Universidad de Alcalá
Escuela Politécnica Superior

GRADO EN INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Técnicas de desanonimización en Tor

Autor: David Fuentes Miguel

Tutor/es: Manuel Sánchez Rubio

2022

UNIVERSIDAD DE ALCALÁ
Escuela politécnica Superior

GRADO EN INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Técnicas de desanonimización en Tor

Autor: David Fuentes Miguel

Tutor: Manuel Sánchez Rubio

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

FECHA:

AGRADECIMIENTOS

Quiero agradecer a todos mis amigos y familia, que me han dedicado su tiempo y apoyo en esta etapa tan importante de mi vida. También quiero agradecer a los profesores que he tenido, que han ido despertando mi curiosidad y formándome como persona y como profesional.

ÍNDICE

ÍNDICE DE FIGURAS

1. RESUMEN

A día de hoy, no es extraño saber que no todo en internet es accesible desde los buscadores convencionales como podrían ser Google, Bing o Yahoo!, por ejemplo.

Existe mucho contenido no indexado que abarca en su mayoría temas relacionados con actividades delictivas, desde cibermercados negros hasta provisión de servicios como lavado de dinero o hasta terrorismo.

A este contenido es posible entrar con varias herramientas, pero la más famosa y de la que hablará en este trabajo es The Onion Router (Tor).

Gracias a Tor, a los usuarios y los servicios que alberga se les proporciona un fuerte anonimato debido a cómo funciona internamente su red.

Existen usuarios que usan este tipo de herramientas para navegar y consultar webs convencionales y salvaguardar su anonimato, pero otros muchos aprovechan para ofrecer productos y servicios ilícitos y sacar beneficio de ellos de una manera que les resulte segura.

Como bien es sabido, la existencia de cibermercados negros es algo real y algo que está presente desde hace mucho tiempo, como ejemplo SilkRoad o Hydra Market, dos de los más grandes cibermercados negros que las fuerzas de seguridad lograron cerrar.

Es por esto y por otro tipo de cosas como por ejemplo la tenencia o distribución de contenidos censurados por las que se deberían buscar formas de identificar a quienes andan detrás y ponerles a disposición judicial.

Palabras Clave: Tor, red de anonimato, desanonimizar, nodos, enrutamiento cebolla.

2. ABSTRACT

Today it is known that not everything on the Internet is accessible from conventional search engines such as Google, Bing or Yahoo!, for example.

There is a lot of non-indexed content that mostly encompasses content related to criminal activities, from cyber black markets to the provision of services such as money laundering or even terrorism.

It is possible to access this content with several tools, but the most famous and the one that this writing will talk about is The Onion Router (Tor).

Thanks to Tor users and the services it hosts, are provided with strong anonymity due to how their network works internally. There are users who use this type of tools to browse and consult conventional websites and safeguard their anonymity, but many others take advantage of it to offer illicit products and services and get benefits in a way that is safe for them.

As is well known, the existence of cyber black markets is something real and something that has been present for a long time, as an example there are cyber markets like SilkRoad or Hydra Market, two of the greatest cyber black markets that the security forces managed to close.

It is for this and for other types of things such as the possession or distribution of censored content, we should search ways to identify those who are behind and put them at judicial disposal.

Keywords: Tor, anonymity networks, deanonymize, nodes, onion routing.

3. ESTADO DEL ARTE

En la actualidad la Desanonimización es un tema que ha despertado la curiosidad de muchos. Existe un gran número de investigaciones que hablan del tema, en el caso de este trabajo, se ha consultado una serie de estudios que tratan diferentes técnicas de Desanonimización en redes de anonimato como Tor.

En el caso del ataque conocido como Sniper Attack, han sido investigadores como Rob Jansen, del Laboratorio de Investigación Naval de los Estados Unidos, en su publicación en conjunto “The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network”, quienes explican en qué consiste dicho ataque, es un ataque de denegación de servicios, los recursos de memoria que se consumen cuando ellos ejecutaron dicho ataque en un entorno controlado, las posibilidades en cuanto a como defenderse del mismo o los tiempos estimados para el éxito del ataque.

Otro tipo de ataque muy utilizado y efectivo, es el ataque ejecutado con archivos cebo. Este consiste en la difusión de archivos modificados por el atacante para que al abrirse estos le manden cierta información como podría ser por ejemplo la IP real de una conexión de Tor. Se muestra información que el FBI compartió en redes, de un caso llamado “Caso Playpen”, en el que muestran datos numéricos de las detenciones y rescates que se lograron al desmantelar una red mundial de pornografía infantil.

También hay investigaciones realizadas por miembros de la Universidad de Massachusetts Amherst, que estudian los ataques de correlación de tráfico en Tor. Este tipo de ataque se basa en el estudio del flujo de paquetes de entrada y salida que fluyen por la red de Tor. En la publicación “DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning”, miembros de la universidad previamente mencionada explican no sólo cuales métricas son las más utilizadas en este tipo de ataque, sino que también hablan de la potencia de la herramienta DeepCorr, una herramienta de deep learning desarrollada por ellos, explicando su configuración experimental, resultados y entrenamientos.

O como en su presentación para el Congreso 33C3, Vasilios Mavroudis habla de que el peligro no está sólo en lo que se ve de Tor, sino también en ultrasonidos que son imperceptibles para el oído de un humano adulto, pero que por el contrario nuestros dispositivos inteligentes pueden escuchar e interpretar. En la presentación explica como funcionan este tipo de balizas de sonido, y que datos podemos estar enviando sin darnos cuenta.

Como conclusión general, el anonimato absoluto no existe. Detrás de este tipo de ataques se encuentra gente muy habilidosa e ingeniosa, que siempre da con la manera de conseguir romper la seguridad de ciertas herramientas de anonimato como puede ser Tor.

4. INTRODUCCIÓN

4.1. PLANTEAMIENTO

En este trabajo se van a tratar las diferentes posibilidades que ofrece la herramienta Tor en lo referente a la desanonimización de sus usuarios y servicios, comentando diversas técnicas que se podrían utilizar para lograrlo y explicando su funcionamiento.

Primero se comentará la historia que tiene The Onion Router, por qué se creó, y cómo funciona internamente su red, para así facilitar al lector la comprensión de la razón de ser de esta herramienta y sus utilidades.

A continuación, se hablará sobre la Deep Web y la Dark Web, para entender su funcionamiento, utilidades y sus servicios ocultos.

Por último, se hará un recorrido por las diversas técnicas recopiladas que pueden utilizarse para quebrantar el sistema de anonimato de Tor, y de esta forma poder identificar a sus usuarios y servicios.

4.2. OBJETIVOS

El principal objetivo de este escrito es recopilar información acerca de las posibilidades que The Onion Router ofrece en lo referente a la desanonimización de sus usuarios y servicios, para poder identificar a personas que están detrás de actividades delictivas, como por ejemplo el alojamiento de cibermercados negros, o la provisión de servicios como lavado de dinero, distribución de contenido censurado o terrorismo.

Para ello, primero hay que comprender cómo funciona internamente la red Tor y cómo se proporciona el anonimato a sus usuarios y servicios, para después saber por dónde

atacar al sistema y conseguir la información necesaria para desenmascarar a esas personas.

5. THE ONION ROUTER (Tor)

5.1 ¿QUÉ ES Tor?

The Onion Router es una red creada por *TOR Project*, una organización sin ánimo de lucro creada en 2006, aunque la idea de este modelo de red se remonta a la década de los 90 [1].

Su finalidad principal es salvaguardar la privacidad de sus usuarios, y para ello mezcla el tráfico de sus usuarios y lo transmite a varios nodos intermedios de la red de manera aleatoria antes de entregarlo a su destino, todo ello para tratar de ocultar de donde proviene la información. Es por ello que esta herramienta permite a sus usuarios la navegación por la red de manera anónima [1].

5.2. HISTORIA

Una vez que se ha conocido qué es esta herramienta, se procederá a comentar el origen de esta.

