Red de anonimización TOR y cibermercados negros

Estudiante: Xavier Lapuente Salinas

Directora del TFM: Angela María García Valdés

MISTIC – Máster interuniversitario en Seguridad de las TIC

01/06/2018

Resumen

En este documento se muestra un estudio sobre los principios básicos de operación de las redes de anonimización y los mercados negros de la red TOR. Para ello, se explica cómo se proporciona la anonimización a los usuarios y a los servicios de esta red y posteriormente se muestran los principales componentes que forman esta red, sus funciones y como operan. Finalmente se explican algunas técnicas de desanonimización de usuarios y servicios de la red TOR y su aplicación práctica.

En este documento se presenta una descripción de los mercados negros de la red TOR. En esta descripción se incluyen los mercados negros más populares que han existido en la red TOR y una breve historia de ellos. También se analizan los mercados negros más populares que existen actualmente, accediendo a ellos y mostrando el contenido que se puede encontrar en ellos. Posteriormente se describen las actividades ilegales que se realizan en estos mercados y se presentan las criptomonedas, sus características y su relación la red TOR y los mercados negros.

Finalmente se presentan las acciones legales que aplican a la navegación usando la red TOR y a las actividades ilegales que se han analizado anteriormente. Al final del documento se presentan las conclusiones y la bibliografía.

Abstract

In this document we present a research about the main operational ways of the anonymization networks and the TOR network black markets. It is explained how the anonymization is given to the users and services of the network and there are shown the main components of this network, its functions and how they operate. Finally, we explain some ways to break the anonymity of the users and services of the TOR network.

In this document it is presented a description of the TOR network black markets. In this description there will be shown the most popular black markets that have ever existed in the TOR network and their history. There also shown the most popular black markets that nowadays are working by accessing to them and showing the content found there. Later, we will list and describe the cryptocurrencies, their features and their relationship with the TOR network and the black markets.

Finally, there are presented the main illegal actions that are done using the TOR network and the illegal activities analyzed before. At the end of the document there are exposed the conclusions and the information sources used during this research.

Tabla de contenidos

1- Introducción

Actualmente Internet se utiliza para transmitir información en diferentes ámbitos. Sus usos más frecuentes son las comunicaciones personales, laborales, para consultar información o para difundir información de forma masiva, entro otros usos. Un problema que existe al usar Internet para establecer dichas comunicaciones, es que estas son trazables y es posible identificar a los usuarios que han generado dichas comunicaciones.

La red TOR (The Onion Router) es un proyecto que tiene como principal objetivo implementar una red de comunicaciones que no revele la identidad de sus usuarios. Para conseguir este objetivo, existen diferentes componentes en la red que se encargan de ocultar la identidad de los usuarios finales que realizan las comunicaciones.

La red TOR permite a los usuarios que la utilizan mantener la privacidad en la navegación por Internet ocultando la dirección IP que usan para establecer las conexiones.

Por otro lado, el uso de esta red es muy común para interactuar de manera anónima con mercados negros que ofrecen servicios, productos, información, etc. que no está permitido su comercio de forma legal. El hecho de participar en estos mercados a través de TOR, hace que sea muy complicado para las autoridades hallar a las personas que forman parte de estos mercados.

En este trabajo se muestra un estudio sobre los principios básicos de operación de las redes de anonimización y los mercados negros de la red TOR. También se analizan algunas técnicas de desanonimización y las acciones que se llevan a cabo a nivel de legislación en cuanto al uso de esta tecnología.

1.1- Objetivos

En este apartado se presentan de forma priorizada los objetivos del trabajo. Estos objetivos son los siguientes:

- El principal objetivo de este trabajo es describir los componentes de la red TOR, sus interacciones y como se proporciona anonimato a los usuarios y servicios de esta red.

- El segundo objetivo consiste en seleccionar y analizar algunas de las técnicas más populares de desanonimización de usuarios y servicios.

- El tercer objetivo se basa en realizar un estudio de los mercados negros de la red TOR, proporcionando una descripción de cómo los “traders” ocultan sus actividades comerciales y el papel de las criptomonedas en estos mercados.

- El cuarto objetivo es analizar las acciones que se están implantando a nivel de legislación para hacer cumplir la ley.

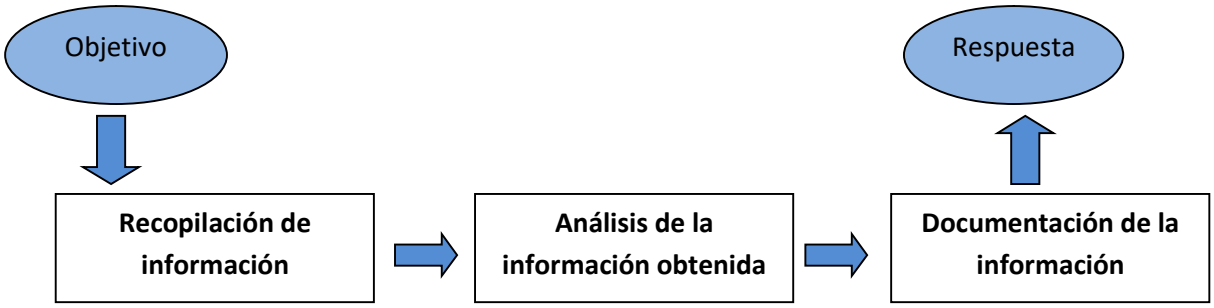
1.2- Metodologia

En este apartado se describe la metodología que se seguirá durante este trabajo. Con el fin de cumplir con los objetivos inicialmente establecidos, se ha propuesto definir las siguientes fases para cada uno de los objetivos:

- **Recopilación de información:** Esta fase consiste en recoger la información pública que existe del tema a analizar, así como obtener información realizando acciones prácticas como conexiones en la red TOR como usuarios de esta, consultando servicios ilegales, etc.

- **Análisis de la información obtenida:** Una vez se disponga de la información necesaria, se procederá a realizar un análisis de ésta, explicando cómo se ha obtenido y complementándola de forma necesaria que aporte valor al trabajo.

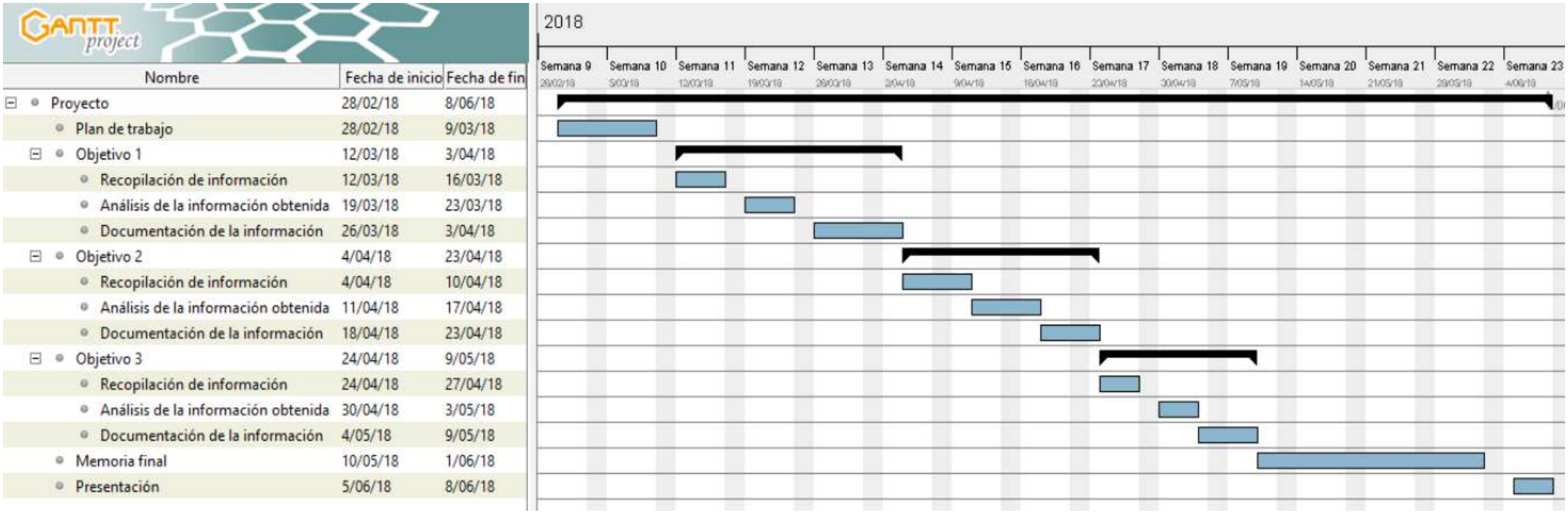
- **Documentación de la información:** Se debe seleccionar qué información recopilada y analizada resulta de utilidad para cumplir con los objetivos del trabajo y exponerla de forma que resuelva las cuestiones planteadas en dichos objetivos.



1.3- Planificación de tareas

En el siguiente apartado se muestra un diagrama de Gantt con las diferentes tareas planificadas que se deben realizar para cumplir los objetivos definidos.

La fecha de inicio de proyecto es el 28/02/2018, y la fecha de finalización de éste es el 08/06/2018, fecha en que se debe entregar la presentación del trabajo.



Nombre	Fecha de inicio	Fecha de fin
Proyecto	28/02/18	8/06/18
Plan de trabajo	28/02/18	9/03/18
Objetivo 1	12/03/18	3/04/18
Recopilación de información	12/03/18	16/03/18
Análisis de la información obtenida	19/03/18	23/03/18
Documentación de la información	26/03/18	3/04/18
Objetivo 2	4/04/18	23/04/18
Recopilación de información	4/04/18	10/04/18
Análisis de la información obtenida	11/04/18	17/04/18
Documentación de la información	18/04/18	23/04/18
Objetivo 3	24/04/18	9/05/18
Recopilación de información	24/04/18	27/04/18
Análisis de la información obtenida	30/04/18	3/05/18
Documentación de la información	4/05/18	9/05/18
Memoria final	10/05/18	1/06/18
Presentación	5/06/18	8/06/18

Figura 1: Diagrama de Gantt con la planificación de tareas del trabajo.

