de encuentro junto con una clave única. El punto de introducción conecta con el servicio oculto y este a su vez conectará con el punto de encuentro creando una comunicación con el cliente.

Los servicios ocultos de Tor pueden estar basado en TCP, SSH, HTTP, FTP, etc. Es cierto que algunos pueden usar los servicios ocultos de Tor para actividades delictivas como crear mercados de venta de drogas o sitios para intercambiar fotografías y vídeos de pornografía infantil, etc. pero el verdadero espíritu de Tor radica en el activista democrático que evade la vigilancia de un gobierno opresivo, las comunicaciones entre una empresa dedicada a las noticias y sus informadores, o el ciudadano que puede navegar tranquilamente por la web sin ser rastreado por las empresas de marketing y anunciantes, entre otros.

3.3. Cifrado de mensajes

Cuando un usuario quiere conectarse con un sitio web usando Tor, se calcula una ruta aleatoria al destino pasando por varios nodos intermedios. Después se consiguen las claves públicas de todos los nodos usando el directorio de nodos.

El mensaje se cifra como una cebolla, por capas, primero se cifra el mensaje con la clave pública del último nodo de la ruta, para conseguir que sólo ese nodo pueda descifrarlo. Adjunto al mensaje se incluyen también cifradas las instrucciones para llegar al destino. Todo el conjunto o paquete formado se cifra de nuevo para que sólo lo pueda descifrar el penúltimo nodo de la ruta. El proceso se repite hasta que se acaba con todos los nodos de la ruta.

Cuando el mensaje llega al primer nodo, este lo descifra con su clave privada y sigue las instrucciones que ha descifrado para enviar el resto del paquete al nodo siguiente. En el siguiente nodo se descifra de nuevo el paquete y se realiza la misma operación. Así hasta llegar al nodo de salida que enviará el mensaje a su destino. Este nodo final, al descifrar el paquete con su clave privada, puede leer el mensaje original (ya no tiene más capas de cifrado), por lo que sería conveniente cifrar el mensaje original. La ilustración 9 muestra de manera gráfica el cifrado de un mensaje enviado con Tor.

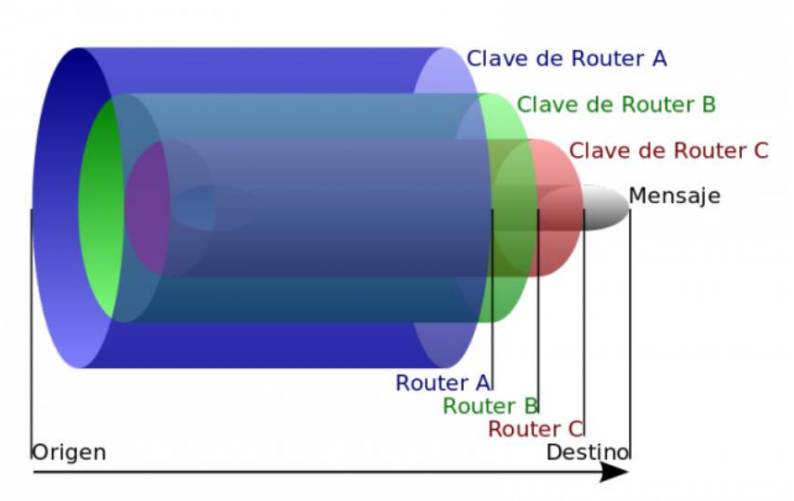


Ilustración 9 Cifrado de un mensaje con Tor

3.4. Relay

Son los routers o nodos que reciben el tráfico de la red Tor y lo pasan al siguiente nodo o al destino. Los tres tipos de nodos que existen son los siguientes:

- **Nodos intermedios** (*middle relays*): Cuando se envía un mensaje a través de la red Tor, pasa por al menos tres nodos antes de llegar al destino. Los dos primeros son nodos intermedios que reciben el tráfico y lo pasan al siguiente nodo. Añaden robustez y velocidad a la red sin hacer parecer al dueño del nodo como fuente del tráfico. Advierten de su presencia dentro de la red para que los usuarios puedan conectarse a ellos. En principio es seguro montar un nodo intermedio propio ya que la IP del nodo no se

mostraría nunca como origen del tráfico, aunque este sea generado por un usuario malicioso para hacer algo ilegal.

- **Nodos de salida** (*exit relays*): El tráfico pasa por el nodo de salida justo antes de llegar destino. Advierten de su presencia a toda la red Tor para que los usuarios puedan utilizarlos. La dirección IP de estos nodos es interpretada como la fuente del tráfico, por lo que, si un usuario comete una ilegalidad empleando la red Tor, el nodo de salida asume la culpa de los hechos. Las personas que ponen en marcha este tipo de nodos tienen que asumir que van a tener complicaciones, avisos de copyright y posiblemente les contacten las agencias de seguridad.

- **Puentes** (*bridges*): El proveedor de servicios o ISP puede observar el tráfico de red y saber qué se está utilizando Tor. En algunos países como China el uso de Tor está censurado o puede ser peligroso o sospechoso y bloquean las IP de todos los nodos de Tor que son públicos. Para poder conectar con la red Tor existen los puentes, nodos alternativos que no están listados públicamente. Dificulta que el ISP sepa que se está usando Tor, pero no lo hace totalmente invisible. Tor Project distribuye direcciones bridge aleatorias [15].

La información actualizada y el estado de los nodos se puede consultar en la página de Tor Project [16].

3.5. Autoridades de directorio y descriptores

Las autoridades de directorio son nodos especiales que mantienen una lista de los nodos que hay en funcionamiento y publican un consenso de forma colectiva. Funcionan como servicios de directorio.

Actualmente existen diez autoridades de directorio [17] cuya ubicación viene preconfigurada en el navegador Tor facilitando su usabilidad.

Los descriptores almacenan información de los nodos públicos de Tor. Se descargan de las autoridades del directorio y se pueden consultar desde la página de *Tor Project* [18]. Los hay de varios tipos, los más comunes se muestran en la siguiente tabla:

Tipo descriptor	Descripción
Descriptor del servidor (server descriptors)	Información que cada nodo publica de sí mismo.
Descriptor de información extra	Información extra y autopublicada por los nodos pero que generalmente los usuarios de Tor no necesitan conocer y por tanto no se descarga por defecto.
Micro descriptor	Documento minimalista con la información que los usuarios de Tor necesitan para trabajar con la red.
Documento del estado de la red o consenso	Documento con entradas del estado de los router que publican las autoridades de directorio cada hora.
Entrada de estado del router (router status entries)	Información de los nodos que proporcionan las autoridades de directorio. Incluye flags, heurística para la selección de nodos, etc.
Descriptor de servicios ocultos	Información autopublicada por cada servicio oculto que sólo puede solicitarse a través de procesos Tor.

3.6. Direcciones .onion

Cuando se crea un servicio oculto y se despliega en Tor se crea una pareja de claves RSA de 1024 bits y un fichero llamado *hostname* que contiene la dirección pública para acceder al servicio.

Para crear la dirección se calcula el *SHA1* de la clave pública generada. De los 160 bits que forman el *hash*, se toma la mitad y se codifica en *Base32*, de manera que todos los nombres de dominio tengan una longitud de 16 caracteres y solo contengan números entre 2-7 y letras entre *a-z*. Por último se añade el sufijo *.onion*.

Algunas direcciones no son tan aleatorias y tienen un patrón fijo en el nombre para que sea más sencillo de recordar, como es el caso de *Facebook* (*facebookcorewwwi.onion*). Fijar caracteres en el nombre de dominio más coste computacional tendrá, ya que se obtiene a partir de la clave pública y habrá que generar tantas claves como sean necesarias hasta dar con el patrón.

3.7. Servicios

Tor Project ha dispuesto una página con distintos servicios sobre la red Tor [19]. A continuación, se hace una pequeña introducción sobre ellos.

3.7.1. ExoneraTor [20]

Consultar si una IP ha sido usada como un nodo de Tor en una determinada fecha. Mantiene una base de datos de direcciones IP que han formado parte de la red Tor. En la ilustración 10 se muestra el resultado sobre la búsqueda de la IP *197.231.221.211* en la fecha *02/02/2018*. La dirección se corresponde con el nodo de salida *IPredator* de Tor.

Ilustración 10 ExoneraTor

3.7.2. Relay Search [16]

Esta herramienta permite visualizar datos sobre los nodos y los puentes en la red Tor haciendo uso de palabras clave. Se pueden realizar búsquedas por nicknames parciales ("*pred*"), direcciones IP parciales ("*197.231.*"), fingerprint ("*9798DVG4*"), combinando más de un elemento ("*pred 197.231.*"), búsquedas más específicas como por país ("*country:fr*") o información de contacto ("*contact:arma*") o con alguna bandera especial ("*flag:Running*"). En la ilustración 11 se muestra el resultado de la búsqueda de los nodos Tor en España, donde en el momento de la búsqueda había 75 nodos tanto online (en verde) como offline (en rojo).

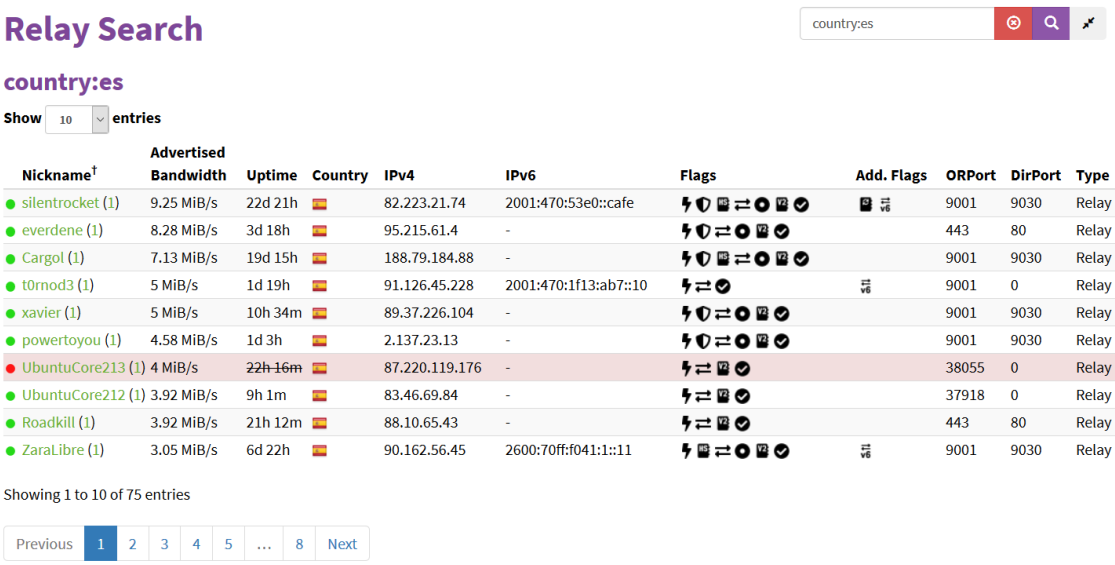


Ilustración 11 Relay Search

3.7.3. Consensus Health [21]

Muestra información y estadísticas sobre el actual directorio de consenso y los votos para facilitar la depuración del proceso de consenso.