Durante la década de los años 90, no eran desconocidas las carencias de seguridad en Internet, al igual que la escasa capacidad para realizar un seguimiento y vigilancia de la red. Por estas razones, en el año 1995 Mike Reed, David Goldschlag y Paul Syverson, miembros del Laboratorio de Investigación Naval de los Estados Unidos (NRL), comenzaron a investigar la manera de crear conexiones de Internet que no mostraran datos relativos a la comunicación (remitente, mensaje y destinatario) y que estas no pudieran ser monitorizadas. Juntos desarrollaron los primeros modelos de lo que hoy en día se conoce como enrutamiento cebolla [2].

Más adelante, a principios de los años 2000, Roger Dingledine comenzó a trabajar en el enrutamiento cebolla junto a Paul Syverson y a Nick Mathewson. Debido a varios intentos de replicar la idea del enrutamiento cebolla del NRL, Roger le dio al proyecto el nombre de Tor, The Onion Routing [2].

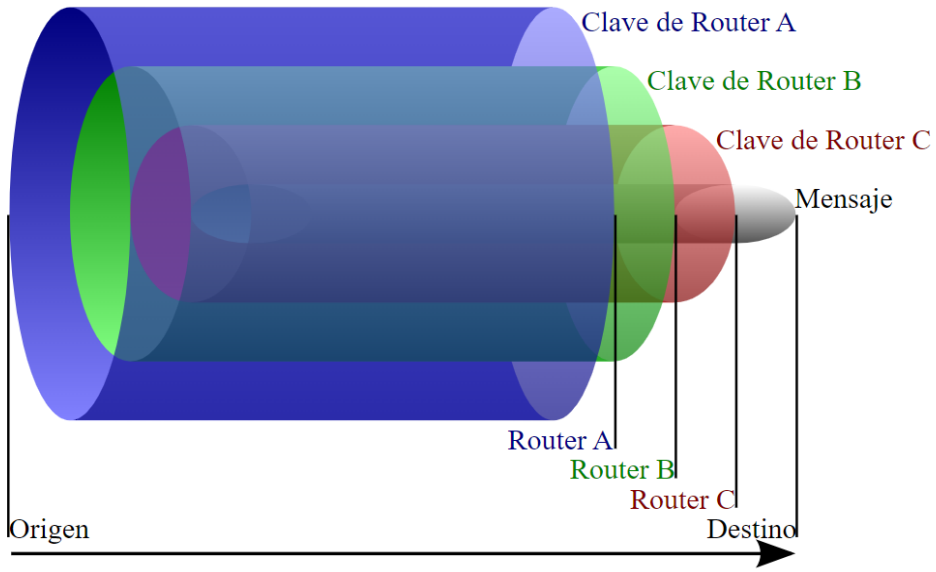
En 2004, y a modo de reconocimiento del beneficio que ofrecía Tor a los servicios digitales, la Electronic Frontier Foundation (EFF) comenzó a financiar el proyecto y en 2006 nace la organización sin ánimo de lucro The Tor Project, para mantener el desarrollo de Tor [2].

Un año más tarde, y con el fin de sortear la censura por parte de ciertos gobiernos, la EFF comenzó a crear puentes con la red Tor para que sus usuarios pudieran acceder a la web abierta sin consecuencias. Esto supuso un gran cambio y resultó un gran aumento en la popularidad de Tor, pero seguía suponiendo una barrera para las personas con menos conocimientos técnicos por lo que en 2008 comenzó el desarrollo de la herramienta TOR Browser que conocemos hoy en día [2].

5.3. FUNCIONAMIENTO

Como ya se ha mencionado antes, Tor sigue el modelo desarrollado por el NRL llamado enrutamiento de cebolla. Se le denomina así por el nivel de protección que este garantiza a la hora de enrutar el tráfico que pasa por la red, cubriendo el paquete con varias capas como si fuera una cebolla.

Figura 1. Enrutamiento Cebolla.



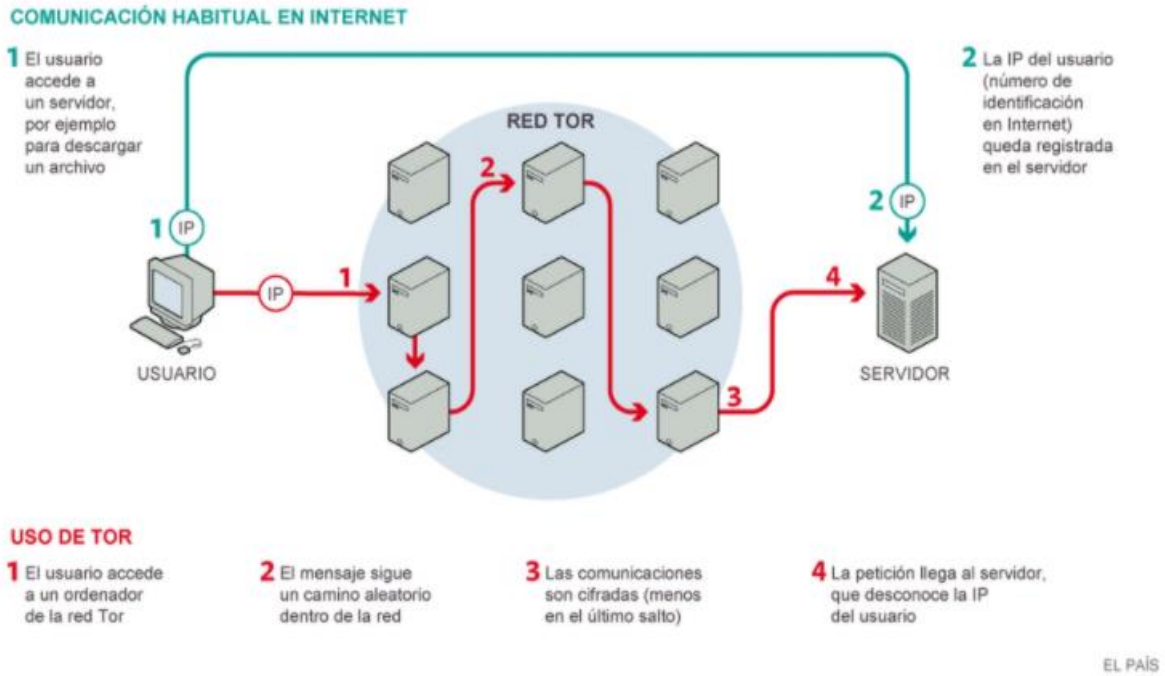
Extraída de la bibliografía [3].

Normalmente, en la red convencional, el tráfico suele ser conocido por el destinatario debido al tipo de enrutamiento y comunicación transparente que existe. En las redes de anonimato esta información se encuentra oculta para cualquiera que intercepte el tráfico ya que cada mensaje se envía encriptado por diversos nodos aleatorios de la red para confundir tanto al destinatario y a intermediarios, como a quien intercepte el tráfico de la red, con el objetivo de proteger el anonimato del emisor. La información real sólo la tiene el último nodo por el que pasan los mensajes, denominado nodo salida [3].

Aún con esta arquitectura, Tor está lejos de ser una red de anonimato perfecta ya que, su principal vulnerabilidad radica en el nodo de salida. Cuando la información pasa por dicho nodo, pasa de manera desencriptada por lo que si alguien está monitorizando el tráfico del nodo salida podría tener acceso a la información que el propio navegador intenta proteger [4].