1.4- Estado del arte

En este apartado se presenta el estado del arte de la red TOR y de los aspectos relacionados con esta tecnología que se estudiarán en este trabajo.

La primera versión alfa de software para navegar por la red TOR se publicó el 20 de septiembre de 2002. Este proyecto surgió de la evolución del proyecto Onion Routing del Laboratorio de Investigación Naval de los Estados Unidos. Actualmente The Tor Project, una organización sin ánimo de lucro, es la propietaria del proyecto TOR.

Entre 42.000 y 25.000 usuarios en España han usado la red TOR a diario entre marzo de 2017 y febrero de 2018. En el siguiente gráfico se muestra el uso de esta tecnología en el último año por usuarios en España.

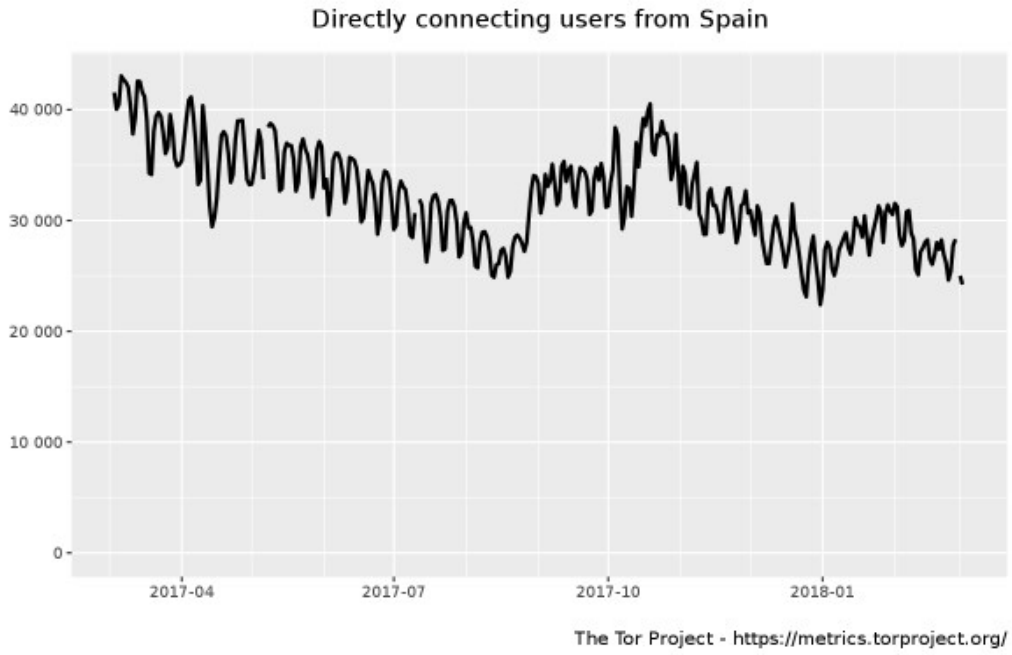


Figura 2. Gráfico que muestra el número de usuarios que han usado la red TOR en España entre marzo de 2017 y febrero de 2018.

A pesar de que el objetivo de la red TOR sea proporcionar anonimato a los usuarios que la usan, actualmente existen diferentes técnicas que permiten desanonimizar a los usuarios que se han conectado a través de ésta red. También existen maneras de desanonimizar servicios de la red TOR que permitirían hallar el usuario que está proporcionando el servicio en la red TOR.

La necesidad de desanonimizar usuarios vine dada por las actividades ilegales que se hancen a través de la red TOR. Estas actividades se desarrollan en diferentes aspectos como el tráfico de drogas, venta de armas y pornografía infantil, entro otros. Este tipo de actividades ilegales se han extendido tanto en la red TOR que actualmente existen mercados negros en esta red conocidos a nivel mundial.

En cuanto a los aspectos legales, en España es legal obtener el software que permite acceder a la red TOR, así como navegar a través de ella, pero hay ciertas actividades que no están permitidas por el código penal.

El código penal en España no permite que se realicen cierto tipo de acciones en la red, ni la publicación o descarga de información que se considera ilícita. Como la red TOR proporciona anonimato a los usuarios que la usan, se considera una buena opción para realizar acciones que no están permitidas por el código penal.

En este trabajo se estudiarán con más detalle las acciones que no se permiten realizar a través de la red TOR así como los controles legales que se aplican en los diferentes ámbitos que afectan a esta tecnología. En este trabajo también se plantearan los aspectos legales que existen con relación a la posesión de nodos TOR que ofrecen anonimato a los usuarios de ésta red, así como las penalizaciones que pueden conllevar la posesión de estos.

2- Descripción de los componentes de la red TOR

En este apartado se presentan los diferentes componentes de la red TOR y se muestra una descripción de las principales acciones que realizan en la red. En primera instancia se describe el proceso de navegación anónima de los usuarios y la publicación anónima de contenidos en la red, posteriormente se listan los componentes que componen la infraestructura de la red TOR y, finalmente, se describen los componentes listados.

2.1- Funcionamiento de la red TOR

En el siguiente apartado se explica cómo funciona la navegación de los usuarios y los servicios en la red TOR y de qué manera se proporciona anonimidad a estos

2.1.1- Navegación de los usuarios

La navegación de los usuarios de la red funciona de la siguiente manera. Los usuarios utilizan un cliente TOR en el dispositivo desde el que se conectan a la red. Lo que hace este cliente TOR para proporcionar anonimidad es cifrar los mensajes (cabeceras IP incluidas) que se envían por Internet de manera que en ningún momento se pueda saber quién es el origen de una conexión. Para ello el cliente TOR elige X nodos TOR al iniciar una conexión a Internet (3 nodos por defecto), establece claves de cifrado con los 3 nodos para cifrar la conexión y establece la conexión a Internet a través de los nodos escogidos.

En la siguiente figura, se muestra el intercambio de mensajes que se realiza cuando se establece una conexión a través de la red TOR.

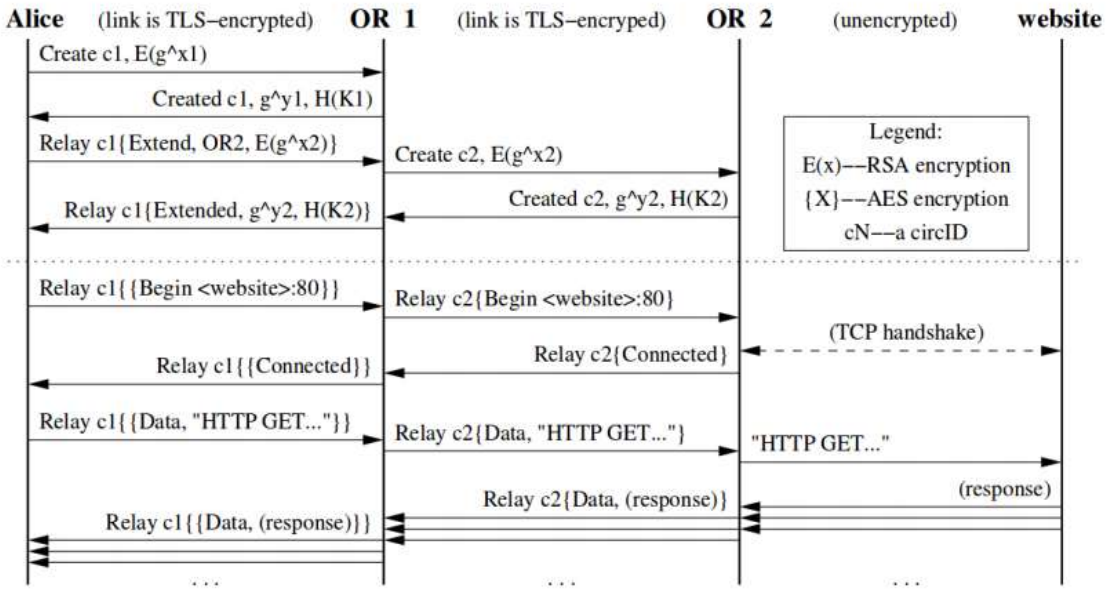


Figura 1: En esta figura se muestra el intercambio de mensajes en una conexión de la red TOR entre el usuario y los routers de la red que proporcionan el anonimato a los usuarios.

Para garantizar el anonimato del usuario, el cliente Tor cifra la petición con diferentes capas de cifrado (tantas como nodos TOR haya escogido). De esta forma por cada nodo TOR por donde pase la petición ese nodo sacará una capa de cifrado.

Por ejemplo, supongamos que un usuario U quiere hacer una petición a un servidor S de forma anónima. U escoge 3 nodos o routers Tor (A, B y C) por donde pasara su petición. El último de los nodos será el que hará la petición a S sin cifrar.

El usuario U y el router A se ponen de acuerdo para saber qué claves utilizan para cifrar los mensajes entre ellos.

Después, U a través del router A se pone de acuerdo con el router B para el uso de claves que utilizará U en la segunda capa de cifrado.

Finalmente U, siguiendo el camino A, B, se pone de acuerdo con C para generar las claves que utilizará en la tercera capa de cifrado.

Con este sistema B se está comunicando con A y no sabe nada de el usuario U, y C se está comunicando con B Y no sabe nada de A ni de U.

Una vez U sabe las claves que debe utilizar con los nodos A, B y C cifra los datagramas con las claves pertinentes y los envía a A.

A utilizará la clave pactada con U para descifrar la conexión con U y verá que tiene un datagrama con origen U y destino B. A continuación le envía los datagramas a B. Este utilizará su clave para descifrar el origen y destino del datagrama. Entonces verá que el origen es A y el destino es C, por tanto le enviará el datagrama a C.

C descifra el datagrama con la clave pactada con U a través de B y ve que el destino es S. Entonces C hace la petición a través de internet a S.

