Universitat Oberta de Catalunya
uoc.edu

Red de anonimización TOR y cibermercados negros

Jorge Luengo García

Trabajo de Fin de Máster (TFM)

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

Tutora:

Ángela María García Valdés

Índice

Listado de ilustraciones

Listado de tablas

Agradecimientos

En primer lugar, agradezco a mi familia la paciencia que han tenido conmigo durante todos estos años, así como la oportunidad para llegar a dónde estoy y poder haber tenido los recursos necesarios para poder formarme.

A mi hermano, que ya no está con nosotros, pero siempre lo recordaré. El chiquitín de la casa al del que siempre envidié su forma de tomarse las cosas y que tanto me aguantó.

Por otro lado, a Belén, que me dio tanto y supo comprenderme y aguantarme en tantos momentos y sentí que siempre estuvo orgullosa de mí. Siempre se lo agradeceré.

A mis amigos, por estar ahí en momentos duros y momentos felices. Y a mis compañeros de trabajo que muchas veces se convirtieron en amigos con los que comparto espacio y tiempo durante largas horas.

Todos vosotros me habéis hecho ser quien soy ahora.

Un abrazo fuerte a todos.

Resumen

Este trabajo proporciona un punto de partida a la red Tor, los conceptos básicos de qué es y cómo funciona. El objetivo de esta red es la anonimización de sus usuarios principalmente, junto a una serie de características que lo hacen diferente de otras redes con el mismo objetivo. Esta característica, la anonimización, puede ser atacada por lo que se describen los ataques principales que se encuentran hasta ahora incluyendo, además, una pequeña prueba de concepto. Tras describir las características principales de la red Tor, se pueden deducir una serie de usos, tanto éticamente aprobados como otros que no. En relación a lo segundo, ofrece la posibilidad a diversos actores con intenciones delictivas a ocultarse tras una capa de anonimización. Esto supone que el nacimiento de los mercados negros dentro de esta red. Los mercados negros son sitios web donde se llevan a cabo transacciones de cualquier tipo de artículos o servicios ilegales en su mayoría. Para mantener el anonimato dentro de estas redes, se utilizan un tipo de monedas denominadas criptomonedas, cuya característica principal es tratar de mantener el anonimato de ambas partes de la transacción. Tanto las acciones llevadas a cabo dentro de la red Tor como la propia navegación a través de ella, se encuentran legisladas por el país de origen. En este caso concreto el trabajo se centra en la legislación española.

Abstract

This paper is going to provide a starting point for the Tor network, the basics of what it is and how it works. The objective of this network is the anonymization of its users mainly, along with a few features that make it different from other networks with the same purpose. The network can be attacked from different attack paths, so the main attacks are described, including and small proof of concept. After describing the main features of the Tor network, several uses can be deduced, both ethically approved, and others totally disapproved. In relation to the second one, it offers the possibility for various people with criminal intentions to be hidden behind a layer of anonymization. This implies the birth of dark markets within this network. Dark markets are websites that allows transactions of any kind of mostly illegal goods or services but has partly legal transactions. In order to maintain anonymity within these networks, a type of coin called cryptocoin is used, the main feature of which is to try to maintain the anonymity of both parties to the transaction. Both actions were carried out within the Tor network and the navigation through it are legislated by the country of origin. In this particular case, the work focuses on the Spanish law.

Glosario de términos

A

AES

Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. 15

B

BGP

El protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP. 21

Bittorrent

Es un protocolo diseñado para el intercambio de archivos punto a punto (peer-to-peer) en Internet. 21

D

DH

El algoritmo de Diffie-Hellman (en honor a sus creadores, Whitfield Diffie y Martin Hellman) permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes. La clave secreta resultante no puede ser descubierta por un atacante, aunque éste obtenga los dos mensajes enviados por el protocolo. La principal aplicación de este protocolo es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones entre dos máquinas. 16

Digest

Se define como la salida de una función de hash. 15

H

hijacking

El hijacking (traducido como "secuestro"), en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo por parte de un atacante. Es un concepto muy abierto, que se puede aplicar a varios como el robo de información, el secuestro de una conexiones de red, de sesiones de terminal, servicios, módems, etc. 21

K

keepalive

Se refiere a un mensaje entre el un servidor y un cliente con el objetivo de indicar que la conexión se mantiene. 15

M

man-in-the-middle

Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. 23

P

padding

S

T

Introducción

Contexto y justificación del trabajo

El objetivo del trabajo es investigar acerca de la red Tor, tratando de interiorizar los conceptos en los que se basan las técnicas actuales para anonimizar las conexiones y por ende a los individuos, empezando desde los principios básicos hasta las técnicas actuales. Las mencionadas técnicas de anonimización suponen que individuos perseguidos por leyes de censura o periodistas pueden seguir comunicándose sin tanto riesgo como anteriormente, dado que el concepto absoluto de anonimidad no existe. Pero aparte de estas alternativas de uso, surgen otras cuyo uso no éticamente aprobable como son los mercados negros, que se apoyan en esta tecnología para llevar a cabo operaciones de intercambio de todo tipo de productos y servicios en su mayoría ilícitos. Descubrir cómo funcionan estos mercados, cómo llevar a cabo una transacción y sus características es parte del objetivo del trabajo. Para desarrollar estas actividades económicas se utilizan un tipo de monedas virtuales denominadas criptomonedas. Entender los principios en los que se basan es otro de los propósitos.

Por último, para tener una idea más clara de cómo se puede utilizar la tecnología antes descrita dentro de España se investigarán y desarrollarán los aspectos legales de este tipo de tecnología dentro de nuestro país, así como alternativas a la red Tor como pueden ser FreeNET o I2P.

Objetivos del trabajo

Los objetivos del trabajo son los que se describen a continuación:

- Proporcionar una Introducción a los conceptos básicos de la DeepNet y la Darknet
- Definir qué es Tor y para qué se utiliza.
- Descubrir cómo funciona Tor, sus principios básicos y cómo es su tecnología.
- Describir qué son los mercados negros y explicar su funcionamiento, así como los diferentes tipos y productos que se pueden comprar.
- Para llevar a cabo las transacciones económicas dentro de los mercados negros se utiliza un tipo de moneda, las criptomonedas. Se estudiarán las características principales de estas monedas.
- Encajar el uso de las tecnologías antes mencionadas en el marco legal español.
- Comparar la red Tor con otras redes orientadas al anonimato.
- Proporcionar una pequeña prueba de concepto de una de las vulnerabilidades.

Enfoque y método seguido

Teniendo en cuenta que habrá varias tareas, la metodología se definirá en función del tipo de tarea, siendo estos los diferentes grupos:

- Investigación y búsqueda de información
    - Partiendo de la base de distintas fuentes; recursos web, libros relacionados con la temática, diversos papers que se pudiera encontrar tanto en la biblioteca de la UOC como en otros sitios, se recopilará y filtrará la información.
- Organización de la información.
    - Todas aquellas fuentes se deben de tratar de una forma correcta, legible y productiva, de forma que se pueda obtener la mejor comprensión de ésta. Es por ello por lo que organizar todo lo obtenido anteriormente es un punto muy importante.
- Instalación de herramientas /aplicaciones necesarias

    - Para el desarrollo de la prueba de concepto ha hecho falta:
        - VirtualBox (https://www.virtualbox.org/)
        - Windows (https://www.microsoft.com/es-es/windows)
        - Python 3 (https://www.python.org/)
- Preparación del vídeo de presentación del trabajo
    - Tendrá que plantearse un guion, en el que se incluirá una presentación, puntos más relevantes, objetivos alcanzados, conclusiones y trabajos futuros.
    - Probablemente se utilice la herramienta sugerida por la universidad:
        - OBS Studio (https://obsproject.com)
- Revisión de la memoria
    - Se hará de forma concienzuda en tres partes.
        1. De contenido contractual en relación a los requisitos
        2. De forma y corrección.
        3. Otra segunda de formato

Planificación del trabajo

Antes de poder llevar a cabo una aproximación del tiempo que pueden llevar cada una de las tareas hay que conocer el punto de partida. La experiencia y conocimiento sobre el tema concreto del proyecto es escasa por parte del estudiante, por lo que se considera que el tiempo de familiarización será considerable, aunque teniendo en cuenta que es una parte esencial del proceso se invertirá el tiempo necesario.

Por otro lado, la situación y dedicación personal del alumno. Actualmente se encuentra trabajando y no dispone de mucho tiempo a la semana. Se estima que entre semana se podrían dedicar unas 6 horas y el fin de semana otras 8. Es decir, una media de 14 horas semanales.

Se describieron una serie de objetivos ordenados por orden de prioridad en los que 1, era mayor prioridad y 7, acorde al pliego de requisitos entregado al inicio del proyecto:

1. Llevar a cabo la inmersión dentro de los fundamentos de la tecnología de anonimización de TOR. Dentro de dicha introducción, se tienen que contemplar, al menos, los siguientes conceptos:
    a. Componentes del sistema.
    b. Interacciones
    c. Proceso de ocultación de usuarios y servicios en la red.
2. Seleccionar y describir dos técnicas de desanonimización de usuarios y servicios.
3. Desarrollar un estudio acerca de los mercados negros de la red TOR. Entre otros puntos a desarrollar, al menos se tienen que cubrir los siguientes:
    a. Cómo operan.
    b. Cómo se ocultan las actividades comerciales.
    c. Relación de las criptomonedas en los cibermercados negros.
        i. Introducción de las criptomonedas
        ii. Características
        iii. ¿Por qué se utilizan en estos mercados?
4. Presente, pasado y futuro de la legislación relacionada con la red TOR.
5. Trabajos futuros
6. Comparativa con otro tipo de redes como FreeNET o I2P.
7. Llevar a cabo un PoC de una de las técnicas encontradas (Valorar dificultad)

Todas las anteriores se fueron encajando acorde a las fechas de entrega establecidas por la universidad:

Entrega	Fecha
PEC1 → Plan de trabajo	12/03/2019
PEC2 → Conceptos acerca de TOR	02/04/2019
PEC3 → Técnicas de desanonimización	30/04/2019
PEC4 → Memoria Final	04/06/2019
PEC5 → Vídeo presentación del proyecto	11/06/2019
Defensa → Defensa del proyecto	17/06/2019 – 21/06/2019

Tabla 1-Planificación temporal

A la fecha de la entrega de la memoria, todos los hitos programados (PEC1 – PEC 4) fueron cumplidos bajo lo acordado.

Breve descripción de los productos obtenidos

Tras el desarrollo del trabajo no existe como tal un producto final. Este trabajo versaba sobre el estado del arte y de los puntos descritos anteriormente. Si es cierto que se ha realizado una pequeña prueba de concepto y como resultado se han obtenido 2 scripts en Python:

- Test3_getIP.py
- Test3_getIP_noExploit.py

Fundamentos de la red TOR

Introducción

La idea de TOR nace como una iniciativa del Tor Project liderado por Roger Dingledine (Dingledine) en 2003 y que no ha parado de crecer desde entonces con la aportación de voluntarios de todo el mundo que ayudan al desarrollo y al soporte de la red TOR.

La red Tor se caracteriza por ser una red de baja latencia capaz de proporcionar “anonimato” de sus usuarios, es decir no revela su dirección IP. Basándose originalmente en el enrutamiento de capas de cebolla, en el que los nodos de la red sólo conocen el anterior nodo y el siguiente hacia dónde deben encaminar el tráfico. Además de estas principales características, se incluyen las de control de congestión, servidores de directorio, control de integridad, políticas de salida configurables y un diseño práctico para servicios de localización oculta a través de puntos de encuentro.

El fundamento de Tor se puede resumir en 3 pasos, tal y como se indica en https://www.torproject.org/about/overview.html:

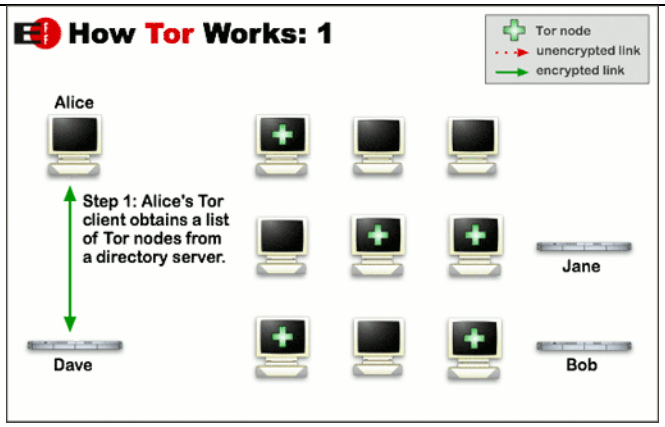
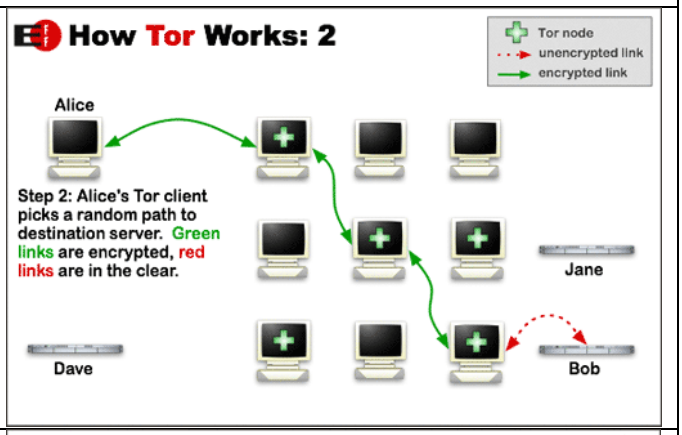
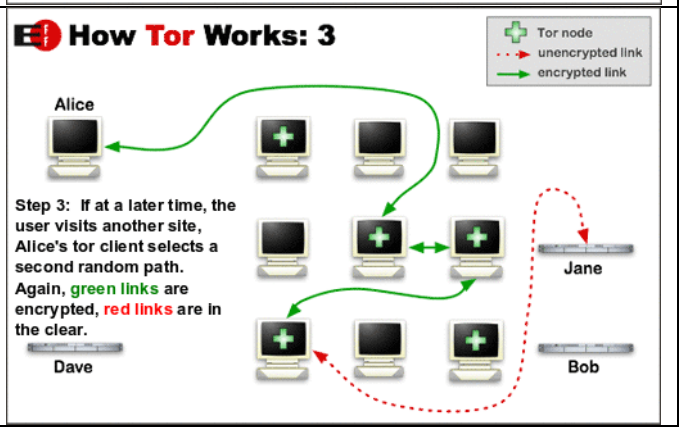
1. Un cliente TOR obtiene una lista de nodos del servidor de directorios	
2. Se escoge un camino aleatorio hasta el servidor de destino donde la comunicación entre los puntos intermedios está cifrada y, únicamente la última conexión va en claro.	
3. Cada cierto tiempo o si el cliente visita otro destino, la ruta es recalculada para evitar el rastreo.	