Este sería el modelo de encaminamiento de la red convencional frente al enrutamiento cebolla:

Figura 2. Modelo de comunicación de internet y de la red Tor



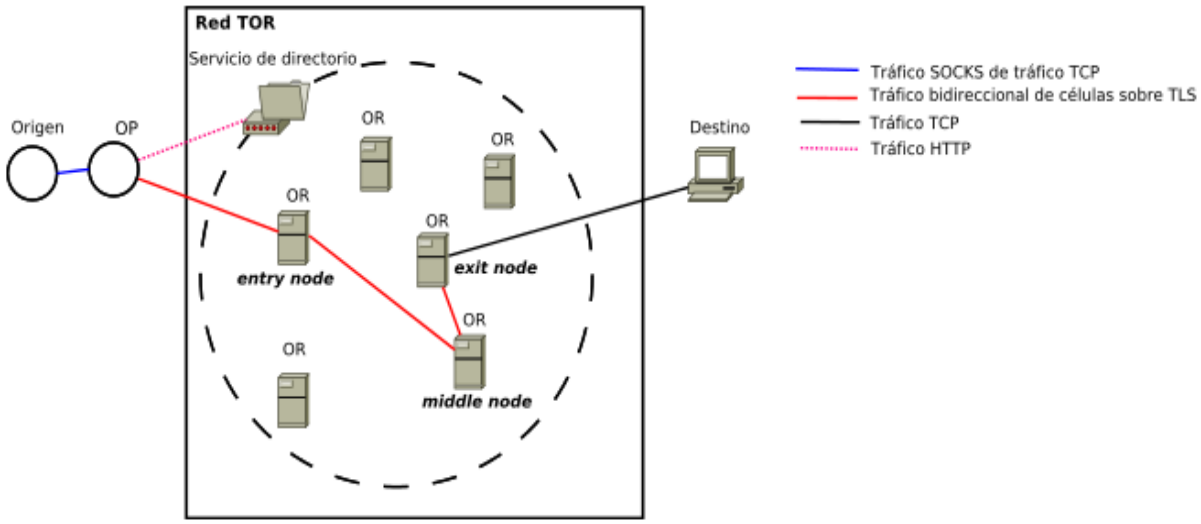
Extraído de la bibliografía [5].

Como se muestra en la Figura 2, mientras que en una conexión estándar la comunicación del usuario con el servidor es directa, quedando la IP real del cliente registrada en el servidor, en Tor funciona diferente. El usuario que navega con Tor Browser manda una petición, por ejemplo de conexión a un sitio ".onion", y esta pasa por una serie de nodos aleatorios de la red. Dicha información va pasando por el nodo entrada, nodo intermedio y nodo salida, cifrada salvo en su último salto, y finalmente llega al servidor, el cual desconoce la IP del cliente.

5.4. COMPONENTES DE LA RED TOR

La red que plantea TOR es compleja, y se conforma por los siguientes componentes:

Figura 3. Composición de la red Tor



Extraído de la bibliografía [6].

En la Figura 3 se muestra un esquema del funcionamiento de la red Tor. En ella podemos ver nombrados una serie de componentes:

- **Origen:** El origen de la conexión es un usuario de la red Tor, el cual utiliza una conexión TCP (Transmission Control Protocol) a través de puertos para obtener los servicios que se alojan en la red [7].

- **Onion Proxy (OP):** Este tipo de nodos son los propios usuarios de la red, que pasan a formar parte de ella al instalar Tor. Los nodos OP son los que establecen los circuitos dentro de la red Tor a través de los nodos Onion Router, y son los encargados de obtener la información de los servicios de los directorios, y gestionar las conexiones de las aplicaciones de los usuarios [7].

- **Onion Router (OR):** Los nodos OR básicamente son los servicios de la red ejecutándose en los clientes. Funcionan como encaminadores del tráfico y en algunos casos también como DNS (Domain Name System).

- **Nodo de entrada (Entry Node):** Los nodos de entrada son los encargados de recibir la información del cliente y de asegurar la privacidad de las comunicaciones. Son nodos intermedios que tras cumplir una serie de requisitos reciben la elevación a través de un *flag* —uno o más bits que se utilizan para almacenar un valor que tiene asignado un significado—. Cada cliente tiene asignados una serie de nodos de entrada, los cuales van caducando y renovándose continuamente, para de esta forma mejorar la seguridad de la red y sus transmisiones.

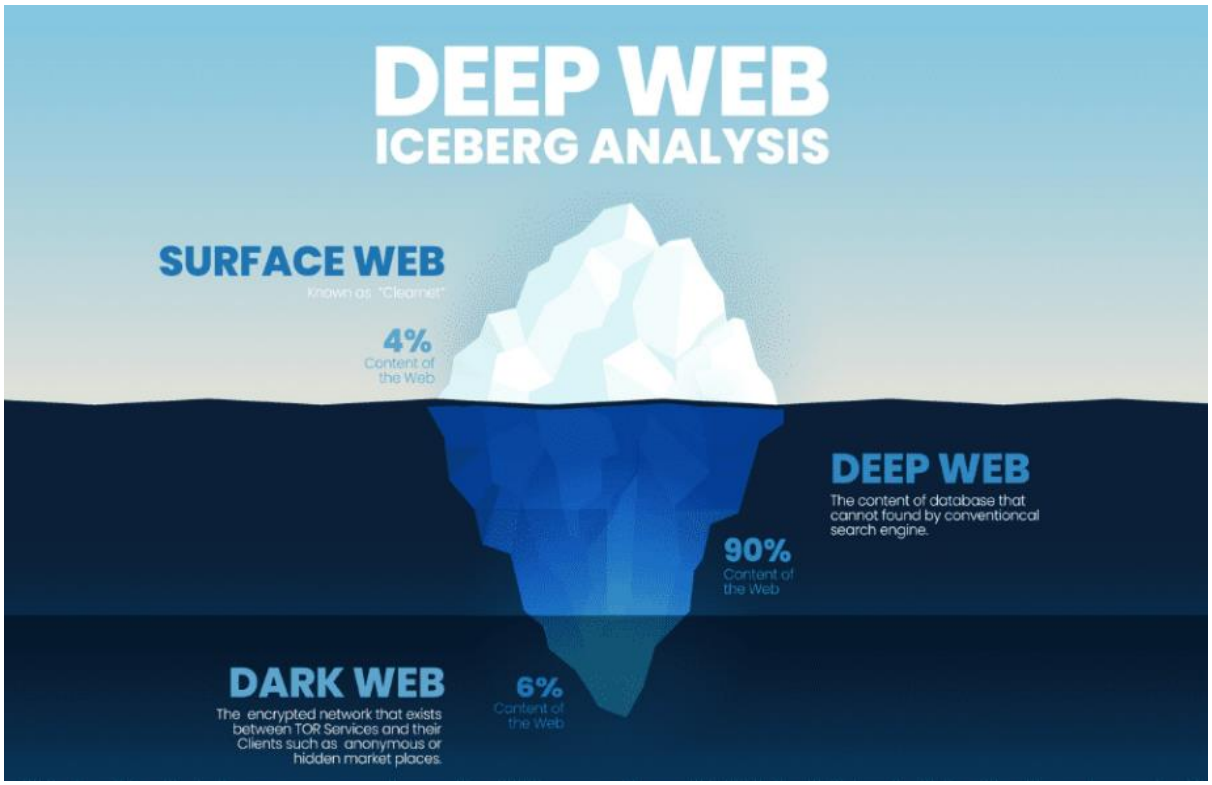
- **Nodo intermedio (Middle Node):** Este tipo de nodo es el más común dentro de la red. Éste solo se comunica con otros nodos, por lo que su tráfico nunca sale de la red Tor. Transmiten información cifrada por lo que no es común que este tipo de nodos sean atacados.

- **Nodo de salida (Exit Node):** Este tipo de nodo es el más sensible. Es el último nodo de la red por el que pasa la información de una comunicación. Debido a que este nodo contiene la información del tráfico sin encriptar es el que más se busca proteger ya que cualquier ataque a este nodo vulneraría la privacidad generada por Tor. Es por ello que este tipo de nodos suele estar mantenido por instituciones o usuarios capaces de afrontar posibles consecuencias legales del uso indebido que pueden darle los usuarios cuyo tráfico pase por estos nodos.

5.5. INTERNET Y SERVICIOS OCULTOS

Internet es una red inmensa, y por ello contiene gran variedad de información, pero eso no implica que toda esté a la vista. En la Figura 4 se puede ver una aproximación del internet al que tienen acceso los buscadores convencionales, y por debajo de él, el contenido no indexado. Este último se podría dividir en dos capas, la Deep Web y la Dark Web.

Figura 4. Tipos de internet



Extraído de la bibliografía [8]

Surface Web: Contiene la información indexada en buscadores convencionales como Google, Bing o Yahoo!. Es la parte a la que los usuarios estándar acceden, y contiene aproximadamente un 4% del contenido de la World Wide Web [9].