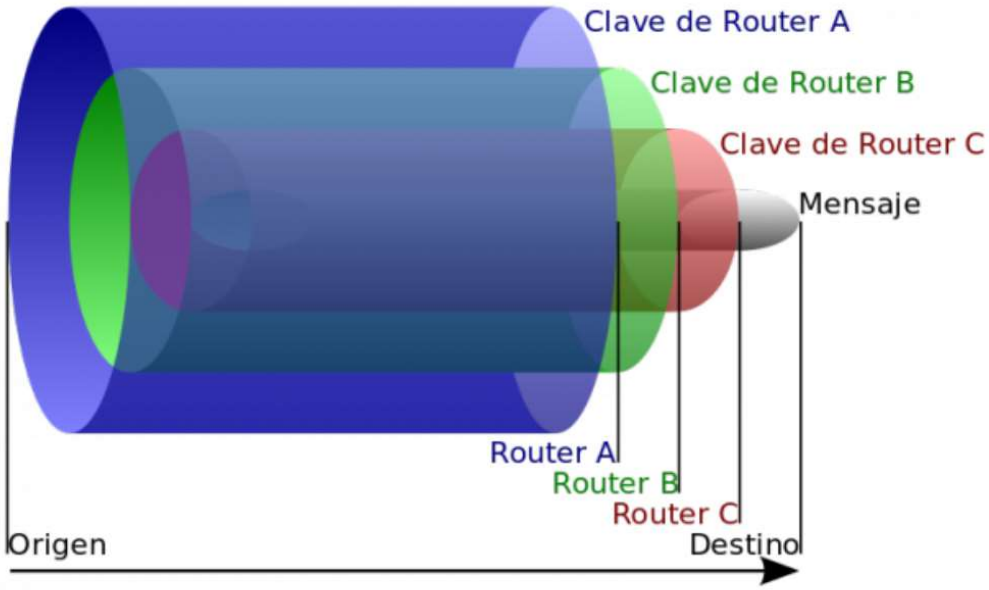


Figura 2: En esta imagen se muestra el encapsulamiento que realiza el cliente TOR del mensaje que desea enviar al destino final de la conexión.

2.1.2- Servicios ocultos

Los servicios que se publican de forma anónima en la red TOR funcionan de la siguiente manera. El proveedor del servicio anuncia el servicio que quiere publicar a distintos nodos de la red, firmándolos con su clave pública para evitar ataques de suplantación.

Los nodos que reciben la información de los servicios son llamados puntos de introducción, y serán los encargados de crear la comunicación entre el cliente TOR y el servicio anónimo a través de un punto de encuentro.

Figura 3: Escenario en que un cliente de la red TOR quiere realizar una petición a un servicio anónimo. Las líneas verdes representan las conexiones TOR (descritas en el apartado 2.1.1 de este documento) en que el servidor anuncia su servicio a puntos de introducción.

El proveedor del servicio asocia un nombre de dominio .onion a su servicio y lo publica a un servidor de directorio. El dominio del servicio .onion no funciona con el servicio de DNS convencional, se usa Pseudo-TLD que trabaja con una arquitectura basada esta tecnología.

Figura 4: Escenario en que el servidor pública su servicio en el servidor que proporciona el servicio de directorio.

Cuando un usuario quiere acceder a un servicio, a través de una conexión TOR como las descritas en el apartado anterior, consulta el servicio de directorio y este le indica el punto de introducción al que debe conectarse y la clave pública del servicio al que quiere acceder.

Posteriormente, el cliente elige un punto de encuentro y genera un identificador para esa conexión al servicio oculto. El cliente le envía un mensaje al punto de introducción firmado con la clave pública del servidor, indicando el punto de encuentro que ha asignado y el identificador de la conexión generado.

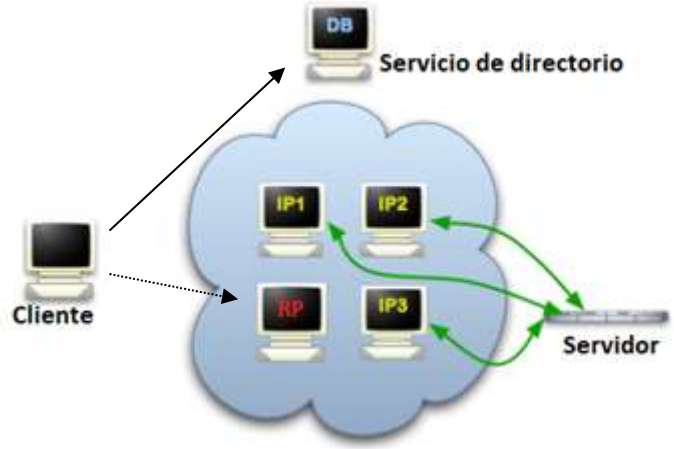


Figura 4: Escenario en que el cliente solicita el nombre del servicio al servidor de directorio y posteriormente se comunica con el punto de encuentro (RP, Rendezvous Point).

El punto de introducción envía el mensaje que ha recibido del cliente al servidor, y éste le proporciona el servicio a través del punto de encuentro. Para proporcionar el servicio, el servidor se conecta al punto de encuentro e identifica el cliente a quién debe proporcionar el servicio a través del identificador de la conexión.

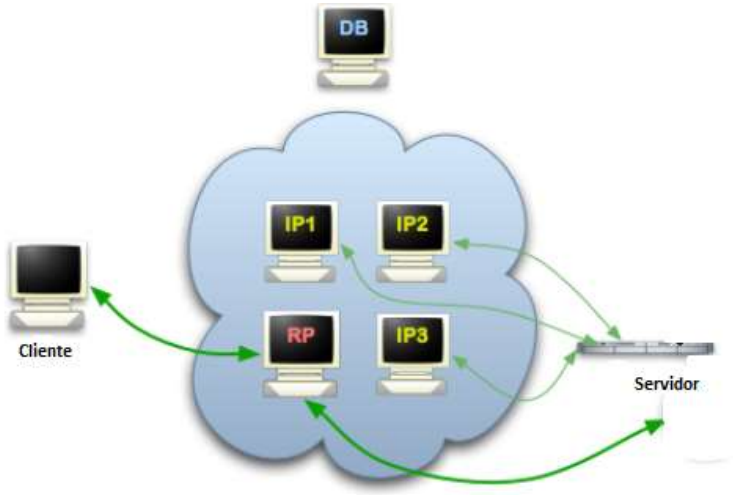


Figura 5: Escenario en que el cliente accede a un servicio y el servidor lo proporciona, ambos a través de un punto de encuentro.

2.2- Componentes de la red TOR

En este apartado se describen los principales componentes de la red TOR. La red TOR está compuesta principalmente por los siguientes componentes: Los nodos TOR, el servicio de directorio y los puntos de encuentro.

Estos componentes son los que permiten a los usuarios de la red TOR navegar por ella de forma anónima. Esta anonimidad se produce tanto la navegación de usuarios como en la publicación de servicios.

2.2.1- Nodos TOR

Los nodos TOR son los nodos de la red que se encargar de proporcionar anonimato a los usuarios de la red. Son como servidores VPN públicos que utilizan los clientes TOR para establecer las conexiones a través de estos nodos.

Estos nodos TOR se clasifican en tres tipos: los nodos intermedios, los nodos de salida y los puentes.

Los nodos intermedios son aquellos que están entre los nodos de salida y los usuarios. Su dirección IP siempre se encuentra cifrada como mínimo por debajo de una capa de cifrado establecida con un nodo de salida, por lo que su IP nunca realizará peticiones a servidores de Internet, tan solo se conectara a clientes TOR y a nodos de salida. Para poder recibir las conexiones éstos nodos publican su presencia a través de la red TOR para poder ser usados.

Los nodos intermedios lo que ven es la negociación de claves entre el usuario final y otro nodo TOR, o entre un nodo TOR y otro nodo TOR. Como ellos están en medio, lo único que pueden ver es tráfico cifrado. En caso de ser el primer nodo del circuito, negocian la primera clave con el originario de la conexión a Internet, pero no verán nada más porque el resto de la conexión irá cifrada con otras claves.

Los nodos de salida son aquellos que realizarán la petición al servidor al que el usuario se quiere conectar. Por tanto, a efectos de Internet, el usuario estará navegando utilizando la IP del nodo TOR de salida que haya escogido.

Los nodos de salida podrán ver las peticiones que van a Internet, pero no podrán saber el origen de la conexión porque la conexión vendrá de un nodo TOR, no del usuario final.

Los nodos puente vienen a ser como los nodos intermedios pero no publican su presencia en la red. Debido a que no publican su presencia solo pueden ser usados por casos particulares en que se conozca su presencia a priori, ya que a través de Internet no es posible encontrarlos.

Los nodos puente verán los mismos que los nodos intermedios ya que asumen el mismo rol en la conexión a Internet de los usuarios.

2.2.2- Servicio de directorio

El servicio de directorio contiene información de la red TOR que es accesible para los nodos TOR y para todos los usuarios de la red. Este servicio publica una base de datos en la que se asocia cada nodo TOR a una información nombrada “router descriptor”. Esta información contiene datos que se necesitan del nodo TOR para poder conectarte a él, como la dirección IP y la huella digital de la clave pública.

Los servicios de directorio tienen la información replicada entre ellos de manera que se mejora la latencia de comunicación con los usuarios y en caso que un servidor de estos servicios no se encuentre disponible, no se produzcan aislamientos de nodos en la red, lo que podría causar una caída en las comunicaciones de la red. Estos servidores se diferencian en dos tipos, los principales o autoridades de directorio y los secundarios, que se usan como cache para reducir latencia o como back up de los servidores principales.

Los servidores que proporcionan este servicio se encuentran distribuidos por la red TOR. A estos servidores se les otorga una confianza que les permite gestionan la suscripción a la red de los clientes (bootstrapping). Para poder proporcionar esta confianza a estos servidores, se firma criptográficamente la información que estos proporcionan para que se pueda verificar que la información que se va a publicar en la base de datos es correcta y prevenir ataques en estos servicios.