Tabla 2-Tor en 3 Pasos

Dado que ya se han planteado los principios básicos y el funcionamiento a grandes rasgos de la red Tor, a continuación, se describe la arquitectura, empezando por los nodos.

Arquitectura

Repetidores (Nodos)

Se determinan repetidores aquellas instancias de Tor que son capaces de tomar el tráfico de entrada y replicarlo a otra instancia de Tor. Es decir, funcionan como proxys transparentes que enrutan el tráfico al siguiente salto de un circuito. Hay que tener en cuenta que cualquier cliente puede actuar como repetidor con la configuración adecuada y el ancho de banda suficiente. Dicha configuración se indica en el fichero *torrc*.

Internos

La característica principal de estos repetidores es que carecen de la capacidad para acceder directamente a los paquetes de datos que viajan entre el cliente y el destino. Se encargan de eliminar la capa de cifrado correspondiente a su propia clave privada y acceder exclusivamente a la única parte necesaria de información para acceder al siguiente salto del circuito.

Externos

Son también denominados nodos de salida. Son capaces de enrutar el tráfico al exterior de la red, suprimir la última capa de cifrado correspondiente y descubrir el contenido del mensaje que se mandó originalmente. Es decir, en definitiva, son conocedores del contenido (en caso de que la conexión no se haya cifrado de extremo a extremo) y del destino del mensaje.

Celdas

La unidad mínima de información que se transmite entre los nodos son las celdas de tamaño fijo (512 bytes). Estas celdas están formadas por una cabecera y un *payload*:

CircId	CMD	Data
2 bytes	1 byte	509 bytes

Ilustración 1 Celda

- Header: incluye las siguientes partes
    - Identificador de circuito (circID): especifica a qué circuito corresponde la celda. Hay que tener en cuenta que varios circuitos pueden ser multiplexados a través de una misma conexión TLS. Además, cada conexión tiene un circID diferente
    - Comando (CMD): indica qué hacer con el *payload*.

Dependiendo del comando que contenga la celda puede haber celdas de dos tipos, las cuáles se describen a continuación.

Celdas de control

Son siempre interpretadas por el nodo que las recibe. Los comandos que pueden incluir este tipo de celdas son los siguientes:

- Padding: se usa como un *keepalive* o para añadir un *padding* al último bloque.
- Create o Created: se utiliza para crear un nuevo circuito.
- Destroy: se invoca para destruir un circuito.

Celdas relay

Tienen un header adicional, el *relay* header, que contiene los campos descritos a continuación.

Ilustración 2 Celda relay

CircId	Relay	StreamID	Digest	Len	CMD	Data
2 bytes	1 byte	2 bytes	6 bytes	2 bytes	1 byte	498 bytes

Ilustración 3 Celda de control

- *streamID:* identifica cada uno de los streams (transmisiones) dentro de un mismo circuito.
- end-to-end checksum (Digest): para verificar la integridad del mensaje
- longitud: indica la longitud del payload
- comando relay: el cual puede ser cualquiera de los siguientes:
    - relay data: para los datos que son enviados a través de la transmisión.

- relay begin: para abrir un nuevo stream.
- relay end: para cerrar un stream.
- relay teardown: para cerrar un stream cuya comunicación se ha roto en algún momento.
- relay connected: para notificar que la conexión con otro nodo se ha establecido correctamente.
- relay extend/extended: para añadir un salto al circuito o reconocerlo
- relay truncate/truncated: para acortar parte del circuito o reconcerlo.
- relay sendme: utilizado para el control de la congestión.
- relay drop: utilizados para implementar falsos circuitos de largo recorrido

Hay que destacar que, tanto el relay header como el relay payload se van cifrando y descifrando a medida que el paquete se va moviendo a lo largo del circuito utilizando, para ello, AES-128 CBC en *counter mode*.

Circuitos

La conexión entre los distintos nodos con el objetivo de mandar un mensaje se conoce como circuitos. Estos poseen la característica de ser de doble sentido, lo cual quiere decir que se pueden tanto enviar como recibir datos por el mismo circuito.

Un circuito está compuesto, al menos, de tres repetidores que actúan como servidores proxy para la comunicación entre un cliente y un destino.

Para establecer la comunicación, lo primero que tiene que preguntar el cliente es acerca de los nodos disponibles. A partir de ahí, pregunta por las claves públicas de cada uno de los nodos por los que va a pasar la comunicación y cifra el contenido del mensaje por capas y en orden inverso al orden de los nodos por los que va a pasar la comunicación.

Originalmente se comenzó utilizando un circuito por transmisión, pero debido al enorme coste que tiene crear un circuito debido a la numerosa cantidad de operaciones criptográficas se decidió multiplexar los circuitos y así poder varios *streams* sobre un mismo circuito.

Más en profundidad, teniendo en cuenta los siguientes actores:

- Cliente Tor instalado en el PC de un usuario
- 3 nodos
- Servicio de Directorio
- Servidor Web

los pasos que se llevan a cabo para la creación de un circuito son los siguientes:

1. El cliente Tor pregunta al Servicio de Directorio por los nodos disponibles.
2. El Descriptor contesta con una lista de nodos disponibles y sus respectivas claves públicas
3. El cliente manda una celda al primer nodo de su circuito con el comando *create* (contiene la primera mitad del algoritmo *DH* cifrada con la clave pública (OR) del primer nodo).
4. El nodo que ha recibido el mensaje manda de vuelta otra celda con el comando *created* conteniendo la otra mitad de la clave DH y el hash de la clave negociada.
5. Para extender el circuito, el cliente vuelve a mandar otra celda, pero esta vez con el comando *relay extend* indicando la dirección del nuevo nodo.
6. El primer nodo descifra el mensaje y lo manda al segundo nodo con un comando *created*.

7. El segundo nodo contesta con un *created cell*. El primer nodo encapsula el paquete y lo manda al cliente
8. Este proceso se repite hasta llegar al último nodo que recibe como dirección de salida la del servidor web.

Hay que indicar que Tor no ofrece cifrado por sí mismo desde el último nodo hasta el servidor web, por lo que se recomienda encarecidamente que se utilice algún tipo de cifrado end-to-end entre el cliente y el servidor como pudiera ser HTTPS.

Servicio de directorio

Es un nodo confiable que almacena el estado de la red. Proporciona una serie de documentos denominados descriptores indicando nodos conocidos y su estado actual. Lo usuarios pueden descargar su estado periódicamente mediante peticiones HTTP.

Descriptores

Para que la red Tor conozca qué tipo de nodo es al que se está conectando y cómo llevar a cabo dicha conexión, se utiliza una serie de ficheros de carácter público denominados *Descriptores*. Para conocer la información que se encuentra en estos documentos no hay más que hacer una petición HTTP. Hay diferentes tipos, entre los que se encuentran los siguientes:

Server Descriptor

Es el descriptor principal que publican los repetidores en las autoridades de directorio. Este documento contiene toda la información sobre el repetidor, incluye sus políticas de salida, detalles sobre el uso del ancho de banda, dirección IP, puerto “OR”, sistema operativo, entre otros detalles.

ExtraInfo Descriptor

Como su propio nombre indica, ofrece información adicional que, a priori, no sería necesaria para establecer la comunicación entre los nodos. Estos descriptores son publicados de forma automática pero no son recuperados de la misma forma por los clientes, sino que tienen que ser solicitados de forma intencionada.

Micro Descriptor

Es aquel que contiene exclusivamente la información necesaria para establecer la comunicación. Actualmente es el que es que se utiliza por defecto con el objetivo de reducir el ancho de banda necesario.

Network Status Document (consenso)

Es el fichero encargado de proporcionar información acerca de la votación de todas las autoridades de Tor. Este fichero contiene una serie de registros denominados *Router Status Entry*

Router Status Entry

Cada una de las entradas del *Network Status Document* se designan como *Router Status Entry*. Estas entradas se utilizan para almacenar información proporcionada por las autoridades de directorio, las cuales incluyen, entre otras, flags y heurísticas para la selección de repetidores por parte de los clientes a la hora de componer circuitos.

Hidden Service Descriptor

Es un documento firmado y publicado por un servicio oculto y cuya característica principal es la de contener un flag "HSDir". El contenido incluye toda la información necesaria para establecer la comunicación con estos servicios ocultos.

Servicios ocultos (hidden services)

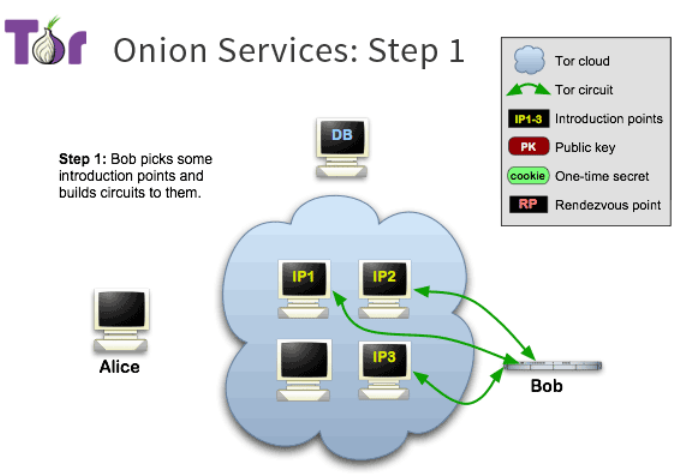
Con el objetivo de poder proporcionar servicios cuya IP no sea descubierta públicamente, se encuentran los servicios ocultos (hidden services). Estos servicios pueden ser de diferentes tipos, desde servidores web a servicios de mensajería.

Para que cualquier usuario de la red Tor pueda conectarse a los antes mencionados, servicios ocultos, deben existir los "redezvous points", donde los usuarios se conectan y descubren la clave pública de los servicios ocultos y se les permite conectarse a ellos.

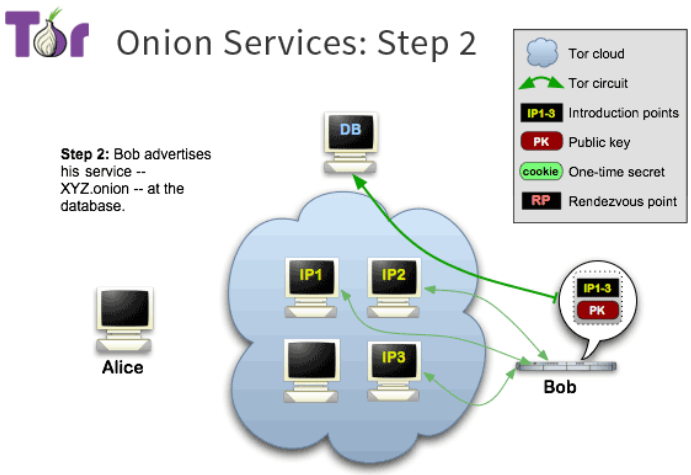
Para que finalmente el cliente sea capaz de conectarse a estos servicios ocultos, el proceso se divide en dos fases: configuración del servicio oculto y establecimiento de la conexión. A continuación, se describen ambos procesos:

Configuración del servicio oculto

1. El servicio oculto crea una serie de circuitos de la red Tor y proporciona a cada *Introduction Point* su clave pública.



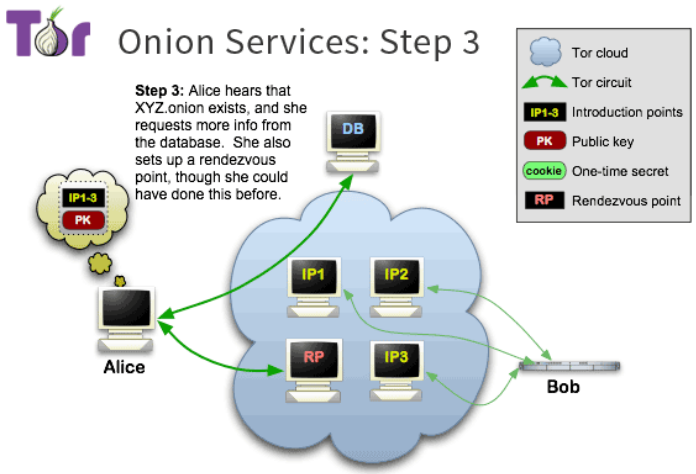
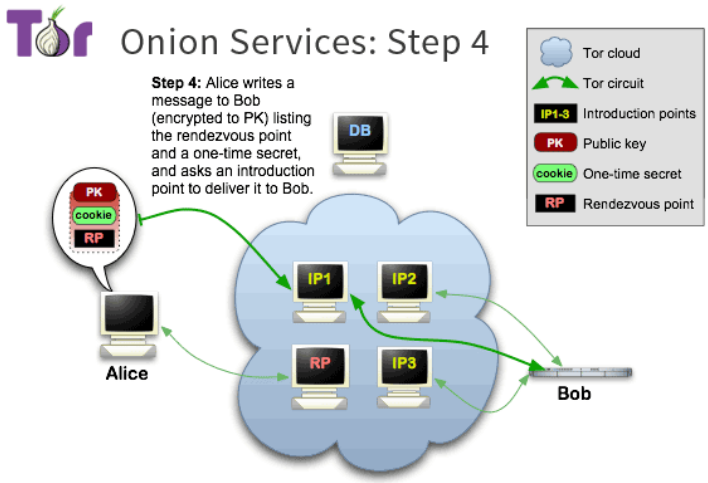
2. El servicio oculto crea un descriptor que contiene su clave pública y un resumen de cada uno de los *introduction points* previamente seleccionados. Por último, firma dicho descriptor con su clave privada y sube el fichero a una tabla hash. El fichero podrá ser obtenido por los clientes haciendo una petición XYZ.onion donde XYZ es un nombre derivado de la clave pública de 16



caracteres. Una vez que este proceso se ha completado se considera que el servicio oculto ha sido configurado.	