3.7.4. Tor Map [22]

Es un mapa interactivo de los nodos en la red Tor junto con información sobre sus localizaciones. En la ilustración 12 se puede ver el mapa mostrando los nodos de salida, los que están en mal estado y los que son autoridades de directorio.

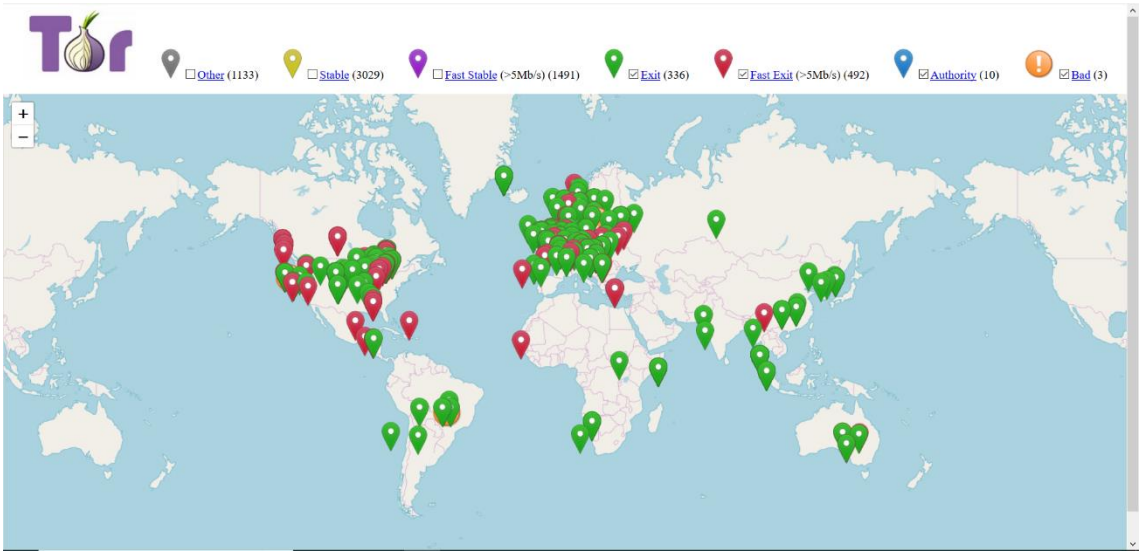


Ilustración 12 Tor Map

3.7.5. OrNetStats [23]

Muestra estadísticas para monitorizar la diversidad en la red Tor. Se puede encontrar información sobre los nodos agrupados por familias, las versiones de Tor o el sistema operativo que ejecutan los nodos, el estado de la IPv6 en los nodos, el estado de los puentes, etc.

3.7.6. DuckDuckGo [24]

El buscador orientado a proteger la privacidad del usuario durante las búsquedas y a no rastrearlas. Permite encontrar detalles de los nodos de la red Tor al introducir las palabras clave "*tor node*" en una búsqueda.

3.7.7. Onionite [25]

Es una aplicación web progresiva que muestra información de los nodos individuales que componen la red Tor. Se pueden realizar búsquedas como en *Relay Search*. En la ilustración 13 se muestra un ejemplo de búsqueda de los nodos de Tor en España.

Ilustración 13 Onionite

3.7.8. Consensus Issues [26]

Sirve para notificar problemas en los consensos a los operadores de las autoridades de directorio. Para poder utilizar el servicio es necesario suscribirse.

3.7.9. Oll's anomaly detection system [27]

Es un listado actualizado de anomalías detectadas y un ranking de los países con un uso anómalo de Tor (el número de usuarios conectados a Tor está fuera de los patrones esperados). Es necesario suscribirse al servicio para ver la información.

4. Prueba de Tor

4.1. Instalación de Tor

Para instalar el navegador Tor, se ha descargado la versión 7.5.3 en español para Windows 10 desde la página oficial [4] y se han seguido los sencillos pasos del instalador. Simplemente hay que seleccionar el lugar donde se quiere instalar Tor. En la ilustración 14 se muestra un momento durante la instalación.

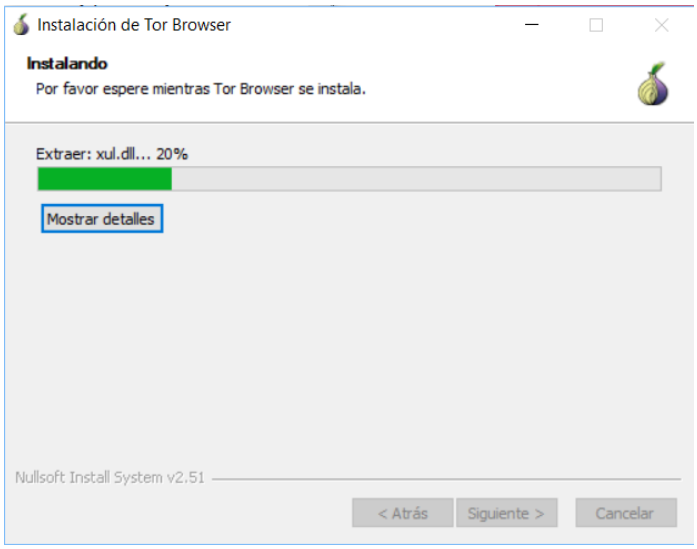


Ilustración 14 Instalación de Tor

De forma sencilla se puede ejecutar el navegador en un sistema Linux, en este caso con Debian 9, descargando desde la página oficial el paquete *tar.xz* de la versión 7.5.3 en español del navegador. Se descomprime el archivo y en la carpeta hay que ejecutar *Tor Browser Setup*. No es necesario ningún tipo de instalación.

4.2. Configuración de Tor

El navegador Tor está preconfigurado para proteger la privacidad y el anonimato en la navegación web, pero hay que tener en cuenta una serie de recomendaciones y hábitos para contribuir en la misma línea o no se garantiza que Tor funcione como se espera.

- No se aconseja usar configuraciones de otros navegadores en Tor porque serán inseguras. Se recomienda usar siempre la configuración del propio navegador Tor.
- No utilizar aplicaciones que comparten archivos Torrent ya que establecen conexiones directas ignorando las configuraciones de proxy, incluso usando Tor. Se puede rastrear las peticiones GET porque se envía la IP real del usuario.
- No se recomienda instalar ni habilitar plugin en el navegador tales como *Flash*, *RealPlayer*, *QuickTime*, etc. Ya que pueden ser manipulados para obtener la dirección IP del usuario.
- Usar siempre las versiones HTTPS de los sitios web. El navegador Tor incluye *HTTPS Everywhere* para forzar a usar siempre la versión encriptada del sitio web al que se quiere acceder.
- No es recomendable abrir documentos descargados mediante Tor mientras se está online. Por defecto el navegador Tor emite un aviso para evitar que el usuario abra documentos manejados por aplicaciones externas. En un documento DOC o PDF se pueden incluir recursos que serán descargados fuera de Tor por una aplicación que los abre, revelando así la dirección IP del usuario. Lo más seguro es abrir esos documentos en una máquina desconectada de la red o utilizar una máquina virtual.
- No hacer uso del navegador en modo pantalla completa ya que se puede usar esta información para rastrear al usuario. Si se intenta maximizar el navegador aparece un mensaje de información.

Al iniciar por primera vez el navegador se puede escoger entre conectar directamente con la red Tor o configurar una conexión en caso de que la conexión a internet esté censurada o se requiera un proxy, ver ilustración 15.

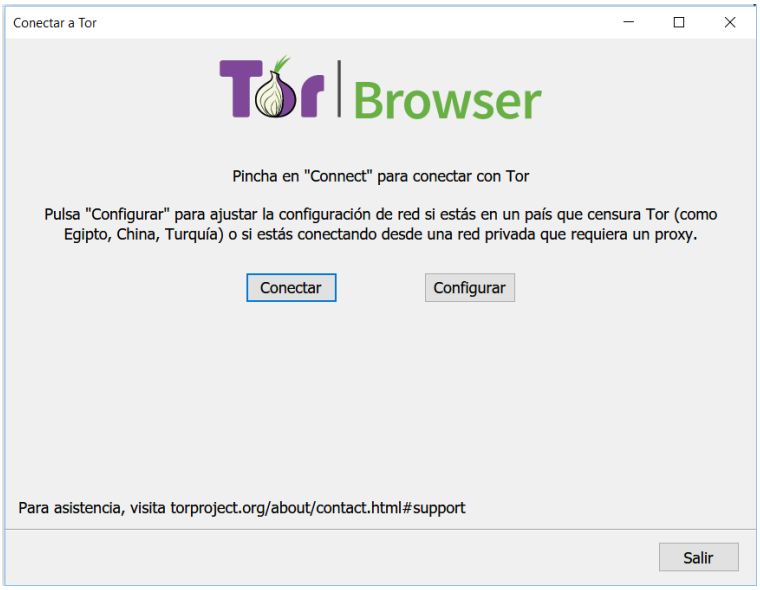


Ilustración 15 Configuración inicial Tor

El navegador se autoconfigura y ya se puede empezar a navegar. Si se hace clic en el símbolo de la cebolla arriba a la izquierda aparece la información del circuito actual por donde se está estableciendo la conexión a internet (ver ilustración 16), en este caso se conecta a un nodo en Francia con IP *163.172.175.174*, después a otro nodo en Estados Unidos con IP *184.105.144.180* y por último un nodo de salida en Alemania con IP *185.117.215.9* después, sale del circuito y alcanza el destino deseado.

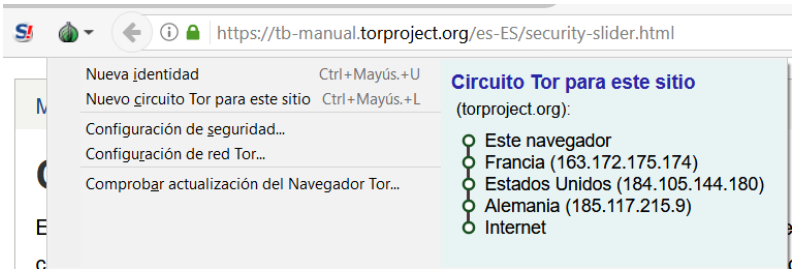


Ilustración 16 Circuito Tor

En la configuración de seguridad se puede ajustar el nivel de seguridad en tres niveles. El nivel más seguro hace que durante la navegación, se deshabilite las opciones de rendimiento JavaScript, algunos tipos de imágenes, algunos símbolos matemáticos (que pueden no ser mostrados correctamente) y no se permite que los elementos audiovisuales HTML5 se autorreproduzcan, tal y como se muestra en la ilustración 17. El nivel medio de seguridad no es tan restrictivo con los audios y vídeos y la mayoría no se deshabilitarán. En el nivel bajo, todas las características del navegador están habilitadas y es la opción más sencilla de usar.

En la configuración de la red Tor se puede indicar si se está en un país que censura a Tor, si se usa un proxy para conectarse a internet o un firewall que sólo permite conexiones a ciertos puertos, ver ilustración 18.

