Red de anonimización TOR y cibermercados negros

TRABAJO FIN DE MÁSTER

Roberto García López

Tutor:

Ángela María García Valdés

- MISTIC - Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Diciembre 2017

Agradecimientos

A mi familia porque sin ellos nada de esto hubiera sido posible.

A mis amigos por los ánimos que me han dado en los momentos malos.

A mis compañeros de universidad por el apoyo que me han dado.

Y a todo el personal de la universidad y sus colaboradores por ayudarme en todo lo que he necesitado.

Muchas gracias.

Resumen

Mi objetivo con este trabajo es realizar un estudio sobre la red de anonimato TOR, con el fin de comprender cómo funciona y conocer características. Seguidamente, me centraré en las formas que existen actualmente para desanonimizar tanto a los usuarios, como a los servicios de esta red.

Actualmente, la unión de la red TOR junto con las monedas virtuales, ha propiciado la creación de numerosos mercados negros en red, que se aprovechan del anonimato que encuentran en esa unión. Analizaré esos mercados, con el objetivo de comprender cómo se comportan.

Por último, profundizaré en las acciones legales que se están realizando en contra de los criptomercados y los delitos que se realizan en ellos.

Abstract

This paper intends to make a study about the TOR anonymity network, with the aim of understand how it works and get to know its caracteristics. Next, I will seek the ways that currently exist to deanonymize the users and services of this network.

Currently, the union of the TOR network with the virtual currencies have favoured the creation of great amount of black markets in the network that take advantage of the anonymity that they find in that union. I will study those markets, in order to understand how they behave.

Finally, I will seek the legal actions that are being made against cryptomarkets and crimes that take place in them.

Contenido

1 Introducción

Actualmente una gran parte de las actividades delictivas que se realizan a través de Internet, se producen dentro de la red TOR. De este hecho, nace la importancia de conocer bien las características de esta red y los cibermercados negros que actúan dentro ella, aprovechándose de sus características y del anonimato que proporcionan.

Voy a estudiar la arquitectura de la red TOR y la manera en que se realizan las conexiones dentro de ella, para así poder entender cómo se produce dicho anonimato y cómo se usa para montar mercados en los que se realizan posibles actividades delictivas. También investigaré qué papel juegan las monedas virtuales en las actividades delictivas que se comenten a través de dicha red.

Para poder combatir estas actividades, investigaré de qué maneras podemos desanonimizar a los participantes en estos cibermercados negros y cómo la ley está actuando contra ellos.

1.1 Objetivos

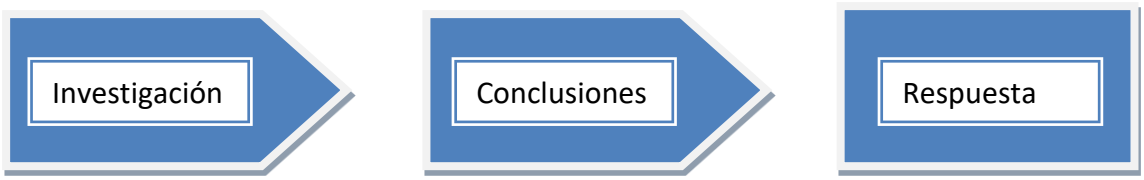
Los objetivos que han de verse logrados al finalizar este TFM, serán los siguientes:

- La comprensión de los fundamentos de operación de la red TOR, a través del conocimiento de sus componentes, sus interacciones y de cómo los usuarios y los servicios se esconden en la red.
- El aprendizaje de técnicas de desanonimización de usuarios y servicios.
- La realización de un estudio sobre los mercados negros de la red TOR, describiendo como operan, cómo los participantes ocultan sus actividades comerciales y cómo están involucradas las criptomonedas en los cibermercados negros.
- Conocer que se está haciendo actualmente a nivel de legislación para que las leyes sean cumplidas.

1.2 Metodología y tareas

Con el objetivo de completar los 4 objetivos propuestos utilizaré la siguiente metodología, compuesta de 3 tareas:

- Investigación y búsqueda de información para cada objetivo.
- Extracción de conclusiones en base a la información encontrada.
- Redacción del contenido que dé respuesta a los objetivos en base a las conclusiones extraídas.



Será un proceso repetido hasta que los 4 objetivos planteados sean resueltos.

1.3 Planificación

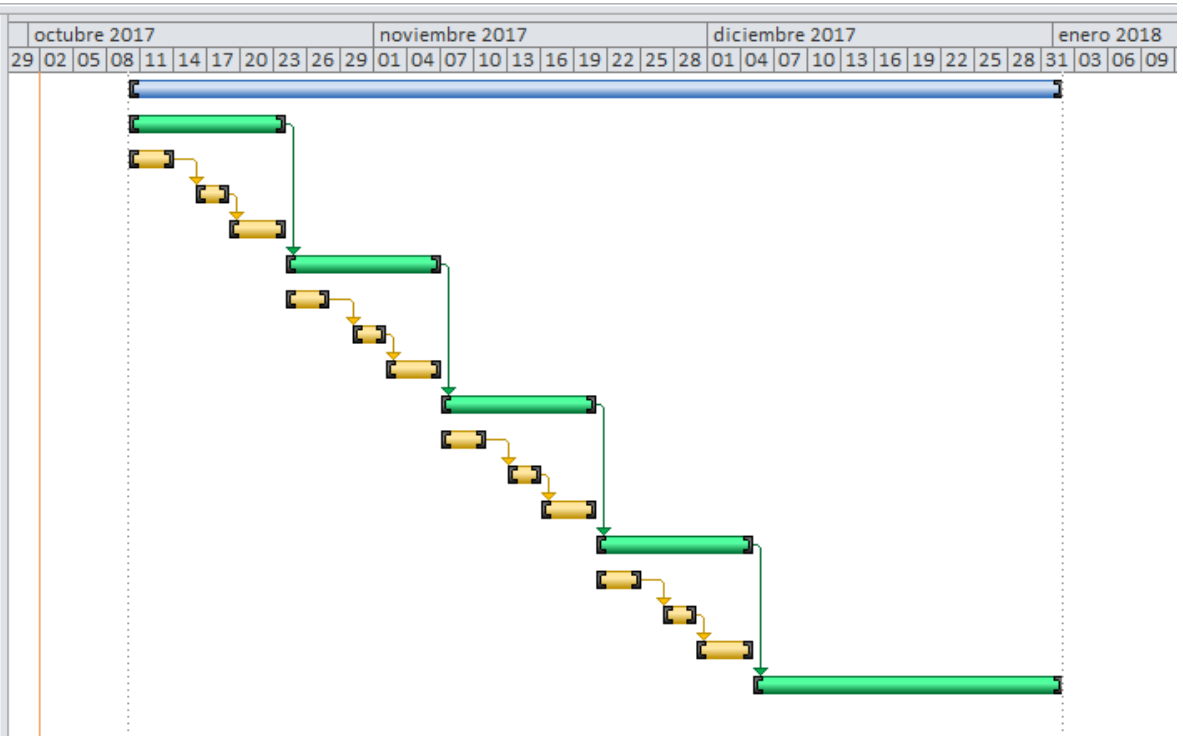
La planificación se ha realizado en base a tres aspectos:

- Los objetivos marcados.
- La metodología elegida.
- Las tareas.

En la siguiente página se puede ver un diagrama de Gantt en el que se representa dicha planificación.

La duración del TFM al completo se representa en color azul, la duración de los objetivos en color verde y la de las tareas en amarillo.

Nombre de tarea	Duración	Comienzo	Fin
TFM	60 días	mar 10/10/17	lun 01/01/18
Primer objetivo	10 días	mar 10/10/17	lun 23/10/17
Investigación	4 días	mar 10/10/17	vie 13/10/17
Conclusiones	3 días	lun 16/10/17	mié 18/10/17
Respuesta	3 días	jue 19/10/17	lun 23/10/17
Segundo objetivo	10 días	mar 24/10/17	lun 06/11/17
Investigación 2	4 días	mar 24/10/17	vie 27/10/17
Conclusiones 2	3 días	lun 30/10/17	mié 01/11/17
Respuesta 2	3 días	jue 02/11/17	lun 06/11/17
Tercer objetivo	10 días	mar 07/11/17	lun 20/11/17
Investigación 3	4 días	mar 07/11/17	vie 10/11/17
Conclusiones 3	3 días	lun 13/11/17	mié 15/11/17
Respuesta 3	3 días	jue 16/11/17	lun 20/11/17
Cuarto objetivo	10 días	mar 21/11/17	lun 04/12/17
Investigación 4	4 días	mar 21/11/17	vie 24/11/17
Conclusiones 4	3 días	lun 27/11/17	mié 29/11/17
Respuesta 4	3 días	jue 30/11/17	lun 04/12/17
Memoria final	20 días	mar 05/12/17	lun 01/01/18



2 Fundamentos de operación de la red TOR

2.1 Qué es la red TOR

La red TOR es una red de comunicaciones distribuida sobre internet en la que el encaminamiento de los mensajes se realiza entre diferentes nodos, de tal manera que ni los mismos nodos conocen la totalidad del camino que recorren los mensajes. Los usuarios no revelan su dirección IP en gran parte de la conexión, por lo que mejora notablemente el anonimato en las conexiones. La información viaja encriptada en capas, con lo que también nos asegura la privacidad de los mensajes.

A continuación, detallaré en más profundidad opera esta red y por consiguiente cómo se consigue el anonimato dentro de ella.

2.2 Componentes de la red TOR

Normalmente cuando realizamos una comunicación a través de Internet usamos un encaminamiento directo a nuestro router, luego a los servidores de nuestro IPS (proveedor de internet) y por último al destinatario, por lo que, si alguien estuviese escuchando dicha comunicación, no tendría problemas en saber el origen y el destino de la misma.

Sin embargo, la red TOR se conforma mediante nodos y manda la información a través de ellos de una forma aleatoria.

Los tipos de nodos que intervienen la comunicación son los siguientes:

- **Nodos OR (Onion Router):** Funcionan como encaminadores y en algunos casos además como servidores de directorio (DNS). La conexión entre los nodos OR es de tipo TLS (Transport Layer Security) de manera que la información que viaja entre ellos lo hace encriptada. Este tipo de nodos, puede actuar de 3 maneras diferentes:
    - Nodo de entrada (Entry guard): Es el primer nodo por el que entra el mensaje.
    - Nodo de salida (Exit relay): Es el último nodo antes del destino.
    - Nodo intermedio (Relay): nodo repetidor.
- **Nodos OP (Onion Proxy):** Los usuarios son los encargados de tener en ejecución en su máquina el software que habilita estos nodos, que son los encargados de buscar el camino de conexión, manejar las conexiones del usuario y obtener la información de servicio de directorio. Los OP aceptan flujos TCP de aplicaciones de usuarios y las multiplexa a través de los nodos OR.
- **Los servicios de directorio:** son servidores que tienen el esquema de interconexión de todos los OR. Los OP se comunican con ellos para conseguir un camino entre los OR para enviar el mensaje al destino. Algunos OR hacen a la vez de OR y de Servicio de directorio.

Las conexiones entre estos tipos de nodos no son permanentes, para evitar el análisis de nuestras comunicaciones, generalmente se escogen nuevos nodos OR cada diez minutos (si existe una comunicación) o cada hora (si no se están transmitiendo datos).

2.3 Cómo funciona la red TOR y el enrutado “cebolla”

Como he comentado anteriormente, normalmente realizamos conexiones de manera directa, sin embargo, la red TOR las realiza de una forma indirecta y aleatoria mediante el enrutado cebolla (Onion Router), buscando así la privacidad y el anonimato de los datos.

Pongamos que un ordenador A quiere mantener una conexión y mandar un mensaje, a través de la red TOR, a la máquina B. Ese ordenador A actuará de nodo OP y lo primero que necesitará es conocer la lista de nodos OR disponibles para realizar dicha conexión. Para ello, realizará una petición a un servidor de directorio en el que se almacenan la lista de nodos disponibles.

A continuación, se establece un camino aleatorio entre A y B que pasa por diferentes nodos OR y se negocia la clave pública con cada uno de estos nodos. Todos los nodos son elegidos al azar y ninguno puede ser usado dos veces.

El ordenador A, utilizará un cifrado en capas de forma asimétrica de la siguiente manera:

Con la clave pública del último nodo de la ruta, se cifra el mensaje y las instrucciones para llegar hasta B desde ese último nodo. De esta manera sólo él podrá descifrarlo.

A continuación, a este paquete de datos se le añaden las instrucciones para llegar desde el penúltimo nodo hasta el último y todo ello se cifra con la clave pública del penúltimo nodo. Y así sucesivamente, hasta que cifremos el mensaje completamente.