Tabla 3-Configuración de un servicio oculto

Establecimiento de la conexión

1. Cuando un cliente quiere conectarse a un servicio oculto lo primero que tiene que conocer es su dirección onion. Para ello tiene que descargarse el descriptor correspondiente desde la tabla hash. Si existe un descriptor XYZ.onion, el cliente conocerá los *introduction points* y la clave pública correcta. Al mismo tiempo, el cliente crea un circuito Tor hacia otro nodo y le pregunta si puede actuar como *rendezvous point* pasándole una cookie de sesión.	
2. Una vez que el *rendezvous point* y el descriptor están en manos del cliente, dicho cliente crea un *introduce message* (cifrado con la clave pública del servicio oculto) que contiene la dirección del *rendevouz point* y una cookie de sesión. Hay que aclarar que toda la comunicación se lleva a cabo a través de circuitos de la red Tor, por lo que la	

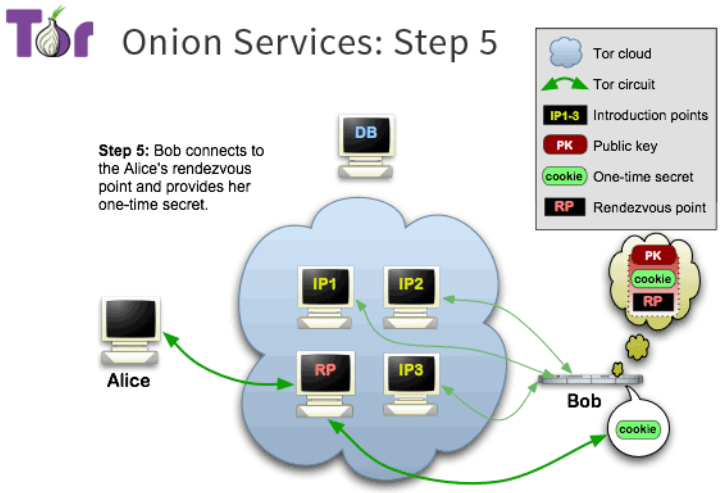
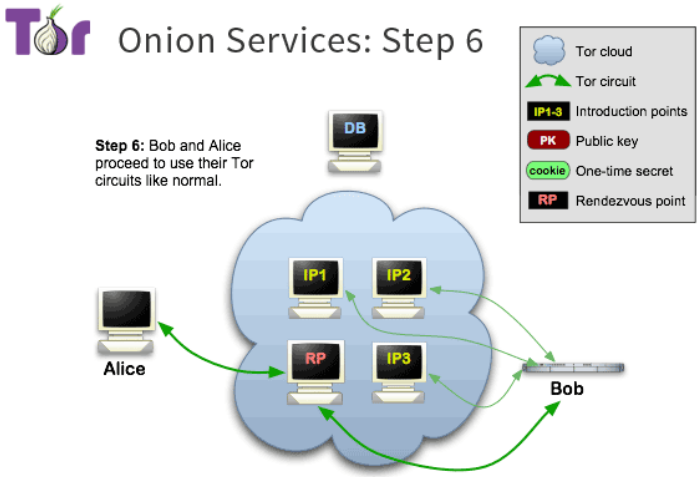
transmisión se mantiene anónima.	
3. El servicio oculto descifra el mensaje cifrado con su clave pública y obtiene la dirección del *rendevouz point* y de la cookie de sesión. Una vez que ya tiene ambos datos, crea un circuito hacia el *rendezvous point* y manda la cookie de sesión hacia dicho *rendezvous point* en un mensaje *rendezvous.*	
4. En el último paso, el *rendezvous point* notifica al cliente acerca de la conexión satisfactoria. Justo después, el cliente y el servicio oculto pueden utilizar los circuitos con el *rendezvous point* para comunicarse. Cabe destacar que el *rendezvous point* únicamente sirve como repetidor de una conexión que está cifrada punto a punto.	

Tabla 4-Establecimiento de una conexión

Técnicas de desanonimización

Las técnicas de desanonimización consisten en llevar a cabo un ataque de tal forma que se descubra la IP real del usuario que inicia la comunicación o de (Farinacci, s.f.)un servicio oculto. Estos ataques se pueden llevar a su vez sobre tres puntos clave: el cliente (el navegador o aplicación concreta que utiliza el cliente para conectarse a la red Tor); el servidor del servicio oculto que puede ser comprometido; o la propia infraestructura de red Tor que puede ser atacada.

https://www.deepdotweb.com/2019/02/20/research-classification-of-attacks-on-tor-clients-and-tor-hidden-services/

Clientes Tor

El ataque por excelencia en la red Tor ha sido el de aprovechar de alguna forma la topología de esta para descubrir la IP real del iniciador de la conexión. Pero de un tiempo a esta parte se han

desarrollado técnicas que implican aprovechar vulnerabilidades de los clientes utilizados para conectarse.

Ataques basados en aprovechamiento de plugin o fallos del navegador

La utilización de alguno de estos plugins para correr aplicaciones de tipo Java, Flash, etc. o simplemente, fallos de configuración del navegador, pueden provocar un bypass de la configuración del proxy de Tor, permitiendo así que la comunicación salga de la red Tor momentáneamente y así, sea descubierta por el atacante. Por defecto, el navegador Tor desactiva la ejecución de estos plugins.

Ataque Torben

Es un taque basado en la modificación de alguna página web con el objetivo de forzar al cliente a utilizar fuentes no confiables y explotar las características de baja latencia de la red Tor para inferir a qué páginas se ha accedido.

P2P

En este ataque se pretende aprovechar la comunicación con servicios peer-to-peer. Por ejemplo, si se está utilizando un cliente de Bittorrent, un atacante podría obtener la dirección IP que utiliza Tor para conectarse con el tracker Torrent. En este caso, aunque la lista de trackers puede ser obtenida de manera anónima, las comunicaciones P2P son comúnmente establecidas de forma insegura comunicándose directamente con el otro peer. Por lo tanto, el atacante podría utilizar una técnica de man-in-the-middle para modificar el contenido de la lista proporcionada a través del tracker de Torrent añadiendo la dirección IP de un peer malicioso. Teniendo en cuenta el hecho de que las comunicaciones con los peers de destino no pueden ser establecidas a través de la red Tor, el atacante tendría la posibilidad de obtener la dirección IP del cliente Tor que inicia la comunicación con el tracker Torrent.

Modificar la selección del primer nodo de Tor

Lo primero a tener en cuenta es que la comunicación entre el cliente y el primer nodo de la red Tor están cifrados, por lo que un atacante externo no podría ver el contenido de la comunicación entre ambos puntos. Sin embargo, sería posible inducir al cliente Tor a conectarse a ciertos nodos controlados por el atacante accediendo a cierta configuración del ISP o del administrador de la red, de tal forma que el primer nodo estaría controlado y la comunicación se vería comprometida.

Raptor

Lo primero de todo, hay que indicar que Raptor se refiere a Routing Attacks on Privacy en Tor, de ahí su nombre. Consiste en un grupo de estrategias que pueden ser lanzadas a través de un Autonomous System (AS) con el objetivo de desanonimizar clientes Tor. Una de las estrategias reside principalmente en el análisis del tráfico de red de comunicaciones asimétricas que marcan la red. Otra estrategia sería la de explotar la rotación natural dentro de las rutas BGP y el enrutamiento de Internet para lograr un análisis de tráfico de red. Por último, existe otro ataque basado en la manipulación del enrutado de Internet mediante acciones de hijacking sobre BGP, las cuales son establecidas para descubrir los nodos de protección Tor de los clientes.

Explotación de puertos no muy conocidos

Este ataque está basado en el hecho de los puertos de salida de la red TOR utilizados para la conexión a Internet son reducidos. Está diseñado para desanonimizar clientes mediante el uso de un grupo comprometido de nodos de entrada y salida. Los nodos de salida del atacante permiten conexiones sobre puertos que no son del todo comunes. Además, para que el ataque

funcione, el atacante tiene que tener control sobre el host del servicio al cual el cliente intenta conectar. El objetivo del ataque es conseguir que el cliente establezca una comunicación que pase tanto por un nodo de entrada como uno de salida comprometidos. Esto finalmente permitiría desanonimizar a la víctima mediante técnicas de correlación del tráfico.

Ataque predecesor

El objetivo de este ataque es el de identificar al cliente que se está conectando. Para ello, a partir obtener el control de una serie de nodos de entrada se podría llegar a inferir el nodo desde el que se está llevando a cabo la conexión.

Uno o varios nodos hacen un estudio de las conexiones entrantes. Cada vez que un cliente se conecta se apunta la conexión. La frecuencia de conexión es de 10 minutos, por defecto. De esta manera se identificará a un cliente por ser el que más veces se conecta a otros nodos.

Teniendo bajo control una serie de nodos de entrada se podría forzar la reconexión para así identificar más rápidamente a los clientes.

Ataques a los servidores

El objetivo de estos ataques sería la de desenmascarar la IP real de los servicios ocultos de Tor. Hay diferentes técnicas que se exponen a continuación:

Recuento de celdas y padding

Este ataque fuerza al servicio oculto a comunicarse con un punto de acceso comprometido. El atacante manda un paquete específico al punto de acceso del servicio oculto para especificar el rendevouz point. Entonces, el punto de acceso enruta el paquete hacia el servicio oculto el cual crea un circuito de Tor para conectar con el rendezvous point del atacante. Una vez que el rendezvous point ha sido entregado, el mensaje (el cual incluye una cookie o un token creado por el cliente) es programado para mandar un número predefinido de celdas hacia el servicio oculto de Tor a través del mismo circuito de Tor. Justo después, el rendezvous point cierra el circuito. El nodo de entrada, que está bajo el control del atacante, monitoriza el tráfico de red sobre los circuitos enrutados hacia él. Una vez que recibe una célula que incluye el mensaje de circuito cerrado, confirmará que ha ocurrido después de la célula, incluyendo las cookies de confirmación, que ha sido recibido y que el número de células es de recibidas y 53 caídas a través del circuito de Tor. Una vez que todas esas condiciones se han dado, el atacante puede concluir que el nodo guardián sobre el que tiene el control ha sido tomado del servicio oculto y, por lo tanto, podría obtener la IP del servicio oculto.

Manipulación de celdas de Tor

Modificando las celdas de Tor se pueden construir un servicio oculto de Tor. Una vez que el cliente manda una celda a un servicio oculto de Tor para establecer una comunicación, la petición atravesará el rendezvous point del atacante. Esto proporciona al atacante la capacidad de alterar el contenido de la celda, y, por tanto, enrutar el tráfico hacia el servicio oculto de Tor y mandar el timestamp de la celda alterada al servidor del atacante. La celda podría no ser identificada como una celda intacta enviada desde el servicio oculto de Tor, lo que activaría el envío de un mensaje de destrucción al cliente. Este mensaje se enrutará desde el nodo de entrada del servicio oculto, que es controlado por el atacante, al servidor central e incluirá información como el ID del circuito, la marca de tiempo de la celda, la dirección IP de origen y el ID del circuito.

Ataque Caronte

Caronte es una herramienta que detecta fugas de información en los servicios ocultos de Tor. Esta información puede incluir la configuración del servidor o incluso la dirección IP del servicio oculto.

Off-path man-in-the-middle-attack

Este ataque está basado en utilizar un ataque de man-in-the-middle sobre un servicio oculto de Tor. Asumiendo que la clave privada del servicio ha sido obtenida por el atacante, lanzar un ataque de man-in-the-middle es posible. El punto clave in dicho escenario es que el atacante no tiene por qué estar localizado a lo largo del canal de comunicación entre el servicio oculto y el cliente.

PoC

Introducción

Con la intención de llevar a la práctica al menos uno de los tipos de ataques de desanonimización anteriormente descritos se ha estudiado y adaptado un PoC (Proof of Concept) o prueba de concepto basada en una de las técnicas que se han descrito en los apartados anteriores.

En este caso se aprovecha una vulnerabilidad de la versión 7.X del navegador Tor que permite ejecutar JavaScript aun teniendo la configuración de seguridad en el máximo nivel en el cual, expresamente se indica que el uso de JavaScript estaría restringido. En numerosos posts de Internet declaran que esta funcionalidad supondría que se podría revelar la IP de origen. Sin embargo, el mero hecho de ejecutar JavaScript no permite conocer la IP de origen dado que, por las características de JavaScript, no se permite la ejecución fuera del propio contexto. Teniendo en cuenta ese punto, únicamente cabrían dos alternativas.

- La primera consistiría en hacer una petición a un servicio externo para obtener la IP, pero si se está navegando a través de un navegador TOR la IP que devolverá el servicio anteriormente mencionado será la del nodo de salida de la red TOR, con lo cual, la IP de origen seguiría oculta.
- La segunda opción, sería invocar a un applet Active X para llevar a cabo la petición fuera de contexto, sin embargo, esta opción sólo está permitida en un navegador Internet Explorer, y, además, necesitaría un paso de autorización explícita por parte del usuario.

En definitiva, el descubrimiento de la IP de origen no es posible, únicamente explotando la ejecución de JavaScript.

Sin embargo, JavaScript sí permite, mediante la ejecución de varias funciones llevar a cabo la generación de una huella del navegador. Con lo cual, aprovechando que JavaScript podría habilitarse en cualquier caso, se podría utilizar para crear huellas de los clientes y así rastrear al objetivo a través de su navegación.

Explicación de la vulnerabilidad

La vulnerabilidad del navegador que se ha utilizado fue publicada por Zerodium a través de su cuenta de Twitter el 10 de septiembre de 2018. Afecta a las versiones 7.x e implica que, aun teniendo establecida la configuración de seguridad del navegador al nivel más alto, se podría seguir ejecutando código javascript.