Deep Web: La Deep Web es el primer nivel de lo que se conoce como internet profundo. Contiene información no indexable como por ejemplo fichas médicas. Es contenido que los buscadores tradicionales tienen prohibido mostrar públicamente, pero no por ello quiere decir que su contenido sea ilegal o que haya que ser un hacker para acceder a él [9].

Dark Web: La Dark Web es la punta más profunda del iceberg de internet. Sólo se puede acceder a este contenido a través de buscadores específicos como por ejemplo Tor o I2P [9].

En esta capa es donde se halla todo el contenido que no se encuentra de una manera accidental, desde cibermercados negros o contenidos censurados, hasta terrorismo [9].

Cabe destacar que no todo el contenido al que se tiene acceso a través de TOR es ilegal.

6. TÉCNICAS DE DESANONIMIZACIÓN EN TOR

Una vez conocidos los diversos usos indebidos que pueden hacerse de esta herramienta, muchos gobiernos se han visto en la necesidad de utilizar una serie de técnicas y ataques para poder desenmascarar a los proveedores de servicios ilícitos en la red, salvaguardar la salud pública y llevar a miembros de organizaciones criminales ante la justicia.

Sabiendo esto, es importante mencionar que dichas técnicas no sólo se utilizan para el bien, existen muchos usuarios que las utilizan para realizar fraudes, extorsiones y demás actividades delictivas.

A continuación, se recogerán diferentes métodos que sirven para revocar el anonimato en Tor y en algunos casos, cómo defenderse de ellos si dejas de lado los buscadores convencionales.

6.1. THE SNIPER ATTACK

El Sniper Attack o ataque del francotirador es un ataque de tipo Denegación de servicios (DoS).

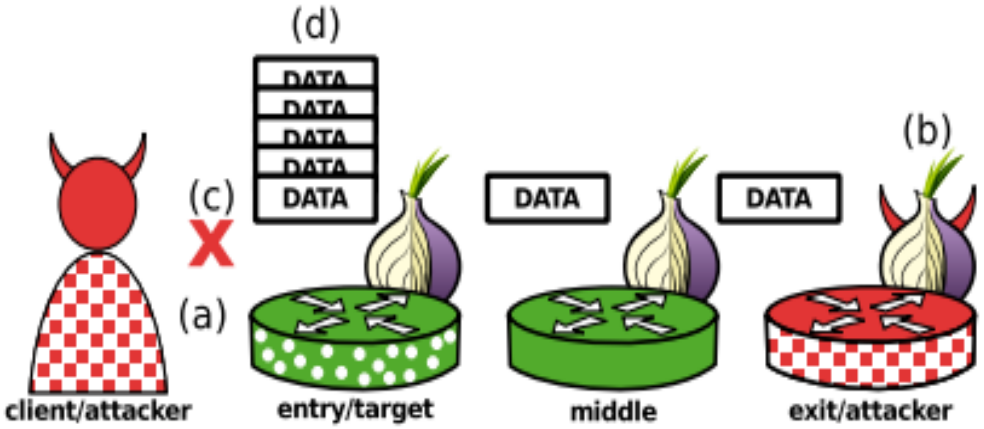
Este ataque explota el algoritmo encargado del control de flujo de la red Tor para bloquear de forma remota un nodo agotando sus recursos de memoria [10].

Existen varias formas de ejecutar este ataque:

En la primera forma [Figura 5], el atacante tiene control del cliente y del nodo de salida, y genera un circuito teniendo como objetivo a una víctima con la posición de nodo de entrada [10,11].

El atacante deja de leer desde la conexión TCP que tiene el circuito atacante, lo que hace que la ventana TCP en la conexión saliente del objetivo se cierre, y guarde en el búfer hasta 1000 celdas (máximo por circuito) [10,11].

Figura 5. Versión 1 de la forma básica de ejecutar Sniper Attack

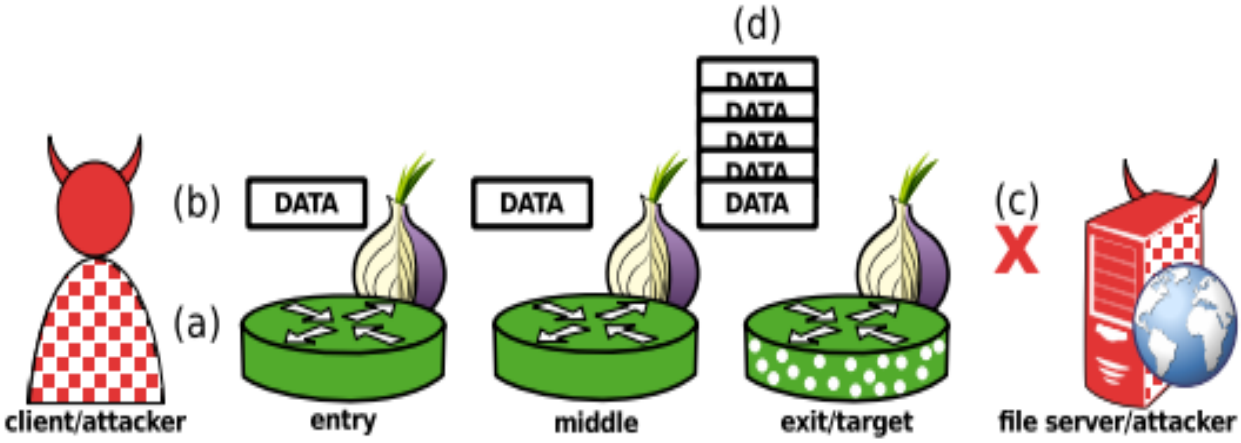


Extraído de la bibliografía [10].

En la segunda forma [Figura 6], el atacante tiene el control del cliente y del servidor, y genera un circuito teniendo como objetivo a una víctima con la posición de nodo de salida.

El atacante genera paquetes y hace que estos se estén mandando de manera continua al objetivo, excediendo así el límite de las 1000 celdas. Esto hace que el servidor deje de leer de la conexión TCP, por ello el objetivo almacenará en su buffer todos los datos que envía el cliente, consumiendo los recursos de memoria del objetivo hasta que el Sistema Operativo mata el servicio de Tor [10,11].

Figura. 6. Versión 2 de la forma básica de ejecutar Sniper Attack



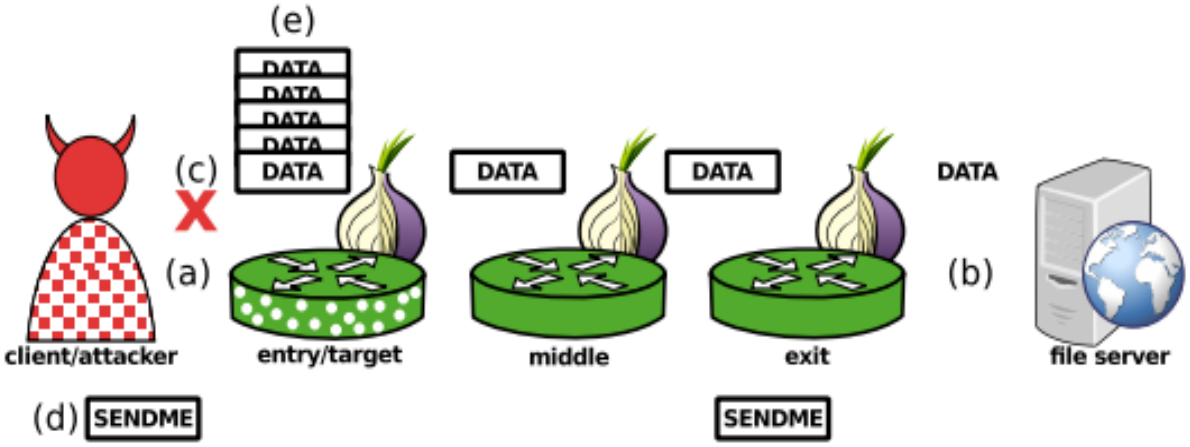
Extraído de la bibliografía [10]

Por último, la manera más eficiente de ejecutar este ataque.