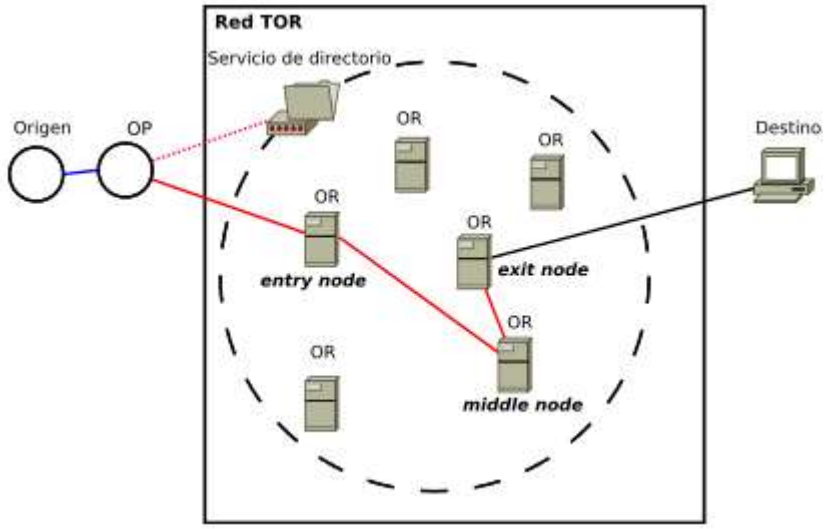


Figura 6: Componentes de la red TOR. En la siguiente figura se pueden ver los diferentes componentes de la red TOR descritos anteriormente. El enlace azul entre el origen y el Onion Proxy representa tráfico SOCKS entre el origen y el proxy creado por el cliente TOR. El enlace rojo representa las conexiones cifradas por TLS entre el proxy creado por el cliente TOR y los nodos de la red que proporcionan anonimato. En enlace negro representa la conexión a Internet que realiza el nodo de salida. En enlace rojo punteado representa la conexión HTTP que establece el proxy creado por el cliente TOR y el servicio de directorio de la red TOR.

2.2.3- Puntos de encuentro

Los puntos de encuentro (Rendezvous Points) son nodos de la red TOR que se utilizan para enviar tanto las peticiones de los usuarios como las respuestas de los servidores. Tanto las peticiones de usuarios como las respuestas de servidores que se hacen a los puntos de encuentro se realizan a través de comunicaciones anónimas como la descrita en el apartado 2.1.1 de este documento. De esta manera se evita que los clientes y servidores se comuniquen directamente entre ellos y lo hacen a través de un punto de encuentro.

3- Técnicas de desanonimización de usuarios y servicios

En este apartado se seleccionan dos técnicas de desanonimización de usuarios y una de servicios de la red TOR, y se muestra una descripción de cada una de ellas. Las técnicas de desanonimización de usuarios seleccionadas son los ataques de correlación de flujo y los ataques de atasco. La técnica de desanonimización de servicios seleccionada es.

3.1- Ataques de correlación de flujo

Estos ataques se basan en analizar conexiones de la red TOR capturadas en diferentes puntos de la red y asociar las conexiones que se hacen a Internet con los usuarios que las realizan. Para que estos ataques tengan éxito, se precisa disponer del control del primer nodo del circuito TOR y el último, el que hace la conexión con el servidor final.

Como las conexiones en la red TOR van cifradas, la comparación entre las conexiones que se capturan en los diferentes puntos de la red no es posible de realizar de forma directa. Por este motivo, existen diferentes técnicas para realizar esta correlación de flujo. Estas técnicas son las siguientes.

3.1.1- Conteo de paquetes

Esta técnica de correlación consiste en contar el número de paquetes que entran y salen del primer nodo del circuito TOR que ha seleccionado el cliente para determinar cuál es el siguiente nodo. Este proceso se repite en otros nodos, hasta que se detecta la conexión con el destino final. Esta técnica es sencilla de realizar, pero para que sea efectiva implica que el atacante tenga visibilidad de muchos nodos de la red, si no se cumple esta premisa, es muy difícil que el ataque tenga éxito.

3.1.2- Análisis de sincronización

Otra técnica de correlación de flujo es el análisis de sincronización. Esta técnica se basa en correlacionar los flujos de datos observando el retardo que existe entre los paquetes de la conexión. El problema que presenta esta forma de analizar los flujos es que cuando se producen pérdidas de paquetes de la conexión, no es posible detectarlas y se incrementa el tiempo de retardo de los paquetes considerando el tiempo de retransmisión como tiempo de retardo. Esto complica la correlación de flujos.

Para solucionar este problema, se propuso un algoritmo de correlación utilizando series de tiempo que se construyen utilizado la información de sincronización de *packing*. Para generar las series de tiempo, se establece una constante T, que representa el tiempo, se divide el flujo de paquetes entre T y se hace un recuento de paquetes que se obtiene del resultado. De la misma manera que el ataque anterior, para que el ataque sea efectivo, se precisa tener el control de un gran número de nodos de la red TOR. Cuantos menos nodos se tengan controlados, menos probable es que tenga éxito el ataque.

3.2- Atasco

Este ataque se basa en alterar las conexiones de un router de la red TOR, para que el resto de conexiones de este router también se vean afectadas. Para ello, el atacante debe controlar un router de la red TOR y poder capturar una conexión entre el router TOR y el servidor final al que se quiere conectar el usuario. A través de este router, el atacante crea circuitos TOR de un solo nodo en todos los demás routers para ver si la latencia de la que conexión que se está observando incrementa o no. Si lo hace, el router está en el circuito que se está analizando y es posible detectar el usuario final de la conexión.

El principal problema que presenta este ataque, es que no es viable aplicar la regla descrita anteriormente teniendo en cuenta la gran cantidad de routers TOR que hay actualmente en la red.

3.3- Desanonimización de servicios ocultos

A continuación se detalla una técnica para desanonimizar servicios ocultos. Para que se pueda desanonimizar un servicio oculto es necesario que este elija como nodo de entrada a la red TOR un nodo controlado por el atacante, para poder determinar el origen del servicio oculto.

También es imprescindible que el atacante tenga control sobre el punto de encuentro entre el servicio y el usuario final. Entonces el atacante podría realizar una correlación del tráfico entre el punto de entrada y el punto de encuentro y desenmascarar el servicio oculto.

Esta técnica de desanonimización se basa en la correlación de flujo, de la misma forma que la descrita en el apartado 3.1 de este documento, con la diferencia que el tráfico que se correlaciona es entre el nodo de entrada en la red TOR del servidor y el punto de encuentro, en vez de correlacionar el flujo entre el nodo de entrada y el de salida.

4- Mercados negros de la red TOR

4.1- Mercados negros

En el siguiente apartado se realiza una descripción de algunos de los mercados negros más importantes que han existido en la red TOR en los últimos años y algunos de ellos siguen teniendo actividad actualmente. A continuación se presentan dos mercados negros muy populares en la red TOR que todavía siguen teniendo actividad, a pesar de que hayan sido censurados y cerrados en diferentes ocasiones.

Finalmente, se presentan dos mercados negros que han sido muy populares y han tenido una gran actividad, pero actualmente no se encuentran operativos. Los mercados negros que se analizarán son los siguientes.

4.1.1- Silk Road

Silk Road es uno de los mercados negros más conocidos que ha existido en la red TOR hasta la fecha actual. Este mercado empezó a estar operativo el mes de Febrero del año 2011 y fue censurado y cerrado por el FBI en diferentes ocasiones. Actualmente este mercado está en su versión 3, ya que las dos versiones anteriores fueron censuradas y cerradas.

Tanto el fundador de esta plataforma como varios de sus comerciantes han sido detenidos y condenados con penas de prisión por las autoridades de diferentes países. El octubre de 2013, el FBI arrestó a Ross William, creador de Silk Road y en junio de 2015 fue condenado a cadena perpetua por una corte general de Manhattan después de haber sido declarado culpable de siete cargos.

A continuación, se muestran una serie de imágenes que se han tomado navegando por la página de Silk Road. Esta navegación se ha realizado utilizando un cliente TOR.

En la siguiente imagen se muestra la página principal de Silk Road. Como en la mayoría de mercados negros, el principal producto de venta de este mercado son las drogas, por este motivo aparecen ciertos productos de este tipo en la pantalla principal de éste.

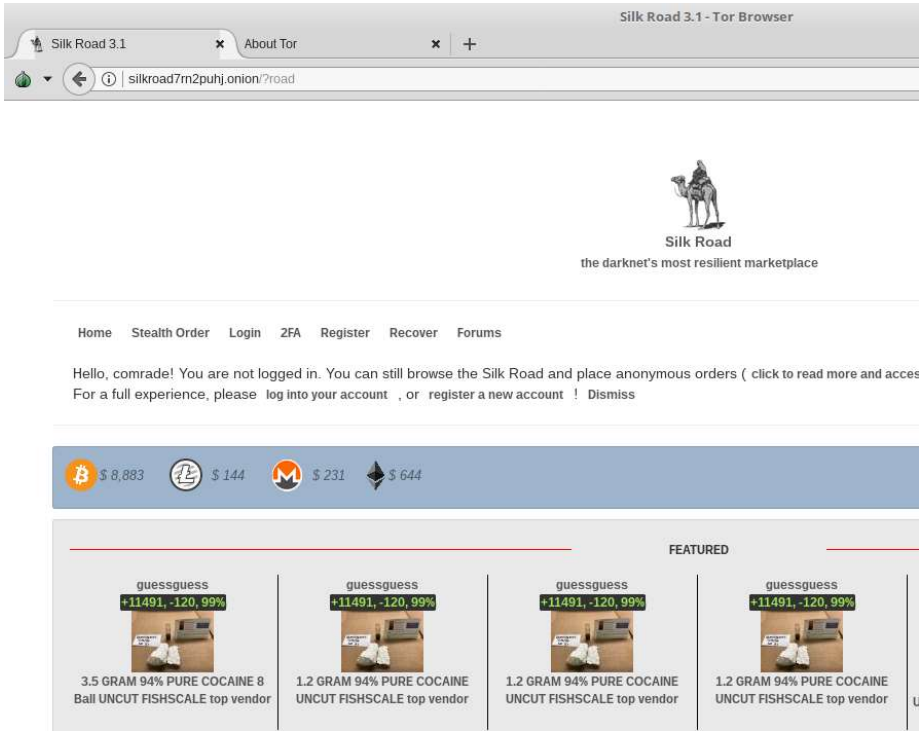


Figura 1: Página principal de Silk Road.

A continuación, se muestra cómo se ofrecen los productos dentro de esta plataforma, así como los productos que más se ofrecen en esta.