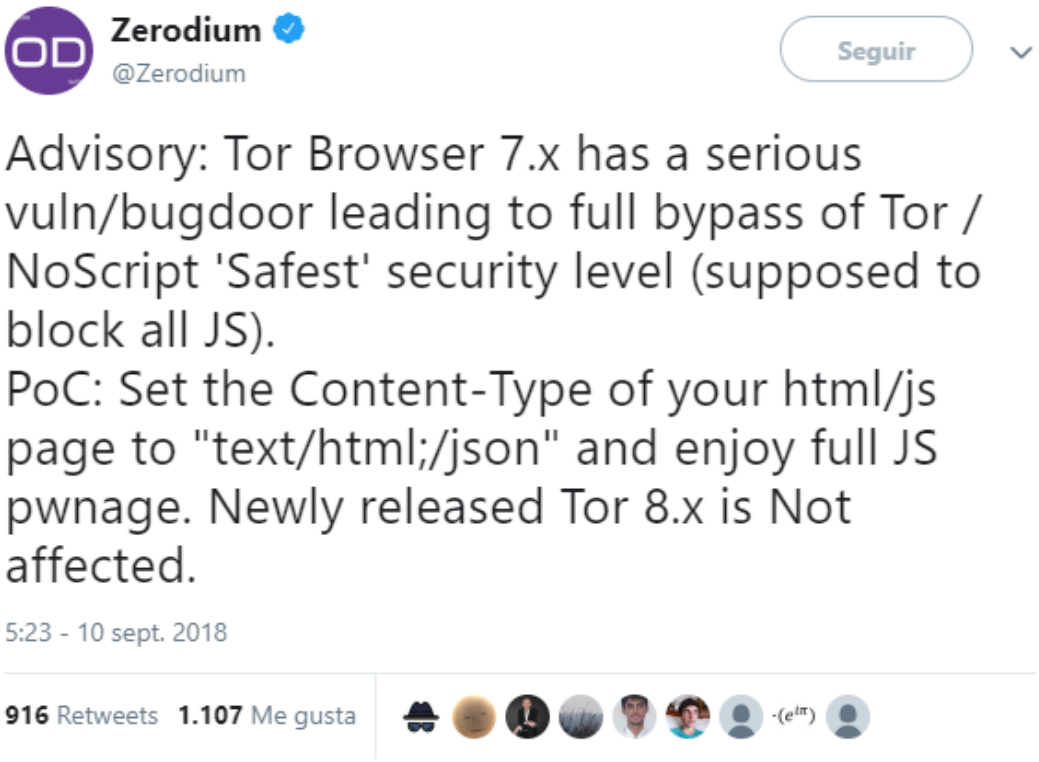


Ilustración 4 Exploit de Tor

Cómo se explota

Para saltarse la restricción del navegador, el Content-Type de la página que provenga del servidor tiene que contener el siguiente header: “Content-Type”, “text” ó “Content-Type”, “text”. En el siguiente repositorio se proporcionó una prueba de concepto que se ha utilizado para demostrar la vulnerabilidad:

https://gist.github.com/x0rz/8198e8e22b1f70fddb9c815c1232b795

Requisitos

Para llevar a cabo la ejecución de la se necesita tener instalada una máquina virtual en la que se va a instalar:

- Versión 7x de Tor
- Python 3
- Script

Instalación y configuración del entorno

Tor

Instalar Tor haciendo una instalación por defecto y deshabilitar lo antes posible la actualización automática. Hay que tener en cuenta que la versión 8.x ya tiene solucionado el bug.

Para poder ver cómo afecta el cambio de manera local y no tener que exponer al exterior un servidor, primero de todo hay que configurar el navegador para que NO acceda a la red TOR y salga directamente al exterior. Es decir, llevando a cabo esta configuración, el navegador funcionaría como cualquier Firefox o Chrome siendo la máquina cliente el nodo de salida:

1. Abrir el navegador
2. Hacer click en el menú de opciones situado en la esquina superior derecha.
3. Hacer click en “Opciones”
4. En la columna izquierda, seleccionar “Avanzado”
5. En el menú “Avanzado”, seleccionar Red y hacer click en “Configuración”.
6. Establecer la configuración tal cual aparece en la imagen y hacer click en “Aceptar”:

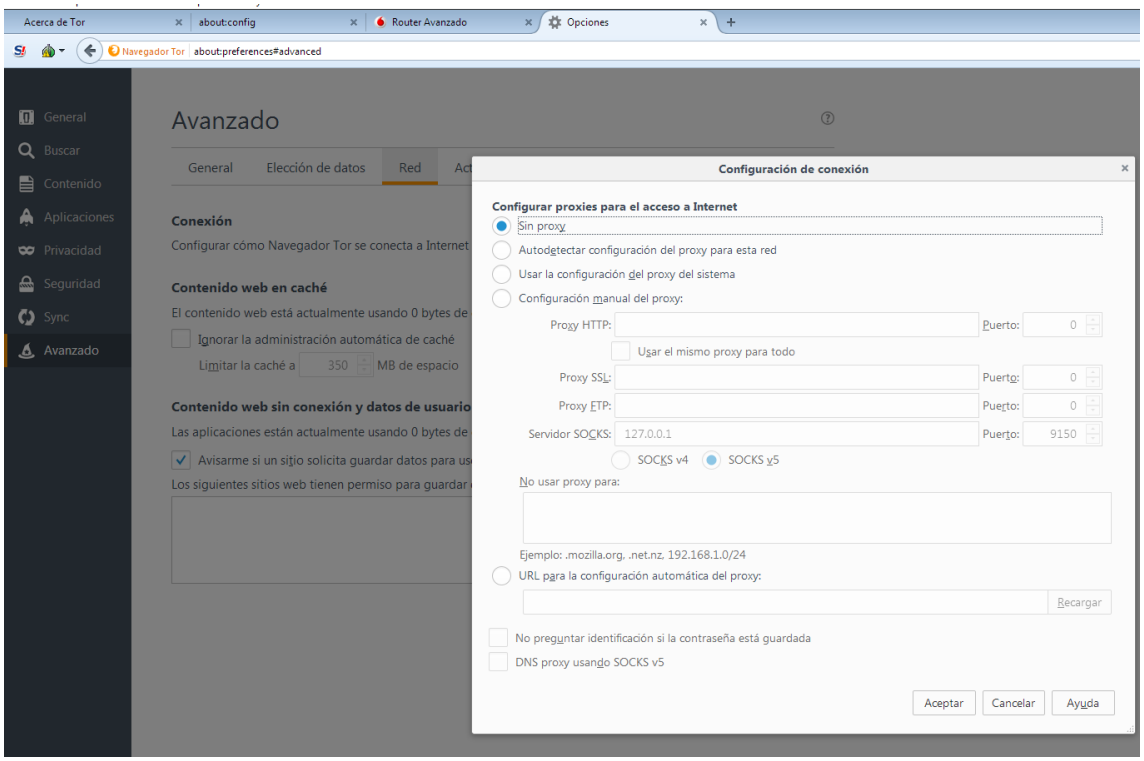
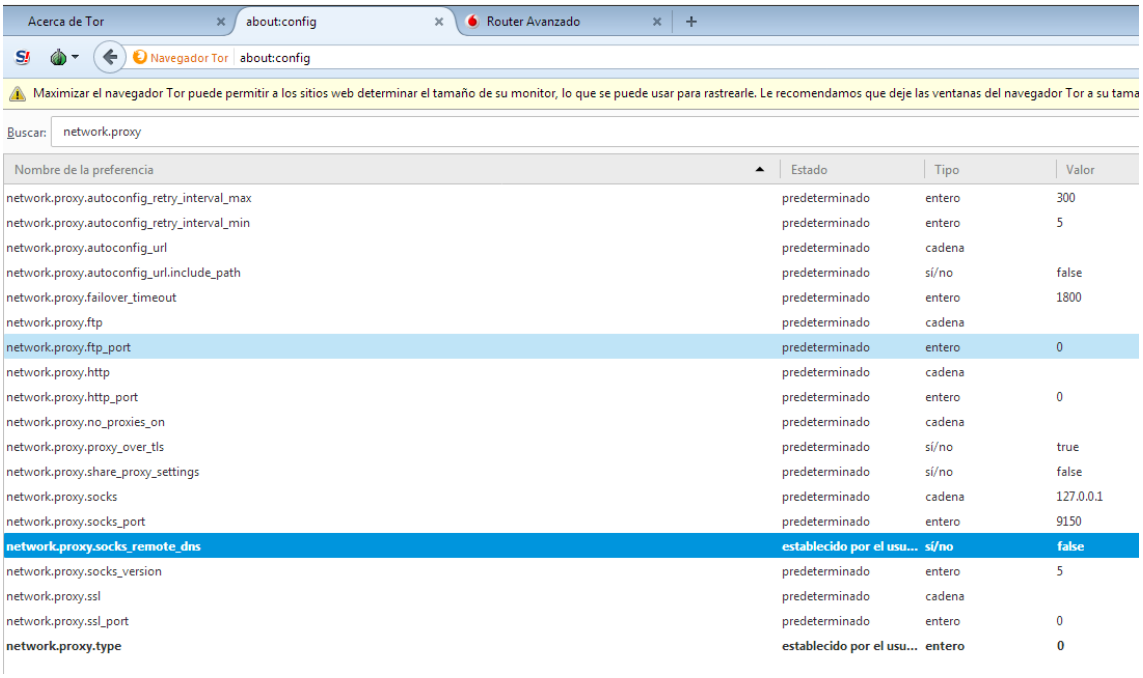


Ilustración 5 Configuración del navegador TOR (I)

7. Seleccionar la barra de navegación y escribir: “about:config”
8. Ir hasta la propiedad “network.proxy.socks_remote_dns” y hacer doble click sobre ella.



Nombre de la preferencia	Estado	Tipo	Valor
network.proxy.autoconfig_retry_interval_max	predeterminado	entero	300
network.proxy.autoconfig_retry_interval_min	predeterminado	entero	5
network.proxy.autoconfig_url	predeterminado	cadena	
network.proxy.autoconfig_url.include_path	predeterminado	sí/no	false
network.proxy.failover_timeout	predeterminado	entero	1800
network.proxy.ftp	predeterminado	cadena	
network.proxy.ftp_port	predeterminado	entero	0
network.proxy.http	predeterminado	cadena	
network.proxy.http_port	predeterminado	entero	0
network.proxy.no_proxies_on	predeterminado	cadena	
network.proxy.proxy_over_tls	predeterminado	sí/no	true
network.proxy.share_proxy_settings	predeterminado	sí/no	false
network.proxy.socks	predeterminado	cadena	127.0.0.1
network.proxy.socks_port	predeterminado	entero	9150
network.proxy.socks_remote_dns	**establecido por el usu...**	**sí/no**	**false**
network.proxy.socks_version	predeterminado	entero	5
network.proxy.ssl	predeterminado	cadena	
network.proxy.ssl_port	predeterminado	entero	0
network.proxy.type	**establecido por el usu...**	**entero**	**0**

Ilustración 6 Configuración del navegador TOR (II)

Una vez seguidos los pasos, ya se puede acceder a un servidor local.

A continuación, hay que configurarlo con las máximas restricciones de seguridad que indican claramente que no se puede ejecutar código JavaScript:

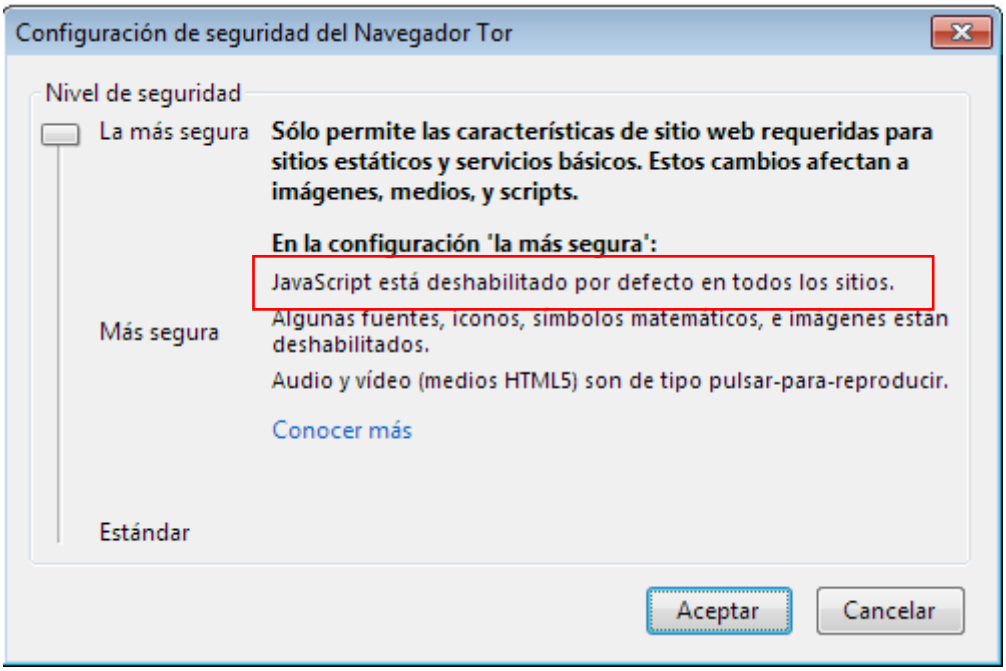


Ilustración 7 Configuración del nivel de seguridad (La más segura)

Demostrando la ejecución

Se ha creado un pequeño servidor en Python para discernir la diferencia entre el uso del exploit o sin él, aprovechando para hacer una consulta de la IP con la que se conecta el equipo al exterior. En este caso la característica del exploit no está activa:

```
#!/usr/bin/python
from http.server import BaseHTTPRequestHandler, HTTPServer

PORT_NUMBER = 8888

class myHandler(BaseHTTPRequestHandler):

        #Handler for the GET requests
        def do_GET(self):
                self.send_response(200)
                #self.send_header('Content-type','text/html')
                self.end_headers()
                self.wfile.write("""<html>Tor Browser 7.x PoC
                                <script type="text/javascript">var userip;</script>
                                <script type="text/javascript" src="https://l2.io/ip.js?var=userip">
                                </script><script type="text/javascript">  document.write("Your IP is :", userip);
                                </script></html>""".encode())
                return

try:
        server = HTTPServer(('', PORT_NUMBER), myHandler)
        print('Started httpserver on port %s' % PORT_NUMBER)
        server.serve_forever()

except KeyboardInterrupt:
        print('^C received, shutting down the web server')
        server.socket.close()
```

Ilustración 8 Código fuente. Exploit no activado.