En este caso [Figura 7], el atacante sólo controla el cliente, y repite lo siguiente de forma paralela.

El cliente crea un circuito teniendo como objetivo a una víctima con la posición de nodo de entrada, y le indica que descargue un archivo de gran tamaño de un servidor de internet externo. El cliente deja de leer de la conexión TCP, lo que hace que se almacenen en buffer las 1000 celdas. El cliente “engaña” a la salida mandando celdas del tipo SENDME, haciendo que se sigan mandando paquetes en el circuito y así consumiendo los recursos de memoria del objetivo. La tasa de envío de estas celdas SENDME tiene una frecuencia lo suficientemente baja para evitar exceder el tamaño de la ventana de los paquetes de salida. Este proceso continuará hasta que el Sistema operativo detenga el servicio de Tor en la máquina objetivo [10,11].

Figura. 7. Versión eficiente de ejecutar Sniper Attack



Extraído de la bibliografía [10]

En lugar de conectarse directamente con la víctima, el atacante puede lanzar el ataque a través de un circuito Tor separado utilizando una segunda instancia de cliente y la opción "Socks4Proxy" o "Socks5Proxy". En este caso, puede beneficiarse del anonimato que la propia red Tor proporciona para evadir la detección. No se detecta un aumento significativo en el uso de ancho de banda al anonimizar el ataque de esta manera [10,11].

Esta técnica no sólo se puede utilizar para tirar nodos de la red de Tor, se pueden realizar una serie de pasos extra que pueden hacer que esta técnica también sirva para desanonimizar usuarios y servicios [10,11].

Ya que Tor acepta conexiones de nodos disponibles en la red, un atacante que controle un nodo de entrada y uno de salida podría quitar el anonimato correlacionando los datos de tiempos y volumen de tráfico que entra y sale por la red.

Para ello el atacante debería poseer un número elevado de nodos de entrada y salida maliciosos, y lanzar una serie de ataques para identificar los diferentes nodos del objetivo. Tras conocer esos datos y con el Sniper attack, podría tirarlos para que la red Tor tenga que cambiar de nodos y seleccionar los controlados por el atacante.

Este proceso se repetiría hasta que TOR seleccione alguno de sus nodos maliciosos como nodos de la víctima, y más adelante por correlación de tráfico sacar la información relevante en lo referente a la desanonimización.

TOR Project hizo una serie de pruebas, teniendo en cuenta que la efectividad del ataque y el tiempo de ejecución de este depende de la cantidad de RAM de los relés ya que, este ataque consume en su totalidad dicho recurso de la víctima, se determinó que para llevar a cabo el proceso completo de la desanonimización haría falta ejecutar el ataque aproximadamente entre 18 y 132 veces, y el tiempo estimado estaría entre las 4 y las 278 horas [11].

La efectividad de este ataque se ve severamente reducida si el relé se reinicia tras su caída o si está debidamente protegido frente ataques de este tipo.

6.1.1 Defensas

Una defensa simple contra el Sniper Attack es hacer que el nodo de entrada monitorice la longitud de su cola, y si esta llena más de 1000 celdas, mate al circuito. Es una buena defensa en general, pero ello no impide que el atacante paralelice el ataque usando múltiples circuitos, consumiendo 1000 celdas en cada uno, lo que es tremendamente efectivo [10,11].

Otra posible defensa podría ser la llamada “SENDMEs autenticados”. Este método se basa en la protección ante SENDMEs de un nodo que realmente no recibió 100 celdas. Para ello, se coloca un número aleatorio de 1 byte en cada celda número 100 al final del empaquetamiento, y ese número debe incluirse al final de la entrega en el paquete SENDME, si no es así, este se rechaza al no estar verificado [10,11].

De igual forma que en el anterior método, esto no protege de ataques en paralelo o de otro tipo de ataques que controlan o ignoran los SENDMEs [10,11].

La mejor defensa, como sugieren los desarrolladores de Tor, es implementar una herramienta personalizada que mate los circuitos que se han quedado sin memoria dentro de Tor. Este sólo se activaría cuando la memoria se encuentre baja, y luego elegiría el circuito con la celda frontal más antigua en su cola de circuitos, evitando el Sniper Attack al matar todos los circuitos de ataque [10,11].

Con esta defensa activa, el siguiente paso del atacante sería hacer que Tor mate un circuito no malicioso. Para ello el atacante debe asegurarse de que la celda más frontal de su cola del circuito malicioso sea por lo menos algo más “joven” que la celda más antigua en cualquier cola de circuitos no maliciosos.

Esto requiere una gran cantidad de ancho de banda que el atacante podría aprovechar para realizar otro tipo de ataques más convencionales como por ejemplo uno de fuerza bruta [10,11].

Actualmente Tor ha implementado una versión de este mecanismo de defensa y sigue trabajando para expandirlo a los buffers de los canales y conexiones para prevenir este tipo de ataques [11].

6.2. DESANONIMIZACIÓN MEDIANTE ARCHIVOS CEBO

Este tipo de ataque se centra en la difusión de archivos corruptos o infectados que hacen posible la identificación, entre otras cosas, de aquellos que los ejecutan en sus equipos.

Pese a lo trivial y simple que puede parecer este ataque, ha sido posible identificar a un gran número de ciberdelincuentes con su ayuda [12]. Su obviedad y simpleza es lo que hacen tan potente este tipo de ataques dentro de la red TOR.

TOR brinda el máximo nivel de anonimato entre todas las herramientas utilizadas para ocultar tu dirección IP real, y mientras que sí que es posible identificar usuarios que utilizan Proxy o VPN a través de sitios de terceros con TOR esto no es posible. Para llegar a desanonimizar a un usuario o servicio en TOR es necesario, por lo general una serie de ataques de difícil implementación, un error humano, o vulnerabilidades del propio navegador [12].

Aunque estas últimas no se den con demasiada frecuencia, nunca se deben excluir. Gracias a ellas, más de 900 usuarios de una de las redes más visitadas de pornografía infantil de la Dark Web, PlayPen, fueron identificados y arrestados. Todos ellos usaban TOR, cosa que en cierto modo genera una falsa sensación de seguridad en los usuarios y les hizo bajar la guardia frente a una serie de documentos modificados por el FBI [12].

Los ciberdelincuentes recibían un documento de texto —Word o PDF—, estos lo descargaban y verificaban en VirusTotal y lo ejecutaban en máquinas virtuales. El documento no muestra en ningún momento ningún rastro de actividad maliciosa, sólo se conectaba al servidor y por lo tanto le enviaba la dirección IP del ciberdelincuente [12].

Por lo general, las máquinas virtuales no bloquean las conexiones y el anonimato que ofrece Tor sólo se mantiene en los sitios abiertos en su red por lo que, incluso habiendo configurado una VPN para que las conexiones que la omiten sean bloqueadas, las fuerzas gubernamentales tendrían acceso a la dirección IP real solicitando al proveedor VPN comercial dicha información mediante una serie de solicitudes formales [12].

Cabe destacar que para que este método funcione es necesario abrir el archivo cebo en la máquina de la víctima.

6.2.1. Defensas

Como contramedida o defensa estaría el abrir los archivos descargados en sistemas operativos como Whonix, que, entre otras cosas, fuerza que todas las conexiones se realicen a través de Tor, haciendo imposible que se filtren las IP de sus usuarios [13].

6.2.2. Caso PlayPen

PlayPen era considerado el portal de pornografía infantil más grande del mundo, contando con más de 150.000 usuarios por todo el mundo [14].

Su creador Steven W.Chase creó el sitio en Tor en Agosto de 2014. El sitio estaba indexado por categorías como el sexo de la víctima, edad e incluso la actividad sexual implicada [14].

El caso y las miles de investigaciones de seguimiento que inició no tiene precedentes en su alcance, según expresaron miembros del FBI. Este caso desencadenó la necesidad de cooperación internacional para enjuiciar a los abusadores de niños en todo el mundo [14].

“Sólo pudimos lograrlo con mucho apoyo de nuestros socios internacionales y oficinas de campo”, dijo el agente especial Dan Alfin, quien investigó el caso como parte de la sección del Bureau de Crímenes Violentos contra Niños [14].