Como se ha comentado anteriormente, el producto más popular son las drogas. En la imagen 2 se aprecia la publicación de Cannabis, estimulantes y otros tipos de substancias ilegales. En la imagen 3 se puede apreciar la venta de documentos como tarjetas de pago y de crédito.

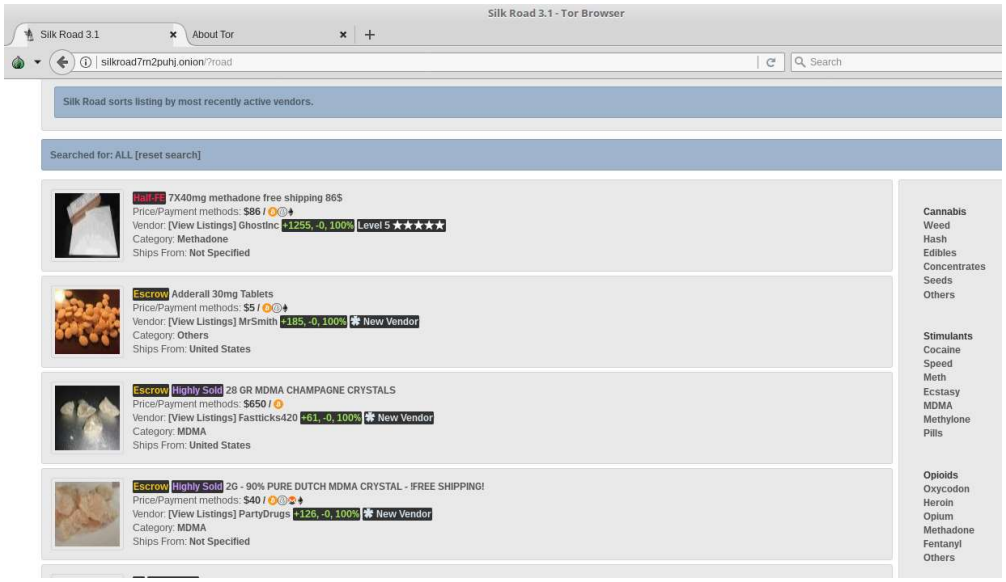


Figura 2: Productos que se ofrecen en el mercado negro Silk Road.

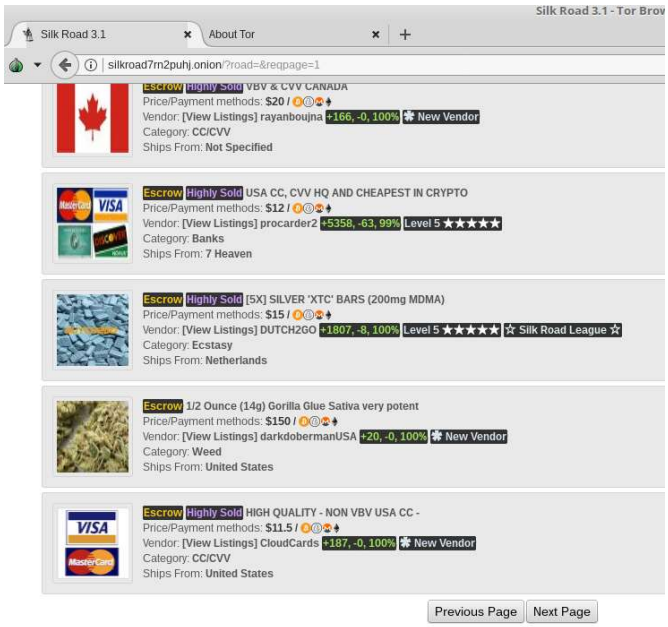


Figura 3: Productos que se ofrecen en el mercado negro Silk Road.

4.1.2- Mercadonegro

Este mercado de la red TOR es el único de los descritos que se encuentra activo. En este mercado se pueden encontrar diferentes categorías de productos. Desde un cliente TOR, hemos accedido a este mercado negro y hemos observado las diferentes categorías de productos que se ofrecen. En la siguiente imagen se muestra la página principal del mercado descrito.

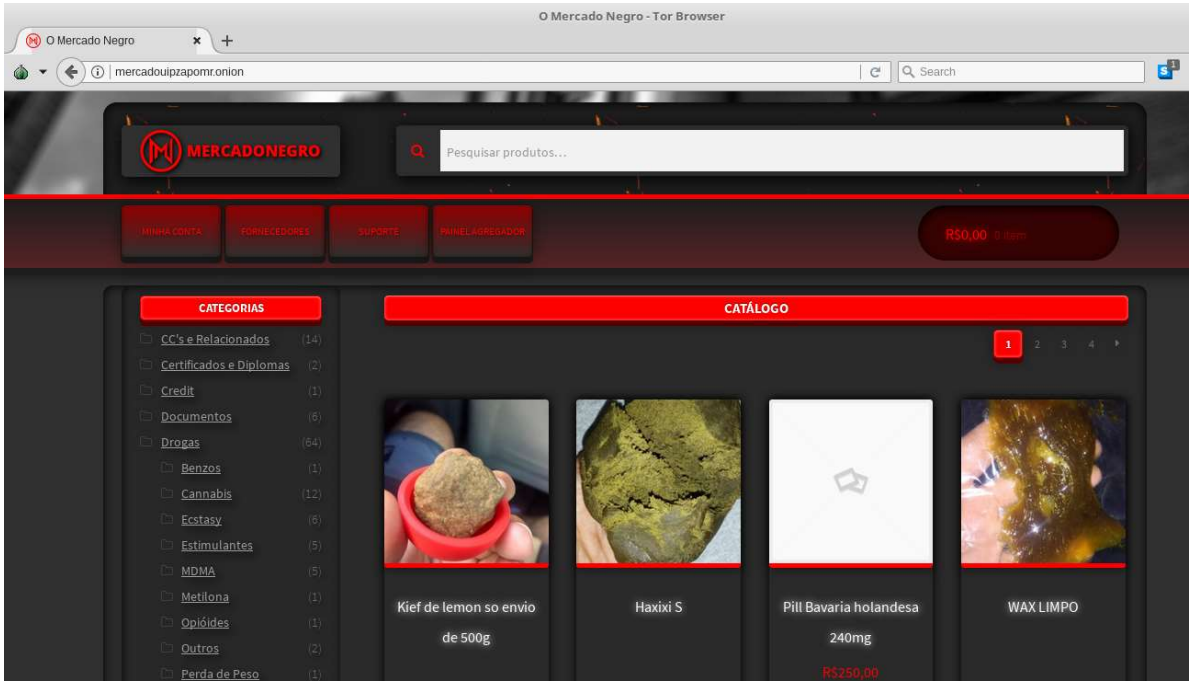


Figura 4: Página principal del mercado Mercadonegro.

Una vez hemos accedido a este, observamos que en el panel izquierdo hay las categorías de productos que se venden. Como se puede observar, estos productos mayoritariamente son drogas y documentos de identidad, pero también se ofrecen libros y otros documentos y servicios.

Las categorías de productos y servicios que publica este mercado negro se pueden ver en la siguiente imagen.

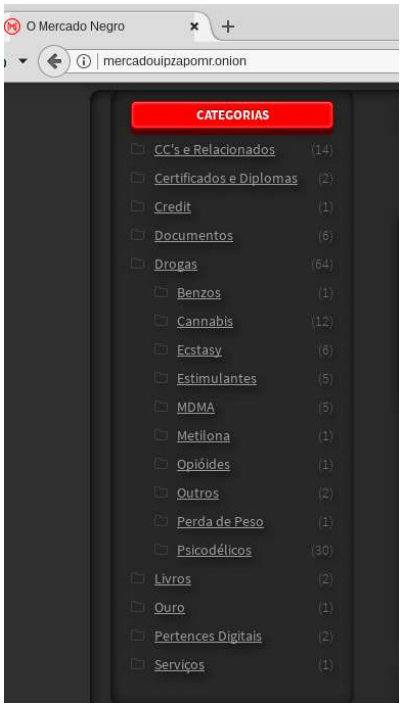


Figura 5: Categorías de productos y servicios del mercado Mercadonegro.

4.1.3- AlphaBay Market

AlphaBay Market fue otro mercado negro que se desplegó en la red TOR y que se ofrecía como un servicio oculto. Se puso en funcionamiento por primera vez el Diciembre del año 2014 y funcionó hasta el 13 de julio de 2017, que en una operación policial en contra de esta plataforma, se censuró su uso y se detuvo a Alexandre Cazes, creador y responsable de este mercado. Éste fue hallado muerto en su celda unos días después de su arresto en Tailandia.

Actualmente no es posible acceder a este mercado ya que el servicio de compra-venta de productos no se encuentra disponible.

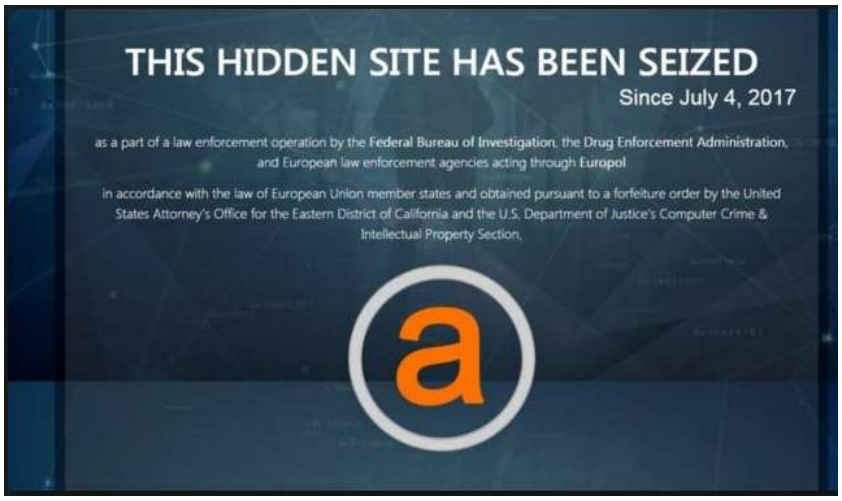


Figura 6: Mensaje donde se indica la censura del mercado negro AlphaBay.