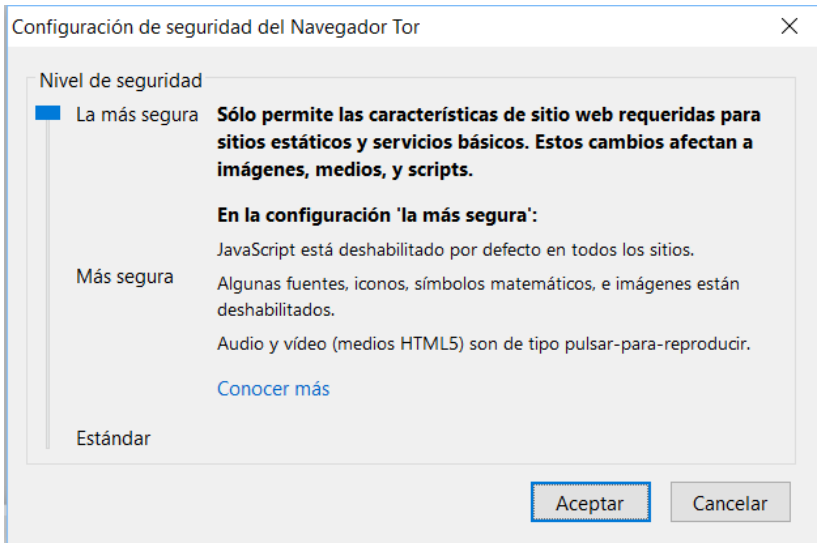


Ilustración 17 Configuración de seguridad Tor

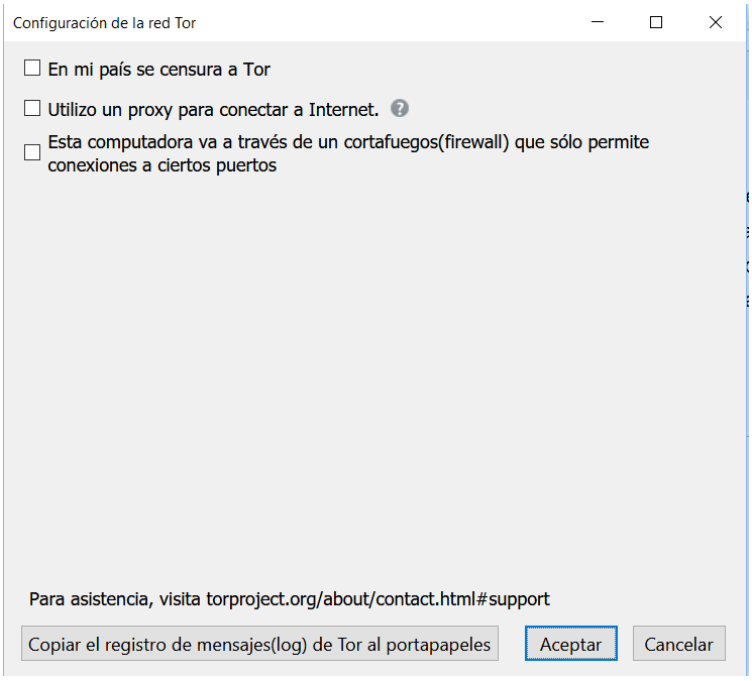


Ilustración 18 Configuración de la red Tor

A parte de estas configuraciones también están las opciones del navegador que son muy parecidas a las del navegador *Firefox* en el que está basado y donde se pueden decidir si se quiere recordar el historial, restringir cookies de terceras partes, guardar las contraseñas, etc.

4.3. Navegando en la Deep Web

Durante la prueba de Tor se ha utilizado el servicio oculto del buscador *DuckDuckGo* [28] y se ha encontrado páginas de tal variedad como se describe a continuación.

4.3.1. The Hidden Wiki [29]

En un servicio oculto de la red Tor con aspecto similar a *Wikipedia* y que sirve como índice para acceder a gran variedad de páginas de dominio *.onion*. En la ilustración 19 se muestra una wiki sobre *Matrix*.

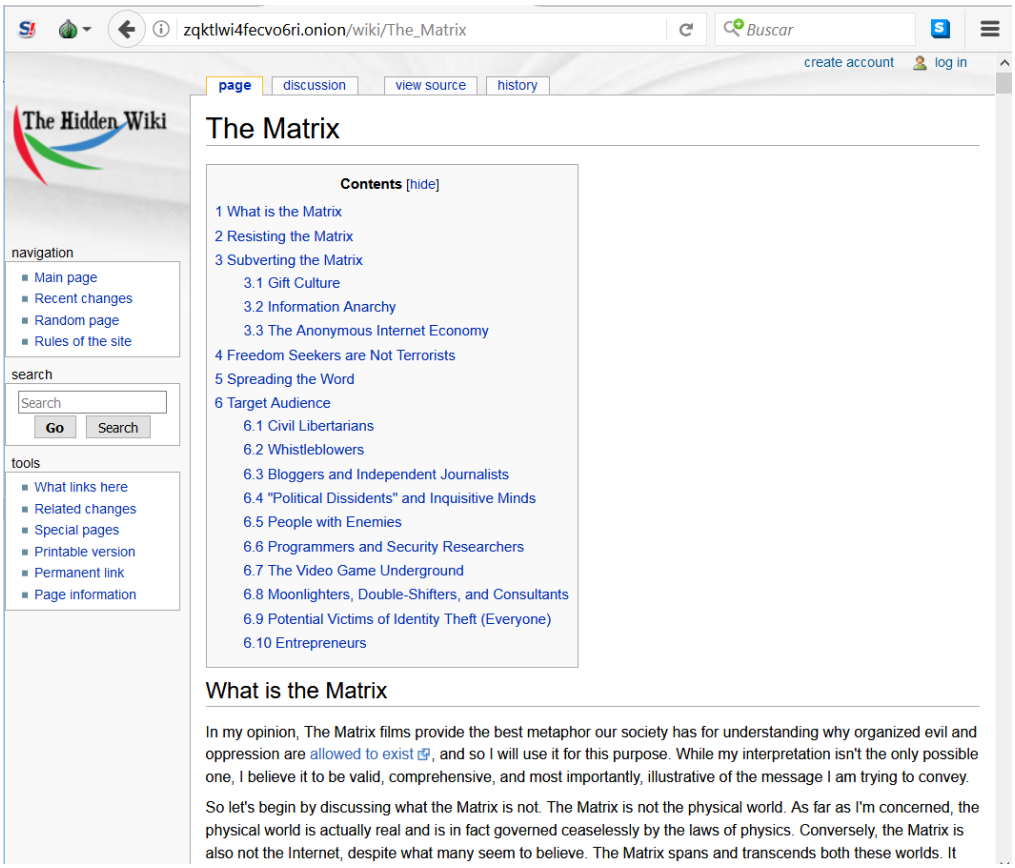


Ilustración 19 The Hidden Wiki

4.3.2. Cebolla Chan 3.0 [30]

Es un foro donde usuarios anónimos pueden charlan de cualquier tema e incluso mercadear, el contenido se muestra sin censura y se considera una de las páginas más polémicas y conocidas de la Deep web, ver ilustración 20. Tiene alrededor de 60.000 usuarios registrados. El foro ha evolucionado tanto que ya tienen versión en la Surface web [31].

4.3.3. Cebolla Board [32]

Es un chat anónimo donde se puede encontrar cualquier tipo de conversación, un ejemplo se muestra en la ilustración 21.

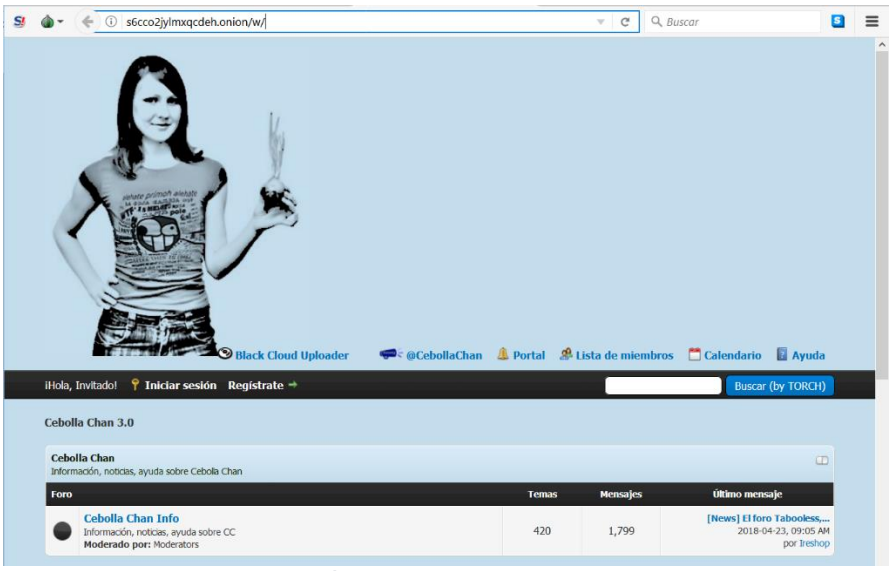


Ilustración 20 Cebolla Chan 3.0

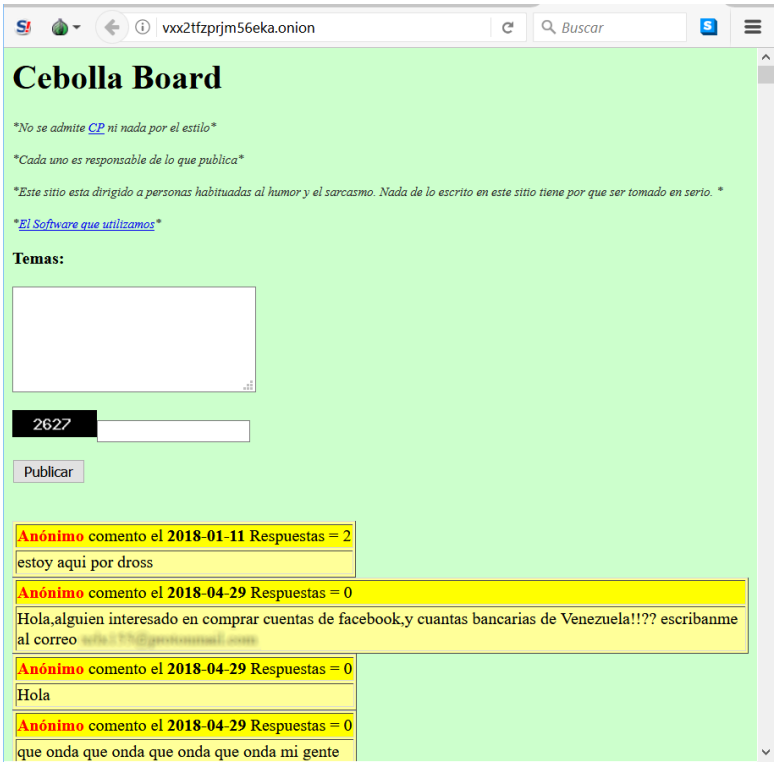


Ilustración 21 Cebolla Board

4.3.4. Chat with strangers [33]

Es un servicio de chat en el que se puede conectar para conversar con un desconocido al azar o también reservar un espacio para hablar con un amigo al que se tiene que pasar una dirección concreta al servicio. En la ilustración 22 se muestra un ejemplo de conversación con otro usuario al azar. La sencilla interfaz permite descargar el *log* de la conversación.