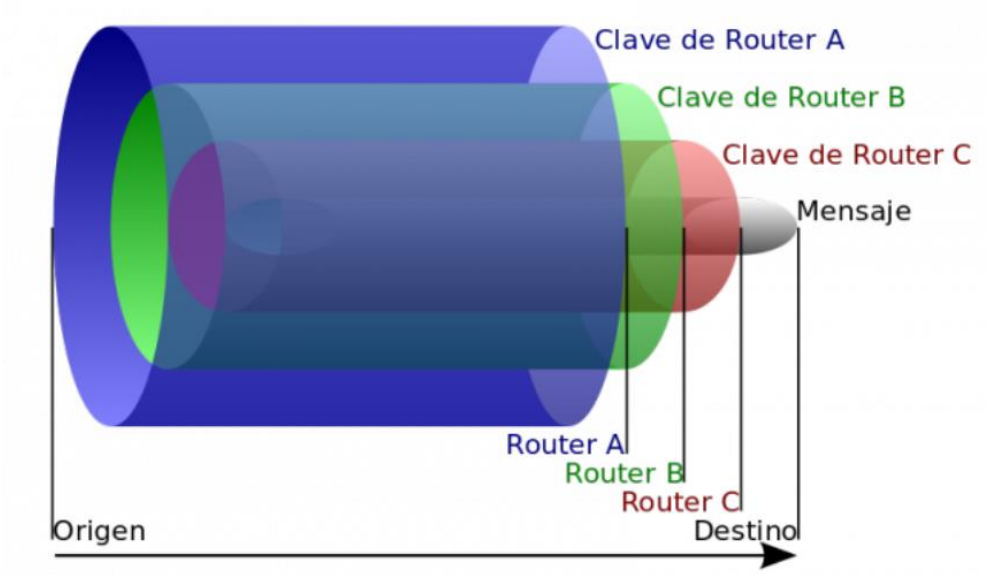


Ilustración 1. Cifrado en capas (Fuente de la imagen: https://www.genbeta.com/)

A este tipo de cifrado en capas, también se le denomina cifrado en forma de cebolla.

Una vez tengamos el mensaje totalmente cifrado se lo enviaremos al primer nodo del camino. Este solamente podrá descifrar la primera capa y así encontrará la forma de llegar al siguiente nodo de la lista, al cual enviará el mensaje. El siguiente nodo lo recibe y desencripta su capa averiguando el siguiente nodo y así sucesivamente.

De esta manera cada nodo sólo tiene acceso a las instrucciones para llegar al siguiente nodo del camino y únicamente el último nodo tendrá acceso al mensaje inicial.

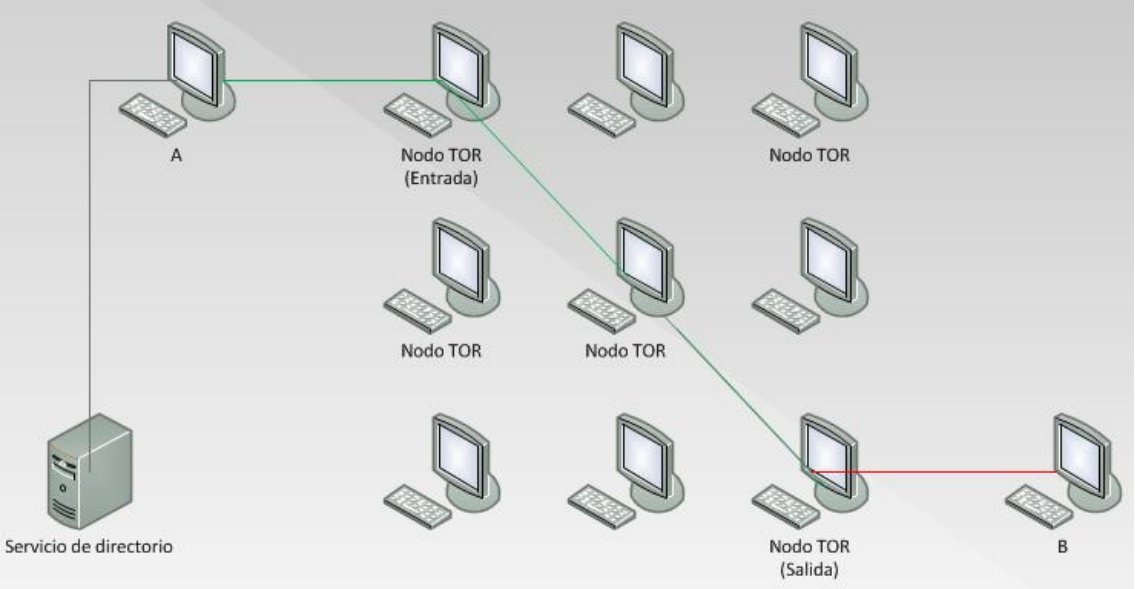


Ilustración 2. Esquema de conexión en la red TOR

La última línea del camino se representa en color rojo debido a que la información ya está totalmente descifrada y, por lo tanto, del nodo de salida al destino B viaja sin cifrar. Es muy recomendable encriptar el mensaje original, para que de esa manera el nodo de salida no tenga acceso al mensaje y viaje seguro hasta el destino.

2.4 Cómo se esconden los usuarios y los servicios dentro de la red TOR

Por las características de la red vistas en el apartado anterior, el usuario queda bastante protegido en cuanto a su privacidad se refiere. El anonimato se consigue porque las peticiones a cualquier servidor se ven como si proviniesen desde el nodo final. Pero a su vez éste sólo ve que esa petición tiene como origen otro nodo diferente, el nodo intermedio y por último éste ve al nodo inicial, el cual ve al usuario que realmente ha hecho la petición. A todo esto, incluimos la confidencialidad, dado que se realizan varias capas de cifrado para que los nodos del circuito no puedan acceder al cuerpo del mensaje o petición.

Aun así, no es un sistema infalible y a éste se le pueden añadir algunas prácticas que mejoren el anonimato. Una de ellas, como he comentado anteriormente, es la de cifrar el mensaje original para que del último nodo hasta el destino final viaje de forma segura.

Otra manera de aumentar la privacidad es, aparte de ser un usuario de la red que emite mensajes, puedes ser también un nodo de la red, de tal manera que, si alguien está analizando las comunicaciones del usuario, no podrá saber si es el que inicia el envío del mensaje o simplemente está participando como nodo en una comunicación ajena.

Hay varias formas de entrar a la red TOR, pero usando el proprio navegador TOR como entrada, aumenta la seguridad ya que está preparado si se configura correctamente para no enviar información personal, como por ejemplo la IP del usuario.

Si se quiere añadir más seguridad, se puede acceder a la red TOR a través de una VPN. Aunque nadie sepa lo que hace un usuario dentro de la red, se puede saber que la está usando y eso puede dar lugar a sospecha y a. De esta manera nadie podrá saber lo que se está haciendo. Se recomienda usar una VPN con una fuerte encriptación y que no deje registro en logs.

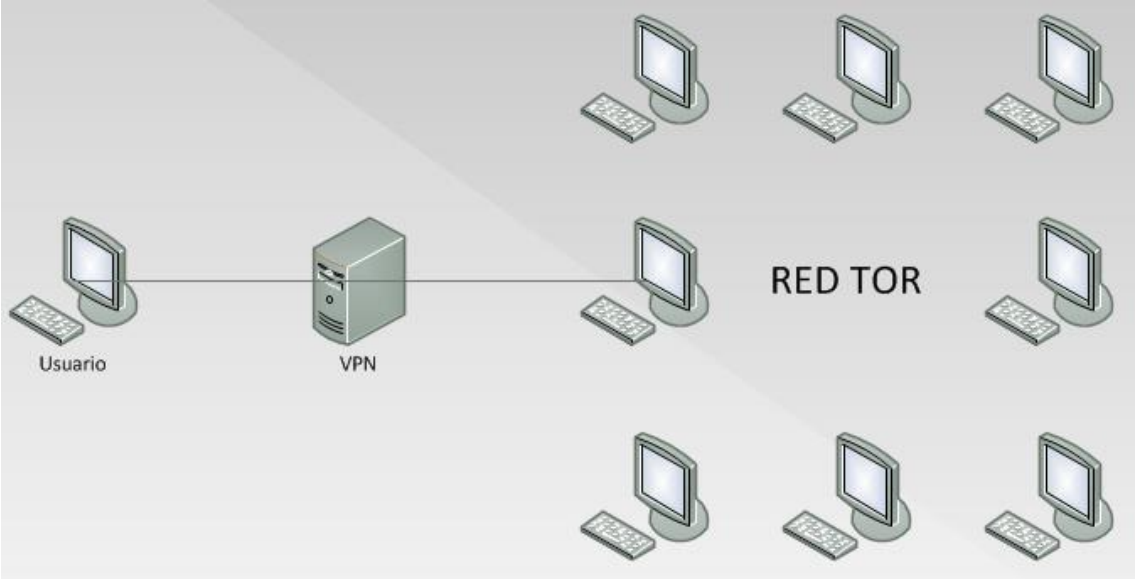


Ilustración 3. Acceso a la red TOR a través de VPN

Por otro lado, tenemos los llamados servicios ocultos (hidden services), que son servicios que ocultan su localización. Pueden ser de cualquier tipo siempre y cuando se basen en el protocolo TCP.

Aunque dentro de estos servicios hay algunos totalmente legales, el anonimato que proporciona la red hace que también haya otros que son delictivos. Estos servicios, evidentemente no son indexados por los buscadores que usamos normalmente.

Un cliente que accede a un servicio oculto realmente no accede a la propia máquina en sí (ya que se desconoce su dirección IP real), sino que accede únicamente al servicio publicado por la máquina. La única forma de acceder a un servicio es a través de su dirección ".onion".

Las direcciones ".onion" se forman de la siguiente manera:

- Se crea una pareja de claves RSA de 1024 bits y un fichero llamado hostname que contiene la dirección pública necesaria para acceder al servicio.
- Se calcula el SHA1 de la clave pública generada.
- De los 160 bits que forman el hash, se toma la primera mitad y se codifica en Base32, consiguiendo que todos los nombres de dominio tengan exactamente una longitud de 16 caracteres y solo contengan números entre 2-7 y letras entre a-z.
- Por último, se añade al nombre generado el sufijo ".onion".

Al realizar peticiones a éstos servicios nunca habrá un nodo de salida, por lo tanto, como no se sale de la red TOR, tanto el origen como el destino se mantendrán anónimos.

Un servicio tiene varios nodos de introducción notificados en una base de datos. Cuando un usuario quiere conectarse a ese servicio, envía una dirección de punto de encuentro y una clave pública a uno de los nodos de introducción del servicio. El nodo se conectará con el servicio y éste con el punto de encuentro, estableciendo así una conexión entre el servicio y el usuario.

El proceso con más detalle se realiza de la siguiente manera:

1. El servicio oculto elige al azar 3 nodos de la red TOR, éstos serán sus puntos de acceso y creará un circuito (formado por 3 nodos) con cada uno de ellos. Además, genera un archivo que contiene los 3 puntos de acceso, su clave pública y el dominio ".onion". Este archivo se sube a un servidor de directorios.

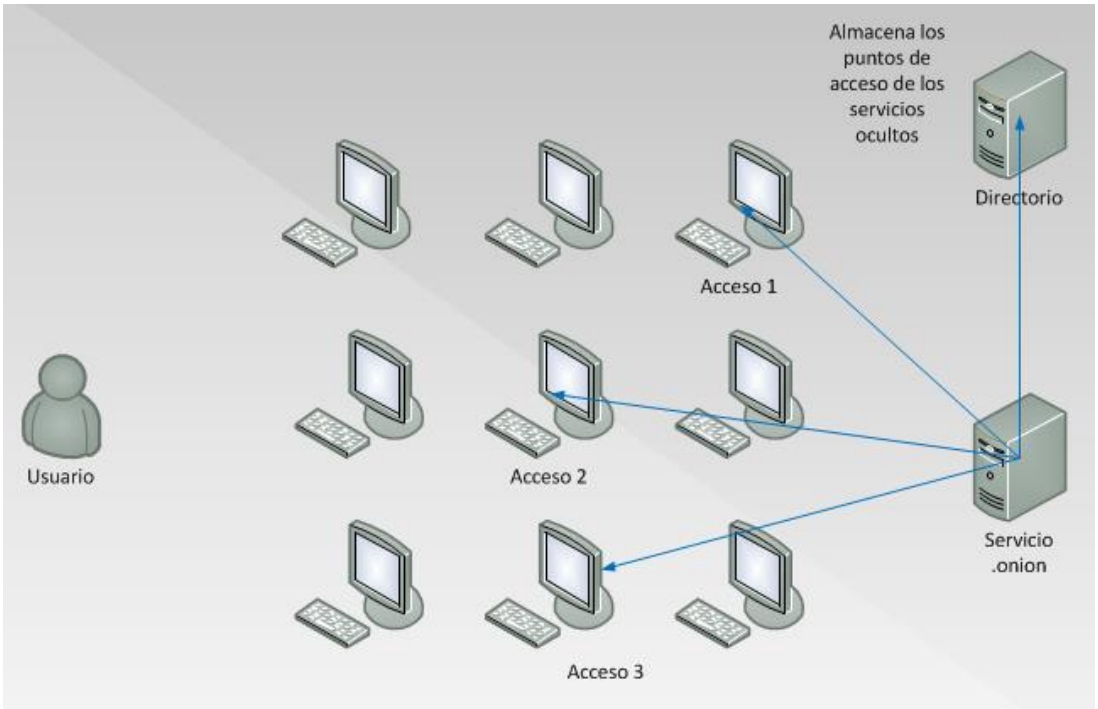


Ilustración 4. Primer paso para la conexión a un servicio oculto

2. Cuando el cliente quiere conectarse al servicio lo hará mediante el dominio ".onion" y para ello recupera del Directorio los puntos de acceso al servicio. Después elige un nodo de la red al azar como punto de encuentro y le entrega una cookie de un solo uso para identificar posteriormente al servicio.