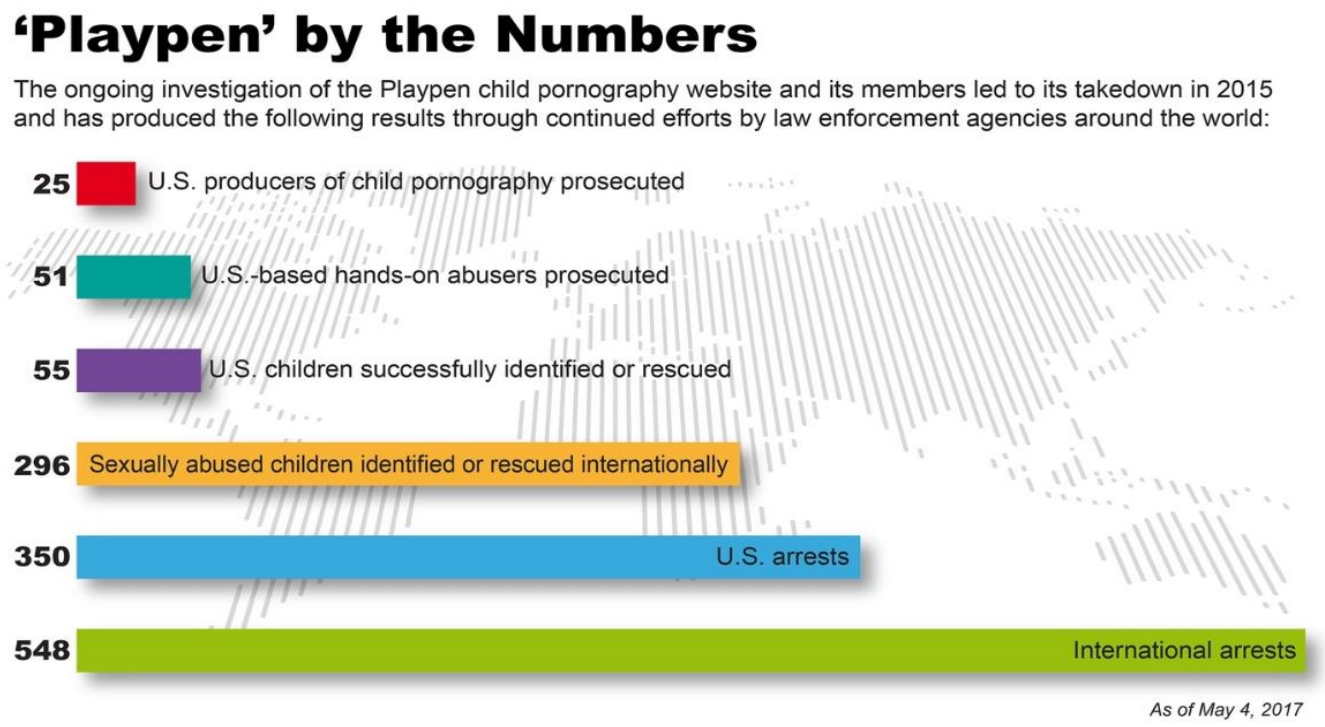
Fue meses después de la apertura del sitio cuando su creador cometió un desliz y reveló la IP única de PlayPen, una ubicación en Estados Unidos. Una agencia vinculada a la aplicación de la ley extranjera fue quien notificó al FBI [14].

Gracias a ello se tomaron medidas como la incautación de una copia del sitio web, emisión de órdenes de allanamiento de cuentas de correo y seguimientos del dinero movido por el sitio, lo que finalmente condujo a Steven Chase, quien fue condenado a 30 años de cárcel [14].

Tras arrestar a los administradores del sitio, en enero de 2015, el FBI en asociación con la sección de Explotación y Obscenidad Infantil del Departamento de Justicia, lanzó la “Operación Chupete”, enfocada en la persecución de los miles de miembros de PlayPen. [14]

Finalmente, además de la eliminación del sitio web el 4 de mayo de 2017, se produjeron los siguientes resultados:

Figura 8. Números del caso ‘PlayPen’



Extraído de la bibliografía [14]

- Fueron procesados 25 productores de pornografía infantil estadounidenses.
- Fueron procesados 51 abusadores prácticos.
- 55 niños estadounidenses fueron identificados y rescatados.
- 296 niños abusados sexualmente fueron identificados y rescatados a nivel internacional.
- Al menos 350 personas estadounidenses arrestadas.
- 548 personas arrestadas a nivel internacional.

Aunque PlayPen lleva años inactivo, sigue habiendo sitios que operan de la misma manera, y es por ello que es necesario conocer diversas formas de romper el anonimato que proporcionan redes como Tor, y de esta forma poder acabar con este tipo de prácticas [14].

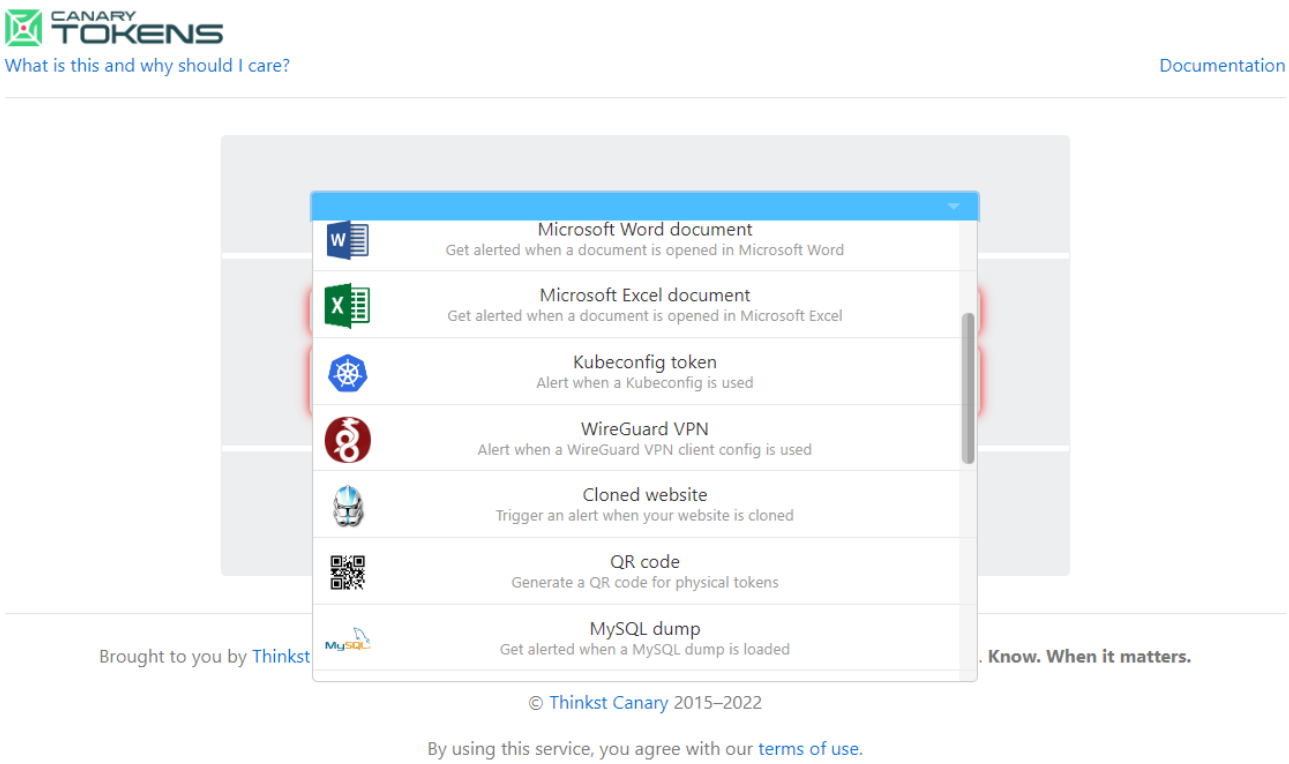
6.2.3. Caso Práctico

La realización del siguiente caso práctico va a consistir en lo siguiente:

- **Creación de un archivo cebo:** Este archivo tendrá la peculiaridad de que al abrirse, este mandará al atacante los datos de conexión reales de la víctima, que lo recibe a través de Tor.
- **Modificación del archivo cebo:** El archivo contendrá el logo de la Universidad de Alcalá, pretendiendo emular ser un documento de la misma.
- **Difusión del archivo cebo:** El atacante procederá a enviar a la víctima el archivo cebo a través de un cliente de correo.
- **Recepción y apertura por parte de la víctima:** La víctima recibirá el archivo cebo a través del cliente de correo, abierto desde Tor. Una vez abierto el documento, al atacante le llegará la notificación con los datos reales de la conexión de la víctima.
- **Consultar datos reales de la víctima:** El atacante abrirá la notificación y obtendrá la IP real de la víctima.