4.3.5. Mail2Tor [34]

Un servicio de correo electrónico anónimo para enviar mensajes manteniendo la privacidad, ver ilustración 23. Utiliza un servicio oculto y los nodos de la red Tor para funcionar de manera que sólo el servidor de correo y el software de Tor es almacenado en los discos duros del servicio oculto y de los nodos. No se almacenan ni los emails ni logs o información sensible que pueda servir para identificar a los usuarios. Este servicio se anuncia a través de su propia página en la Surface web [35].

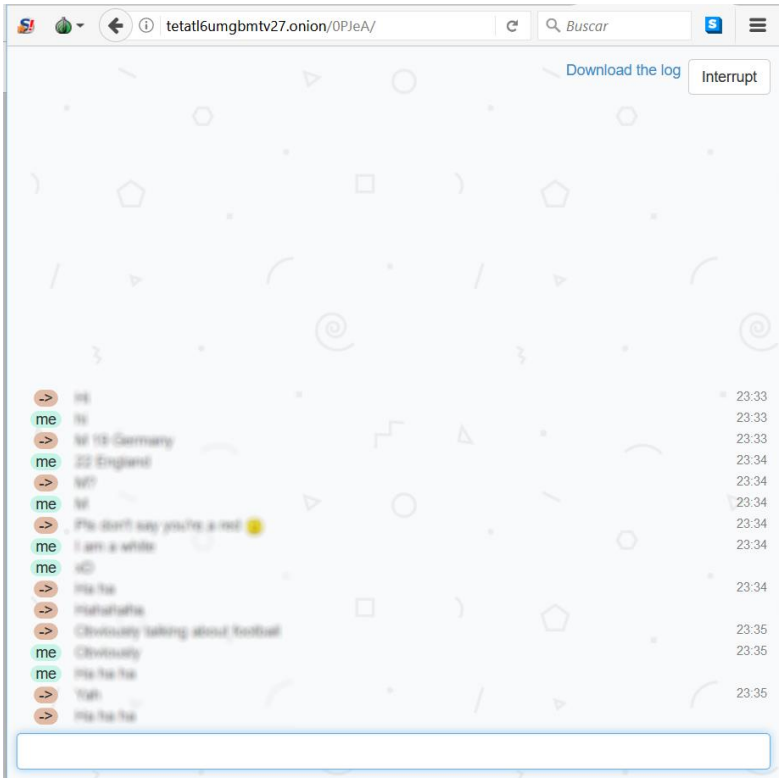


Ilustración 22 Chat With Strangers

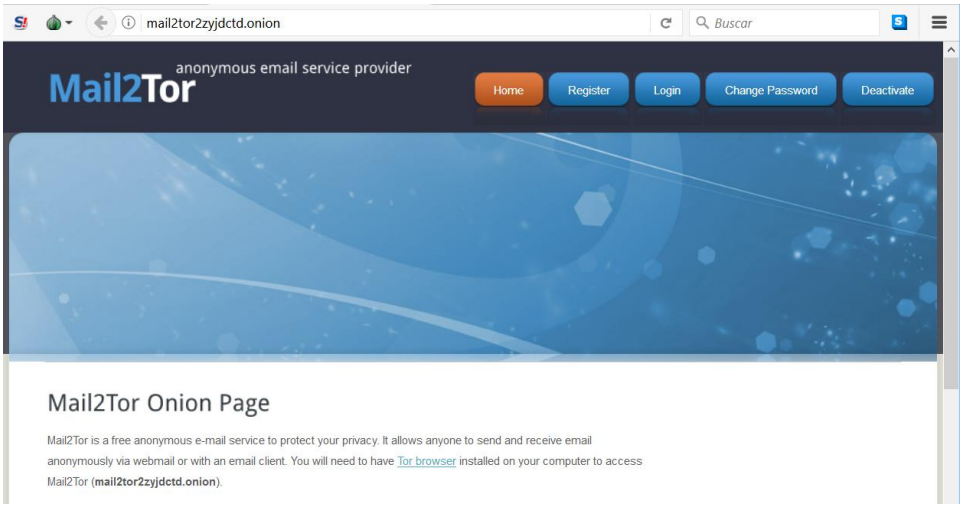


Ilustración 23 Mail2Tor

Ilustración 25 Críptica

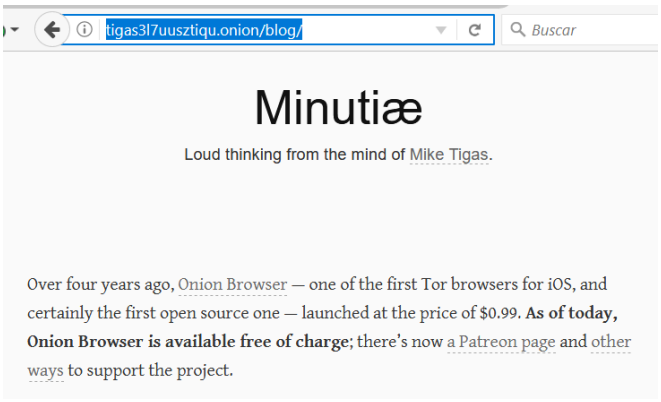


Ilustración 24 Minutiae

4.3.6. Críptica [36]

La versión oculta del blog *críptica.org* en la que se dan consejos y se publican eventos sobre privacidad y seguridad en internet, ver ilustración 24.

4.3.7. Minutiae [37]

Es un blog interesante de *Mike Tigas*, desarrollador, periodista, fotógrafo y hacker cívico en un servicio oculto de Tor, ver ilustración 25. Esta persona es desarrollador líder en *Tabula* (una herramienta de extracción de datos en archivos PDF), *Onion Browser* (navegador anónimo para iOS) y *CivOmega* (un motor de búsqueda abierto).

4.3.8. Deep Web Radio [38]

En esta página se enlazan varias radios online de distintos géneros musicales tanto de la Deep web como de la Surface web, ver ilustración 26.

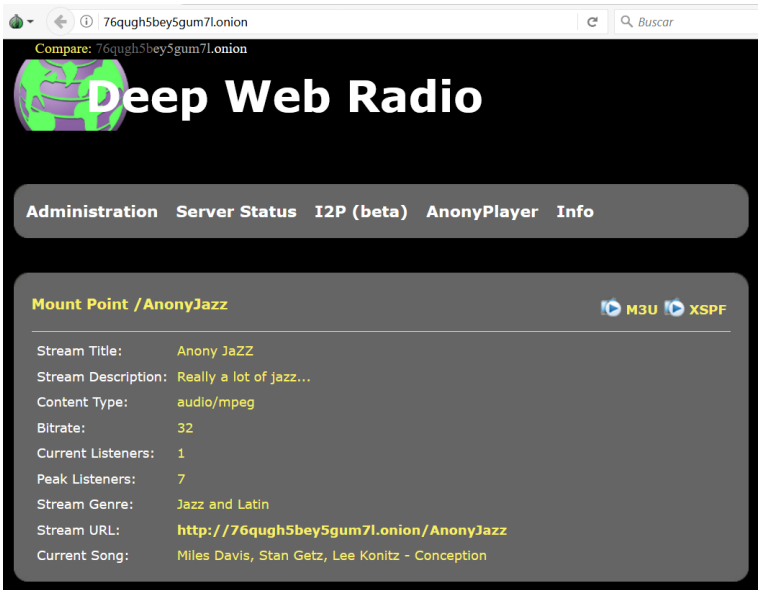


Ilustración 26 Deep Web Radio

4.3.9. Imperial Library [39]

Esta página es un repositorio de libros de todo tipo, la mayoría de ellos en inglés, ver ilustración 27, que se pueden tanto leer online como descargar. Están organizados por género y actualmente cuenta con 129.128 libros en la colección.

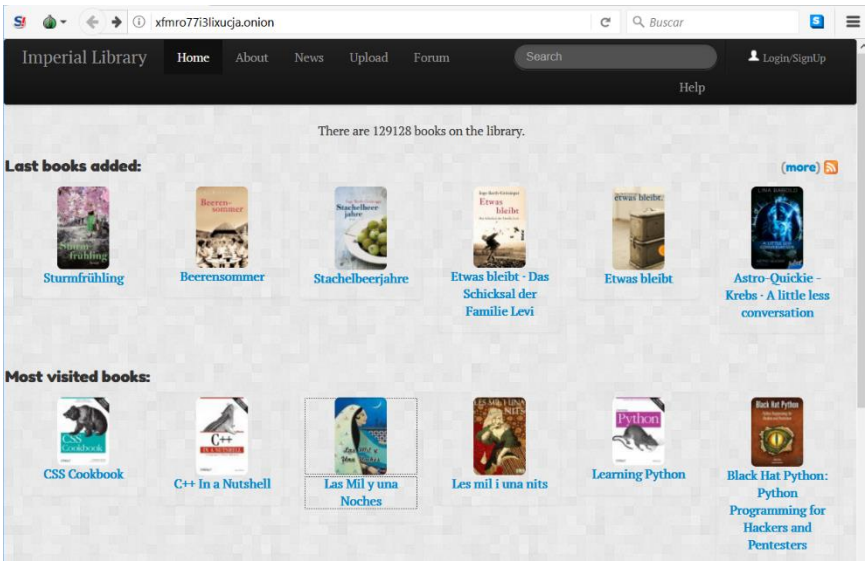
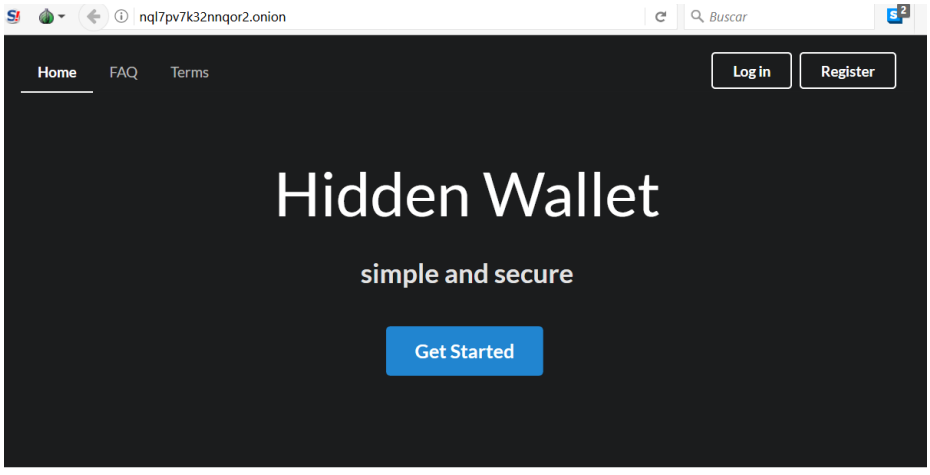


Ilustración 27 Imperial Library

4.3.10. Hidden Wallet [40]

Es el monedero oculto y anónimo más conocido de la Deep web, donde guardar *Bitcoins*. Su misión es construir un futuro financiero abierto, anónimo y justo integrado en un solo software, ver ilustración 28. Equiparan su seguridad a los de cualquier otro banco y aseguran que nunca acceder a los *Bitcoin* de los clientes y el anonimato puesto que están alojados en un servicio oculto de la red Tor.