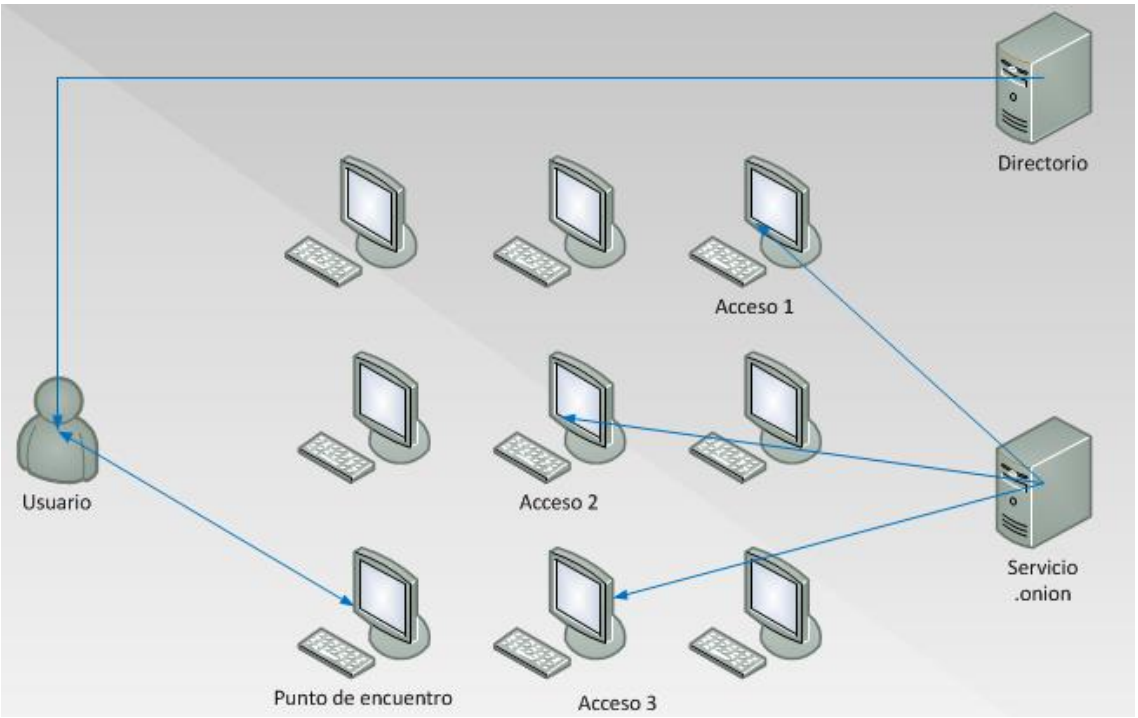


Ilustración 5. Primer paso para la conexión a un servicio oculto

3. Posteriormente el usuario envía a uno de los puntos de acceso un mensaje cifrado con la clave pública del servicio, que contiene la cookie y el nodo que actuará como punto de encuentro.

4. El punto de acceso envía el mensaje al servicio y este al desencriptarlo conocerá el punto de acceso. Finalmente, se conectará a él enviado la cookie de un solo uso para que se le reconozca.

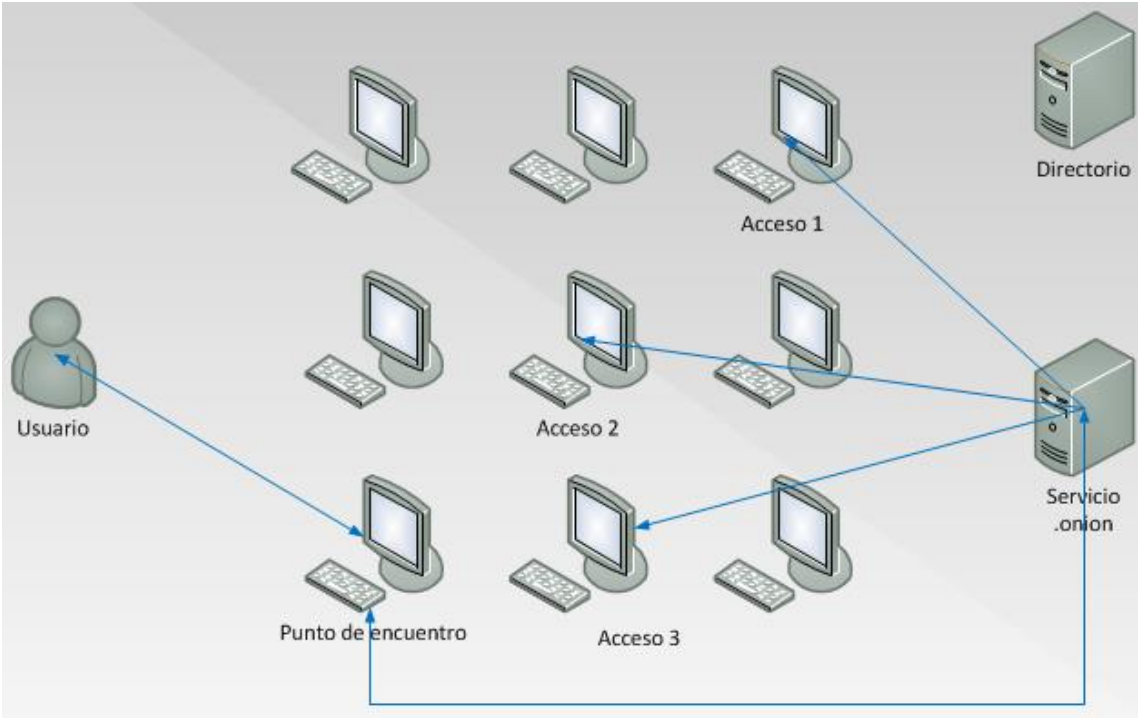


Ilustración 6. Último paso para la conexión a un servicio oculto

La comunicación entre ambos es anónima ya que las conexiones que se producen con el punto de encuentro son conexiones a través de circuitos TOR de 3 nodos cada uno de ellos. Tanto el cliente como el servicio oculto están protegidos ya que ninguno conoce la dirección del otro.

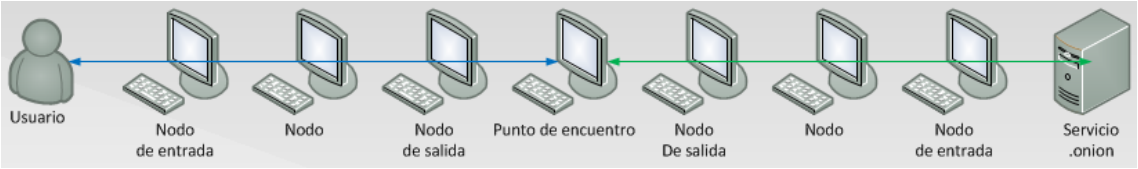


Ilustración 7. Conexión usuario/servicio a través de un punto de encuentro

Sin embargo, a continuación, voy a explicar las técnicas que existen para romper el anonimato que proporciona la red TOR.

3 Técnicas de desanonimización de usuarios y servicios de la red TOR.

A pesar del anonimato que proporciona la red TOR, es susceptible a diversos ataques que pueden comprometer dicho anonimato, tanto para los servicios como para los proprio usuarios.

Una de sus vulnerabilidades proviene del análisis de grandes cantidades de datos del tráfico de la red, a través de los cuales se puedan encontrar patrones que confirmen qué usuario está conectado a la red y qué servicio está usando.

Para vulnerar el anonimato de un cliente de TOR, es necesario comprometer el tráfico tanto el nodo de entrada como el nodo de salida de la red. Sin embargo, para vulnerar el anonimato de un servicio oculto, sólo hace falta analizar el tráfico en el nodo de salida (ya que el nodo de entrada puede ser directamente el atacante).

Como la red TOR es una red distribuida cuyos nodos son libres y cedidos por terceras personas, la mayoría de los ataques que describo a continuación son susceptibles de ser combinados con un ataque Sybil, que consiste en controlar la mayoría de los nodos del sistema distribuido, corrompiendo así la red y pudiendo acceder a mucha más información de lo normal.

3.1 Técnicas de desanonimización de usuarios

3.1.1 Errores de usuarios

Muchas veces son los mismos usuarios los que dejan su identidad al descubierto cometiendo errores, como por ejemplo usar a través de la red TOR direcciones de correo electrónico o nombres de usuario que también usan en Internet. De esta manera, se relaciona el tráfico de TOR de ese usuario con otro tráfico del que se puede averiguar su identidad.

Otro error común es el mal uso del navegador con el que se accede a la red, de tal manera que por ejemplo no se eliminen todas las cookies. Las cookies de DoubleClick serían una excelente forma para identificar usuarios TOR.

También se puede dar el caso de que un usuario busque una dirección ".onion" a través de Internet dejando patente que servicio quiere usar.

3.1.2 Correlación de flujo

Los ataques de correlación consisten en observar los nodos de entrada y salida de TOR, e intentar encontrar patrones que puedan emparejar los tráficos de entrada con los de salida. Como el tráfico que cruza la red TOR está encriptado, se deben observar detalles a bajo nivel, como por ejemplo la longitud de los paquetes, ya que TOR no protege ciertas estadísticas sobre el tráfico de la red, como el tiempo entre paquetes, las direcciones y la frecuencia.

Hay diversas formas de realizar correlaciones de flujo, a continuación, comentaré algunas de ellas:

3.1.2.1 Contando paquetes

En este ataque, se cuentan el número de paquetes que entran y salen en el primer nodo de la red para determinar el siguiente nodo del circuito. El procedimiento se repite en otros nodos hasta que se determina el destinatario. Este método es relativamente sencillo, pero requiere que el atacante sea capaz de observar una gran cantidad de tráfico en la red.

3.1.2.2 Análisis de sincronización

La sincronización de paquetes es otra parte de los datos que puede ser usada para correlacionar flujos de redes. Una forma sencilla de utilizar los datos de sincronización de paquetes es usar algún tipo de función de correlación para intentar correlacionar flujos basados en su retardo entre paquetes.

La debilidad de la mayor parte de este tipo de ataques es que depende de que el atacante controle una gran cantidad de nodos para que pueda tener una gran tasa de efectividad.

3.1.2.3 Correlación activa de sincronización

Este tipo de ataques, son una mejora de las correlaciones basadas en el tiempo. Funcionan teniendo un nodo atacante alterando la señal de retraso de un paquete de una conexión al soltar o retrasar paquetes en un flujo.

3.1.2.4 Búsquedas DNS

Las solicitudes DNS son otra oportunidad para identificar a los usuarios de la red TOR. Esta técnica consiste en la búsqueda de huellas de las propias webs conocidas dentro de tráfico en los nodos de entrada y se comparan con las solicitudes DNS en el tráfico de los nodos de salida que va sin cifrar.

3.1.2.5 Analizando tiempos

Otro ejemplo sería analizar los tiempos, si por ejemplo entra un paquete en un nodo de entrada y sale otro por un nodo de salida a los 250 milisegundos con dirección a un usuario, la repetición de esta latencia varias veces, nos puede llevar a pensar que ese usuario está originando ese tráfico.

3.1.3 Raptor

Esta técnica es más moderna que las anteriores y se basa en romper el anonimato de la red controlando un Sistema Autónomo completo.

Un Sistema Autónomo es una red de gran tamaño que se comporta de forma autónoma en cuanto a su enrutamiento interno, y controla el encaminamiento de tráfico hacia y desde otros sistemas autónomos por medio de protocolos de enrutamiento de frontera llamados BGP (Border Gateway Protocols).

Controlando un Sistema Autónomo, se puede reunir suficiente información para desanonimizar a sus usuarios en cualquiera de las siguientes situaciones:

- Observando el tráfico de datos desde el cliente TOR al nodo de entrada y desde el nodo de salida al servidor publicado en la red TOR.
- Observando el tráfico desde el cliente al nodo de entrada y capturar las respuestas TCP ACKs enviadas desde el servidor web.
- Capturando el TCP ACK de hacia el cliente TOR y el tráfico de datos desde el nodo de salida al servidor.
- Capturando sólo el tráfico TCP ACK desde el nodo del cliente y del servidor, correlando los mensajes de acknowledge de la comunicación TCP.

3.1.4 Ataque predecesor

Uno o varios nodos controlados por el atacante realizan un seguimiento de las conexiones. Cada vez que un cliente reconstruye un circuito, generalmente cada 10 minutos, tendrá que conectarse a otro nodo. Por lo tanto, un cliente realizará más conexiones que otros nodos.

Si un atacante controla muchos nodos, puede hacerlos fallar, obligando así al cliente a tener que realizar más conexiones de las normales y de esta manera obteniendo la oportunidad de obtener mucha más información que en otra situación. La dirección del cliente aparecerá en las conexiones como iniciador de la comunicación mucho más de lo normal.

3.2 Técnicas de desanonimización de servicios

Estas técnicas se basan en el hecho de que hay servicios directorio en el que se guardas bases de datos distribuidas (hash table) con los descriptores de los servicios ocultos.