4.1.4- Agora

Este mercado negro se lanzó en el año 2013 y tuvo actividad hasta agosto del año 2015, cuando fue cerrado en una operación policial. El fundador y administrador de este mercado ha hecho público que está trabajando para mejorar la seguridad de la plataforma y que se está trabajando en implementar las medidas de seguridad oportunas.

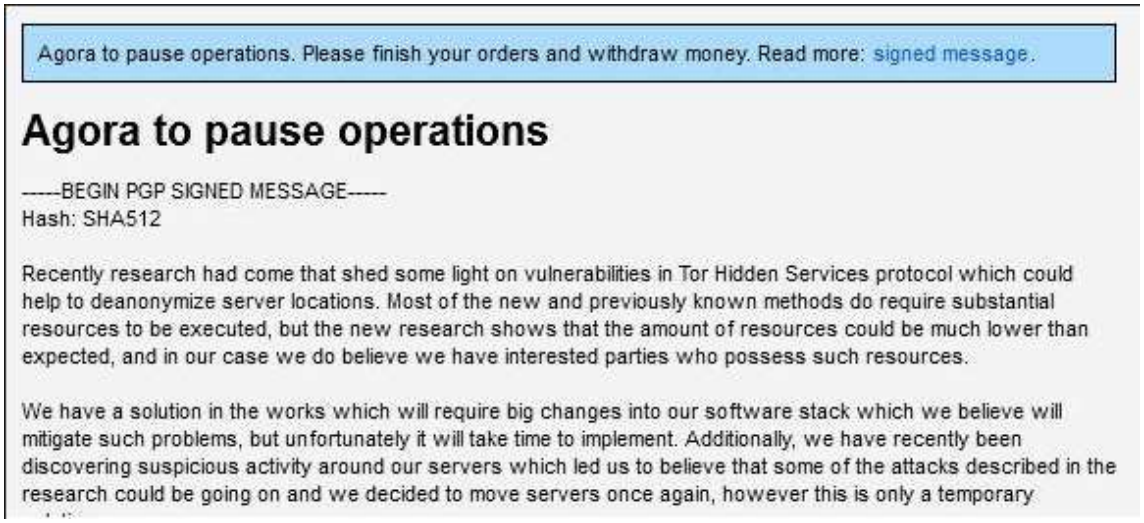


Figura 7: Mensaje donde se indica la indisponibilidad temporal del mercado negro Agora.

4.2- Actividades ilegales

Una vez se han analizado los diferentes mercados negros que han existido en la red TOR y hemos visto uno que actualmente se encuentra activo, se muestran las diferentes actividades ilegales que se pueden realizar en ésta red.

Para ello, utilizando el navegador TOR nos conectamos a la red TOR y buscamos enlaces que se utilicen para poder realizar este tipo de actividades no permitidas por la ley.

Una vez estamos conectados a la red TOR, utilizamos una página llamada “Hidden Wiki” para obtener las direcciones a los servicios que queremos acceder.

En esta página se encuentran muchos enlaces a diferentes tipos de servicios, a continuación se presentan unos ejemplos.

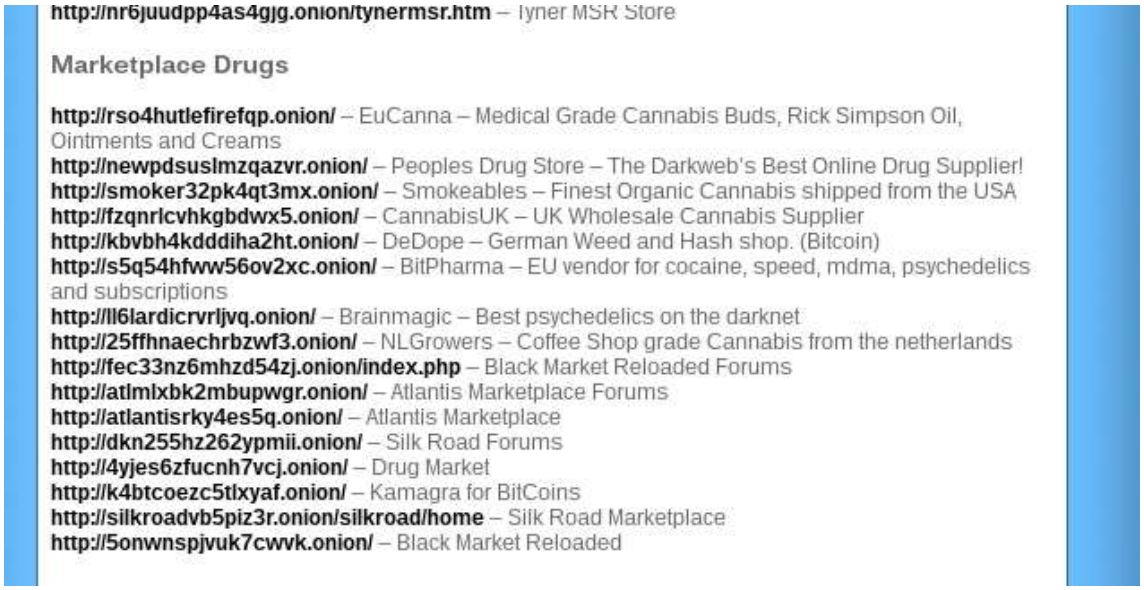


Figura 8: Enlaces de la Hidden Wiki donde se ofrece el tráfico de drogas.

En la imagen mostrada se pueden observar una serie de enlaces que ofrecen la venta de diferentes tipos de drogas. Estos enlaces no se encuentran siempre disponibles, están disponibles de forma temporal.

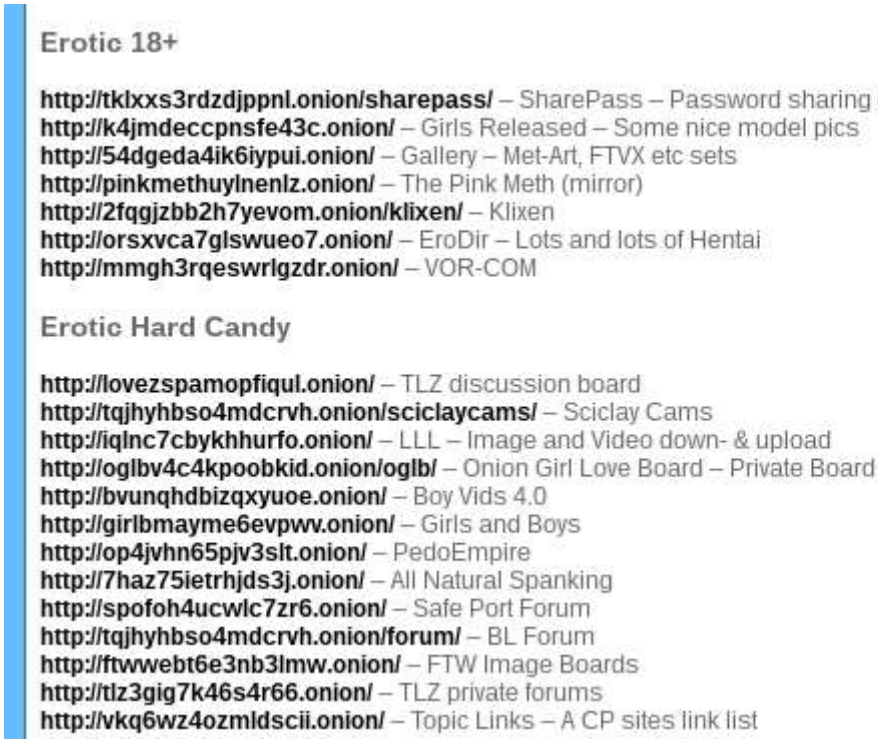


Figura 9: Enlaces de la Hidden Wiki donde se ofrecen servicios de pornografía.

En esta imagen se encuentran enlaces que ofrecen al consumidor contenido pornográfico de diferentes tipos. De la misma forma que los enlaces anteriores, éstos no se encuentran siempre disponibles, si no que están disponibles de forma temporal.

Commercial Services

- Mobile Store - Factory unlocked iphones and other smartphones.
- Rent-A-Hacker - Hacking, DDOS, Social Engeneering, Espionage, Ruining people.
- Onion Identity Services - Selling Passports and ID-Cards for Bitcoins.
- HQER - High quality euro bills replicas / counterfeits.
- Hitman Network - Group of contract killers from the US/Canada and EU.
- Apples4Bitcoin - Cheap Apple products for Bitcoin.
- EuroGuns - Your #1 european arms dealer.
- Silkroad - Anonymous marketplace with escrow (Bitcoin)
- UK Guns and Ammo - Selling Guns and Ammo from the UK for Bitcoins.
- UK Passports - Original UK Passports.
- USfakeIDs - High quality USA Fake Drivers Licenses.
- USA Citizenship - Become a citizen of the USA, real USA passport.
- Kamagra for Bitcoin - Same as Viagra but cheaper!

Figura 10: Enlaces de la Hidden Wiki donde se ofrecen diferentes tipos de servicios.

En estos enlaces no se comercializa con drogas ni con contenido, si no que se comercializa con documentos de identidad, armas, criptomonedas, sicarios y otros tipos de productos y servicios.

Si entramos en algunos de los enlaces podemos ver los siguientes productos.