Hidden wallet is the most popular anonymous wallet on the deep web. We are on a mission to build a more open, anonymous, and fair financial future integrated in a single piece of software.

Ilustración 28 Hidden Wallet

4.3.11. TorShops [41]

Esta página, ver ilustración 29, ofrece sus servicios para diseñar y poner en marcha una tienda *.onion* con integración de pagos con *Bitcoins*, centro de mensajes con clientes, inventario, administración de pedidos, copias de seguridad diarias, etc.

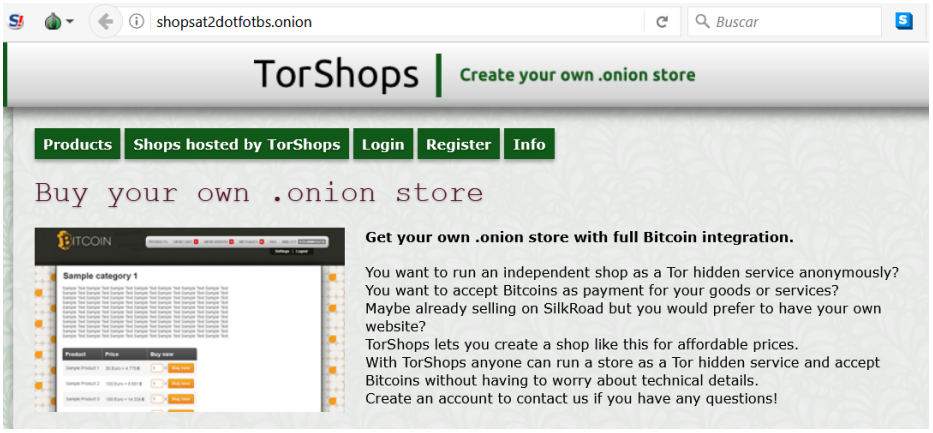


Ilustración 29 TorShops

4.3.12. OnionShare [42]

Es una herramienta de código abierto para compartir de forma anónima y segura archivos de cualquier tamaño. Desde la página oficial accesible desde la Surface web, se puede descargar la herramienta para los distintos sistemas operativos (*Windows*, *Mac*, *Linux*, etc.).

Se crea un servidor web accesible a través de un servicio oculto Onion de Tor y se genera una URL para acceder y poder descargar los archivos. No es necesario configurar un servidor a parte o de terceros, el mismo usuario desde su ordenador mantiene y comparte temporalmente los ficheros usando un servicio oculto de Tor. El usuario que tenga que recibir los datos sólo necesita abrir la URL en un navegador Tor para descargar la información. Este tipo de herramientas son muy útiles para compartir información de forma privada como por ejemplo los periodistas con sus informadores.

4.3.13. Ricochet [43]

Es una herramienta en código abierto de mensajería instantánea que protege la privacidad eliminando los metadatos para que nadie pueda identificar a los miembros de la conversación ni lo que están hablando. No se revela la identidad ni la localización, no hay servidores intermedios, monitores, censura o hackeos.

Utiliza la red Tor para conectar a los usuarios sin utilizar servidores de mensajes, crea un servicio oculto que es utilizado como punto de encuentro entre los contactos sin revelar la dirección IP.
Desde su página oficial en la Surface web se puede descargar en su versión para *Windows*, *Mac* o *Linux*.

Esta herramienta es un experimento y como tal se avisa en su página de se ha de utilizar con precaución y evaluando los riesgos y el nivel de exposición.

5. Cibercrimen

Tras la investigación y prueba de Tor se ha detectado la cara más oscura de la red, los servicios denominados *criptomercados* o *darknet markets*, son servicios ocultos de tiendas online para comercializar productos no permitidos (drogas, medicamentos, armas, billetes falsificados, servicios poco éticos, etc.) y que utilizan *criptomonedas* (*bitcoins*, *moneros*, etc.) como métodos de pago. Estos mercados se aprovechan de la característica de anonimato que Tor ofrece.

No es posible cuantificar el número de *criptomercados* existentes actualmente en la red Tor y es posible que algunos estén tan restringidos que sólo un grupo reducido de personas tengan acceso a ellos. Además, son relativamente nuevos y existe poca documentación o investigación sobre ellos, aunque las autoridades muestran su interés y preocupación y se están realizando informes interesantes [44] que seguro irán en aumento en los próximos años.

El primer *criptomercado* y uno de los más famosos fue *Silk Road* que apareció en febrero de 2011. Su creador *Ross William Ulbricht* fue condenado a cadena perpetua por tráfico de drogas, blanqueo de dinero y fraude de identidad entre otros cargos y el site fue cerrado por el FBI en octubre de 2013. Tras este ejemplo surgieron otros mercados intentando atraer el público que había dejado *Silk Road*, entre ellos *Silk Road 2.0* o *Sheep*. Este último se cerró después de una gran acogida alegando que habían explotado una vulnerabilidad y habían robado 5400 *bitcoins* de los usuarios. Otras fuentes informaron que los propios administradores del sitio se habían quedado con los fondos.

El problema de los *criptomercados* es la falta de garantías, no se adecuan a las legislaciones vigentes, se rigen por sus propias reglas internas y por supuesto los consumidores no tienen garantías de ningún tipo, están muy expuestos a estafas, timos y fraudes.

En noviembre de 2014 tuvo lugar la operación internacional *Onymous* en la que participaron fuerzas policiales de Europa y Estados Unidos, y se cerraron varios mercados como *Silk Road 2.0*, *Cloud 9* e *Hydra*. En marzo de 2015 se cerró repentinamente el *criptomercado Evolution* y sus administradores se quedaron con 12 millones de USD de los monederos de compradores y vendedores.

De igual modo, existe la posibilidad y el temor de que un grupo terrorista puede usar la red Tor para sus comunicaciones entre los miembros y organizar así atentados, además de preverse de armas en los *criptomercados*. Teniendo en cuenta las características de la red Tor, si los terroristas toman medidas de precaución podría ser complicado que las fuerzas de seguridad pudieran seguirles la pista a nivel de red. Pueden crear un servicio oculto *.onion* y blindarlo, utilizando la opción de Tor *HiddenServiceAuthorizeClient*, así como otras medidas de cifrado del disco duro donde está alojado el servidor local y protegerlo con contraseña.

Hoy en día, los *criptomercados* protegen la identidad de compradores y vendedores, además las criptomonedas protegen la identidad en las transacciones, pero las fuerzas de seguridad no son ajenas a esta realidad, actúan, ya han cerrado potentes *criptomercados* y lo seguirán haciendo, puesto que no es posible asegurar el anonimato y la privacidad al cien por cien.

6. Vulnerabilidades de Tor

La red Tor evoluciona constantemente y se actualiza periódicamente, hay muchos desarrolladores detrás esforzándose por que la red sea segura y fiable, pero por sus propias características es susceptible de sufrir ataques que pongan en peligro el anonimato de los usuarios. Los ataques pueden ser activos o pasivos y pueden producirse desde dentro de la red o desde fuera, dependiendo de la posición del atacante. A continuación, se describen los ataques más relevantes que ha sufrido o puede llegar a sufrir Tor.

6.1. Vulnerabilidades del propio navegador

Tor Browser está basado en el navegador *Mozilla Firefox*, pero con modificaciones y tanto **el propio navegador como las extensiones pueden presentar vulnerabilidades** que un atacante puede aprovechar para des anonimizar a los usuarios.

Tor Browser viene preconfigurado con la ubicación de cada autoridad de directorio, por lo que el usuario no ha de hacer nada en este sentido, facilitando la usabilidad del software. Sin embargo, este enfoque genera una vulnerabilidad, si un usuario descargara un ejecutable de *Tor Browser* modificado, podría estar configurado con autoridades de directorio falsas y conectarse a nodos controlados por la *NSA*, por ejemplo. Por ello, es recomendable descargar *Tor Browser* desde fuentes confiables y comprobar la firma digital *PGP* del archivo.

La página oficial de Tor dispone de información e instrucciones [45] para verificar que el paquete descargado para instalar el navegador Tor es el oficial y no uno manipulado.

6.2. Ataque Sybil

Consiste en aprovechar la característica de Tor de que **cualquiera puede desplegar un nodo** en la red y de hecho existen nodos en multitud de países distribuidos por el planeta. Un atacante puede aprovecharlo para desplegar miles de nodos y **hacerse con el control de la red**, en esto consiste el ataque *sybil*. Si se consigue controlar la mayor cantidad posible de nodos de la red, ya que no es infinita, se participará con mayor probabilidad en más circuitos como nodo de entrada, intermedio o de salida. El atacante tiene el poder de des anonimizar a los usuarios y puede servir como maniobra previa a otro tipo de ataque que altera la red y por tanto la confianza de los usuarios en ella.

Para protegerse de este tipo de ataques, la red Tor dispone de un script para comprobar si hay aumentos repentinos y anormales de nuevos nodos [46].

6.3. Ataque Predecesor

El objetivo de este tipo de ataques es identificar a los usuarios de la red mediante la **reconstrucción de circuitos**. Para ello se crean unos o más nodos con la intención de realizar seguimientos de las conexiones y contabilizar las veces que un nodo aparece en un circuito. Cada vez que un cliente reconstruye un circuito, esto ocurre cada diez minutos, se vuelve a conectar a otros nodos, por lo que el atacante identifica al usuario que tenderá a conectarse más veces que cualquier otro nodo. El nodo que aparece más veces tiene más probabilidad de ser un nodo cliente. Si el atacante controla gran cantidad de nodos, puede hacerlos fallar de forma deliberada [47] para hacer que los clientes se reconecten de manera continua y aumentar así el éxito del ataque.

6.4. Ataque de Correlación de Tráfico

Este ataque tiene como objetivo **establecer una relación**, con alta probabilidad de ser correcta, **entre un cliente Tor y el servidor final**, es decir, los dos extremos de la conexión. El atacante tiene que controlar el nodo de entrada y el nodo de salida del circuito donde está conectado el cliente e intentar establecer una relación objetiva entre los datos entrantes y los datos salientes analizando los paquetes, por ejemplo, el tamaño o su frecuencia.

6.5. Ataque Reconstrucción Circuital

Este ataque es muy complejo y complicado de llevar a cabo ya que se basa en **controlar los tres nodos de una conexión**. El atacante puede llegar a conocer tanto al cliente como al servidor de destino mediante una reconstrucción. La NSA estaba estudiando cómo llevar a cabo este ataque, así se refleja en uno de los documentos filtrados por Snowden [48].

6.6. Ataque Round-Trip Travel Time

Consiste en un ataque desde el servidor de destino, el extremo final de la conexión y desde donde se intenta **forzar al cliente a realizar un gran número de conexiones** o redirecciones para analizar la frecuencia de tiempo de ida y vuelta. De esta manera se puede deducir que las conexiones provienen de una misma ruta si las frecuencias son similares.