Para levantar el servidor, se ejecuta el siguiente comando desde el cmd:

- *python testp3_getIP_noExploit.py*

Tiene como resultado:

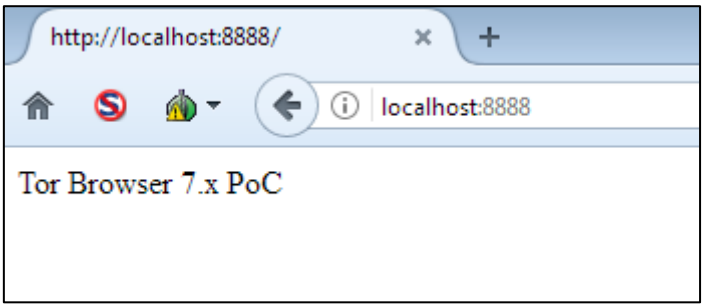


Ilustración 9 Resultado de la ejecución sin exploit activado

Sin embargo, si se añade el código que explota la vulnerabilidad:

- *python testp3_getIP.py*

Este sería el código fuente resultante:

```
#!/usr/bin/python
from http.server import BaseHTTPRequestHandler, HTTPServer

PORT_NUMBER = 8888

class myHandler(BaseHTTPRequestHandler):

        #Handler for the GET requests
        def do_GET(self):
                self.send_response(200)
                self.send_header('Content-type','text/html') # Aprovechando la vulnerabilidad
                self.end_headers()
                self.wfile.write("""<html>Tor Browser 7.x PoC
                                <script type="text/javascript">var userip;</script>
                                <script type="text/javascript" src="https://l2.io/ip.js?var=userip">
                                </script><script type="text/javascript">  document.write("Your IP is :", userip);
                                </script></html>""".encode())
                return

try:
        server = HTTPServer(('', PORT_NUMBER), myHandler)
        print('Started httpserver on port %s' % PORT_NUMBER)
        server.serve_forever()

except KeyboardInterrupt:
        print('^C received, shutting down the web server')
        server.socket.close()
```

Ilustración 10 Código fuente. Exploit activado.

Y al hacer una llamada desde el navegador Tor, el resultado sería diferente:

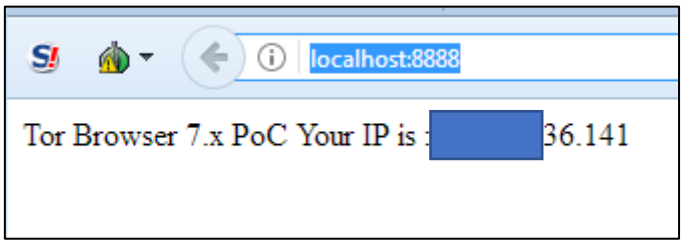


Ilustración 11 Resultado de la ejecución con exploit activado

Posible aprovechamiento de la vulnerabilidad

Conociendo que se podría activar la ejecución de JavaScript simplemente añadiendo el header que hace falta se podrían utilizar una serie de comandos JavaScript para ir recopilando y estudiando la huella que vamos dejando a lo largo de la red Tor. Es decir, si un grupo de atacantes decidiera levantar un grupo de servidores en los que, mediante dicho código fueran capaces de identificar a un individuo podría llegar a trazar su origen.

Una de las páginas que lleva a cabo una generación de huella digital y expone los datos sería la siguiente:

https://fpcentral.tbb.torproject.org/

En esta página se puede consultar la huella digital que deja cada uno de los navegadores. Se puede acceder tanto desde el Internet común como a través de la DarkNet utilizando un navegador Tor con la configuración de red por defecto. Inicialmente, recopila algo de información, pero cuando realmente genera una huella con un grupo grande de marcadores que haría cada cliente único sería mediante la ejecución de JavaScript. Si tuviéramos la configuración establecida como segura, en la que no permite la ejecución de JavaScript, al iniciar la página se vería algo así:

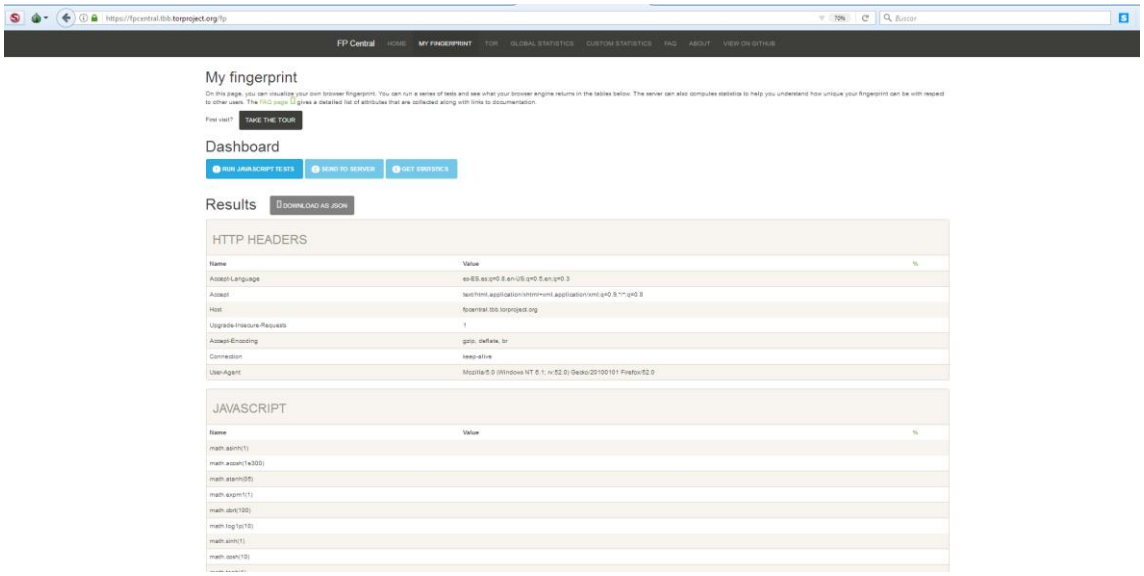


Ilustración 12 Página web fingerprint(I)

Como se puede observar, los parámetros de abajo relacionados con JavaScript no se han rellenado y al pulsar sobre el botón de JavaScript no sucede nada.

En caso de tener habilitada la ejecución de JavaScript, e ir pulsando en cada uno de los botones aparecería lo siguiente:

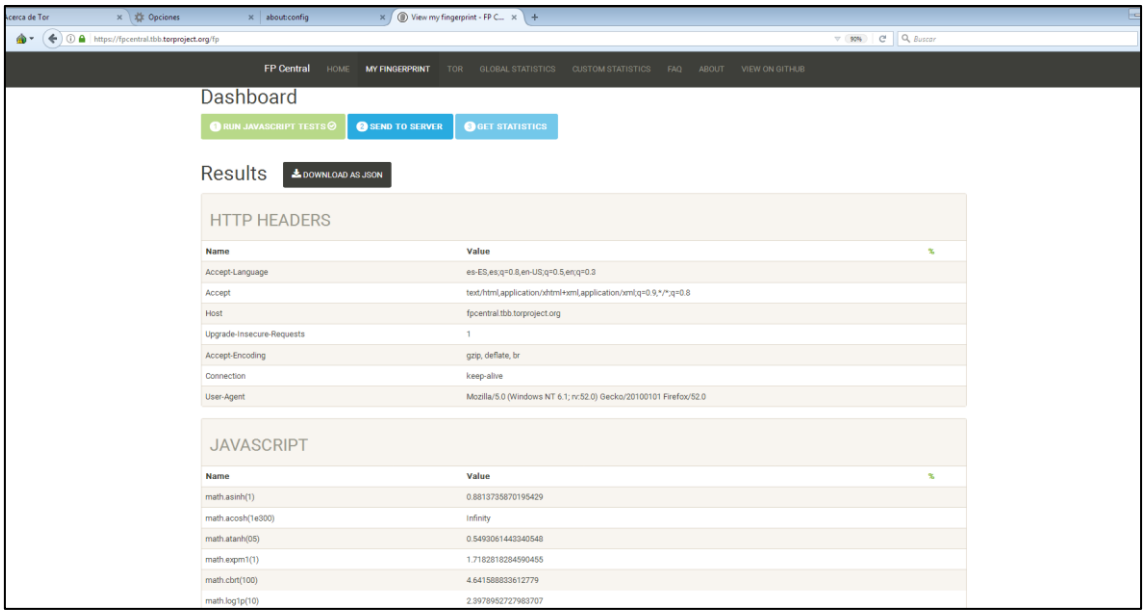


Ilustración 13 Página web fingerprint(II)

Después de hacer click en “2 SEND TO SERVER”

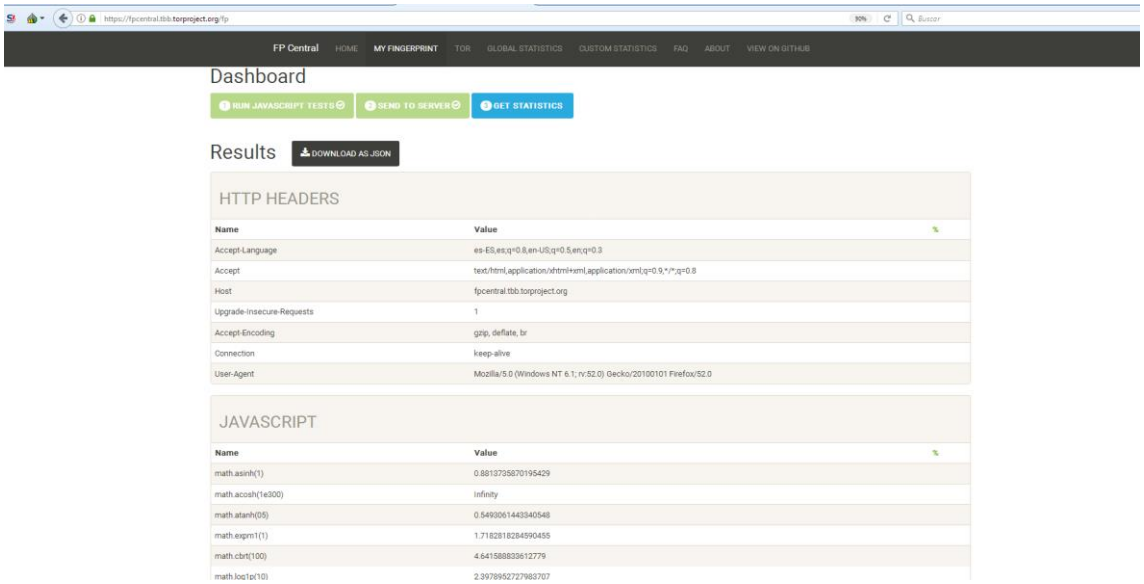


Ilustración 14 Página web fingerprint(III)

Tras hacer click en "3 GET STATISTICS" proporcionaría información en comparación a otros usuarios, lo que daría una idea de cuan anónimo es el cliente que está navegando:

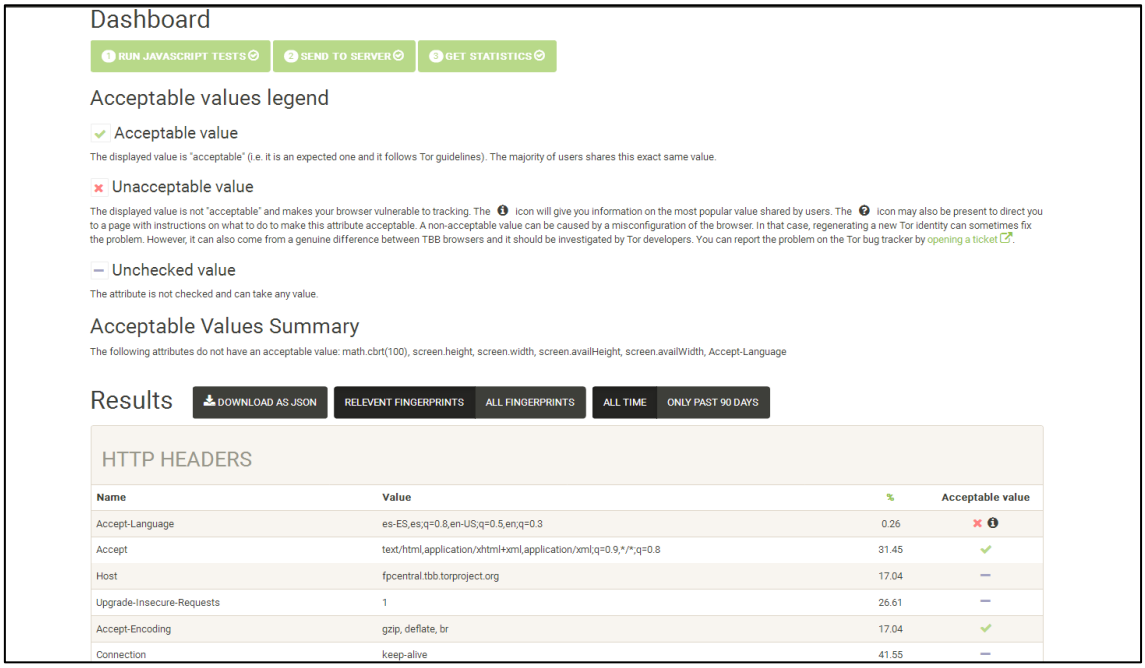


Ilustración 15 Página web fingerprint(IV)