Para que un cliente pueda acceder al descriptor de un servicio oculto deberá poder calcular su identificador de la siguiente manera:

descriptor-id = sha1(permanent-id | sha1(time-period | descriptor-cookie | replica))

- El descriptor-cookie se trata una variable opcional, que consiste un secreto compartido entre un servicio oculto y sus clientes que impide el cálculo de los identificadores y por tanto el acceso no autorizado al mismo. Con ello se consigue que el listado de puntos de introducción quede cifrado y, para un cliente que desconozca este secreto, sea imposible acordar un punto de encuentro con el servicio oculto.
- El valor de time-period cambia cada 24 horas, y es el responsable de que los identificadores, y por tanto los HSDirs responsables de un servicio oculto, cambien periódicamente.
- replica se trata de una variable de tipo entero que toma dos posibles valores: 0 y 1. De esta forma se consigue generar un par de identificadores (utilizando ambos valores) distribuidos en diferentes partes del círculo.
- La variable permanent-id tiene un valor fijo y se obtiene a partir de los primeros 80 bits del SHA1 de la clave pública del servicio oculto.

Por lo tanto, en base a la variable “descriptor-cookie”, podremos distinguir entre los servicios que podemos calcular su descriptor id y los que no. En base a esta forma de almacenar los descriptores comentaré más adelante las formas desanonimizar los servicios ocultos.

El control por parte de un atacante de un lado de la comunicación con un servicio oculto significa que puede controlar un nodo de entrada del servicio oculto para implementar un ataque de correlación de tráfico y revelar la ubicación real del servicio oculto. En particular, un atacante puede:

- Dada la dirección ".onion" de un servicio oculto con una lista no encriptada de puntos de acceso, puede determinar si sus nodos de entrada son utilizados por este servicio oculto.
- Puede determinar las direcciones IP de los servicios ocultos que usan los nodos de guardia del atacante.
- Puede determinar si los nodos de entrada del atacante son utilizados por cualquiera de los servicios ocultos, incluso si la lista de puntos de introducción está encriptada.

3.2.1 Obtención de direcciones ".onion"

El primer paso para desanonimizar un servicio oculto, debe ser la obtención de su dirección ".onion". Como es de esperar, no existe un repositorio con todas estas direcciones. Por lo tanto, si no se dispone de ella, simplemente con montar un nodo servicio de directorios (HSDir), un atacante ya podría empezar a recoger direcciones ".onion" durante días a partir de los descriptores que fuera almacenando. Cada 24h, se van a añadir nuevos descriptores de servicios, por lo que podrá obtener una gran cantidad de información valiosa.

Aparte de las direcciones, un atacante también podría obtener estadísticas sobre el número de peticiones recibidas por servicio oculto, el número de servicios ocultos observados, el número de servicios ocultos por días observados, etc.

También existen mercados donde se venden archivos con miles de estas direcciones.

3.2.2 Descriptores no encriptados

Los nodos de entrada son nodos especiales debido a que los clientes y servicios ocultos eligen (y rotan periódicamente) para acceder a la red de TOR. Por tanto, los nodos de entrada son los únicos nodos que tienen acceso a IPs reales de quienes acceden a TOR.

Por ello, para que este ataque sea satisfactorio y se consiga la dirección IP, es imprescindible que el servicio oculto elija como nodo de entrada un nodo controlado por un atacante y que la comunicación (atacante – servicio oculto) discurra por un punto de encuentro elegido por el mismo.

Si un atacante quisiera obtener la dirección IP real (122.122.122.122) del servicio oculto con dirección ejemplo.onion. Uno de los ataques que podría realizar sería el siguiente:

1) Un nodo controlado por el atacante es seleccionado como nodo de entrada por parte del servicio oculto ejemplo.onion.
2) El cliente (atacante) establece una conexión con ejemplo.onion.
    - Al ser el atacante quien establece la conexión, puede decidir un nodo de encuentro que él controle.
    - Esta conexión tiene asociada una cookie creada por el cliente (atacante) y transmitida también al servicio oculto, que utiliza el nodo de encuentro para poder distinguir entre conexiones.
3) Cuando el servicio en ejemplo.onion se conecta con el punto de encuentro malicioso:
    - El nodo de encuentro puede asociar esta conexión iniciada por ejemplo.onion con la conexión iniciada por él mismo, ya que contienen la misma cookie.
    - El nodo de encuentro envía un tráfico anómalo hacia ejemplo.onion, seguido de una petición para cerrar la conexión.
4) Por último, el nodo de entrada controlado por el atacante asocia la conexión recibida desde 122.122.122.122 con la conexión del nodo punto de encuentro con el servicio ejemplo.onion, si:
    - El nodo de entrada recibe la petición de cierre de conexión después de que el nodo de encuentro reciba la conexión de ejemplo.onion con la cookie creada por el atacante.
    - El número de paquetes recibidos por el nodo de entrada corresponde con el patrón de 50 paquetes enviado por el nodo de encuentro.

Ilustración 8. Conexión atacante/servicio a través de un punto de encuentro controlado por el atacante

Siguiendo este proceso, el atacante podrá asociar la dirección IP 122.122.122.122 con el servicio oculto ejemplo.onion.

La dificultad de este ataque reside en que es necesario que le servicio oculto elija el nodo del atacante como nodo de entrada. Para conseguir esto hay diversas maneras de inhabilitar nodos de entrada hasta que el servicio oculto elije uno controlado por el atacante. Por ejemplo, el atacante podría:

- Falsear el ancho de banda de otros nodos para que el suyo sea elegido por tener mejor conexión.
- Crear ciclos o loops entre nodos obligándoles a rechazar nuevas conexiones y por lo tanto inhabilitándolos.
- Usar un Sniper Attack, que es un ataque de denegación de servicios, para deshabilitar nodos y tener mayor oportunidad de ser elegido.

Un Sniper Attack no es un ataque de desanonimización en sí mismo, pero se usa para aumentar las probabilidades de otros. Consiste en lo siguiente, si se comprometen un nodo cliente y un nodo de salida y se crea un circuito entre ellos, se pueden generar desde el nodo de salida grandes cantidades de paquetes hacia el nodo cliente. En ese momento, el nodo cliente da la orden de dejar de leer paquetes, por lo que el nodo de entrada tendrá una gran cantidad de paquetes sin procesar, no sabrá qué hacer con ellos y quedará inhabilitado.

3.2.3 Descriptores encriptados

Si la lista de puntos de distribución está encriptada, un atacante no podrá establecer una conexión con un servicio oculto, por lo que el ataque anterior no puede realizarse. Sin embargo, se puede usar otro método y así determinar si un servicio oculto está usando un nodo de entrada controlado por el atacante. Si esto se produjera, se puede aprovechar la oportunidad para desanonimizar el servicio oculto.

No se puede distinguir entre los servicios ocultos que encriptan sus puntos de acceso, pero como son relativamente pocos comparados con el resto, se puede realizar lo siguiente:

- En el nodo de entrada, se busca una característica de patrón de tráfico para los circuitos de introducción.
- Se descartan los circuitos de introducción que se originan en la misma dirección IP que cualquiera de los servicios ocultos con descriptores no encriptados.
- Para todos los circuitos de introducción restantes, se marcan sus orígenes como posibles ubicaciones de servicios ocultos encriptados.

3.2.4 Reconstrucción de circuitos

En teoría, mediante fingerprinting, se puede seguir el tráfico que transcurre en una comunicación a través de la red TOR y de esta manera reconstruir el circuito por el que transcurre, pudiendo así desanonimizar tanto a usuarios como a servicios. Para llevarlo a cabo, un atacante deberá controlar el nodo de entrada y el nodo de salida del circuito del cliente.

Aunque los responsables del proyecto TOR reconocen este problema, se considera muy complicado de explotar y probablemente nunca nadie ha conseguido hacerlo.

4 Mercados negros de la red TOR

4.1 Los mercados negros de la red TOR

De la unión de las redes de anonimato (ej. Red TOR) y del uso de criptomonedas (ej. Bitcoin) nacen los criptomercados, que son servicios ocultos en la red, donde se pueden realizar actividades comerciales anónimas. Debido a esto, son el lugar idóneo para que crezcan las actividades delictivas y para que los compradores encuentren servicios que de otra manera les sería mucho más difícil, o imposibles de conseguir.

Tal es el anonimato que se proporciona, que se calcula que sólo el 5% de los operadores del mercado negro, asociados con Tor-Bitcoin, han podido ser desmantelados.

Sin embargo, no debemos olvidar que estos mercados intentan operar al margen de la ley y que la única regulación que se aplica dentro de ellos es la que los dueños de los portales deciden, por lo que las estafas son constantes en este ámbito.

4.1.1 Historia de los criptomercados

El primero caso relevante de estos mercados negros fue Silk Road. Fue creado en 2011 y cerrado por el FBI en 2013. En él se realizaban múltiples actividades ilegales como lavado de dinero, tráfico de drogas, venta de documentos falsos, contratación de sicarios, etc. Su creador, Ross William, fue condenado a cadena perpetua por 7 delitos entre los que se encuentran el tráfico de drogas, lavado de dinero y fraude de identidad.

El cierre de Silk Road dejó un hueco en el mercado que muchos otros servicios intentaron ocupar, por ejemplo, al poco tiempo apareció Silk Road 2.0 dedicándose a la venta de armas, drogas e información privada. Algunos de estos servicios fueron:

- Dark Market: dedicado a la venta de tarjetas de crédito, contraseñas robadas y equipos para realizar fraude electrónico. Fue cerrado por el FBI en 2008.
- Darkode: dedicado a la venta de tarjetas de crédito, botnets, spam, etc.
- Liberty Reserve: dedicado al negocio financiero ilegal. Fue cerrado en 2013.
- PedoBook: dedicado a la pornografía infantil. Cerrado en 2012.
- Fereedom Hosting: dedicado a la pornografía infantil. Cerrado en 2013 por el grupo de activistas Anonymus.
- PlayPen: dedicado a la pornografía infantil. Fue cerrado en 2015 por el FBI.
- Sheep Marketplace: dedicado a la estafa, cerró de forma fraudulenta en 2013 llevándose unos 6 millosnes de dólares en bitcoins de sus usuarios.
- Evolution: mercado negro de drogas que cerró en 2015 llevándose 12 millones de dólares en bitcoins de sus clientes.
- Agora: dedicado a la venta de drogas. A finales de 2015 sus mismos administradores lo cerraron.
- Atlantis. Vendía drogas y servicios de hacking hasta que en 2013 sus administradores lo cerraron.
- TheRealDeal Market: se dedicaba al lavado de dinero, servicios de hacking, venta de software malicioso, cuantas robadas y drogas.

Pero el criptomercado que verdaderamente ocupó el espacio de Silk Road fue AlphaBay Market, llegando a tener un volumen 10 veces más grande. Fue lanzado oficialmente el 22 de diciembre de 2014 y muchas organizaciones lo han reconocido como el servicio líder de venta de drogas y armas en Internet. El FBI comentó que AlphaBay disponía de un catálogo de 250.000 productos, en su mayoría ilegales, como drogas u otras sustancias psicoactivas. Asimismo, contenía 100.000 ofertas de documentación fraudulenta o robada, como asimismo dispositivos de acceso, productos falsificados, malware y servicios de hackeo y comisión de delitos informáticos, armas de fuego y otros servicios delictivos. Las ventas diarias de la web variaban entre 600.000 y 800.000 dólares al día, ganando AlphaBay un millón de dólares anuales en comisiones.

El final de este mercado llegó el pasado 5 de Julio siendo clausurado por las autoridades estadounidenses y la Europol. En esa misma operación se realizó el cierre de otro importante mercado negro llamado Hansa Market.

Ilustración 9. Imagen de la Europol del cierre de AlphaBay y Hansa

Sin embargo, se está volviendo a repetir la historia. A pesar de la importante operación policial, otros criptomercados están creciendo y ocupando el hueco dejado por AlphaBay y Hansa. Actualmente Dream Market, lanzado en 2013, parece el líder de estos mercados negros.

4.1.2 Actividades ilegales más comunes en los criptomercados

4.1.2.1 Tráfico de drogas

Los compradores y vendedores han encontrado en las redes de anonimato el lugar perfecto para realizar sus transacciones. A través de los diferentes criptomercados podemos comprar todo tipo de drogas, de diferentes categorías, medicinas, esteroides, alucinógenos, estimulantes, etc.

No sólo se venden drogas como producto final, también se venden las materias primas y utensilio para su producción.

4.1.2.2 Pedofilia y pornografía infantil

El anonimato que confieren estos mercados negros, ha propiciado que sean el lugar idóneo para el acceso a este tipo de contenidos.

4.1.2.3 Venta ilegal de armas

Se pueden encontrar una gran variedad de tipos de armas, desde pistolas, fusiles o granadas hasta sus diseños para impresoras en 3D. También podemos encontrar pequeños gadgets que actúan como armas blancas.

4.1.2.4 Sicarios

Los asesinos a sueldo usan la darknet para publicitarse y ofrecer sus servicios. Dependiendo de lo que se contrate, tendrá un precio u orto y algunos de ellos se niegan a matar a menores, altos cargos, etc., aunque en realidad muchos de ellos son farsantes.

4.1.2.5 Venta de documentación falsa

A través de los criptomercados se pueden comprar pasaportes falsos, documentos nacionales de identidad, carnés de conducir, etc. Podemos comprar hasta dinero falso.

4.1.2.6 Localización, acoso y extorsión

Los hackers ofrecen sus servicios para realizar este tipo de delitos, usando la red como medio para encontrar a las víctimas. Es una forma de hacer cyberstalking (uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien), cyberbullying o conseguir pornografía infantil.