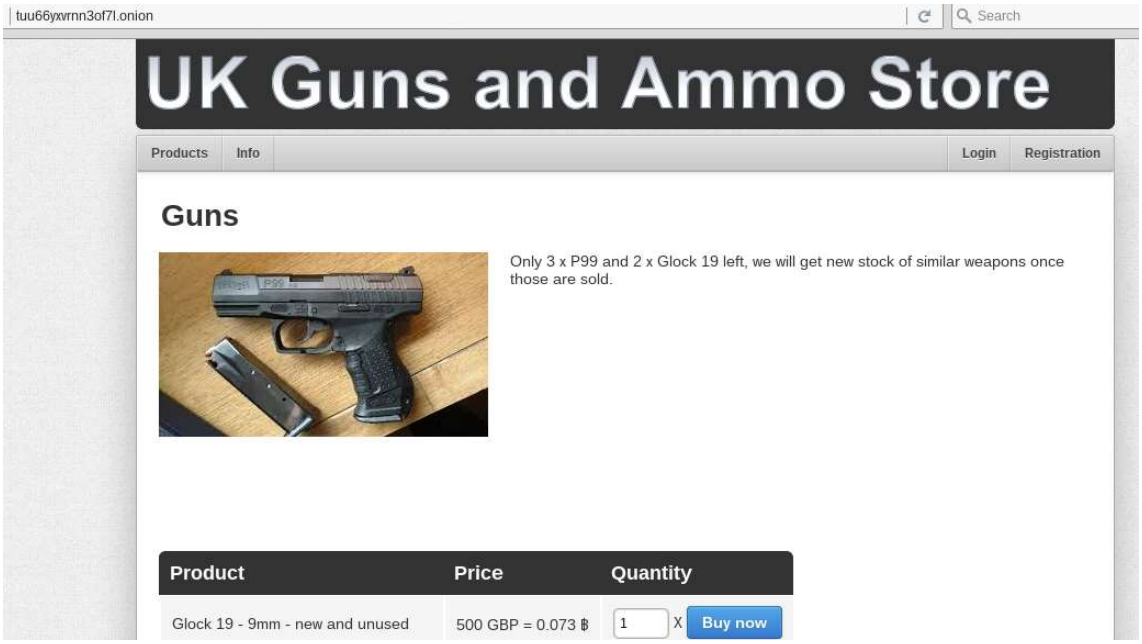


Figura 11: Servicio de compra de armas a través de una página de la red TOR.

Figura 12: Servicios de venta de pasaportes de UK a través una página de la red TOR.

En las imágenes x y x se pueden observar diferentes productos que se ofrecen en páginas de la red TOR. La moneda de pago es el Bitcoin y en ninguno de los casos mostrados existe una garantía por parte del vendedor que el producto que se ofrece es el que realmente se envía, de qué funcione correctamente, ni tan solo de que realmente se realice el envío. Existe un intermediario que valida la operación de compra-venta, pero al no tener referencias reales del vendedor ni del intermediario, no es posible realizar compras con garantías.

4.3- Criptomonedas

En este apartado se describen las principales criptomonedas que existen actualmente, sus propiedades, su funcionamiento y los uses que se hacen de estas tanto la red TOR como en otros ámbitos.

La red TOR y las criptomonedas tienen una estrecha relación por lo que respecta a uno de sus principales características, la anonimidad. A través de la red TOR se pueden realizar muchas actividades ilícitas de forma anónima, las más comunes son la creación de mercados negros comercializando con productos y servicios no permitidos. El papel de las criptomonedas en este escenario es crucial, ya que mediante estas se realizan los pagos en los mercados negros. De esta forma se consigue realizar actividades comerciales de forma anónima a través de la red TOR y poder realizar pagos de forma anónima a través de las criptomonedas.

4.3.1- Bitcoins

En noviembre de 2008 se registró por primera vez un artículo con título *Bitcoin:Un sistema de efectivo electrónico de Peer-to-Peer* firmado con el nombre Satoshi Nakamoto. En este artículo se detallaba cómo usar una red P2P para la generación de un sistema de transacciones que no dependiera de la confianza de un tercero. El 4 de enero del año 2009, el autor del artículo mencionado registra el primer bloque de la blockchain de Bitcoin y emito los primeros bitcoins. También se lanza el primer cliente Bitcoin de código abierto.

El Bitcoin es la criptomoneda más popular que existe actualmente y se basa en la tecnología blockchain para gestionar y validar las transacciones, así como guardar un histórico de éstas. El Bitcoin tiene las siguientes características:

- No pertenece a ningún estado ni país y se puede usar en todos los estados de la misma forma.
- Es una tecnología descentralizada. No se gestiona por ninguna entidad, gobierno, banco o empresa.
- Su tecnología no permite falsificar, reusar o duplicar bitcoins.
- Se pueden hacer transacciones y disponer de ellos de forma anónima. Las cuentas de bitcoins no se asocian a personas, si no a clave privadas que no es necesario hacer público su propietario.
- Las transacciones son irreversibles.
- Se pueden comprar bitcoins con euros, dólares o cualquier otra divisa y viceversa.

Al no existir intermediarios no existen comisiones por disponer de esta moneda, por grande que sea la cantidad de bitcoins que dispongas. En las trasferencias sí que se cobra una comisión al emisor de ésta ya que se deben pagar los costes a los "mineros" que hacen que dicha transacción se haga efectiva.

Las direcciones bitcoins se generan a partir de una clave secreta ECDSA. Al revés no es posible, ya que los algoritmos de criptografía que se usan para generar la clave pública no permiten realizar operaciones a la inversa, por lo que no es posible obtener la clave privada a partir de la clave pública.

Con una clave privada, puedes firmar datos de forma que cualquiera que tenga tu clave pública puede verificar que esos datos los has firmado tú. La clave pública es usada como dirección pública de la cuenta de bitcoin.

Una dirección bitcoin es un hash de 160 bits de un par de claves (una pública y una privada).

Una dirección bitcoin se genera de la siguiente manera:

1- Se obtiene una clave privada ECDSA.

2- Se obtiene la clave pública correspondiente a dicha clave privada.

3- Se hace el hash SHA-256 de la clave pública.

4- Se ejecuta el hash RIPEMD-160 del resultado de la operación anterior.

5- Se añade la versión de cuenta al byte reservado para ello.

6- Se hace el hash SHA-256 al resultado de la operación anterior.

7- Se hace el hash SHA-256 otra vez al resultado de la operación anterior.

8- Se toman los primeros cuatro bytes del resultado obtenido en la operación anterior.

9- Se añaden los 4 bytes tomados al final del resultado obtenido en el punto 4.

10- Se convierte el resultado de una cadena de caracteres a una cadena en base58.

4.3.2- Ethereum

Ethereum es una tecnología muy popular que permite la creación de contratos inteligentes basándose en blockchain. Ethereum también dispone de una criptomoneda llamada Ether. De la misma forma que el bitcoins, ether se puede intercambiar entre cuentas y se usa también para pagar comisiones a los nodos que hacen que sea posible realizar transacciones a través de la blockchain de esta tecnología.

Ethereum permite a los desarrolladores crear mercados, gestionar contratos y registrar transacciones (entre muchas otras opciones) de forma que se gestionen de manera descentralizada utilizando la tecnología blockchain.

La principal diferencia entre Bitcoin y Ether es que Bitcoin se ha convertido en una moneda digital relativamente estable, Ether en cambio, tiene un uso muchos más diverso como crear nuevos tokens de pago, contratos inteligentes, aplicaciones descentralizadas, etc.

4.3.3- Usos

Las criptomonedas actualmente se usan para una gran variedad de propósitos. Los principales usos de las criptomonedas se distribuyen en los siguientes:

- Pagar productos o servicios como si se tratara de dinero convencional aprovechando las bajas comisiones que ofrecen estas monedas.
- Utilizar plataformas de pago alternativas a las convencionales.
- Inversión, estas monedas están siendo cada vez más usadas y sus precios tienden a tener subidas desmesuradas (ver figuras 13 y 14).
- Pagos de productos o servicios ilegales aprovechando la difícil trazabilidad de las transacciones entre este tipo de monedas.
- Evasión de impuestos aprovechando la propiedad descrita en el punto anterior.

A continuación se analiza la subida de valor de las criptomonedas descritas anteriormente.

El valor de cotización del Bitcoin ha variado mucho desde el momento que se creó esta moneda, convirtiéndose en un valor de mercado cada vez más valioso.

Valor del Bitcoin desde el año 2013 hasta la actualidad:

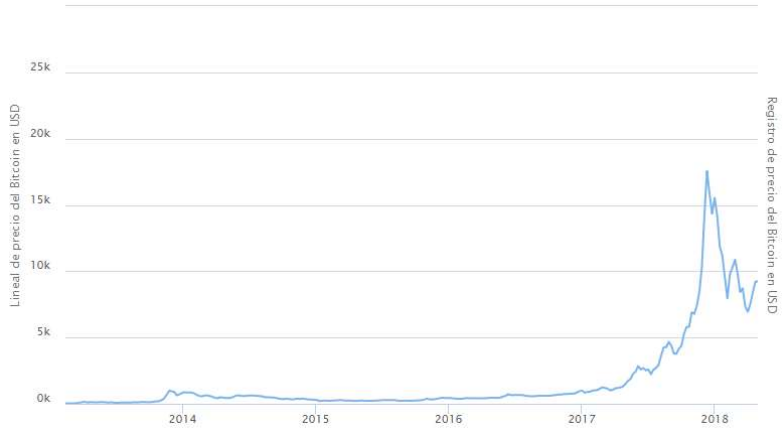


Figura 13: Valor del Bitcoin desde el año 2013 hasta la actualidad.

En el caso de Ether, su evolución ha sido parecida a la del Bitcoin en cuanto a su aumento de valor en el mercado.

Valor del Ether desde el año 2013 hasta la actualidad:

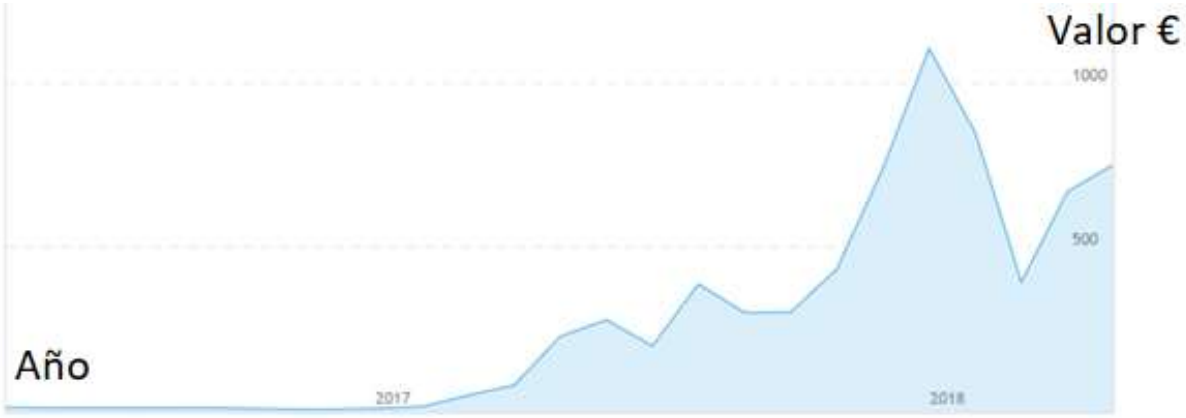


Figura 14: Valor del Ether desde el año 2016 hasta la actualidad.