Al principio de la página explica cada una de las clasificaciones: "Acceptable Value", "Unnaceptable Value" o "Unchecked Value" y a continuación, se incluye toda la lista de parámetros comparados y el veredicto de cada uno de ellos:

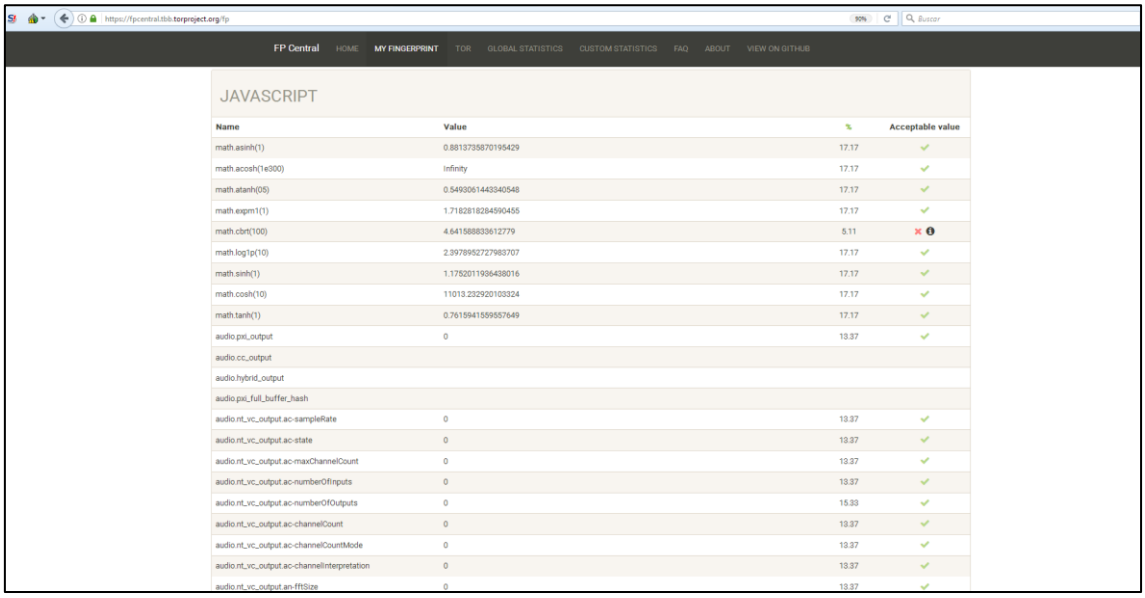


Ilustración 16 Página web fingerprint(V)

Conclusiones

Como se ha demostrado, una vulnerabilidad en el navegador podría llevar a provocar una falsa sensación de seguridad en la que el usuario piensa que cuenta con un grupo de contramedidas activadas cuando realmente no se están aplicando. Es cierto, que poder ejecutar JavaScript por parte del navegador podría facilitar cierta información que pudiera ser utilizada para crear una huella del cliente y que un atacante pudiera llegar a rastrear la navegación, sin embargo, no supone que directamente se pudiera revelar la IP del cliente.

Mercados negros

Introducción

En la siguiente sección se indica qué son los mercados negros y cómo operan, pero antes de eso es necesario hacer una pequeña aclaración previa para que el contenido expuesto a continuación pueda ser entendido.

Según (Wikipedia), la Deep Web es *"…el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores.4 El término se atribuye al informático Mike Bergman."* y la Dark Web *"es el contenido público de la World Wide Web1 que existe en darknets, redes que se superponen a la internet pública y requieren de software específico, configuraciones o autorización para acceder. Forma parte de la internet profunda, la parte de la web no indexada por los motores de búsqueda".* Digamos que la **Dark Web** es un subconjunto de la **Deep Web** utilizado con fines que en su mayoría no son del todo lícitos o al menos éticamente cuestionables.

Es por eso por lo que los mercados negros son una parte de la Dark Web donde los ciberdelincuentes aprovechan el anonimato que proporciona la tecnología para llevar a cabo transacciones que no se encuentran fuera del marco legal de los estados.

Historia

El comercio electrónico empezó en 2006, tiempo después de que estudiantes de Standford y el MIT utilizaran una red denominada ARPANET para llevar a cabo la compraventa de cannabis. Al final de los 80, grupos de noticias se utilizaron como puntos de encuentro entre gente que

buscaba y ofrecía información acerca de todo aquello relacionado con droga, sin embargo, las transacciones se llevaban a cabo fuera del mercado online. A medida que avanzaba la popularización de Internet, alrededor de los años 90, las herramientas de discusión online acerca de temas ilícitos creció igualmente, por ejemplo, The Hive, lanzado en 1997, se utilizó como un punto de discusión donde se compartía información sobre drogas.

Desde el año 2000, industrias emergentes relacionadas con la venta de armas fueron creciendo. En 2006 se lanzó The Farmer's Market y se migró a la red Tor en 2010. Fue cerrado por los Estados Unidos y considerado como una versión previa a Silk road, en la que se utilizaron servicios de pago como PayPal o Western Union, lo cual permitió trazar las operaciones de los pagos y que el FBI cerrarra el mercado.

EL primer mercado negro moderno llegó con Silk Road, albergado en la red Tor y fundado por Ross Ulbricht bajo el pseudónimo de "Dread Pirate Roberts" mediante el uso de Bitcoins (ver XXX, poner referencia a capítulo posterior acerca de Bitcoins). Este mercado fue lanzado en febrero de 2011. Al comienzo, únicamente había una pequeña cantidad de cuentas disponibles y, más adelante se fueron ofreciendo nuevas cuentas en una subasta y, finalmente se vendían a un precio fijo. En octubre de 2013, el FBI cerró la página web y arrestó a su fundador.

El 70% de los productos que se podían comprar en Silk Road eran drogas. También se vendían licencias de conducción falsas e incluso algunos artículos legales. Los términos de servicio especificaban que estaba prohibida la venta de cierto tipo de sustancias, tales como pornografía infantil, tarjetas de crédito robadas, etc.

Justo después de que Silk Road fuera clausurado, un gran número de mercados se fueron abriendo y fueron cerrados al mismo tiempo.

Silk Road marcó un antes y un después en lo que a dark markets se refiere. De finales de 2013 hasta 2014 nuevos mercados fueron lanzados como Sil Road 2.0 o Ágora pero al tiempo que iban naciendo iban siendo cerrados a los pocos días. Utopia es el nombre de otro de esos mercados.

En 2014, la operación Onymous, llevada a cabo por el FBI y NCA, clausuró varios servicios ocultos tales como Silk Road 2.0 o Ágora.

En 2015 crecieron los mercados descentralizados y que utilizaban servicios de escrow. Incluso llegó a haber robos de criptomonedas como el que se produjo por parte del mercado Evolution, que llegó a llevarse 12 millones de dólares americanos.

Como ejemplo de mercado descentralizado está el servicio OpenBazaar.

En abril de ese mismo año, abrió el primer mercado negro dedicado a la venta de ciber armas, además de drogas, TheRealDeal

Al final de agosto de ese mismo año, el mercado de Ágora cerró tras descubrir algún tipo de actividad sospechosa en sus servidores que podía ser debido a un fallo de desanonimización en Tor.

En octubre de 2015, AlphaBay fue reconocido como uno de los mayores mercados. A partir de ese momento hasta abril de 2016 hubo cierta estabilidad en los mercados, sin embargo, en abril,

Términos utilizados en la Deep Web

Antes de comenzar a movernos por la Deep web es necesario conocer el vocabulario y que se utiliza dentro de este mundo:

Términos Generales

- Cipherspcace: se refiere a cualquiera de las redes orientadas al anonimato y a las actividades delictivas que hay detrás
- Onionland: es un subconjunto del cipherspace referido únicamente a la red Tor.
- Clearnet: hace referencia a la red de Internet de uso común.
- Mariana's web: según el mito son las webs menos accesibles, con los peores vídeos principalmente.
- Carding: robo de datos de tarjetas de crédito
- Stats: estadísticas en relación a la reputación de los vendedores
- Escrow: depósito en inglés. Durante la transacción, existe un tercero que mantiene el dinero retenido hasta que la transacción se haya completado.
- Stealth: métodos para camuflar los envíos que son utilizados por los vendedores.
- Honeypot: cebos de las autoridades para desenmascarar a los usuarios que llevan a cabo actividades delictivas.
- Love letter: notificación oficial de los cuerpos de seguridad cuando han confiscado un paquete.

Acrónimos

- DNM: el "dark net market", es decir, el mercado negro de la Deep web.
- BTC: Bitcoin, la criptomoneda aceptada en todos los mercados negros.
- FE: del inglés "finalize early", indica que la transacción puede realizarse más rápidamente si se salta el sistema de escrow.
- LE: del inglés "law enforcemente" para referirse a los cuerpos de seguridad de los Estaados Unidos.
- CP y JP: ver "Hard Candy" y "Jailbait" justo debajo´.

Términos sensibles

- Snuff: vídeos de torturas, violaciones, asesinatos y suicidios.
- Hard Candy (CP): un manual en la Hidden Wiki de cómo conseguir pornografía infantil.
- Jailbait (JB): pornografía o contenido erótico con menores en la pubertad o adolescencia.
- Scat fetish: de "escatológico", para los vídeos relacionados con este fetichismo.

Qué se puede conseguir en los mercados de la Dark Web

Digamos que casi cualquier cosa legal o ilegal estaría a nuestro alcance a través de estos mercados, pero principalmente se ofertan una serie de servicios como los que se describen a continuación:

- Activismo político: intercambio de ficheros censurados. Movimientos relacionados con la ideología anarquista.
- Anonimato y seguridad: todo tipo de instrucciones para mejorar el anonimato dentro de la red Tor.
- Blogs, foros y tablones de imágenes: pueden ser foros y blogs que hablen de cualquier tema, aunque predominan los temas de hacking y el intercambio de imágenes.
- Libros: ingentes cantidades de bibliotecas recopiladas en formato digital sobre temas variopintos. Algunos de ellos libres de copyright y otros con él que se distribuyen de manera ilegal.

- Servicios comerciales: explotación sexual, artículos robados, armas, munición, documentación falsa.
- Servicios de correo y mensajería anónimos: diferentes servicios de correo tanto gratuitos como de pago cuya premisa principal es la de tratar de preservar el anonimato del usuario.
- Servicios financieros: cuentas de PayPal y tarjetas de crédito robadas. Falsificación de billetes, etc.
- Servicios de hosting: alojamiento web y de imágenes cuya prioridad es el anonimato. Algunos de ellos prohíben la subida de ficheros ilegales y otros, en cambio, no tienen ninguna restricción.
- Secretos de estado y soplones: hay varias páginas donde se publican secretos de estado. Entre las más famosas destaca un mirror de WikiLeaks.
- Páginas eróticas: contenido pornográfico de todo tipo tanto de pago como de libre acceso.

Pilares de los dark markets

Para que estos mercados puedan funcionar han de cumplir una serie de características que se describen a continuación.

Cifrado y anonimización de las comunicaciones.

Todas las comunicaciones que se establecen entre los usuarios y los vendedores se llevan a cabo de forma cifrada. Por lo general se utiliza alguna herramienta que utilice el estándar OpenPGP para ello. El estándar OpenPGP es un protocolo no propietario utilizado para cifrar las comunicaciones de correo electrónico utilizando criptografía de clave pública. Basado en programa original PGP (Pretty Good Privacy), el protocolo OpenPGP define formatos estándar para cifrar ficheros, firmas y certificados para el intercambio de claves públicas. OpenPGP puede ser implementado por cualquier compañía sin pagar tasas de licencias a nadie.

Utilización de criptomonedas

Las criptomonedas son, en términos generales, una especie de moneda virtual que permite llevar a cabo transacciones con un alto porcentaje de anonimidad (más adelante se explicarán qué son las criptomonedas en profundidad). La criptomoneda más popular es el Bitcoin.

Sistemas de reputación

La reputación como vendedor es lo que proporciona teórica fiabilidad a las transacciones con algunos de los vendedores de este tipo de comunidad. Unos usuarios advierten de aquellos que no son fiables y suelen proporcionar valoraciones muy completas.

En ocasiones, algunos nuevos vendedores incluso regalan su producto o lo venden a un precio muy bajo con el objetivo de obtener buena reputación para comenzar con su actividad comercial.

Escrow y multisisg escrow

Para tener cierta seguridad de que la transacción comercial se va a llevar a cabo de forma satisfactoria se puede utilizar un *escrow*. Un *escrow* es un tercero en el que el comprador deposita el importe de la transacción y se encarga de mantener ese importe retenido hasta que el comprador confirma que ha llegado la mercancía. En ese momento se completa la transacción y el dinero pasa a ser recibido por el vendedor, no sin antes cobrar una cierta comisión. Además,

ofrece un servicio de disputas para proteger al comprador. Se podría decir que serían como el *PayPal* de la Dark Web.

Por otro lado, otra forma de proteger la transacción sería utilizar un *Multi-Signature Escrow*. Esta protección está basada en retener el dinero en una dirección firmada por ambos actores de la transacción, de tal forma que únicamente ambas partes involucradas pueden interactuar con ese dinero.

¿Cómo funcionan?

Para poder acceder a este tipo de mercados lo primero que nos hace falta es el navegador Tor. Acceder a la Deep Web y buscar alguno de los sitios donde están publicados los dominions.onion como The Hidden Wiki. A partir de ahí, realizaremos una búsqueda en algún índice como puede ser de los mercados actuales. Accederemos a cualquiera de ellos y nos registraremos únicamente utilizando un usuario y una contraseña. Una vez que ya estemos registrado tenemos a nuestra disposición un montón de artículos de cualquier tipo a los que podremos acceder como si estuviéramos comprando en Amazon, con incluso las valoraciones de los usuarios y los productos vendidos.

En la siguiente captura de pantalla se puede observar cómo sería uno de estos mercados.