En primer lugar, hay que crear el archivo cebo. Para ello usaremos la herramienta Web CanaryTokens.

Figura 9. CanaryTokens



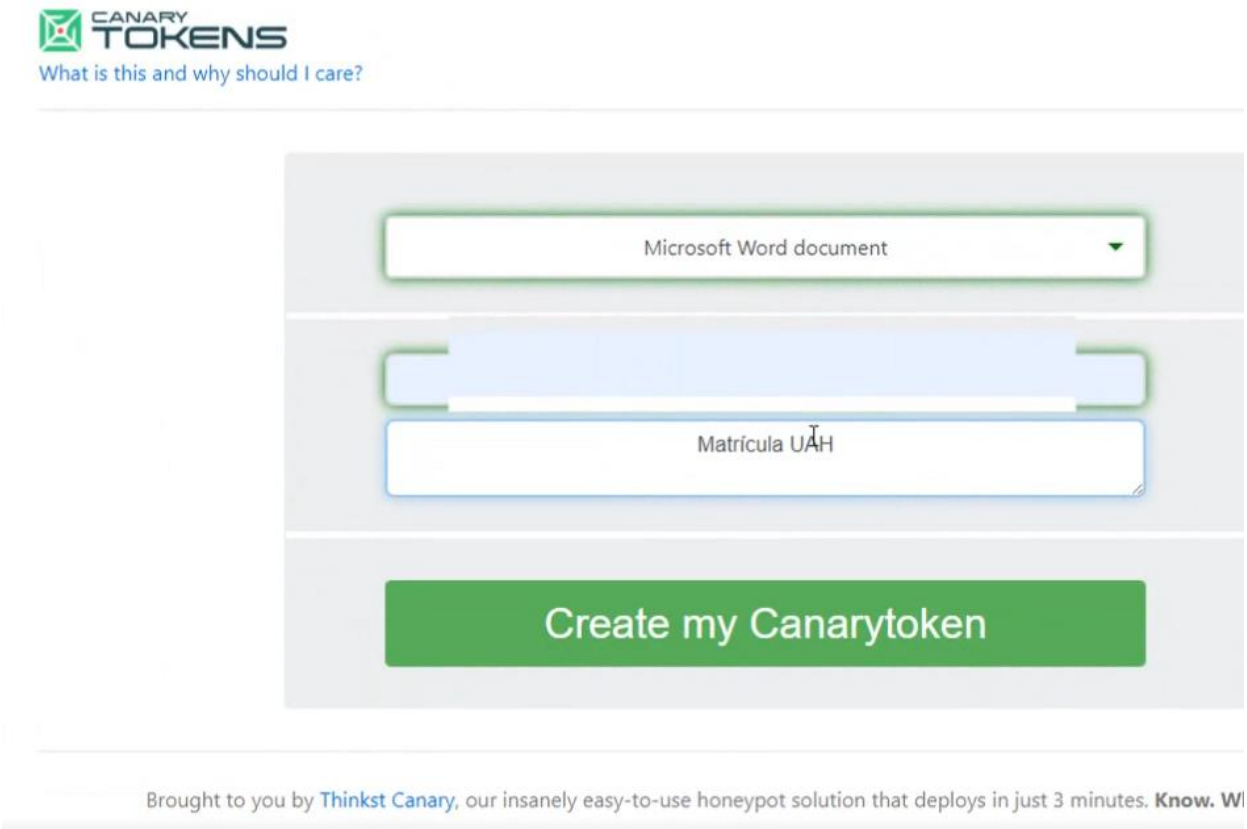
Archivo de creación propia

En esta herramienta web, seleccionaremos el tipo de archivo que queremos crear. La herramienta cuenta con un gran repertorio de tipos de archivos, desde documentos de Office o PDF, hasta alertas de cuando se cargan ficheros SQL.

El segundo recuadro es para ingresar la dirección de correo en la que queremos que llegue el aviso de la apertura del documento, nos llegará una notificación con varios datos, entre ellos el código de token generado, fecha de apertura del documento y la dirección IP real de la máquina de la víctima.

El tercero y último es la descripción.

Figura 10. Creación de documento Word



Archivo de creación propia

En este caso, el archivo que generaremos será un documento Word que emulará ser documentación de la Universidad de Alcalá.

Figura 11. Descarga del archivo cebo

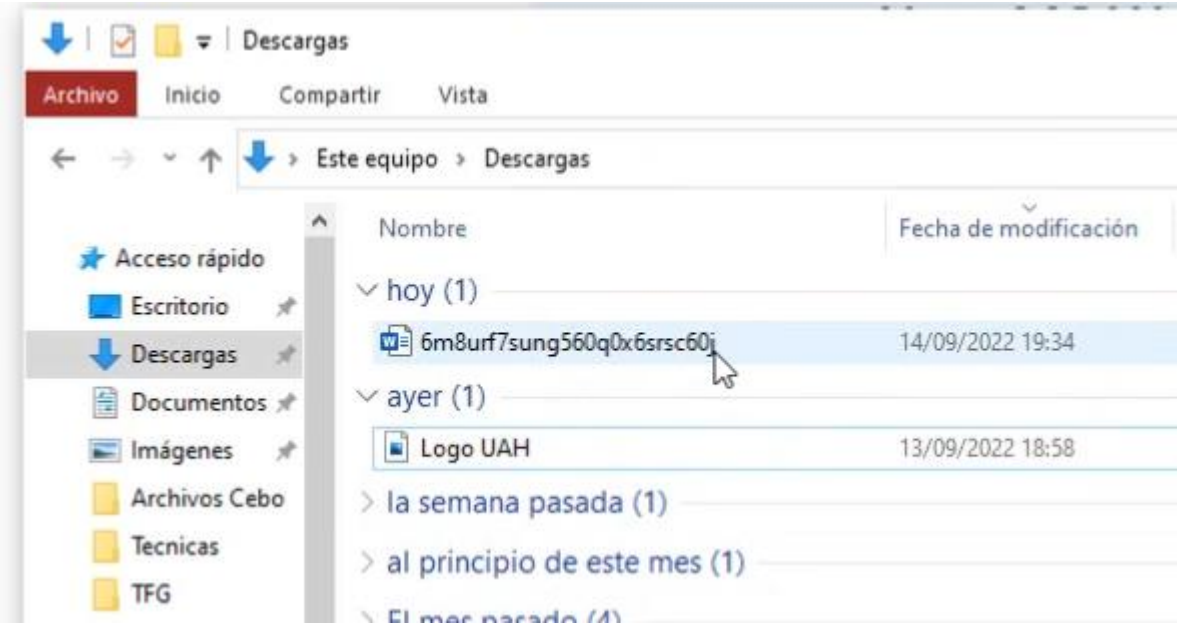
Archivo de creación propia

Una vez hemos creado el archivo nos saltará esta pestaña, donde descargaremos nuestro archivo.

El archivo generado será un documento Word vacío y como nombre tendrá el ID del token generado por la herramienta. Este documento se puede modificar a placer sin afectar al comportamiento del mismo. En este caso, se le cambiará el nombre y pegará el logo de la Universidad.

A continuación, vemos el formato en el que se nos descarga nuestro archivo cebo.