5- Acciones legales

En este apartado se analizan las acciones legales que se han tomado respecto al uso de la red TOR. Este análisis se centra en la legislación que aplica en España en cuanto a los aspectos que se deben tener en cuenta cuando se hace uso de esta tecnología.

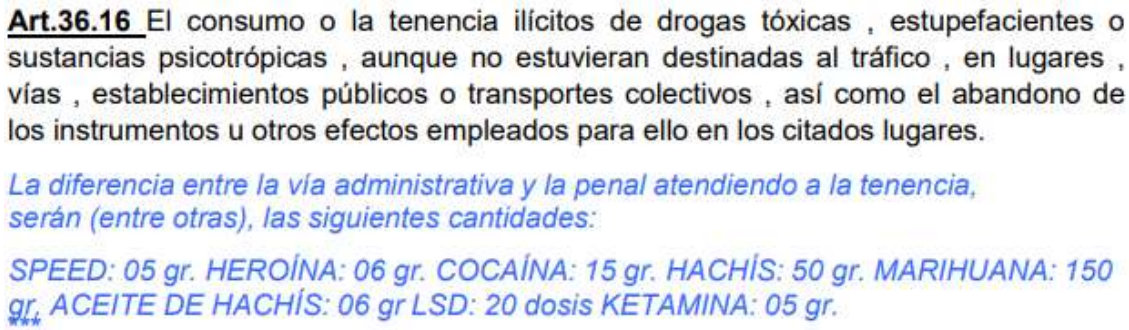
5.1- Actividades ilegales

En España está permitida la adquisición del software necesario para navegar por la red TOR, así como está permitida la navegación por esta red, independientemente de que se acceda a páginas dónde se promuevan actividades ilícitas. A continuación se muestran una serie de delitos informáticos que están regulados por el Código Penal independientemente de que cual sea su forma de acceso. El Código Penal no contempla si el acceso se realiza a través de la red TOR o si se accede sin tomar medidas para proteger su identidad.

También cabe destacar que el hecho de acceder desde la red TOR dificulta a las autoridades conocer la identidad del usuario que realiza la conexión a contenido ilegal. A continuación se muestran algunas de las acciones reguladas por el Código Penal.

- Compra o venta de drogas

La compra de drogas se castiga con penalizaciones económicas de 601 a 10400 euros (dependiendo de las cantidades de droga) según el art. 36.16 de la Ley de Seguridad Ciudadana. Este artículo especifica lo siguiente:


Art.36.16 El consumo o la tenencia ilícitos de drogas tóxicas , estupefacientes o sustancias psicotrópicas , aunque no estuvieran destinadas al tráfico , en lugares , vías , establecimientos públicos o transportes colectivos , así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares.

La diferencia entre la vía administrativa y la penal atendiendo a la tenencia, serán (entre otras), las siguientes cantidades:

SPEED: 05 gr. HEROÍNA: 06 gr. COCAÍNA: 15 gr. HACHÍS: 50 gr. MARIHUANA: 150 gr. ACEITE DE HACHÍS: 06 gr LSD: 20 dosis KETAMINA: 05 gr.

Figura 15: Art. 36.16 de la Ley de Seguridad Ciudadana con las cantidades que diferencian si el delito se procesa por la vía administrativa o penal.

En cuanto a la venta de estas, los delitos figuran en el art. 368 del Código Penal y las penalizaciones, al igual que con la compra, dependen de las cantidades que se dispongan.

El artículo 368 del Código Penal dispone: "*Los que ejecuten actos de cultivo, elaboración o tráfico, o de otro modo promuevan, favorezcan o faciliten el consumo ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas, o las posean con aquellos fines, serán castigados con las penas de prisión de tres a seis años y multa del tanto al triplo del valor de la droga objeto del delito si se tratare de sustancias o productos que causen grave daño a la salud, y de prisión de uno a tres años y multa del tanto al duplo en los demás casos. No obstante lo dispuesto en el párrafo anterior, los tribunales podrán imponer la pena inferior en grado a las señaladas en atención a la escasa entidad del hecho y a las circunstancias personales del culpable. No se podrá hacer uso de esta facultad si concurriere alguna de las circunstancias a que se hace referencia en los artículos 369 bis y 370*".

Penalizaciones:

Número de plantas o peso bruto	Cantidad útil estimada	Penas solicitadas por el Ministerio Fiscal en escrito de acusación
12 plantas	641 gramos	3.538 € multa y 2 años de prisión
8 plantas / 11.710 gramos	3.262 gramos	15.000 € multa y 1 año y 6 meses de prisión
4 plantas / 2130 gramos	563 gramos	2.000 € multa y 1 año y 6 meses de prisión
3 plantas / 3.516 gramos	956 gramos	8.000 € multa y 2 años de prisión
2 plantas / 1.897 gramos	858 gramos	5.000 € multa y 2 años y 3 meses de prisión

Figura 16: Penalizaciones por la cantidad de drogas que se dispongan (cultiven, elaboren, trafiquen)

- Pornografía infantil

Está regulado por el Código Penal (art. 189.5) el acceso o posesión de pornografía infantil, por lo que si se accede a este tipo de contenido el castigo impuesto será de pena de prisión de uno a cinco años.

Artículo 189.5 del Código Penal: *Al que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección*.

La reforma 1/2015 del art. 189.5 amplía las conductas para abarcar estos supuestos: *a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.*

6- Conclusiones

La primera conclusión que se extrae es que la navegación a través de la red TOR proporciona anonimato, no obstante, existen diferentes técnicas que pueden comprometer este anonimato tanto en la navegación de los usuarios como en la publicación de servicios en esta red.

La segunda conclusión que se presenta es que para poder realizar los ataques que se describen en este documento es necesario tener el control de nodos de la red TOR y en la mayoría de casos, se precisa tener el control del nodo que realiza la petición final al servidor de destino.

Finalmente, se concluye que la desanonimización de los usuarios y servicios es viable mediante las diferentes técnicas analizadas, pero es muy difícil conseguirlo teniendo en cuenta el tamaño de la infraestructura de la red TOR actual.

En este apartado se presentan las conclusiones de los objetivos tratados en este documento. Las conclusiones extraídas son las siguientes:

Sobre el análisis de los mercados se concluye que:

- Los mercados negros tienen un papel muy importante en la comercialización de productos y servicios ilegales a nivel mundial.
- A pesar de que las autoridades persiguen y censuran los mercados negros, estos se lanzan de nuevo en diferentes versiones y siguen con sus actividades.
- A pesar de que la red TOR proporciona anonimato, en muchas ocasiones las autoridades han acabado descubriendo a las personas responsables de la creación y gestión de los mercados negros.

Sobre el estudio de las criptomonedas se concluye lo siguiente:

- Ofrecen muchas ventajas innovadoras a sus propietarios que hacen que sus valores se incrementen hasta convertirse en productos de inversión.
- Al proporcionar anonimato a los propietarios de las monedas en su posesión y transferencias hace que sea el método de pago perfecto para los mercados negros.

Sobre el análisis de la legislación respecto a la red TOR se concluye que:

- Actualmente no se restringe a nivel legal el acceso a contenidos de Internet a través de la red TOR en España.
- El acceso a contenidos o la realización de actividades ilegales a través de la red TOR no garantiza que las autoridades sean incapaces de descubrir la identidad real de los usuarios, así que los delitos por estos accesos o estas actividades ilegales aplican exactamente de la misma medida se accedan a través de la red TOR o de las formas convencionales sin ocultar la identidad del usuario.

7- Bibliografía

Página oficial del proyecto TOR.

- https://www.torproject.org/

Carlos Borrego Iglesias. Departament d'Enginyeria de la Informació i de les Comunicacions Universitat Autònoma de Barcelona. Tecnologías avanzadas de Internet. Teaching material.

- http://www.deic.uab.es/material/102749-Arch.pdf

Jesús Díaz (INCIBE). Tor, servicios ocultos y desanonimización Publicado el 07/01/2015.

- https://www.certsi.es/blog/tor-servicios-ocultos-desanonimizacion

Pedro Catillo. Vulnerabilidades en Tor ponen en peligro el anonimato en los servicios ocultos. 27 julio, 2015.

- https://securityinside.info/vulnerabilidades-en-tor-anonimato-servicios-ocultos/

Sam DeFabbia-Kane. Universidad de Wesleyana. Analizando la Efectividad de Ataques de Correlación Pasivos en la red de Anonimato TOR. 2011.

- https://www.slideshare.net/chemai64/analizando-la-efectividad-de-ataques-de-correlacion-pasivos-en-la-red-de-anonimato-tor

Roger Dingledine, Nick Mathewson, Paul Syverson. Naval Research Lab. Tor: The Second-Generation Onion Router.

- https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

ROBERT AUGUSTUS HARDY, JULIA R. NORGAARD. Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. 04 November 2015.

- https://www.cambridge.org/core/services/aop-cambridge-core/content/view/560A8645D47BBDDC4E71101EC1C100CA/S1744137415000454a.pdf/reputation_in_the_internet_black_market_an_empirical_and_theoretical_analysis_of_the_deep_web.pdf

Página oficial del Proyecto Bitcoin.

- https://bitcoin.org/es/

Histórico de valores del Bitcoin y de Ether.

- https://es.investing.com/crypto/bitcoin/btc-usd-historical-data
- https://es.tradingview.com/symbols/BTCUSD/

Estadísticas de uso de la blockchain.

- https://blockchain.info/es/charts

Página oficial del proyecto Etherum.

- https://www.ethereum.org/ether

Iván M. P. LEY 4-2015 SOBRE SEGURIDAD CIUDADANA COMENTADA CONSENTENCIAS Y LEGISLACIÓN

- http://www.policiacanaria.com/sites/default/files/ley-4-2015_sobre_seguridad_ciudadana_comentada_con_sentencias_y_normativa_ur2.pdf

Agencia Estatal Boletín del Estado:

- https://www.boe.es