4.1.2.7 Terrorismo

Los grupos terroristas se aprovechan de estas redes para congregarse y comunicarse con sus militantes.

Disponen de sitios para divulgar sus ideologías, incitar al odio y a la guerra e incluso donde recogen fondos a través de criptomonedas. También ofrecen manuales para comprar armamento para sus simpatizantes.

4.1.2.8 Hacktivismo

Los hackers usan la red TOR y otras redes de anonimato para operar en grupo y se suelen congregan en foros a los que sólo se puede acceder con invitación. Su filosofía es la de hacer lo correcto según su moral, sea o no legal.

4.1.2.9 Malware y software malicioso

Este tipo de software unido al uso de botnets, se aprovecha del anonimato de la red TOR para que el tráfico que generan sus acciones no pueda ser rastreado.

También podemos encontrar a la venta diferentes trozos de código (exploit) que explotan vulnerabilidades, ya sean conocidas o incluso algunas todavía no descubiertas por los profesionales de las TIC.

4.1.2.10 Piratería

En la darknet se pueden encontrar números contenidos que vulneran las leyes de los estados, en relación a los derechos de autor. Cada vez estas leyes persiguen más estos contenidos y eso hace que sean más prolíferos en las redes de anonimato.

4.1.2.11 Revelación de documentación secreta y/o confidencial

Últimamente este tipo de acciones se han puesto de moda debido al caso Wikileaks o el caso Snowden, en el que un antiguo consultor de informática de la CIA y la NSA, desveló información secreta.

4.1.2.12 Material visual con contenido violento

Se pueden conseguir vídeos o películas que muestran acciones muy violentas contra personas o animales.

4.2 Las criptomonedas

Las criptomonedas son un medio virtual para el intercambio de bienes y servicios a través de transacciones electrónicas sin intermediarios.

Las características que hacen que sean la forma más popular de pago en los criptomercados, son las siguientes:

- Anónimas: aseguran un alto grado de privacidad.
- Seguras: romper su seguridad es casi imposible.
- Sin intermediarios: las transacciones se realizan directamente de persona a persona.
- Descentralizadas: no estás controladas por ningún estado o entidad financiera.
- Internacionales: pueden usarse en casi todos los países del mundo.

Aunque hubo algún intento anterior, se puede considerar que la primera criptomoneda fue el bitcoin en 2009. El pseudónimo de su creador/a es Satoshi Nakamoto y se desconoce su verdadera identidad. En la actualidad, sin duda es la moneda virtual más famosa y con más valor al cambio.

En un mercado negro en red, donde se realizan actividades ilegales, evidentemente no se puede pagar mediante los medios ordinarios que disponemos ya que se perdería el anonimato y quedaría registrada la operación. Por lo tanto, para poder hacer uso de un criptomercado, habría que disponer de alguna de las monedas virtuales que el portal acepte. Por ejemplo, en AlphaBay, uno de los portales más famosos que ha existido en la red TOR se podía pagar con tres tipos de criptomonedas que son, bitcoins, moneros y ethers.

4.2.1 Bitcoin

El bitcoin nació en el año 2009. Está compuesto de un software libre y de una red P2P formada por miles de ordenadores que dan soporte a la infraestructura. Esta red es la encargada de soportar y registrar los movimientos que se producen. Estos movimientos se anotan en un registro distribuido llamado blockchain.

Como máximo se podrán extraer 21 millones de unidades de bitcoins. El valor de la moneda se sustenta en la confianza de la misma, por lo que cualquier pequeña duda que se crea alrededor de ella, hace que su valor caiga. Esto no ha impedido que a día de hoy tenga un valor bastante alto.

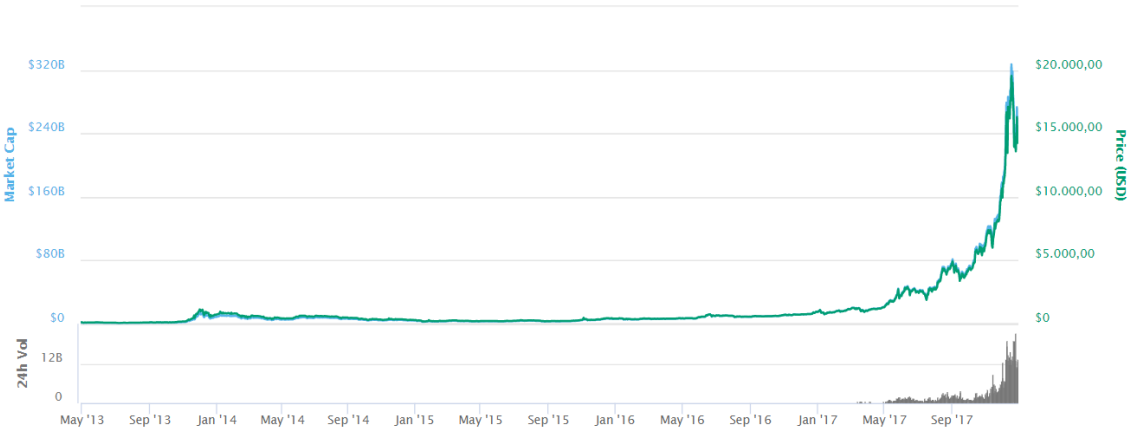


Ilustración 10. Valor actual bitcoin/USD

4.2.1.1 Mineros de bitcoin

Dentro de la red P2P de bitcoin, podemos encontrar un grupo de nodos con especial relevancia que se denominan mineros. Éstos nodos se encargan de realizar las operaciones de la criptomoneda y vigilan al resto de nodos de forma pasiva.

Para validar las operaciones, los mineros deben resolver fórmulas matemáticas (hashes) que sintetizan en muy pocos caracteres una gran cantidad de información. Cada vez que un minero encuentra un hash válido se lleva, una recompensa en bitcoins.

Crear un hash a partir de un conjunto de datos es bastante fácil, pero la red bitcoin lo pone más complejo para que no todo el mundo pueda hacerlo. Se requiere que cada hash generado de cada bloque sea diferente a todos los anteriores y que se cree de una forma determinada, debiendo tener una serie de ceros al principio.

Para crear hashes diferentes se incluye en la transacción un trozo de información aleatorio llamado “nonce” y se crea el hash. Si este no se ajusta al formato requerido, el “nonce” se cambia y se prueba otro nuevo creando un nuevo hash.

Esta operación puede conllevar múltiples intentos hasta encontrar un hash que se adecue a los requisitos, de hecho, suelen ser millones de intentos, por ello hay un motón de mineros intentado ser los primeros en crear el hash y llevarse la recompensa.

4.2.1.2 Funcionamiento de blockchain

Los registros en blockchain son cadenas de bloques, donde cada bloque de información se conecta con otro bloque de tal manera que la cadena no puede ser modificada o borrada una vez sea registrada. Cada máquina que compone la red P2P tiene una copia del registro y todas las transacciones son públicas, aunque anónimas.

La copia completa del blockchain contiene todas las transacciones ejecutadas hasta el momento en la historia del bitcoin. Cada bloque contiene el código hash del bloque anterior, creando así la cadena de bloques desde el primer bloque se creó. Para que el orden de la cadena sea el correcto, todos los bloques están ordenados de forma cronológica partiendo del primer bloque original. Este orden hace que el gasto doble sea complicado, ya que sería poco práctico modificar toda la cadena blockchain después de que haya pasado un tiempo porque se tendrían que modificar todos los bloques anteriores. El doble gasto es una mala práctica donde un usuario intentan mandar bitcoins a dos direcciones distintas.

Una cadena blockchain es válida sólo si todos los bloques y transacciones que forman parte de ella son válidos y sólo si comienza por el bloque original.

Pala cualquier bloque sólo hay un camino al bloque original, sin embargo, desde el bloque original hacia delante, se pueden producir bifurcaciones cuando dos bloques han sido creados con sólo unos pocos segundos de diferencia. En este caso, los nodos siguen construyendo la cadena sobre el bloque que hayan recibido primero.

Los bloques de cadenas más cortas (bloques huérfanos) no se usan para nada, de tal manera que cuando se produce una transacción, todas las transacciones que forman parte de la cadena corta se reagrupan en las transacciones pendientes y se incluyen en otro bloque. La recompensa de los mineros en las cadenas más cortas no se traslada a las cadenas largas, por lo que se necesita un periodo de maduración de 100 bloques para la generación de esta recompensa. Este tiempo de maduración, sólo se aplica a los mineros generadores de bloques de bitcoin y es una medida de evitar el doble gasto. Eso significa que un minero no podrá gastar sus bitcoins generados hasta que su bloque esté a 101 bloques del más reciente que se haya generado.

4.2.1.3 Monederos

Los movimientos o transferencias de bitcoins se realizan entre los monederos (wallets) de cada usuario, que es el software que proporciona las claves para acceder a tus bitcoins. Estos monederos, se componen por una clave pública y una clave privada. Cada transacción que se registra en el blockchain queda asociada a la calve pública del usuario, por lo tanto, a través de esa clave pública se pueden consultar los movimientos del usuario y la cantidad de bitcoins que posee. Esto no quiere decir que se pierda el anonimato, ya que la clave pública no identifica de ninguna manera al mismo.

La clave privada se usa para confirmar las operaciones, de esta manera el usuario será el único que pueda realizar transferencias.

Para que una transacción entre dos carteras pueda ser ejecutada, tiene que haber consenso en la red mediante el proceso de minería, para evitar así fraudes en las transacciones.

4.2.1.4 Formas de conseguir bitcoins

- Minando: como ya he explicado, consiste en poner equipos a la disposición de la red P2P, para resolver problemas matemáticos. A los mineros se les compensa con bitcoins.
- Desde una plataforma de intercambio: donde un usuario puede acordar el cambio de dinero corriente por bitcoins.
- Visitando páginas de internet o resolviendo captchas: viendo publicidad o resolviendo captchas es una manera sencilla de conseguirlos.

4.2.2 Monero

De su grupo de siete desarrolladores sólo dos han revelado su nombre: Ricardo Spagni y Francisco Cabañas. Nació en abril de 2014 y su tecnología (CryptoNote) es diferente a la del bitcoin, proporcionando más anonimato que esta. Esto se logra ya que no se registran en la blockchain ni a la persona que recibe ni a la que envía la moneda. De la misma manera, no se muestran las cantidades enviadas, haciendo las operaciones 100% secretas.

Es una moneda descentralizada y fue el portal AlphaBay el que la dio popularidad, al permitir pagar con ella. Al aportar una mayor privacidad que el bitcoin, la ha hecho como una de las más populares divisas virtuales en los criptomercados.

Otra de sus características es la fungibilidad, todas las monedas son iguales, es decir, no hay tokens identificables en su red y todas son intercambiables entre sí.

La cantidad de moneros que se pueden producir es infinita y su valor actual es el siguiente:

Ilustración 11. Valor actual monero/USD

4.2.2.1 Protocolo CryptoNote

Es el protocolo que permite que las transacciones de moneros no puedan ser rastreadas. Cuando se realiza una transacción se ponen los moneros en una "bolsa" en los que se encuentran los moneros de otras transacciones, para que sean mezclado los unos con los otros. Una vez se han mezclado, se envían las cantidades justas a sus destinatarios, pero no van a llegar los moneros de su emisor, sino los de otro usuario que depositó divisas en la misma bolsa. De esta manera se desconoce quién es el emisor de las transacciones.

Para que el anonimato sea completo, se usa la firma de anillos, que se basa en mostrar tres posibles rutas entre sí que dan la sensación de ser correctas, pero sólo una de ellas lo es. De esta manera, los nodos intermedios de la operación, también quedan en el anonimato.

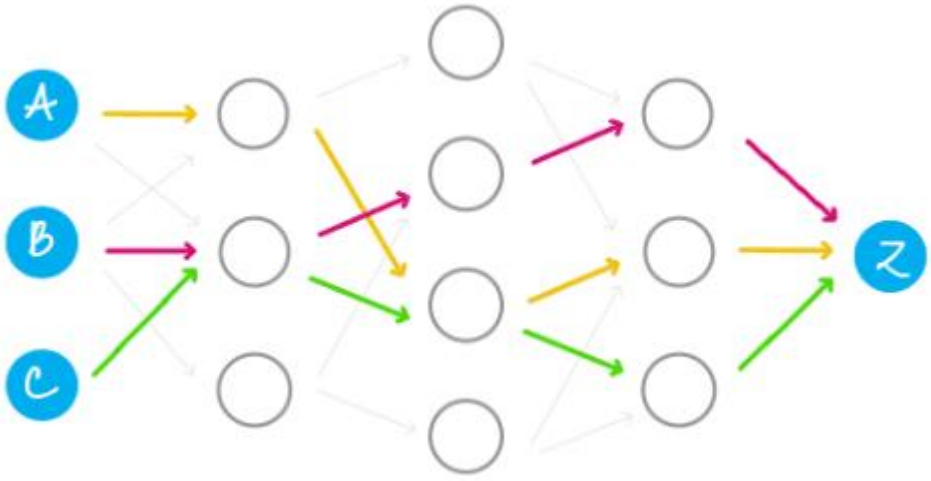


Ilustración 12. Alternativas de camino en una transacción de moneros

4.2.2.2 Formas de conseguir moneros

- Minando: de manera similar al bitcoin, los mineros que prestan recursos a la red monero reciben como recompensa esta criptomoneda.
- Plataforma de intercambio: la forma más sencilla de conseguir moneros es realizar un intercambio con otras monedas virtuales o alguna otra moneda corriente.