6.7. Ataque Sniffer

Consiste en que los nodos de salida realicen ataques *man-in-the-middle* para **leer la información enviada por el cliente**. Esto es posible sobre todo en conexiones no cifradas, que no utilizan el protocolo HTTPS, aunque existen numerosas herramientas para atacan conexiones cifradas tales como *SSLStrip*. Estos nodos maliciosos al final acaban siendo detectados y catalogados con la bandera *BadExit* para que no se continúen utilizando.

6.8. Ataque Raptor

Este tipo de ataques se basan en **hacerse con el control de un nodo autónomo de la red Tor** y aplicar ciertas técnicas para comprometer las conexiones y el tráfico que pase a través de él y llegar a obtener la identidad de los usuarios, así como el contenido de los paquetes que se envían. Existen cuatro posibles situaciones dentro de este ataque.

- Un atacante puede obtener los nodos de entrada y salida de las conexiones y conseguir la dirección IP real del usuario, pero no la información de los paquetes transmitidos.
- El atacante puede monitorizar el tráfico de entrada y los paquetes TCP ACK entre cliente y servidor, obteniendo así la ruta completa, aunque cambia cada poco tiempo, lo que le sirve para identificar al emisor y el contenido de los paquetes.
- Se puede monitorizar el tráfico desde el nodo malicioso, identificar al nodo de salida y controlar el tráfico desde este nodo al servidor de destino, así como los paquetes ACK, pudiendo observar toda la información de los mensajes intercambiados entre cliente y servidor.
- El atacante también puede controlar el tráfico TCP ACK identificando la dirección IP del cliente y del servidor desde el nodo malicioso.

Estos ataques se pueden detectar monitorizando posibles ataques de control de nodos de la red Tor y controlando la ruta de datos (con *Traceroute* por ejemplo) para identificar anomalías en los datos.

6.9. Censura Global

Tor puede ser bloqueado mundialmente si todos los gobiernos obligan a los proveedores de servicios de internet a **bloquear los nodos de la red Tor** cuyo listado de IPs está publicado y por tanto son conocidos. Con esta medida se impediría el funcionamiento de Tor a la vez que se podría realizar una inspección profunda de paquetes.

Como se ha visto anteriormente, Tor dispone de medidas para evitar la censura, los puentes (bridges), pero no se podría absorber todo el tráfico si la censura fuera mundial, por lo tanto, acabarían con Tor.

Otro método de censura sería que los *webmasters* bloquearan las conexiones de los nodos de salida, bloqueando las IPs de la lista pública de nodos de salida [49], de manera que los usuarios Tor no puedan conectarse a los sitios web.

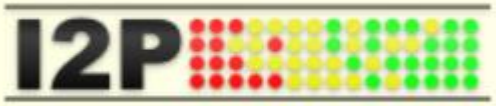
A la vista de lo sencillo que puede resultar acabar con la red Tor, sus administradores no ocultan el listado de direcciones IP de los nodos en un intento de **concienciar sobre la importancia de la privacidad y el anonimato en internet**, objetivo por el cual se creó Tor. Por esto es importante dar a conocer a los usuarios de internet la realidad sobre Tor y sus ventajas.

7. Alternativas a Tor

El navegador Tor es el más popular y el más utilizado, pero a continuación se describen las principales alternativas para navegar de forma privada y más segura.

7.1. I2P [5]

También conocida como *Proyecto invisible de internet* permite construir, desplegar y mantener una red para una comunicación segura y anónima ya que cifra el tráfico de la



red creando una capa dentro de UDP y TCP/IP mediante claves privadas y públicas. Se puede administrar el balance entre anonimato, fiabilidad, ancho de banda y latencia. Usa tecnología *DarkNet* para cifrar los datos a través de capas y está diseñada para permitir a los pares comunicarse unos con otros anónimamente ambas partes, el que envía el mensaje y el que lo recibe, no son identificables entre ellos y tampoco por terceras partes.

En I2P para conectar a cada usuario con el destino donde quiere navegar se utilizan túneles de entrada y salida. El funcionamiento sería tal y como se muestra en la ilustración 30. Cuando el cliente A se conecta a I2P se escogen dos nodos (Nodo B y Nodo C) y se crea un túnel de salida y se escogen otros dos nodos para crear un túnel de entrada (Nodo D y Nodo E). Cuando el cliente A envía una petición la recibe el nodo B que a su vez se la envía al nodo C. Este nodo le enviará la petición al nodo de entrada del servidor de destino que a su vez se lo reenviará al nodo del final del túnel de entrada del servidor que a su vez se lo hará llegar al servidor de destino.

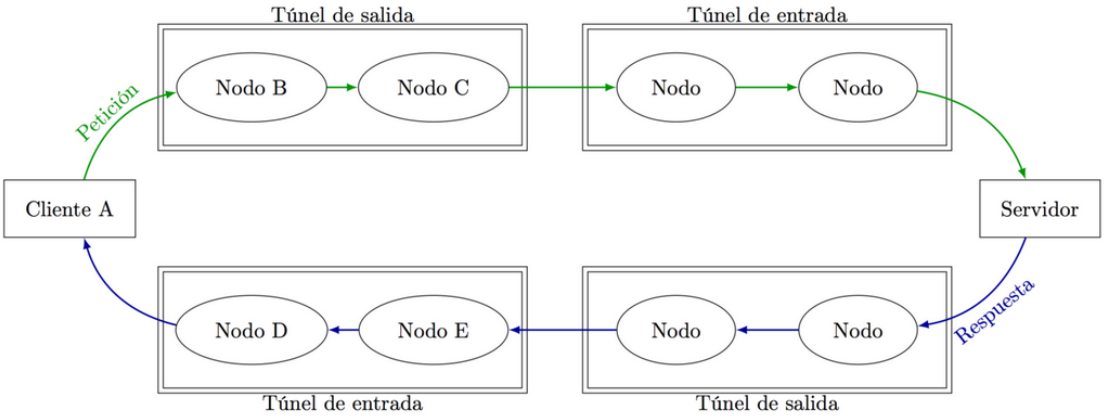


Ilustración 30 Túneles en I2P

Los clientes no necesitan un túnel para cada conexión que quieren realizar, sino que pueden utilizar el mismo túnel para varias conexiones y pueden tener varios túneles en paralelo. Además, los servidores pueden responder a todas las peticiones por el mismo túnel de salida. Los túneles son unidireccionales y aportan mayor privacidad que los nodos bidireccionales como (los circuitos de Tor), ya que si se realiza un análisis del tráfico se necesitan el doble de nodos comprometidos o el doble del tiempo de monitorización.

La duración de los túneles es limitada (10 minutos) y cada túnel pertenece a un único usuario por lo que se pueden aplicar técnicas de evasión, como añadir retrasos intencionados en cada punto del túnel, evitando así el análisis del tráfico.

I2P está disponible de forma gratuita para *Windows*, *Mac OS X*, *Linux* y *Android*.

7.1.1. Comparativa: I2P vs Tor

Se ha realizado una tabla para comparar las características y aspectos relevantes entre I2P y Tor.

Aspecto	I2P	TOR
Tipo de red	Distribuida y auto gestionada	Modelo de confianza con directorios autoritativos
Capacidad de red	*Inproxy*	*Inproxy* y *Outproxy*
Modo conexión	Un mismo túnel de salida para enviar a todos los destinos	Un circuito para cada conexión de destino
Rapidez conexión	Mayor rapidez de conexión gracias al uso del mismo túnel y de túneles paralelos	Menor rapidez porque se necesita un circuito para cada conexión y mayor complejidad en montaje de servicio oculto
Rendimiento	Menos optimizado, por ejemplo, en los túneles de salida	Más optimizado, por ejemplo, en el tráfico de nodos de salida
Consumo memoria	Mayor, depende del número de túneles abiertos, conexiones, transferencias, etc.	Menor, los nodos consumen cantidad limitada de recursos y no afecta a la máquina donde se ejecutan
Privacidad	Mayor privacidad por el uso de túneles unidireccionales	Menor privacidad, los nodos son bidireccionales
Modelo intercambios de datos	Descentralizada. Más difícil detectar nodos malignos	Centralizada. Más facilidad de detectar nodos malignos
Servicios internos	Más extenso, eficiente y robusto. Admite aplicaciones como *BitTorrents* y está optimizado para compartir ficheros	Menos extenso, eficiente y robusto. Los *Hidden Services* son menos eficientes y enfocados a anonimato básico basado en navegación
Facilidad perpetrar ataques	Menor, es necesario atacar un mayor número de nodos	Mayor, solo es necesario atacar unos pocos directorios autoritativos
Probabilidad éxito ataque análisis de tráfico	Menor por el uso de túneles unidireccionales cada 10 minutos y su pertenencia al usuario	Algo mayor, por usar circuitos cuya renovación depende de los directorios autoritativos
Probabilidad éxito ataque denegación servicio	Mayor	Menor
Cantidad de usuarios y recursos disponibles	Menor	Mayor
Resistencia a la censura	Menor	Mayor
Tipo de protocolo soportado	UPD, TCP, ICMP	TCP
Lenguaje programación	Java	C

7.2. FreeNet [6]

Se trata de una plataforma de seguridad *peer-to-peer* de código abierto, una red de distribución de información descentralizada y resistente a la censura, que permite navegar por Internet de forma anónima y segura. Compatible con las tecnologías *OpenNet* y *DarkNet*. No dispone de un servidor central por lo que disminuye la probabilidad de ser pirateado y los propios responsables del mantenimiento de Freenet no tienen acceso a ninguna información de los usuarios. Su objetivo es proporcionar libertad de expresión a través de las redes de pares P2P no estructurada de nodos no jerarquizados para una fuerte protección del anonimato. La información almacenada se encripta antes de llegar a los servidores por lo que no puede ser leída por *trackers*.

Cuando dos nodos comparten un archivo o actualizan una página, el documento queda insertado en la red, por lo que una vez se ha realizado la inserción ya no es necesario que el nodo siga operativo para poder acceder al contenido. Freenet es como una gran caché que se distribuye a través de los nodos que pueden funcionar como nodos finales o como intermedios de enrutamiento. Cada nodo aloja documentos asociados a claves y una tabla de enrutamiento que asocia los nodos con un historial. No hay conexiones directas ni reconocimiento de nodos de esta manera los usuarios consiguen un alto nivel de anonimato.

Desde la página oficial se puede descargar el ejecutable o instalador para *Windows*, *Mac OS X* y *Linux*.

7.2.1. Comparativa: FreeNet vs Tor

Se ha realizado una tabla para comparar las características y aspectos relevantes entre Freenet y Tor.