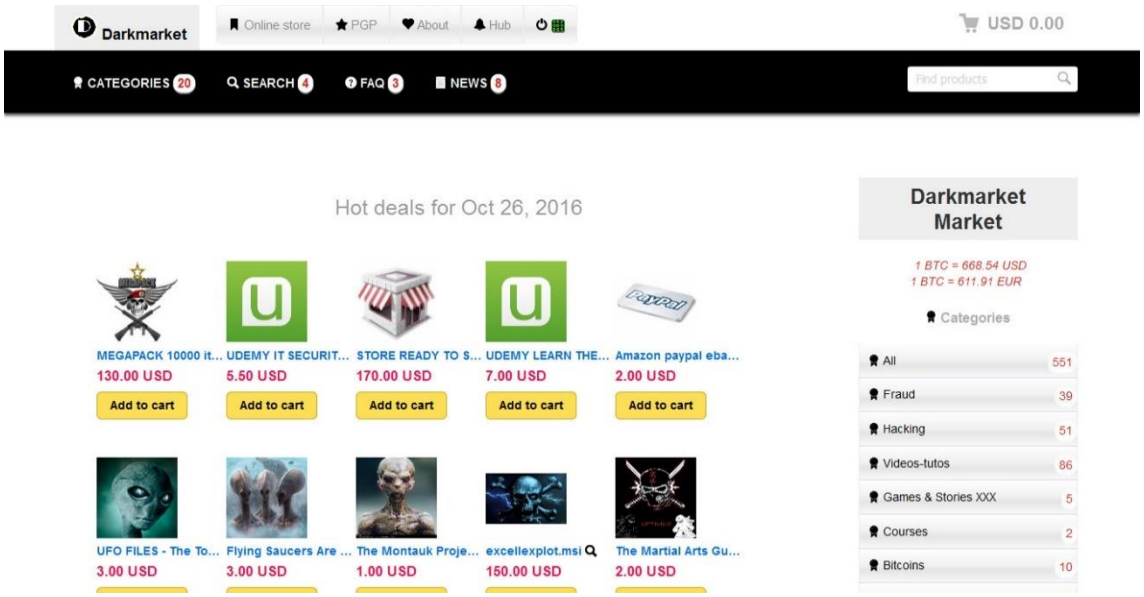


Ilustración 17 Mercado negro

Para poder pagar en estos mercados es necesario tener algún tipo de criptomoneda disponible. Dependiendo del mercado unas monedas u otras serán aceptadas.

Criptomonedas

Introducción

Anteriormente se ha mencionado el término criptomoneda como uno de los pilares de los mercados negros dado que es una forma de intercambio de que proporciona anonimidad en las transacciones. En definitiva, son un tipo de divisa alternativa y de moneda digital. Una de sus características es que tienen un control descentralizado, es decir, su control no depende de una entidad común, un banco central, como ocurre con las divisas comunes. Habitualmente, se basan en una cadena de bloques (blockchain) que sirve como una base de datos de transacciones financieras.

No se puede hablar de criptomonedas sin hablar de blockchains. Los blockchains son una serie de bloques de datos con una estructura en la que la información contenida se organiza en bloques. Gracias a técnicas criptográficas permite guardar un histórico de las transacciones acometidas proporcionando seguridad de que la cadena no ha sido modificada por terceros. Dicha estructura sólo permite la adición de nuevas transacciones sin necesidad de que un tercero que aporte confianza sobre la cadena.

Estas características permiten que una misma moneda no pueda ser gastada dos veces por un mismo usuario. Funciona como un notario de todas las transacciones que se han llevado a cabo con dicha moneda.

Características

Este tipo de monedas cumplen una serie de características que se detallan a continuación:

- Descentralización: no están vinculadas a ningún organismo gubernamental ni financiero.
- Operabilidad: al no estar reguladas por un mercado oficial, la disponibilidad para operar con ellas es total, es decir 24 horas, 7 días a la semana.
- Minería y blockchain: no existen billetes ni un equivalente en oro de las monedas. Los mineros validan una serie de transacciones a través de la resolución de problemas matemáticos a cambio de criptomonedas.
- Transparencia: todas las transacciones se registran de manera pública en los blockchain
- Aceptación: las criptomonedas tienen el valor que los individuos le quieran dar y aceptar. No existe un organismo que regule su precio.
- No dependen de la política: al estar desligadas de las instituciones, los tipos de moneda y economía.
- Regulación: actualmente no existe una legislación estricta al respecto, pero este año hacienda avisará a los usuarios que hayan realizado compraventa de divisas. Se deberían declarar los beneficios como rentas sujetas al IRPF. (el economista (declaración de criptomonedas))

Actores

Dentro del sistema de las criptomonedas intervienen una serie de actores durante todo el proceso. Todos ellos tienen su papel fundamental y sin alguno de ellos no sería posible que se pudieran utilizar las criptomonedas.

Mineros

Son aquellos que “crean” las criptomonedas. Pueden quedarse el beneficio de estas o inyectarlo de nuevo en el mercado. Son la oferta del mercado de las criptomonedas.

El minado de una criptomoneda es un proceso por el cual se resuelve un algoritmo criptográfico que requiere de una gran capacidad de cómputo. Cada 10 minutos se libera un nuevo problema matemático y el primero en resolverlo se queda la recompensa, siempre y cuando el resto de los miembros de la red esté de acuerdo en que la respuesta es correcta.

En el comienzo de estas monedas, particulares llevaban a cabo el proceso de minado desde sus propios ordenadores personales con la intención de sacar algún beneficio. Dado a que cada vez es más complejo llevar a cabo estos cálculos, actualmente no es rentable hacerlo desde un ordenador personal y organizaciones y gobiernos llevan a cabo dicho minado desde granjas construidas exprofeso para esta actividad.

Inversores

Son usuarios de este mercado que tienen como objetivo sacar rentabilidad de la compraventa de estos activos.

Comerciantes

Intercambian las monedas con el fin de mantener el mayor valor de acuerdo a la especulación del mercado.

Carteras

Son carteras virtuales donde los usuarios almacenan su dinero. Constan de una clave pública para recibir dinero y una clave privada para gastarlo. El usuario del monedero es anónimo, pero todas las transacciones quedan registradas públicamente en una cadena de blockchain.

Criptomonedas más populares

Bitcoin

Bitcoin es una moneda creada con la intención de no tener que contar con intermediarios como bancos y compañías de crédito. Está basado en una contabilidad distribuida denominada blockchain de la que se ha hablado en una sección anterior.

Ventajas

- Es fácil de adquirir y la más popular de todas ellas.
- Es la más soportada en los sitios de intercambio.
- Es la más antigua y cuenta con la comunidad más grande de desarrolladores e inversores.
- Está siendo adoptada como forma de pago por grandes compañías.

Desventajas

- La velocidad en las transacciones es uno de sus grandes problemas, graves problemas de escalabilidad. Tardando 10 minutos en confirmarse una transacción y con un ratio de 7 transacciones por segundo.
- La minería de estas monedas se ha convertido en una tarea tan compleja que sólo está al alcance de grandes granjas dedicadas a ello en las que el precio de la energía eléctrica no sea un gran problema.
- Las comisiones en cada transacción cada vez son más altas por lo que hace que no tenga sentido su uso para transacciones pequeñas.

Evolución de su precio

Ilustración 18 Historial del precio del Bitcoin. Fuente : https://www.buybitcoinworldwide.com/es/precio/

Ethereum

Creada en 2015, es un proyecto mucho más extenso que el de Bitcoin, dado que no sólo se creó con el objetivo de ser moneda virtual, sino que tiene otros objetivos.

Este tipo de mercado permite crear aplicaciones descentralizadas, denominadas dapps, que utilizan su propio blockchain, así como contratos inteligentes.

El nombre de la moneda es el Ether y se utilizan para todas aquellas transacciones dentro del mundo de Ethereum

Lo que la hace diferente es la posibilidad de utilización de un blockchain sin tener que crear uno de cero. Para ello hace uso del lenguaje Solidity.

Ventajas

- Es la más popular en cuanto a contratos inteligentes lo que supone una gran ventaja frente a otro tipo de criptomonedas.
- Es utilizada como plataforma para el lanzamiento de ofertas iniciales de monedas. Por poner un ejemplo, en 2017 se recaudaron 6,7 mil millones de dólares, lo que nos indica el gran potencial que posee.
- La velocidad en las transacciones es uno de sus puntos fuertes, permitiendo el envío de dinero en pocos segundos.

Desventajas

- Grandes problemas de escalabilidad para confirmar y verificar las transacciones debido a su mecanismo de trabajo denominado Prueba de Trabajo

- Sólo utiliza un único lenguaje de programación, Solidity, lo que hace más difícil su entrada al desarrollo.
- No es el único en el mercado con los mismos objetivos y, sin embargo, no es el que tiene la tecnología más pulida. Existen otros como NEO o Cardano que, a día de hoy, poseen una mejor tecnología.

Evolución de su precio

Ilustración 19 Historial del precio del Ethereum. Fuente: https://www.miethereum.com/ether/precio-actual-historico/

Ripple

Es otra criptomoneda cuya característica principal es que nace con el objetivo de solucionar el problema de los pagos internacionales. Es decir, se basa en la rapidez y el bajo coste de las transacciones.

En el caso de esta moneda, más de la mitad de sus monedas está en posesión de la empresa que lo creó por lo que su situación descentralizada lleva a que muchos usuarios critiquen su esencia centralizada.

Ventajas

- Pagos extremadamente rápidos en relación a otras criptomonedas. Se pueden realizar pagos en cuestión de segundos.
- Comisiones mucho menores que en el caso de otras criptomonedas.
- Probada en el mundo real para llevar a cabo pagos internacionales con el respaldo de grandes instituciones financieras como American Express y el Banco Santander.

Desventajas

- La centralización de la moneda va en contra de los principios e las criptomonedas por lo que supone grandes críticas de la comunidad.
- Algunos bancos han empezado a crear sus propias monedas, lo que podría hacer que rápidamente perdiera valor en el mercado.
- La transparencia de la moneda podría ser una desventaja para según qué usuarios.

Bitcoin Cash

Como su propio nombre indica es una moneda derivada del original Bitcoin mencionado en apartados anteriores. Nació como un fork de Bitcoin debido que se quisieron llevar a cabo una serie de cambios y no se llegó a un acuerdo.

El objetivo del Bitcoin Cash es claro, resolver algunos problemas existentes en la cadena de bloques de Bitcoin, en concreto los que respecta a escalabilidad.

Ventajas

- La velocidad con la que se producen las transacciones respecto al Bitcoin es mucho mayor. Todo ello gracias al aumento del tamaño del bloque del blockchain hasta 32MB, mucho mayor al del Bitcoin original, 1MB.
- El coste de las comisiones es mucho más reducido debido a evitar el congestionamiento.

Desventajas

- Se espera que en un futuro sea totalmente descentralizada pero actualmente cuenta con un CEO, lo que supone ser criticada por el mercado de las criptomonedas.
- La minería de esta moneda es tan costosa como la del Bitcoin pero con una rentabilidad actual menor, lo que hace que su minado sea menos atractivo.
- No tiene la misma liquidez que otras monedas que se encuentran en el top 10.

Histórico

Ilustración 20 Historial del precio del Bitcoin Cash. Fuente: coinmarketcap.com

EOS

Lo más curioso de esta moneda es que consiguió entrar en el top 10 de las criptomonedas antes incluso de lanzar la plataforma.

Ahora que la plataforma ya está en funcionamiento, los desarrolladores pueden crear aplicaciones descentralizadas y contratos inteligentes, pero, a diferencia de Ethereum, con una gran mejora tecnológica.

Ventajas

- Mucho más escalable que Ethereum hasta lograr el ratio de 10000 transacciones por segundo.
- Se puede programar en distintos lenguajes, entre los que se incluye C++, lo que hace que la puerta de entrada a la programación de esta moneda sea mucho más sencillo.
- Cuenta con un gran equipo, lo cual supone un punto a favor para su éxito.

Desventajas

- Principalmente, la poca madurez de la moneda. Aún falta tiempo para determinar los resultados de esta criptomoneda.

Histórico

Ilustración 21 Historial del precio del EOS. Fuente: coinmarketcap.com

Legislación

Deepnet, darknet y mercados negros

Hay una serie de cuestiones que hay que aclarar respecto a la Deepnet, la Darknet y los Mercados negros. Dependiendo de cada país, existe una legislación más o menos restrictiva frente a estos puntos. En concreto, en España, la situación es la siguiente:

¿Es ilegal acceder a la DarkNet?

El mero hecho de acceder a la Dark Net no es ilegal en sí mismo en España. Sí lo es en otro países como Austria, China, Egipto o Rusia, incluso el uso de navegadores para acceder a ello.

¿Es ilegal comprar o acceder a los contenidos de la Darknet?

Hay que tener en cuenta que gran parte del contenido y los productos que se pueden encontrar en la Darknet son ilícitos, pero puede que haya algunos que no lo sean. Adquirir esos productos lícitos no tendría consecuencias legales, aunque fuera a través de la Darknet.

En cambio, si los productos a los que se intenta acceder son ilegales, el mero hecho de llevar a cabo la compra de uno de ellos podría suponer ser arrestado por las fuerzas y cuerpos de seguridad del estado.

En cuanto a la visualización, no sería ilícito verlos salvo que se accediera de manera intencionada a pornografía infantil, en cuyo caso el artículo 189.5 del Código penal castiga con una pena de tres meses a un año de prisión o con multa de seis meses a dos años a aquellos que adquieran o posean pornografía infantil, así como aquellos que accedan a sabiendas a pornografía infantil.

¿Es ilegal vender droga a través de la DarkNet?

Efectivamente, tal como se recoge en el artículo 368 del código penal de 1995:

"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 a 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"

Criptomonedas

Cuando empezó el auge de las criptomonedas existían muchas dudas de cómo tributarían o si llegarían a hacerlo. Hasta el 2018 no se resolvió esta incógnita y finalmente se ha determinado que si una persona se dedica a la compraventa de criptomonedas tiene que tributar por ello.