4.2.3 Ether

Ethereum es una plataforma que utiliza blokchain para ofrecer gran variedad de servicios. Fue creada en 2015 por Vitalik Buterin, con el objetivo de crear un instrumento para aplicaciones descentralizadas y colaborativas. De esta plataforma nace Ether, que es un token que puede ser utilizado en transacciones que usen esta plataforma.

Funciona parecido a bitcoin a través de blockchain y el proceso de minería. Los mineros son los responsables de verificar grupos de transacciones de ether para formar "bloques" y codificarlos resolviendo complejos algoritmos.

Los nuevos bloques se enlazan entonces a la cadena de bloques anterior y el minero en cuestión recibe una recompensa, es decir, un número fijo de tokens de ether.

A diferencia del bitcoin que está limitado a 21 millones, los ethers no están limitados, de ahí su precio inferior. Su valor actual es:

Ilustración 13. Valor del ether/USD

Pero lo realmente interesante de esta moneda es que se basa en Ethereum, una plataforma capaz de crear contratos inteligentes.

4.2.3.1 Contratos inteligentes

Un contrato inteligente, es un software diseñado para cumplir condiciones automáticamente en base a otras que se van cumpliendo. Esta forma de operar, es una gran evolución con muchas posibilidades. Podría suponer hasta la desaparición de los departamentos contables de las empresas, ya que la red Ethereum realizaría todos los registros de las operaciones y estas se ejecutarían en base a la lógica que se les aplique. Estamos hablando de un sistema financiero automático, autorregulado, transparente y resistente a fraudes.

Sus beneficios son:

- Eliminan al intermediario, agilizando los procesos y reduciendo los costes.
- La seguridad que proporcionan al estar registrados en un sistema distribuido.
- Cualquiera puede ver la actividad del mercado en la cadena de bloques.

Sin embargo, se trata de un sistema joven de momento, no exento de problemas. Por ejemplo, el código de un contrato se traduce literalmente, por lo que cualquier error en su escritura podría provocar resultados no deseados. Como Ethereum trabaja sobre blockchain, los contratos nunca podrían ser modificados.

4.2.3.2 Formas de conseguir ethers

- Minando: como en los anteriores ejemplos, la minería de ethers se basa en prestar recursos a la red que sustenta su infraestructura.
- Plataforma de intercambio: al igual que los moneros, los ethers se pueden conseguir a través del intercambio bitcoins-ethers.

4.2.4 Otras criptomonedas

Existen más de 100 monedas virtuales y su popularidad o importancia es cambiante dependiendo del momento. Otras criptomonedas de relevancia en este momento son:

- PeerCoin: Se encuentra basada en la combinación de los dos algoritmos proof of skate y proof of work. Su principal ventaja es que su red consume menor energía y se pueden crear ilimitadamente monedas.
- Ripple: Es un protocolo que busca el desarrollo de un sistema de crédito basado en la confianza, asentándose en como una ruta de pago alternativa a través de redes de confianza. Los nodos funcionan como sistema de cambio que pueden dar créditos o solicitarlos. Existen 100 millones de unidades.
- Litecoin: Es una moneda virtual parecida al bitcoin con tres diferencias fundamentales:
    - Realiza el procesamiento de un bloque 4 veces más rápido.
    - Existen 84 millones de unidades que se dividen en 100 millones de unidades más pequeñas.
    - Utiliza un scrypt que facilita la minería para no necesitar equipamiento sofisticado.
- Dogecoin: Su principal diferencia radica es que cuenta con un bloque de tiempo de 1 minuto para realizar una transacción y no existe límite de unidades (en su emisión se emitieron 100 billones de monedas) y las comisiones por enviar y recibir esta moneda son muy pequeñas.

4.3 ¿Cómo operan los mercados negros en la red TOR?

Escondidos tras el anonimato que proporciona la red TOR y las monedas virtuales, estos criptomercados funcionan básicamente como un portal de ventas tipo Amazon, eBay, etc., donde los vendedores anuncian sus productos y los compradores eligen lo que desean.

La popularidad de estos mercados reside en el nivel de confianza que son capaces de ofrecer y la calidad de los artículos que venden. Como en este ámbito no hay ninguna regulación, son los propios portales los que ponen sus propias reglas, con el objetivo de que el cliente se sienta seguro comprando. Las buenas experiencias harán que aumente la popularidad del criptomercado y por lo tanto su volumen de negocio. Muchos de ellos, tienen un sistema de puntuación a los vendedores donde se puede ver el nivel de confianza de los mismos y leer las opiniones tanto positivas como negativas de los compradores.

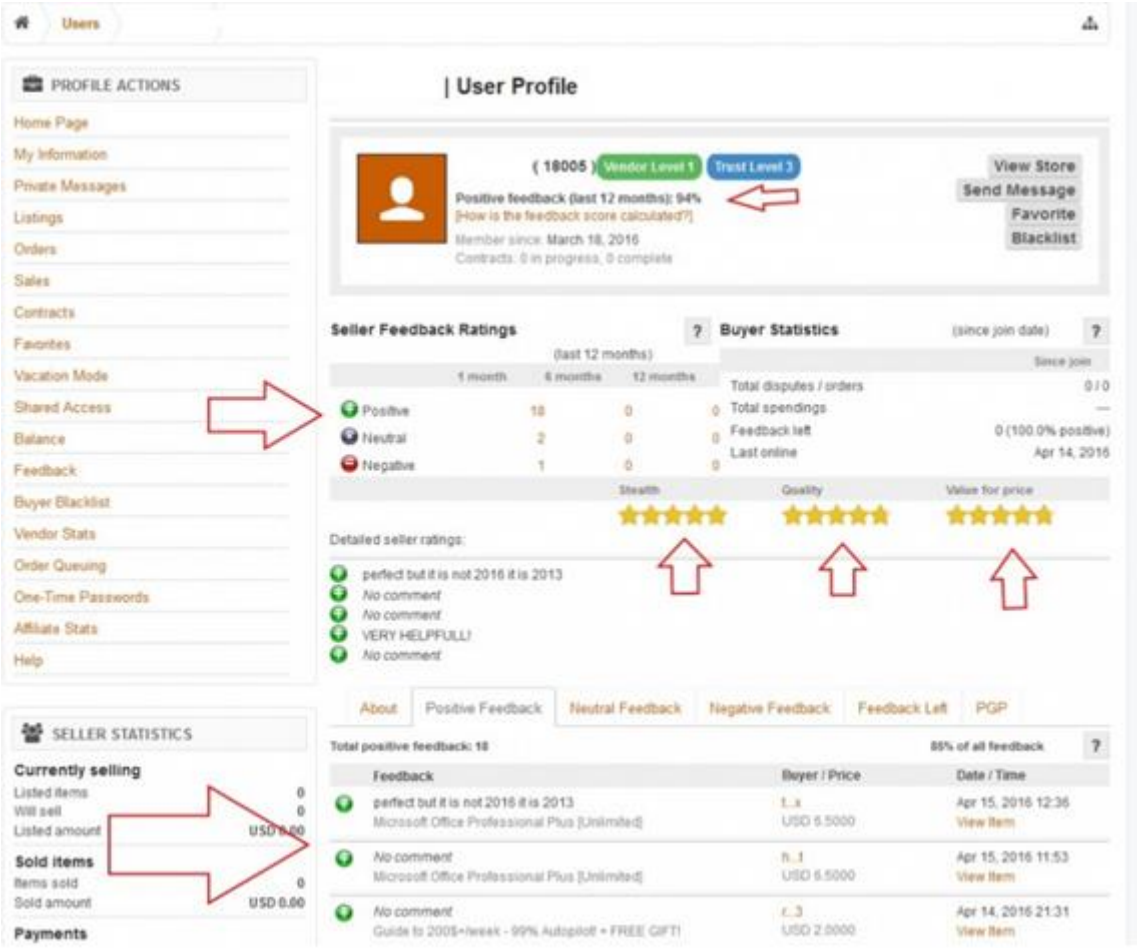


Ilustración 14. Opiniones sobre un vendedor en AlphaBay (Fuente: https://ramonalarconsanchez.com)

Esto no quiere decir que, porque los vendedores tengan una buena reputación o el portal buena fama, sea un mercado seguro. Como los criptomercados no están sujetos a las leyes, como ya he comentado, siempre se corre el riesgo de ser estafado. De hecho, ha ocurrido varias veces que un portal popular y con buena reputación, ha cerrado de pronto llevándose el dinero de sus usuarios. Otra posible opción para que los usuarios pierdan sus fondos, es que alguna autoridad cierre el portal por ser ilegal y se quede con ellos.

A continuación, describiré los pasos que tiene que seguir un cliente para realizar una compra y los pasos que tiene que seguir un vendedor para ofrecer sus servicios en un criptomercado. Para ello, seguiré con el ejemplo de AlphaBay.

4.3.1 Cómo realizar una compra en AlphaBay

El primer paso, si conocemos la dirección ".onion" de nuestro criptomercado, es realizar un registro en él. Para ello, nos pide tres campos obligatorios:

- Username: nombre de usuasio
- Password: contraseña
- PIN: código de 6 dígitos necesario para algunas gestiones

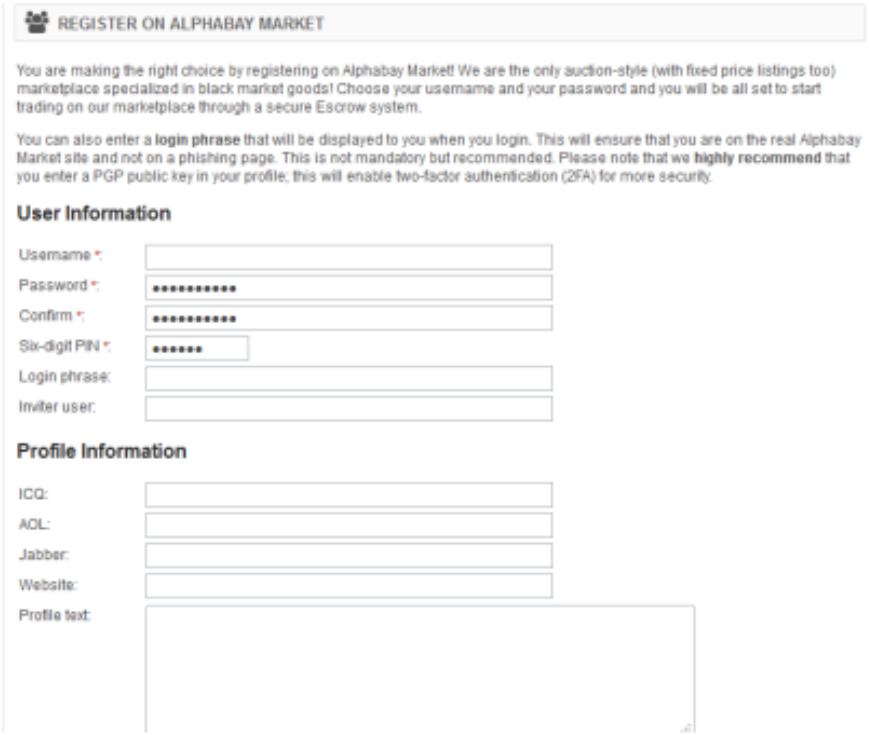


Ilustración 15. Pantalla de registro de AlphaBay (Fuente: https://ramonalarconsanchez.com)

Al estar en un mercado negro, para preservar nuestra privacidad, no tiene sentido dar un correo electrónico, por lo que si perdemos nuestra contraseña necesitaremos otro mecanismo para recuperarla. AlphaBay, tras registrarnos, no das unas palabras que deberemos apuntar y que nos identificarán en un futuro para cambiar las pass.

En este momento, podremos acceder a su portal de venta:

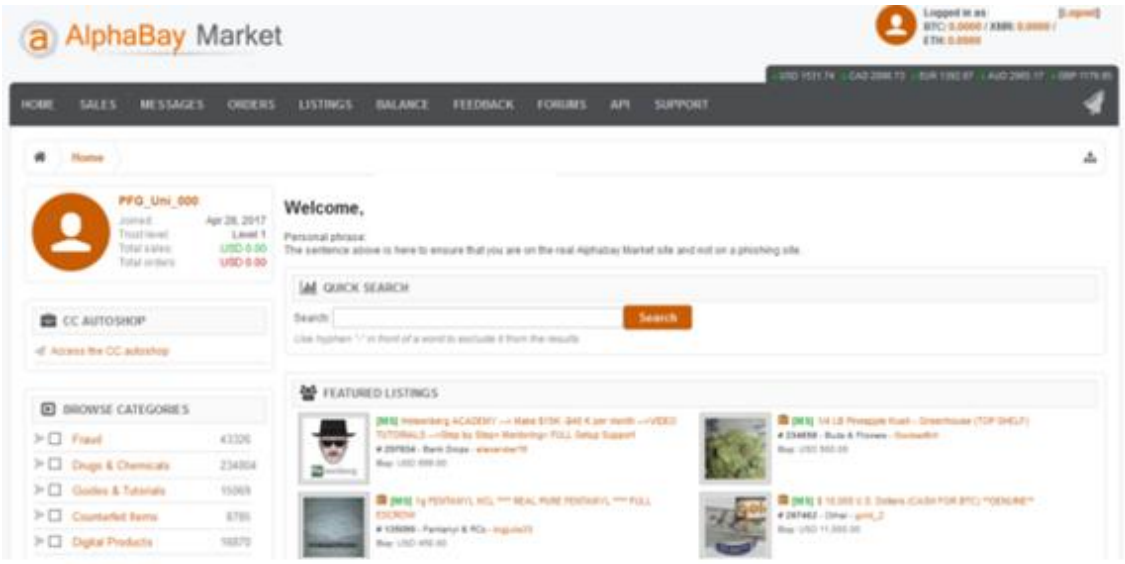


Ilustración 16. Portal AlphaBay (Fuente: https://ramonalarconsanchez.com)

Si disponemos de alguna de las criptomonedas comentadas anteriormente, podremos realizar una compra.