Aspecto	FreeNet	TOR
Tipo de red	Distribuida	Modelo de confianza con directorios autoritativos
Capacidad de red	*Inproxy*	*Inproxy* y *Outproxy*
Rapidez conexión	Menor, se trata de una red lenta	Mayor, el servicio es más eficiente y con mayor entropía
Privacidad	Menor privacidad por almacenar ficheros de otros usuarios en el sistema de ficheros local en la *Data Store* con muy poco control sobre ella	Mayor privacidad, no almacena ningún fichero en el sistema archivos local sin autorización del usuario
Usabilidad	Menor, utilizando un *FProxy*, *TCMI* o a través de *API*	Mayor, como navegador o desde una aplicación externa enrutando las peticiones

Modelo intercambios de datos	Descentralizada. Más difícil detectar nodos malignos	Centralizada. Más facilidad de detectar nodos malignos
Servicios internos	Bastantes más posibilidades, al ser como una base de datos distribuida donde cada nodo almacena información de otros usuarios	Menos extenso, eficiente y robusto. Los *Hidden Services* son menos eficientes y enfocados a anonimato básico basado en navegación
Seguridad	Mayor, existen menos vectores de ataque y por ser menos popular	Menor, número de amenazas más extenso dada su popularidad. En especial problemas de seguridad en nodos de salida comprometidos
Facilidad perpetrar ataques	Menor, por ser red distribuida es necesario atacar un número de sistemas en constante aumento	Mayor, por estar centralizado, solo es necesario atacar unos pocos directorios autoritativos
Cantidad de usuarios y recursos disponibles	Menor	Mayor
Tipo de protocolo soportado	UPD, TCP, ICMP	TCP

7.2.2. Comparativa: I2P vs FreeNet

De la misma manera se ha realizado una tabla para comparar I2P con Freenet.

Aspecto	**I2P**	**FreeNet**
Tipo de red	Distribuida	Distribuida
Capacidad de red	*Inproxy*	*Inproxy*
Rapidez conexión	Mayor	Menor, por la cantidad de *peers* a los que se conecta un nodo
Rendimiento	Más óptimo	Menor, por ser una red lenta
Disponibilidad	Menor	Mayor, un nodo puede ser apagado y el servicio continúa disponible (por almacenar información en los *Data Stores*)
Integración	Mayor facilidad para crear túneles y que otras aplicaciones puedan usar I2P	Menor integración con otras aplicaciones
Servicios internos	Tiene capacidad de ofrecer casi cualquier servicio de un nodo, SSH, Telnet, servidores web, etc.	Menor oferta de servicios
Niveles seguridad en conexión	Menor, solo se puede decidir qué nodos restringir	Mayor, permite segmentación en grupos de amigos y crear pequeñas

		darknets, controlando mejor las *peers* de la instancia
Probabilidad éxito en ataques	Menor por el uso de túneles unidireccionales cada 10 minutos y su pertenencia al usuario	Mayor
Resistencia a la censura	Menor	Mayor gracias al tipo de modelo distribuido con *Data Stores*
Sistema de resolución de nombres	Menos completo y seguro, sólo **.i2p*	Más completo y seguro ya que todos los contenidos son claves resueltas internamente
Documentación existente	Mayor	Menor
Tipo de protocolo soportado	UPD, TCP, ICMP	UPD, TCP, ICMP

7.3. Disconnect [50]

Es un complemento de Tor que desconecta al usuario de los sitios que le intentan rastrear y bloquea el site. Dispone de una opción gratuita de protección para un navegador con el bloqueador de seguimiento y la posibilidad de realizar búsquedas de forma privada. El siguiente nivel de protección es de pago y permite bloquear el seguimiento y el malware de todo el dispositivo, la conexión a internet será un 44% más rápida, el ancho de banda necesario para navegar será un 39% menor, se ahorra batería del dispositivo. En la opción *Premium* se oculta la dirección IP tras un VPN de la compañía. Está disponible para los navegadores *Chrome*, *Firefox*, *Safari*, *Opera* y *Samsung Browser* en *Windows*, *iOS* y *Android*.

7.4. Whonix [51]

Es un sistema operativo gratuito (basado en *Debian*), actualmente en desarrollo, diseñado para funcionar en una máquina virtual emparejado con Tor. Permite navegar de forma privada ocultando la dirección IP mientras se navega utilizando una red única conocida como *Whonix-Workstation* que se ejecuta en el sistema privado. Tiene dos interfaces de red virtuales, una se conecta a través de NAT y conecta con la red Tor y otra acoplada con una LAN virtual. Disponible para *Windows*, *Linux*, *OS X* y *Qubes*.

7.5. Yandex [52]

Se trata de un navegador gratuito bastante popular que ofrece anonimato para navegar por internet. Impide cualquier tipo de seguimiento y dispone de una característica adicional para escanear archivos en busca de malware. Es compatible con *Windows*, *Mac*, *Linux*, *Android* y *iOS*. Cuenta con plugin para desactivar *flash*, *ad-blockers* y los que protegen de sitios no seguros. También tiene protección contra *DNS spoofing* que encripta todos los datos y previene ataques de corrupción de cache.

7.6. Proyectos obsoletos

Otras alternativas menos activas o que ya han sido abandonadas son *Mixminion* [53], *Mixmaster* [54] y *Free Haven* [55]. También hay una alternativa *Dissent* [56] que se encuentra en su primera etapa y sirve para la comunicación anónima entre grupos.

8. Conclusiones

Tras el paseo por la Deep web y el análisis de la información recopilada, se puede extraer algunas conclusiones que se describen a continuación.

La red Tor se creó con el **objetivo de ofrecer a los usuarios anonimato, privacidad y seguridad en internet** y que no se tiene cuando se navega de manera normal por la red ya que puede ser y muchas veces es controlada de manera que se sabe lo que el usuario hace por la red, se le relaciona y se crean perfiles (la mayoría de las veces con fines comerciales) además de no saber exactamente qué datos personales se recogen de los usuarios ni hasta dónde son enviados, compartidos, cedidos o vendidos. Pese a que con Tor se anonimiza la navegación y permite que nadie pueda espiar lo que se está haciendo en internet es necesario remarcar que, como todo, **existen vulnerabilidades** y por tanto **la privacidad y el anonimato no está asegurados al cien por cien**.

Pese a que hay más alternativas, la **red Tor es actualmente la más conocida y extendida**. Valorar si Tor es bueno o malo para la sociedad implica ver ambas caras, como se ha intentado mostrar en este trabajo y todo depende del uso que las personas hagan de las características y funcionalidades de Tor. Se puede usar para hacer el bien y ayudar a la sociedad o por el contrario se pueden aprovechar para cometer actividades delictivas, en contra de la sociedad y que dañan la imagen de toda la red.

Tor permite **en los países donde impera la censura** que los usuarios puedan conectarse a internet a través de los bridges, pudiendo ejercer su derecho de libre expresión, así como **compartir información** o denunciar hechos que van en contra de los derechos humanos. Los servicios ocultos de Tor permiten una comunicación segura para determinados sectores como el periodismo donde la privacidad entre periodista y fuente es básica.

Por otro lado, **Tor es aprovechado por ciberdelincuentes** que hacen uso de los servicios ocultos, criptomonedas y el cifrado para sus actividades delictivas. También conviene remarcar que **se pueden encontrar contenidos parecidos utilizando Google** navegando por la Surface web por lo que **el cibercrimen no solo se encuentra en la Deep web** y es necesario desmitificar esta idea. También hay disponibles contenidos ilegales que no están indexados por los buscadores, pero son accesibles con un navegador normal luego no son servicios ocultos de Tor y son accesibles desde la Surface web, (no están en la Dark net). Ejemplos son anuncios en páginas de compra venta para la venta de drogas, grupos de Facebook para intercambio de material pornográfico infantil [57]. En Instagram se combate a diario contra hashtags y perfiles creados para la venta de drogas [58]. Así mismo se pueden encontrar páginas en la Surface web anunciando servicios (como asesinos a sueldo [59]) aunque en la mayoría de los casos se trata de

estafadores. Con el terrorismo ocurre lo mismo, no es difícil encontrar contenidos, como el vídeo de un asesinato retransmitido a través de Facebook Live [60].

Una **censura global a Tor supondría un paso atrás en la libertad** y privacidad de los usuarios. Un aumento de la vigilancia y medidas opresivas que van en contra del principio de libertad de expresión y de libre albedrío.

El uso que se le dé a Tor tanto si es bueno como malo depende de las personas que lo utilizan y, por tanto, **Tor en sí no es el problema**. En la Dark web es posible encontrar contenidos ilegales de una manera más sencilla que en la Surface web, pero eso no implica que toda la red se dedique en su mayoría a los *criptomercados* ni mucho menos, si no que este tipo de contenidos existe en todo internet. No todo el mundo sabe acceder a la Dark net por lo que interesa que tratan de estar en la Surface web para llegar al máximo número de personas. El mensaje que se debería enviar a los usuarios es que se debería educar más en hacer el bien, en crear y utilizar las herramientas, como Tor, en acciones que ayuden a los demás y no en beneficio propio.

En este trabajo final de máster se ha seguido el plan de trabajo establecido al inicio y **se han cubierto los objetivos marcados**, se ha realizado una introducción a la Deep web, se ha descrito la red Tor su estructura y funcionalidades. Se ha realizado una instalación y prueba del navegador Tor para descubrir qué tipo de información y servicios ocultos se podían encontrar, así mismo se han analizado respecto al tema del cibercrimen y cómo se lucha contra la ciberdelincuencia. Además, se han descrito algunas de las principales vulnerabilidades que afectan a la red Tor y posibles alternativas como I2P o Freenet. Por último, se han plasmado las conclusiones del trabajo.

Durante la realización del trabajo final de **máster no se ha producido ninguno de los riesgos planteados ni otras situaciones que hayan afectado a la planificación temporal**. Se considera que se han cumplido los objetivos marcados para este trabajo, se han llevado a cabo las tareas programadas, se ha seguido la metodología y se han cubierto las fases según el plan previsto y a tiempo.

Como **líneas de trabajo futuro** se propone la instalación y prueba de I2P y Freenet para comprobar de primera mano las diferencias con Tor y analizar de un modo más profundo las características y funcionalidades de cada una, así como los servicios que se pueden encontrar con dichas redes. Además, se propone la creación de un servicio oculto en la red Tor para demostrar lo relativamente fácil que es crear contenido en dicha red.

Referencias

[1] «IANA Sitio Oficial,» [En línea]. Available: https://www.iana.org/. [Último acceso: marzo 2018].

[2] «Emercoin Sitio Oficial,» [En línea]. Available: https://emercoin.com/. [Último acceso: marzo 2018].

[3] «Namecoin Sitio Oficial,» [En línea]. Available: https://namecoin.org/. [Último acceso: marzo 2018].

[4] «Sitio oficial Tor,» [En línea]. Available: https://www.torproject.org/. [Último acceso: mayo 2018].

[5] «I2P vs Tor,» [En línea]. Available: https://geti2p.net/es/comparison/tor. [Último acceso: marzo 2018].

[6] «Sitio oficial Freenet,» [En línea]. Available: https://freenetproject.org/. [Último acceso: marzo 2018].

[7] «Mapa de la Dark web,» [En línea]. Available: https://www.hyperiongray.com/dark-web-map/. [Último acceso: abril 2018].

[8] «Servicios onion activos,» [En línea]. Available: https://metrics.torproject.org/hidserv-dir-onions-seen.html. [Último acceso: abril 2018].

[9] «US Naval Research,» [En línea]. Available: https://www.nrl.navy.mil/. [Último acceso: marzo 2018].

[10] «Electronic Frontier Foundation,» [En línea]. Available: http://www.eff.org/. [Último acceso: marzo 2018].

[11] «Torflow software,» [En línea]. Available: https://torflow.uncharted.software/. [Último acceso: marzo 2018].