La persona que lleva a cabo esta actividad, no sólo tiene que tributar al recibir una cantidad de dinero en Euros sino también al llevar a cabo un intercambio dado que el contribuyente ha desarrollado una actividad económica que da lugar a obtención de renta que se califica como ganancia o pérdida patrimonial: *"El intercambio de una moneda virtual por otra moneda virtual diferente constituye una permuta, conforme a la definición contenida en el artículo 1.538 del Código Civil, que dispone: 'La permuta es un contrato por el cual cada uno de los contratantes se obliga a dar una cosa para recibir otra'"*

Otras redes aparte de Tor

Aunque Tor es una de las redes más conocidas para acceder a la Deep Web no es la única. Existen otras también bastante conocidas que aportan una serie de características que las hacen atractivas por otros motivos. A continuación, se muestran dos ejemplos, junto con sus ventajas e inconvenientes.

FreeNET

Introducción

El proyecto de FreeNET data de 1999. Ian Clarke publicó su proyecto de fin de carrera en el que se describía un algoritmo que al ser ejecutado por un grupo interconectado de nodos proporcionaba un sistema robusto de almacenamiento indexado con claves y recuperación sin ningún elemento centralizado o administración. Cada uno de los nodos mantiene una parte de almacenamiento cifrada con el propósito de almacenar ficheros relacionados con la red FreeNET.

El sistema que planteó permitiría interactuar a sus usuarios de una manera similar a la World Wide Web, pero teniendo el anonimato como una característica principal. Al liberar el ensayo, Clarke invitó a cualquier voluntario que sintiera curiosidad ayudarle a desarrollar su ensayo, dando como resultado el proyecto que se conoce hoy en día como FreeNET.

Características

Aparte de las características de anonimidad presupuestas posee las siguientes características:

- Totalmente descentralizado
    - La información puede ser insertada dentro de Freenet para descargarla sin ninguna dependencia de un servidor centralizado. Todo lo que se necesita para que esa información pueda ser descargada es proporcionar la clave del contenido a cualquiera que deseemos que se descargue dicho contenido y será capaz de descargarlo en cualquier momento.
- Caché adaptativa

    - Dispone de una caché de ficheros que se va ajustando a la demanda lo que le permite escalar de una forma mucho más rápida que otros sistemas y proporcionar un mejor sistema de balanceo de carga.
- Fuerte seguridad
    - Freenet soporta desde hace tiempo el concepto de "Content Hash Keys", garantizando la integridad de los ficheros subidos. También soporta e "Signed Subspace Keys" que permite firmar contenido digital.
- Traspaso de la corrección de errores
    - Freenet permite la tecnología de "Forward Error Correction" que permite que un fichero sea reconstruido

FreeNet vs TOR

Una de las características principales de esta red es que es una red inproxy, es decir, solamente permite la navegación dentro de la red, a diferencia de Tor que es una red outproxy, donde los usuarios pueden salir hacia Internet utilizando la plataforma de anonimato. Además, permite crear pequeños grupos de "amigos" con los que mantener pequeñas redes.

Por otro lado, en cuanto a servicios ocultos a diferencia de otros sistemas donde es necesario que el servidor que mantiene el servicio oculto siga encendido para que esté accesible, en este caso, el resto de nodos que hayan visitado el servicio contienen una copia cacheada en su propio datastore.

En cambio, no todos son ventajas. La velocidad de esta red es mucho más lenta en comparación con la red Tor, sobre todo al principio donde sólo se tiene acceso a unos pocos nodos "amigos". A medida que la red fuera creciendo, la navegación se haría más rápida y más anónima.

I2P

Introducción

El proyecto I2P nace en el año 2003 de la mano de un grupo de hackers con el objetivo de modificar Freenet para permitir el uso de transportes alternativos, como puede ser JMS. Tenía que ser una red virtual privada resistente a la censura y que tuviera buenos niveles de desempeño y escalabilidad.

Es una red privada que expone una capa sencilla que pueden utilizar las aplicaciones para anónimamente mandar mensajes entre ellas. La red está basada en mensajes estrictamente pero existe una librería disponible para permitir comunicaciones en streaming sobre ellos. Todas las comunicaciones están cifradas punto a punto e incluso los destinos son identificadores criptográficos basados en una pareja de claves públicas.

El sistema entero es de código abierto, mantenido y desarrollado por un pequeño equipo alrededor del mundo que se dedica a que el sistema siga funcionando.

Características

A continuación, se describen las diferentes características de la red I2P:

- Descentralizada
    - No existe un punto central que pudiera ser atacado para comprometer la integridad, seguridad o anonimato de la comunicación del sistema.
- Ejecutar cualquier servicio

    - Una de las principales características es que permite la creación de prácticamente cualquier servicio sin necesidad de configuraciones complejas.
- Protección del contenido por medio de una clave adicional
    - Es necesaria una clave adicional para poder descifrar el contenido de los ficheros.
- Reconfiguración dinámica
    - En respuesta a varios ataques es capaz de reconfigurarse de tal modo que puede hacer uso de varios recursos según van estando disponibles.
- Libre y gratuito
    - Todos los aspectos de la red son de código libre y gratuitos.

I2P vs Tor

La principal diferencia es el número de usuarios y recursos disponibles, en el que Tor cuenta con mucho más apoyo, y por tanto es mucho más resistente a la censura.

Por otro lado, en vez de utilizar un enrutado de tipo "cebolla" como Tor, lo hace de tipo "ajo", es decir, envía varios paquetes, no solo uno. Cada mensaje es un diente y el conjunto de ellos es un ajo, de ahí la analogía, lo que hace mucho más difícil el análisis del tráfico.

Además, se utilizan túneles unidireccionales de salida y entrada. Esto se traduce en que tanto el cliente como el servidor construyen su propio túnel. Se necesitan, por lo tanto, dos túneles (uno de salida y otro de entrada) para enviar la información y otros dos para recibirla. Dentro de cada túnel la información se organiza a su vez mediante el protocolo de enrutamiento de cebolla.

Trabajos futuros

Como trabajos futuros tengo una serie de propuestas que se describen a continuación:

- Desarrollo de la prueba de concepto, llegando a utilizar el framework BEEF, (https://beefproject.com/) y viendo hasta qué punto podría utilizarse para descubrir datos del cliente.
- Dada la naturaleza de la vulnerabilidad, llevar a cabo la utilización de uno de los proxys más famosos de Python https://mitmproxy.org/ para incrustar el header en páginas que no lo tuvieran y así bypasear la protección de la configuración segura.
- Probar a emular una estructura de una red de Tor de ejemplo con ayuda de la herramienta Shadow (https://shadow.github.io/) y ver cómo se podrían aplicar algunos de los ataques de red a esta infraestructura.
- Ampliar la información relativa a Tor, incidiendo a más bajo nivel en cómo funciona toda la criptografía necesaria.
- Cambiar el foco de trabajo a las otras dos redes presentadas en la memoria: FreeNet e I2P

Conclusión

El trabajo presentado supone un punto de entrada a la red Tor, su funcionamiento y principales características, así como principales ataques que podría sufrir la infraestructura, incluyendo, además, una prueba de concepto. Siento la característica principal el anonimato, esta red se ha acabado utilizando para actividades delictivas entre las que destacan las transacciones a través de los mercados negros. Para tratar de que los intercambios a través de dichos mercados sean lo más anónimos posibles se utilizan criptomonedas, que dificultan seriamente el rastreo de las

transacciones. Estas actividades se encuentran dentro de un marco legal dependiente del país de origen. En este caso en España hay ciertas leyes que penalizan algunas de las transacciones que se pudieran llevar a cabo a través de esta red.

Tor no es la única red orientada al anonimato. Se introducen otras como I2P y FreeNet; y se comparan con la principal propuesta.

A principio del trabajo se plantearon una serie de objetivos y fueron organizados de mayor a menor por orden de relevancia, incluyendo 2 últimos puntos que, a priori, no se sabía si iba a haber tiempo suficiente para llevarlos a cabo:

1. Llevar a cabo la inmersión dentro de los fundamentos de la tecnología de anonimización de TOR. Dentro de dicha introducción, se tienen que contemplar, al menos, los siguientes conceptos:
    a. Componentes del sistema.
    b. Interacciones
    c. Proceso de ocultación de usuarios y servicios en la red.
2. Seleccionar y describir dos técnicas de desanonimización de usuarios y servicios.
3. Desarrollar un estudio acerca de los mercados negros de la red TOR. Entre otros puntos a desarrollar, al menos se tienen que cubrir los siguientes:
    a. Cómo operan.
    b. Cómo se ocultan las actividades comerciales.
    c. Relación de las criptomonedas en los cibermercados negros.
        i. Introducción de las criptomonedas
        ii. Características
        iii. ¿Por qué se utilizan en estos mercados?
4. Presente, pasado y futuro de la legislación relacionada con la red TOR.
5. Trabajos futuros
6. Comparativa con otro tipo de redes como FreeNET o I2P.
7. Llevar a cabo un PoC de una de las técnicas encontradas.

Finalmente, y como se puede leer en este documento, todos esos puntos han sido cubiertos con el rigor y profundidad acorde tiempo del que se ha dispuesto.

Bien es cierto que la prueba de concepto podría haber sido más atractiva mostrando algún tipo de ataque sobre la arquitectura de red pero, en cualquier caso, se ha cumplido con el objetivo planteado inicialmente.

En cuanto a la planificación, se ha seguido acorde a lo pactado inicialmente, tal vez el progreso no ha sido lineal entre entregas (aunque siempre se ha cumplido con los hitos), pero hay que tener en cuenta los distintos aspectos e imprevistos que pueden surgir en el día a día.

En definitiva, la memoria del TFM cumple con los criterios establecidos por la universidad, en cuanto a organización, planificación y contenido pactado.

Referencias

(s.f.). Obtenido de https://es.wikipedia.org/wiki/Cadena_de_bloques

(INCIBE), J. D. (s.f.). *https://www.incibe-cert.es/blog/tor-servicios-ocultos-desanonimizacion*.

Bergantiños, J. I. (s.f.). *http://www.criptored.upm.es/guiateoria/gt_m001m1.htm (Onion routing y Red Tor).* Obtenido de http://www.criptored.upm.es/guiateoria/gt_m001m1.htm

Bitcobie (Ripple). (s.f.). Obtenido de https://www.bitcobie.com/ripple/

Bitcoin Paper. (s.f.). Obtenido de https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Blockchains y criptomonedas: fundamentos y características. (s.f.). Obtenido de https://www.criptonoticias.com/informacion/blockchains-criptomonedas-fundamentos-caracteristicas/

Configurar Tor en red local. (s.f.). Obtenido de https://superuser.com/questions/1117383/can-i-use-tor-browser-without-using-tor-network

Criptomoneda (Wikipedia). (s.f.). Obtenido de https://es.wikipedia.org/wiki/Criptomoneda

delitosinformaticos.com. (s.f.). Obtenido de https://delitosinformaticos.com/06/2018/delitos/como-se-regula-la-deep-web-y-darknet-en-nuestro-ordenamiento-juridico

Dingledine, R. (s.f.). *https://www.freehaven.net/~arma/cv.html.* Obtenido de https://www.freehaven.net/~arma/cv.html

el economista (declaración de criptomonedas). (s.f.). Obtenido de https://www.eleconomista.es/declaracion-renta/noticias/9800447/04/19/Renta-2018-Ha-realizado-operaciones-con-criptomonedas-Hacienda-vigila-el-bitcoin-y-tendra-que-declararlo-en-la-casilla-389.html

Farinacci, F. (s.f.). *https://es.slideshare.net/FabrizioFarinacci1/deanonymize-tor-hidden-services-76463821*.

Genbeta (FreeNET). (s.f.). Obtenido de https://www.genbeta.com/a-fondo/asi-es-freenet-deep-web-alternativa-a-tor-e-i2p

Get Client's IP Address from Javascript...and more. (s.f.). Obtenido de https://l2.io/

https://darknetmarkets.co/wp-content/uploads/2016/10/Darkmarket-Homepage.jpg. (s.f.). *Foto de darkmarket*.

https://es.wikipedia.org/wiki/Cadena_de_bloques. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Cadena_de_bloques

https://www.deepdotweb.com/2018/11/28/clickstream-tracking-of-users-of-the-tor-browser-a-research-paper/. (s.f.).

https://www.deepdotweb.com/2019/02/20/research-classification-of-attacks-on-tor-clients-and-tor-hidden-services/. (s.f.). Obtenido de www.deepdotweb.com.

https://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web. (s.f.). Obtenido de https://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web

I2P. (s.f.). Obtenido de https://geti2p.net

In-progress drafts of new specifications and proposed changes. (s.f.). Obtenido de https://gitweb.torproject.org/torspec.git/tree/proposals

Main Tor Specification. (s.f.). Obtenido de https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

Montoya, D. E. (2016). *Deep Web: TOR, FreeNET & I2P. Privacidad y Anonimato.* Madrid: 0xWord.

opinred (Criptomonedas). (s.f.). Obtenido de https://opinred.com/criptomonedas-que-son-caracteristicas-y-tipos/

Project, T. (s.f.). *https://2019.www.torproject.org/docs/onion-services.html.en.* Obtenido de Onion Services.

seguridad, C. y. (s.f.). *https://www.adictosaltrabajo.com/2016/11/10/criptografia-y-seguridad/.*

Silk Road (Wikipedia). (s.f.). Obtenido de https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

Special hostsnames in Tor. (s.f.). Obtenido de https://gitweb.torproject.org/torspec.git/tree/address-spec.txt

The Hacker News . (s.f.). Obtenido de https://thehackernews.com/2018/09/tor-browser-zero-day-exploit.html

TOR. (s.f.). Obtenido de https://www.torproject.org

Tor path specification. (s.f.). Obtenido de https://gitweb.torproject.org/torspec.git/tree/path-spec.txt

Tor. (s.f.). *Tor design.* Obtenido de https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

Tor version 3 directory server specification. (s.f.). Obtenido de https://gitweb.torproject.org/torspec.git/tree/dir-spec.txt

Tor-top-changes-tor-2004-design-paper-part-1. (s.f.). Obtenido de https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-1

Tor-top-changes-tor-2004-design-paper-part-2. (s.f.). Obtenido de https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-2

Tor-top-changes-tor-2004-design-paper-part-3. (s.f.). Obtenido de https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-3

Wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/

yolandacorral.com (tor vs freenet). (s.f.). Obtenido de https://www.yolandacorral.com/tor-vs-freenet/