Para poder traspasar criptomonedas de nuestro monedero al monedero del criptomercado, deberemos conocer su dirección, que nos será proporcionada por a través de su portal:

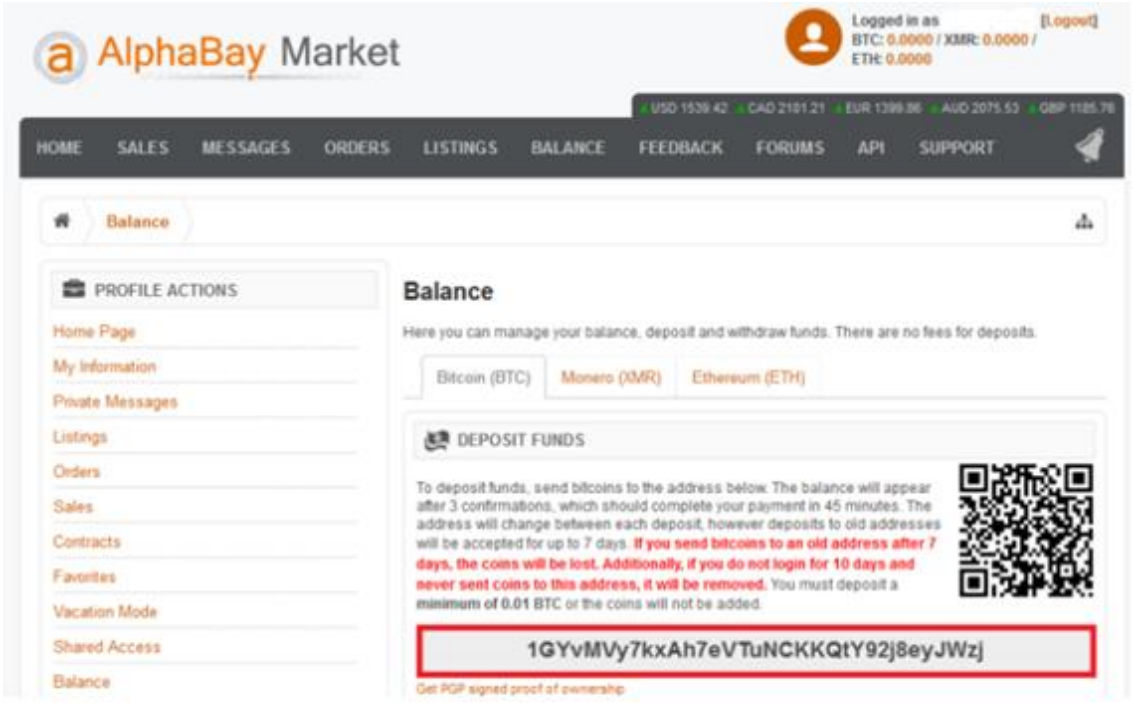


Ilustración 17. Dirección del monedero de AlphaBay Market (Fuente: https://ramonalarconsanchez.com)

Con esta dirección de destino y rellenando un formulario con la cantidad que deseamos transferir, podremos realizar la operación desde nuestro monedero.

Una vez se apruebe la operación, podremos hacer uso de ese dinero. Hay que tener en cuenta que AlphaMarket cambia la dirección del monedero cada vez que se hace un ingreso para que nadie pueda rastrearla.

Ahora que tenemos fondos podremos realizar una compra, tras elegir un artículo pinchamos en “buy now”:

Ilustración 18. Artículo de AlphaBay (Fuente: https://ramonalarconsanchez.com)

A continuación, veremos las condiciones de compra y podremos introducir los datos necesarios como, por ejemplo, la dirección de la entrega del producto. Esta información se encripta para que sólo el vendedor la conozca. Hay que tener en cuenta que la dirección de nuestra casa podría identificarnos:

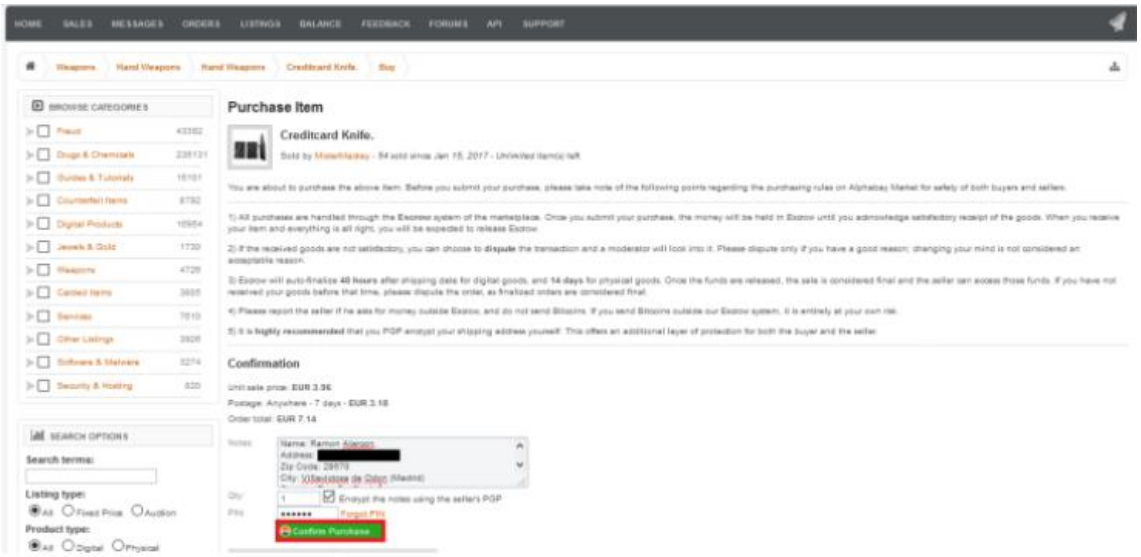


Ilustración 19. Introducción de datos en AlphaBay (Fuente: https://ramonalarconsanchez.com)

Cuando confirmemos la compra, el importe quedará en un fondo del criptomercado (estado del pedido "Processing"), a la espera de que el vendedor confirme el envío (estado del pedido "Shipped"). Una vez que el comprador reciba el pedido, el vendedor deberá pulsar "Finalize" para recibir los fondos.

4.3.2 Cómo darse de alta como vendedor en AlphaBay

Si estamos registrados en el criptomercado, cualquiera puede hacerse vendedor. Cuando iniciamos el proceso, nos muestra las condiciones del mismo:

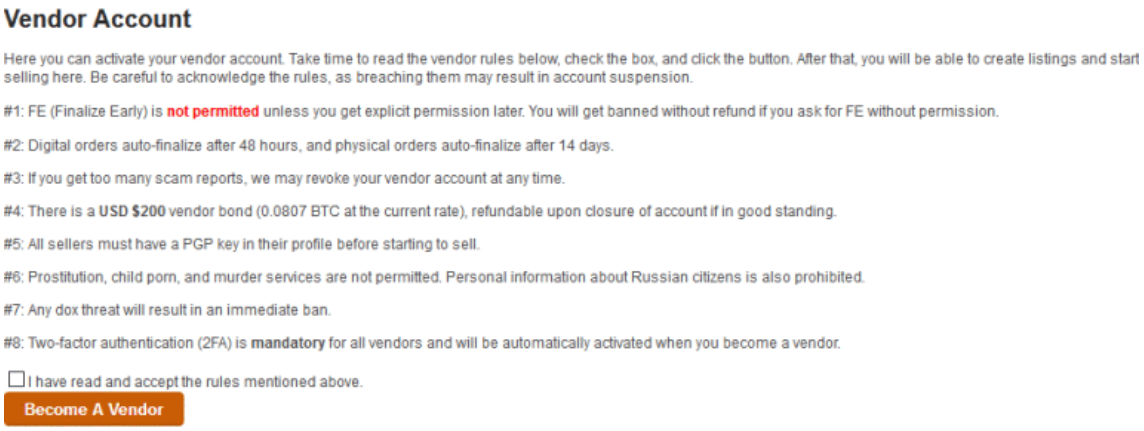


Ilustración 20. Condiciones de AlphaBay (Fuente: https://ramonalarconsanchez.com)

Cualquiera del incumplimiento de estos puntos puede suponer la suspensión de la cuenta. Estas reglas son:

- No se pueden finalizar los pronto los pedidos sin consentimiento del comprador.
- El vendedor obtendrá los fondos del pedido o cuando el comprador finalice el pedido, o tras 48h para pedidos digitales, o tras 14 días para pedidos físicos.
- Si un vendedor recibe demasiados pedidos de estafa, los administradores podrán cancelar su cuenta.
- Un vendedor deberá depositar $200 en concepto de fianza, que perderá en el caso de que sea expulsado.
- Todo vendedor deberá tener una clave pública en su perfil para que los compradores puedan contactar con ellos cifrando la información.
- En este portal, está prohibida la venta de prostitución, pornografía infantil, servicios de asesinato e información personal de ciudadanos rusos.
- Se prohíbe amenazar a los usuarios con publicar información sobre su identidad.
- Se obliga a que el vendedor se autentique cada vez en 2 pasos. El vendedor tiene que descifrar un mensaje con su clave privada y dentro de él encontrará un código para iniciar sesión.

Como se puede ver se fomentan unas reglas para que los compradores sientan seguridad comprando en este criptomercado. Sin embargo, cuando cerró en Julio de este año, todos ellos perdieron sus monederos.

5 Legislación

5.1 ¿Es legal en España usar la *dark net*?

Existen países en los que la navegación por la red oscura está prohibida como, por ejemplo, Arabia Saudí, China, Irán, Rusia, etc. Sin embargo, en España el uso de los navegadores que dan acceso a esta red, no está prohibido, la legalidad o ilegalidad vendrá dado por las acciones que se realicen dentro de la red.

Como norma general, navegar por las redes anónimas es totalmente legal, aunque se visiten páginas donde se promuevan actividades ilegales, la mera visita de estas páginas no constituye un delito.

La excepción a la regla la encontramos en la pornografía infantil, ya que según el artículo 189.5 del Código Penal, el acceso a contenido de este tipo, será castigado con una pena de prisión de uno a cinco años:

"El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá 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."

Por lo tanto, no se persigue la tecnología, es decir, la red TOR no es en sí misma ilegal, sino que lo que se considera ilegal es valerse de ella para la realización de actividades delictivas.

A continuación, enumero los 3 delitos más comunes en los criptomercados y cómo son sancionados por nuestras leyes:

- La venta de droga, legislado en el artículo 368 del código Penal:

"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."

- La compra de drogas ilegales:

Recogida en el artículo 36.16 de la Ley de Seguridad Ciudadana y que acarrea una multa de entre 601€ a 10400€:

"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 compra de armas ilegales:

Prohibida por el artículo 563 del Código Penal que establece una pena de prisión de uno a tres años en caso de:

"tenencia de armas prohibidas y la de aquellas que sean resultado de la modificación sustancial de las características de fabricación de armas reglamentadas"

Estos han sido algunos ejemplos para comprender como nuestras leyes castigan los delitos, independientemente del medio a través del cual se realicen. Por lo tanto, al no existir una regulación específica sobre los sistemas de anonimización, debemos desviarnos a la legislación sobre delitos informáticos y ciberseguridad.

5.2 Delitos informáticos

En líneas generales y basándonos en el convenio europeo sobre ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, podemos clasificar nuestras leyes contra delitos informáticos en los siguientes grupos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos – Artículos 197 a 201 (Ley Orgánica 1/2015, de 30 de marzo).
- Delitos informáticos: falsedad documental (Artículos 386 a 400 bis), sabotaje informático (Artículo 264 a 264 quater) y estafa o fraude informático (Artículos 248 a 251 bis), Ley Orgánica 1/2015, de 30 de marzo.
- Delitos relacionados con el contenido: de índole sexual, en gran medida pornografía infantil – Artículos 183 a 183 quater, artículos 187 a 190 (Ley Orgánica 1/2015, de 30 de marzo).
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines – Artículos 270 y siguientes del Código Penal.
- Delitos por actos de índole racista y xenófoba cometidos por medios de sistemas informáticos – Artículo 510 y siguientes del Código Penal.

- Otros delitos que pueden desarrollarse en el ámbito digital: amenazas y coacciones (Artículos 169 a 172) y calumnias e injurias – (Artículos 205 a 216), Ley Orgánica 1/2015, de 30 de marzo.