[12] «Tor and bank fraud,» [En línea]. Available: http://krebsonsecurity.com/2014/12/treasury-dept-tor-a-big-source-of-bank-fraud/. [Último acceso: marzo 2018].

[13] «Operación onymous,» [En línea]. Available: https://www.certsi.es/technologyForecastingSearch/CERT/Alerta_Temprana/Bitacora_de_ciberseguridad/operacion_onymous. [Último acceso: marzo 2018].

[14] «Vulnerabilidades Tor,» [En línea]. Available: https://www.certsi.es/alerta-temprana/bitacora-ciberseguridad/vulnerabilidad-tor-capaz-revelar-ip-los-usuarios. [Último acceso: marzo 2018].

[15] «Direcciones puente Tor,» [En línea]. Available: https://bridges.torproject.org/bridges. [Último acceso: abril 2018].

[16] «Relay Search Tor Service,» [En línea]. Available: https://metrics.torproject.org/rs.html#toprelays. [Último acceso: abril 2018].

[17] «Autoridades directorio Tor,» [En línea]. Available: https://metrics.torproject.org/rs.html#search/flag:Authority. [Último acceso: abril 2018].

[18] «Descriptores de Tor,» [En línea]. Available: https://collector.torproject.org/. [Último acceso: abril 2018].

[19] «Servicios Tor,» [En línea]. Available: https://metrics.torproject.org/services.html. [Último acceso: abril 2018].

[20] «ExoneraTor Service Tor,» [En línea]. Available: https://exonerator.torproject.org/. [Último acceso: abril 2018].

[21] «Consensus Health Service Tor,» [En línea]. Available: https://consensus-health.torproject.org/. [Último acceso: abril 2018].

[22] «Tor Map Service,» [En línea]. Available: https://tormap.void.gr/. [Último acceso: abril 2018].

[23] «OrNetStats Tor Service,» [En línea]. Available: https://nusenu.github.io/OrNetStats/. [Último acceso: abril 2018].

[24] «DuckDuckGo Tor Service,» [En línea]. Available: https://duckduckgo.com/. [Último acceso: abril 2018].

[25] «Onionite Tor Service,» [En línea]. Available: https://onionite.now.sh/. [Último acceso: abril 2018].

[26] «Consensus Issues Tor Services,» [En línea]. Available: https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-consensus-health. [Último acceso: abril 2018].

[27] «OII's anomaly detection system Tor Service,» [En línea]. Available: http://lists.infolabe.net/lists/listinfo/infolabe-anomalies. [Último acceso: abril 2018].

[28] «DuckDuckGo servicio oculto,» [En línea]. Available: https://3g2upl4pq6kufc4m.onion/. [Último acceso: abril 2018].

[29] «The Hidden Wiki,» [En línea]. Available: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page. [Último acceso: abril 2018].

[30] «Cebolla Chan 3.0,» [En línea]. Available: http://s6cco2jylmxqcdeh.onion/w/. [Último acceso: abril 2018].

[31] «Cebolla Chan 5.0,» [En línea]. Available: http://cebollachan.foro.pro/. [Último acceso: abril 2018].

[32] «Cebolla Board,» [En línea]. Available: http://vxx2tfzprjm56eka.onion/. [Último acceso: abril 2018].

[33] «Chat with strangers,» [En línea]. Available: http://tetatl6umgbmtv27.onion/. [Último acceso: abril 2018].

[34] «Mail2Tor email service,» [En línea]. Available: http://mail2tor2zyjdctd.onion/. [Último acceso: abril 2018].

[35] «Mail2Tor,» [En línea]. Available: http://mail2tor.com/. [Último acceso: abril 2018].

[36] «Críptica Blog servicio oculto,» [En línea]. Available: http://cripticavraowaqb.onion/. [Último acceso: abril 2018].

[37] «Mike Tigas Blog Servicio Oculto,» [En línea]. Available: http://tigas3l7uusztiqu.onion/blog/. [Último acceso: abril 2018].

[38] «Deep Web Radio Servicio oculto,» [En línea]. Available: http://76qugh5bey5gum7l.onion/. [Último acceso: mayo 2018].

[39] «Imperial Library Servicio oculto,» [En línea]. Available: http://xfmro77i3lixucja.onion/. [Último acceso: mayo 2018].

[40] «Hidden Wallet Servicio oculto,» [En línea]. Available: http://nql7pv7k32nnqor2.onion/. [Último acceso: mayo 2018].

[41] «TorShops Servicio oculto,» [En línea]. Available: http://shopsat2dotfotbs.onion/. [Último acceso: mayo 2018].

[42] «OnionShare,» [En línea]. Available: https://onionshare.org/. [Último acceso: abril 2018].

[43] «Ricochet,» [En línea]. Available: https://ricochet.im/. [Último acceso: abril 2018].

[44] «Informe sobre Criptomercados,» [En línea]. Available: http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf. [Último acceso: mayo 2018].

[45] «Verificar paquete instalador Tor,» [En línea]. Available: https://www.torproject.org/docs/verifying-signatures.html.en . [Último acceso: mayo 2018].

[46] «Script anti Sybil,» [En línea]. Available: https://gitweb.torproject.org/doctor.git/tree/sybil_checker.py. [Último acceso: mayo 2018].

[47] «A node failure Paper,» [En línea]. Available: https://pdfs.semanticscholar.org/1a37/224ed0e5ce36c4b987a8f169a52ca8745aa0.pdf. [Último acceso: mayo 2018].

[48] «Documento filtrado Snowden,» [En línea]. Available: https://search.edwardsnowden.com/docs/TorStinks2013-10-04_nsadocs_snowden_doc. [Último acceso: mayo 2018].

[49] «Direcciones nodos salida Tor,» [En línea]. Available: https://check.torproject.org/exit-addresses. [Último acceso: mayo 2018].

[50] «Disconnect - Complemento Tor Sitio Oficial,» [En línea]. Available: https://disconnect.me/. [Último acceso: mayo 2018].

[51] «Navegador Whonix Sitio Oficial,» [En línea]. Available: https://www.whonix.org/. [Último acceso: mayo 2018].

[52] «Navegador Yandex,» [En línea]. Available: https://browser.yandex.com/. [Último acceso: mayo 2018].

[53] «Mixminion Sitio oficial,» [En línea]. Available: http://mixminion.net/. [Último acceso: marzo 2018].

[54] «Mixmaster Sitio oficial,» [En línea]. Available: http://mixmaster.sourceforge.net/. [Último acceso: marzo 2018].

[55] «FreeHaven Sitio oficial,» [En línea]. Available: http://www.freehaven.net/. [Último acceso: marzo 2018].

[56] «Dissent Sitio oficial,» [En línea]. Available: http://dedis.cs.yale.edu/dissent/. [Último acceso: marzo 2018].

[57] «Noticia grupo Facebook pornografía infantil,» [En línea]. Available: http://www.lavanguardia.com/sucesos/20170307/42513461545/pornografia-infantil-elrubius-facebook-grupo-criaturitas-del-senorrr.html. [Último acceso: mayo 2018].

[58] «Venta drogas en Instagram,» [En línea]. Available: https://drugabuse.com/featured/instagram-drug-dealers/. [Último acceso: mayo 2018].

[59] «Sitio hire a killer,» [En línea]. Available: http://www.hire-a-killer.com/. [Último acceso: mayo 2018].

[60] «Noticia retransmisión asesinato Facebook,» [En línea]. Available: https://www.elperiodico.com/es/internacional/20160614/el-terrorista-retransmitio-el-asesinato-de-los-dos-policias-en-francia-por-facebook-live-5204541. [Último acceso: mayo 2018].

[61] «Anonimato y cibercrimen,» [En línea]. Available: http://fiadi.org/deep-web-anonimato-y-cibercrimen/. [Último acceso: marzo 2018].

[62] «Cibercrimen en la Deep web,» [En línea]. Available: https://cec.mpba.gov.ar/sites/all/themes/cec/cibercrimen/160612_Deep_Web.pdf. [Último acceso: marzo 2018].

[63] «Cibercriminales y bitcoins,» [En línea]. Available: https://www.muyseguridad.net/2018/01/31/cibercriminales-proxy-tor-robar-bitcoins-cibercriminales/. [Último acceso: marzo 2018].

[64] «Conociendo la Deep web,» [En línea]. Available: https://www.vix.com/es/btg/tech/55817/como-entrar-a-la-deep-web-y-que-cosas-necesitas-saber-al-respecto. [Último acceso: marzo 2018].

[65] «CyberCamp 2016,» [En línea]. Available: https://www.youtube.com/watch?v=PYu9Zkwmhw0. [Último acceso: marzo 2018].

[66] «Inmenso océano Deep web,» [En línea]. Available: https://elpais.com/diario/2005/10/20/ciberpais/1129772426_850215.html. [Último acceso: marzo 2018].

[67] «Internet profunda mejor que Deep web,» [En línea]. Available: https://www.fundeu.es/recomendacion/internet-profunda-mejor-que-deep-web/. [Último acceso: marzo 2018].

[68] «Mitos y realidades Deep web,» [En línea]. Available: http://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-internet-profunda. [Último acceso: marzo 2018].

[69] «Primeros pasos Tor,» [En línea]. Available: http://www.eldiario.es/turing/Primeros-pasos-navegacion-segura-Tor_0_126337372.html. [Último acceso: marzo 2018].

[70] «Redes anonimas CERTSI,» [En línea]. Available: https://www.certsi.es/blog/redes-anonimas-mas-alla-de-tor. [Último acceso: marzo 2018].

[71] «Tor en Android,» [En línea]. Available: https://www.xatakandroid.com/seguridad/como-conectarse-y-usar-tor-en-android. [Último acceso: marzo 2018].

[72] «Tor en Windows,» [En línea]. Available: https://ssd.eff.org/es/module/c%C3%B3mo-usar-tor-en-windows. [Último acceso: marzo 2018].

[73] «Tor paso a paso,» [En línea]. Available: https://es.gizmodo.com/como-empezar-a-utilizar-el-navegador-anonimo-tor-paso-1680401465. [Último acceso: marzo 2018].

[74] «Tor servicios ocultos CERTSI,» [En línea]. Available: https://www.certsi.es/blog/tor-servicios-ocultos-desanonimizacion. [Último acceso: marzo 2018].

[75] «Tor y cibercriminales,» [En línea]. Available: https://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/. [Último acceso: marzo 2018].

[76] «Un vistazo a la Deep web,» [En línea]. Available: https://internautas21.com/deep-web-entrar-links-imagenes-videos/. [Último acceso: marzo 2018].

[77] «Valor datos en Dark Web,» [En línea]. Available: https://omicrono.elespanol.com/2018/03/cuanto-cuesta-una-cuenta-en-la-dark-web/. [Último acceso: marzo 2018].

[78] «Visitando Deep web,» [En línea]. Available: https://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado. [Último acceso: marzo 2018].

[79] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org. [Último acceso: marzo 2018].

[80] «Licencias de obras,» [En línea]. Available: http://www.fundacionmelior.org/content/grafica/copyright-vs-creative-commons. [Último acceso: abril 2018].

[81] «Licencia Creative Commons,» [En línea]. Available: https://creativecommons.org/licenses/by-nc-nd/3.0/es/. [Último acceso: abril 2018].