El impacto de las nuevas tecnologías en la sociedad ha hecho que la legislación introduzca nuevos conceptos que anteriormente no existían o eran desconocidos para el legislador. Nuestro ordenamiento jurídico ha ido incorporando modificaciones sustanciales en figuras ya existentes y también introduciendo algunas nuevas.

La Ley Orgánica 1/2015 de 30 marzo que modifica la Ley Orgánica 10/1995 de 23 de noviembre del Código Penal, es una de las consecuencias de este proceso de adaptación, en la cual se recoge una nueva categoría de "delitos informáticos o ciberdelitos". Esta nueva forma de delito, tiene como característica principal a las nuevas tecnologías, ya sean como medio, objeto o bien jurídico protegido.

Los artículos modificados, en materia de delitos informáticos, por la Ley Orgánica 1/2015 de 30 marzo, son los siguientes:

- Delito de intrusión informática (Artículo 197 bis apartado primero).

"1. El que por cualquier medio o procedimiento vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

- Interceptación de transmisiones de datos informáticos (artículo 197 bis apartado segundo).

"2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

- Producción o facilitación a terceros para la realización de los delitos anteriores (artículo 197 ter).

"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 bis:

a.- un programa informático, concebido o adaptado principalmente para cometer dichos delitos

b.-una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

- Responsabilidad del funcionario público (artículo 198).

"La autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa pro delito y prevaliéndose de su cargo, realiza cualquiera de los delitos contra la intimidad o contra la seguridad de los sistemas informáticos".

- Delitos por dañar datos o sistemas informáticos (artículo 264).

“1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.”

- Delito por interrumpir el correcto funcionamiento de un sistema informático (artículo 264 bis).

“1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.”

- Producción o facilitación a terceros para la realización de los delitos anteriores (artículo 264 ter).

“Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información”

En el Código Penal, podemos encontrar la tipificación de otros delitos informáticos:

- Delitos informáticos relacionados con la propiedad intelectual e industrial (artículo 270 del CP).

"Será castigado con la pena de prisión de seis meses a cuatro años, y multa de doce a veinticuatro meses, el que , con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares , de los correspondientes derechos de propiedad intelectual o de sus cesionarios.2. La misma pena se impondrá a quien , en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular, ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".

- Fraudes informáticos (artículo 248.2 del CP).

“También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero".

- Sabotaje informático (artículo 263.1 del CP).

"El que causare daños en propiedad ajena no comprendidos en otros títulos de este Código, será castigado con multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño."

Otros delitos que, aunque no atentan contra los sistemas informáticos, se pueden cometer a través de ellos, serían:

- Amenazas (artículo 169 y ss del CP) realizadas o difundidas a través de cualquier medio de comunicación.
- Calumnias e injurias (artículo 205 y ss CP) realizadas o difundidas a través de cualquier medio de comunicación.
- Inducción a la prostitución de menores (artículo 187 CP).
- Producción, venta, distribución, exhibición o posesión de material pornográfico en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (artículo 189 CP).

Por lo tanto, estos y otros ejemplos son la respuesta de nuestra legislación a una nueva realidad en la que las TIC constituyen una parte esencial de la misma. Sin embargo, no podemos pensar que esta es la solución, sino únicamente los primeros pasos de un camino que evoluciona cada vez más rápido. Será todo un reto conseguir que las leyes avancen a la velocidad suficiente para cubrir las necesidades de la sociedad.

Muchos de los cambios que hemos ido introduciendo, son debidos a la Directiva 2013/40 UE del Parlamento Europeo que sustituye la Decisión Marco 2005/222 del Consejo. Esta directiva, tiene como objetivo aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

5.3 La ciberseguridad

Aunque la Unión Europea en el pasado ha dado pasos para mejorar la ciberseguridad, como por ejemplo la Convención de Budapest de 2001, es en 2013 cuando se empiezan elaborar un plan a mayor escala para cubrir todos los aspectos de la ciberseguridad y no sólo del ciberdelito.

La Unión Europea escribe el artículo "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" en el que se describe la estrategia que la UE pretende adoptar en materia de ciberseguridad. Los cinco objetivos principales que se pretenden son:

- Tener la capacidad de soportar y recuperarse de los ciberataques. LA UE aboga por una legislación y mejora de la concienciación en materia de seguridad.
- Reducción drástica de los ciberdelitos, desarrollando leyes específicas para "tipos de cibercrimen", junto con la creación de alianzas para su persecución.
- Desarrollo de una política de ciberdefensa en el ámbito de la Política Común de Seguridad y Defensa, creando sinergias entre la sociedad civil y las fuerzas militares para la protección de los activos críticos.
- Desarrollo de las infraestructuras y los recursos tecnológicos necesarios en el ámbito de la ciberseguridad. Se promoverá la creación de un mercado único para productos de seguridad.
- Establecimiento de una política internacional de la Unión Europea coherente en materia de ciberespacio y promoción de los valores fundamentales de la Unión.

La estrategia que se desea adoptar es muy amplia y define la guía que debe seguir la UE en materia de ciberseguridad en ámbitos tan diferentes como los recursos industriales, tecnológicos, la justicia, la política exterior, la defensa, etc., y ámbitos de otros tipos como, por ejemplo:

- Protección de los derechos fundamentales, de la libertad de expresión, de los datos personales y de la privacidad en el ciberespacio de igual forma que en el mundo real.
- Acceso universal con el convencimiento de que una amplia conectividad a escala mundial no debe ir acompañada de medidas de vigilancia y censura.
- Refuerzo de las capacidades en materia de ciberseguridad sin perjuicio de la mejora del acceso a la información.

En base a esta estrategia, encontramos el último paso de la UE en materia de ciberseguridad en la Directiva 2016/1148, o más comúnmente llamada como la Directiva NIS "Network and Information Security". Fue publicada el 19 de julio de 2017 y ha entrado en vigor el 9 de agosto.

Esta directiva, nace con el objetivo de asumir las medidas necesarias para garantizar la seguridad en las redes y en los sistemas de la información. Se pretende lograr un elevado nivel de ciberseguridad dentro de la UE.

Para alcanza su objetivo, se establecen las siguientes exigencias:

- Obliga a los Estados miembros a adoptar una estrategia nacional de seguridad de redes y sistema de información. Para la cual, los Estados miembros deberán designar autoridades competentes en seguridad de redes y sistemas de información.
- Asimismo, obliga a que los Estados miembros a que designen uno o varios Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT).
- Creación de un Grupo de cooperación entre los Estados miembros para facilitar el intercambio de información.
- Obliga a los Estados miembros a que identifiquen los Operadores de Servicios Esenciales (OSE) y los Proveedores de Servicios Digitales (PSD) establecidos en su territorio para cada sector.

Para ser considerado un OSE, se deben cumplir los siguientes requisitos:

- Debe ser una entidad que presta un servicio esencial para el mantenimiento de actividades sociales o económicas.
- La prestación de dicho servicio depende de las redes.
- Un incidente (definido por la propia Directiva como todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información) tendría efectos perturbadores en la prestación del servicio.

Un proveedor de servicios digitales (PSD) será toda persona jurídica que preste un servicio digital y se recogen 3 tipos:

- Mercado en línea
- Motor de búsqueda en línea
- Servicios de computación en nube

Los OSE y los PSD deberán:

- Adoptar las medidas necesarias para gestionar los riesgos que se plantean en la seguridad en las redes y los sistemas de información.
- Adoptar las medidas necesarias de prevención de incidentes.
- Adoptar las medidas necesarias para en caso de incidente, minimizar los efectos y poder garantizar la continuidad de los mismos.
- Comunicar inmediatamente a la autoridad competente o a los CSIRT nacionales aquellos incidentes de ciberseguridad que tengan efectos significativos, es decir, aquellos que afecten a la continuidad de los servicios esenciales que prestan.

Cada estado miembro será el encargado de establecer unas medidas para garantizar el cumplimiento disposiciones nacionales aprobadas y unas sanciones en caso del incumplimiento de las mismas.

En la Directiva NIS, se reconoce la importancia de la cooperación internacional, permitiendo acuerdos con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades del Grupo de cooperación. En tales acuerdos se tendrá en cuenta la necesidad de garantizar una protección de datos adecuada.

6 Conclusión

Como tantos otros avances en la historia de la tecnología, la red TOR fue creada con un propósito militar, sin embargo, acabó dando servicio a millones de personas que buscan el anonimato en sus comunicaciones. Muchas de estar personas, se benefician de esta red de forma legítima protegiendo su intimidad, sin embargo, muchas otras aprovechan la clandestinidad que proporciona para realizar actividades delictivas.

Aunque la idea generalizada en la sociedad sobre esta red es que proporciona un anonimato absoluto, la realidad es otra bien distinta, ya que existen numerosas formas de romper ese anonimato. Sin ir más lejos, un usuario inexperto, es muy probable que deje en su navegación cierta cantidad de información que pueda identificarle. Por lo tanto, es una red que, aunque protegerá nuestra intimidad en gran medida, no es infalible.

La irrupción de este tipo de redes de anonimato, junto la creciente expansión de las monedas virtuales, ha propiciado el entorno apropiado para el crecimiento de mercados negros en la red y las actividades delictivas que se cometen en ellos. Debido a las características de las redes anónimas y de las criptomonedas, las autoridades tienen muy difícil combatir los delitos que se cometen en dichos mercados, sin embargo, se han realizado con éxito numerosas operaciones en contra de ellos.

Muchas veces, la sociedad avanza mucho más rápido que las leyes y el caso del cibercrimen es un claro ejemplo. Es ahora, cuando empezamos a comprender que los ciberdelitos no son sólo un conjunto de hechos que combatir, sino que, se necesitan planes nacionales de ciberseguridad que protejan los ciudadanos en las redes y aseguren los servicios que se proporcionan a través de ellas. En este sentido, está avanzando nuestra legislación, tanto nacional como europea.

7 Bibliografía

[1] *Alberto García. Obtenido de https://www.adslzone.net/2017/07/14/alphabay-cierra-el-mayor-mercado-negro-de-la-dark-web-tras-una-redada/*

[2] *Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Weinmann. (2013). Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. University of Luxembourg, Luxembourg.*

[3] *B.O.E. Obtenido de https://www.boe.es/doue/2013/218/L00008-00014.pdf*

[4] *B.O.E. Obtenido de https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf*

[5] *B.O.E. Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-1995-25444*

[6] *B.O.E. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2015-3439*

[7] *B.O.E. Obtenido de https://www.boe.es/doue/2016/194/L00001-00030.pdf*

[8] *Jesús Díaz. Obtenido de https://www.certsi.es/blog/tor-servicios-ocultos-desanonimizacion*

[9] *Marcos Díaz. Obtenido de https://clickjuridico.es/es-legal-navegar-por-la-deep-web/*

[10] *Patricia Olvera Rodríguez. Obtenido de http://crimina.es/crimipedia/topics/web-profunda-darnet-tor/*

[11] *Patricia Olvera Rodríguez. Obtenido de http://crimina.es/crimipedia/topics/web-profunda-darnet-tor/*

[12] *Jose María Alonso. Obtenido de http://www.elladodelmal.com/2015/03/raptor-el-anonimato-en-la-red-tor-deep.html*

[13] *enclavedederecho. Obtenido de https://enclavedederecho.com/deep-web-internet-profundo/*

[14] *Fernando Davara. Obtenido de http://fernandodavara.com/ciberseguridad-la-vision-de-la-union-europea-2/*

[15] *Fernando Davara. Obtenido de http://fernandodavara.com/directiva-nis/*

[16] *Mario Pérez Esteso. Obtenido de https://geekytheory.com/que-es-y-como-funciona-la-red-tor*

[17] *Guillermo Julián. Obtenido de https://www.genbeta.com/seguridad/como-funciona-la-red-tor*

[18] *Guillermo Julián. Obtenido de https://www.genbeta.com/actualidad/como-espia-la-nsa-a-los-usuarios-de-tor*

[19] *Miguel Jorge. Obtenido de http://es.gizmodo.com/europol-anuncia-el-mayor-golpe-contra-la-dark-web-de-la-1797091281*

[20] *David Heinemeier. Obtenido de http://hackeruna.com/2017/02/02/privacidad-y-seguridad-en-internet-la-web-oscura-deepweb/*

[21] *Miriam Guardiola. Obtenido de http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal*

[22] *Alex Preukschat. Obtenido de https://www.oroyfinanzas.com/2013/10/bitcoin-block-chain/*

[23] *Salo, J. Recent Attacks On Tor. Aalto University.*

[24] *Sánchez, R. A. ramonalarconsanchez. Obtenido de https://ramonalarconsanchez.com/2017/07/31/darknet-de-tor-util-para-los-periodistas-peligrosa-para-los-estados/*

[25] *Pedro Castillo. Obtenido de https://securityinside.info/servicios-ocultos-en-tor-como-pasan-desapercibidos/*

[26] *Pedro Castillo. Obtenido de https://securityinside.info/vulnerabilidades-en-tor-anonimato-servicios-ocultos/*

[27] *Sam DeFabbia-Kane. Obtenido de https://es.slideshare.net/chemai64/analizando-la-efectividad-de-ataques-de-correlacion-pasivos-en-la-red-de-anonimato-tor*

[28] *Wikipedia. Obtenido de https://es.wikipedia.org/wiki/Tor*