Figura 12. Archivo descargado

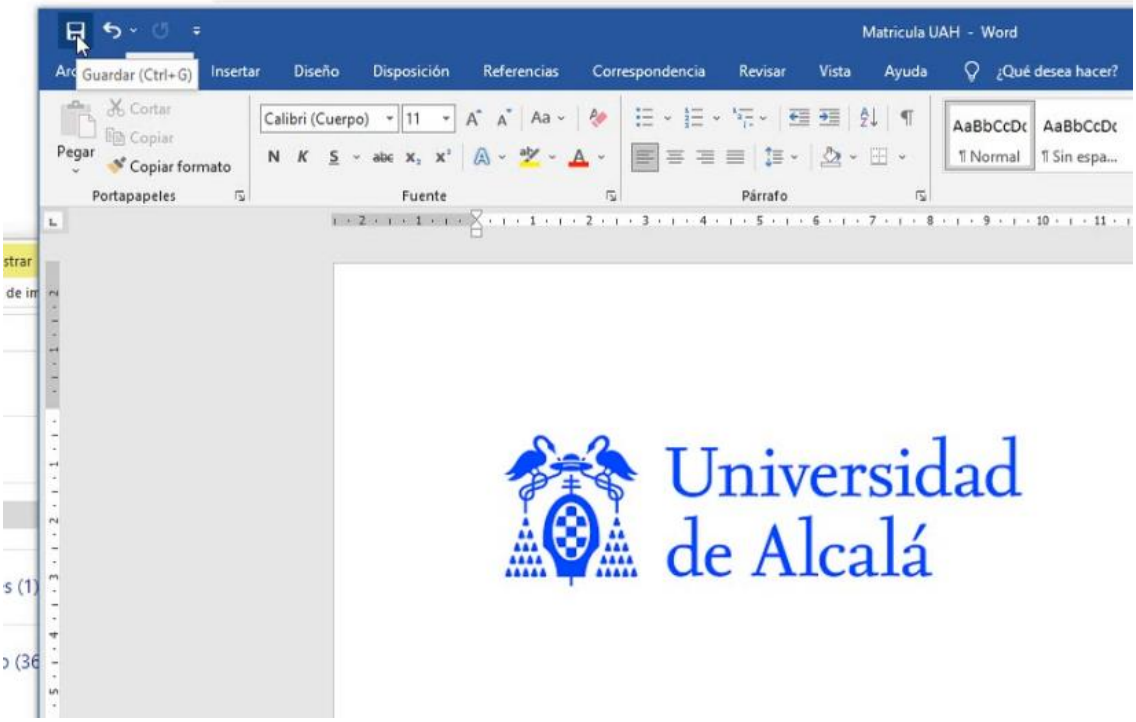


Archivo de creación propia

Al ser abierto y debido a su programación, el archivo cebo mandará una notificación a través de un cliente de correo a su creador, el atacante, con datos reales relativos a la conexión de su víctima.

Una vez descargado se procede a su cambio de nombre y a su edición, en este caso el pegado del logo de la Universidad de Alcalá.

Figura 13. Archivo modificado



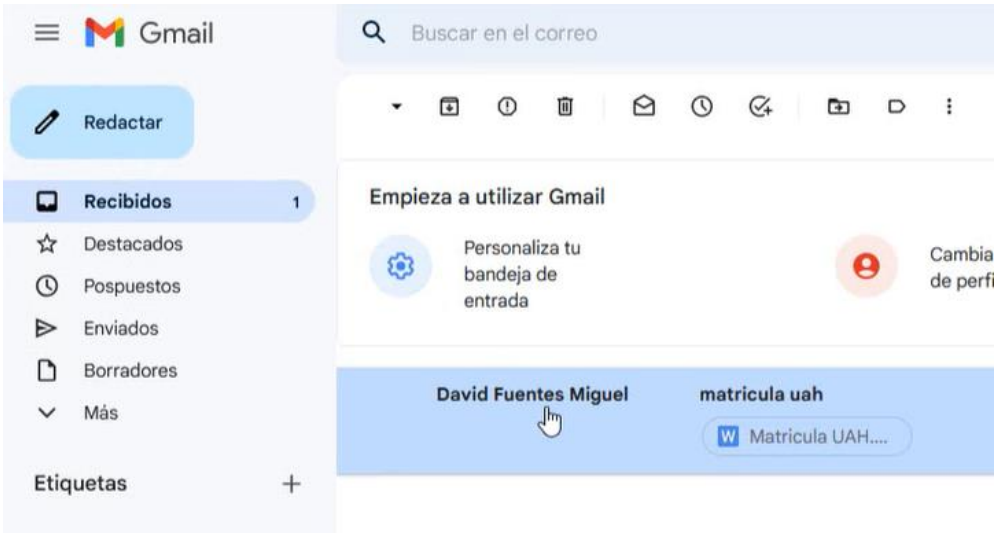
Archivo de creación propia

Una vez modificado, el atacante lo distribuye a sus víctimas. En el caso de este trabajo se ha usado el cliente de correo para su distribución.

Una vez el atacante ha enviado el archivo cebo, la víctima deberá abrirlo para que este se ejecute y mande los datos reales de la conexión al atacante.

La víctima, que está usando Tor Browser, abre su cliente de correo, y recibe un correo con el archivo que aparentemente es como cualquier otro correo:

Figura 14. Cliente de correo de la víctima

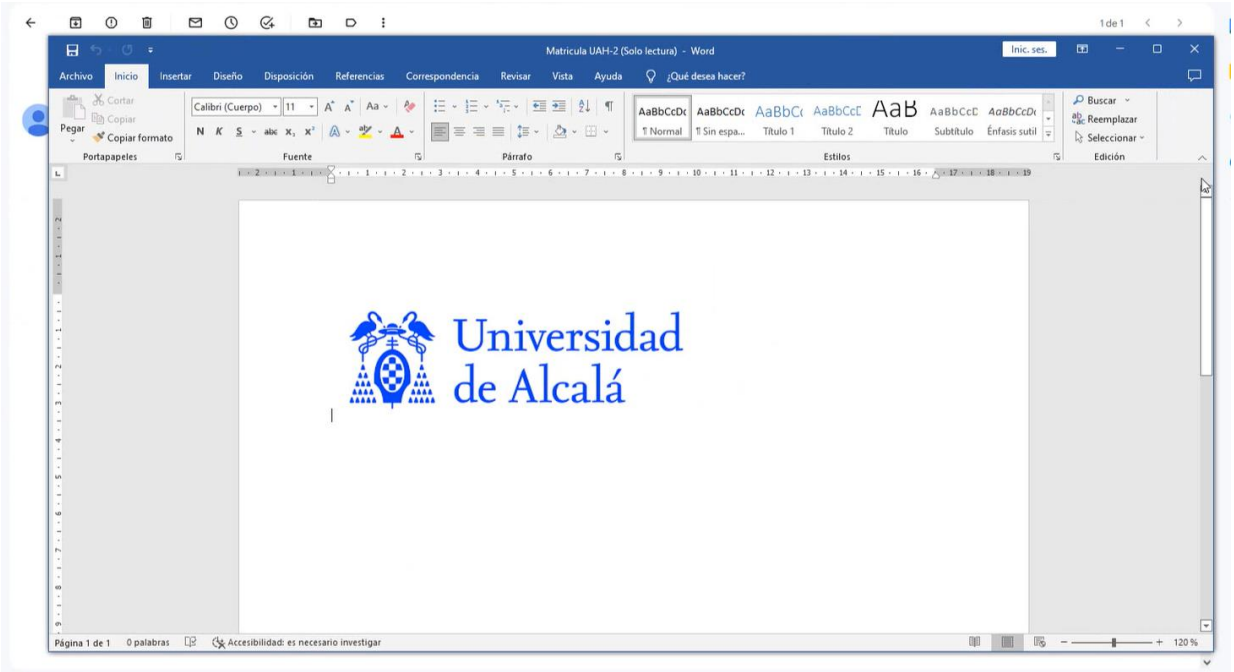


Archivo de creación propia

Aparentemente es un correo normal, recibido por el cliente de correo Gmail, abierto a través de Tor Browser.

Al abrirlo, se muestra lo siguiente:

Figura 15. Archivo Cebo

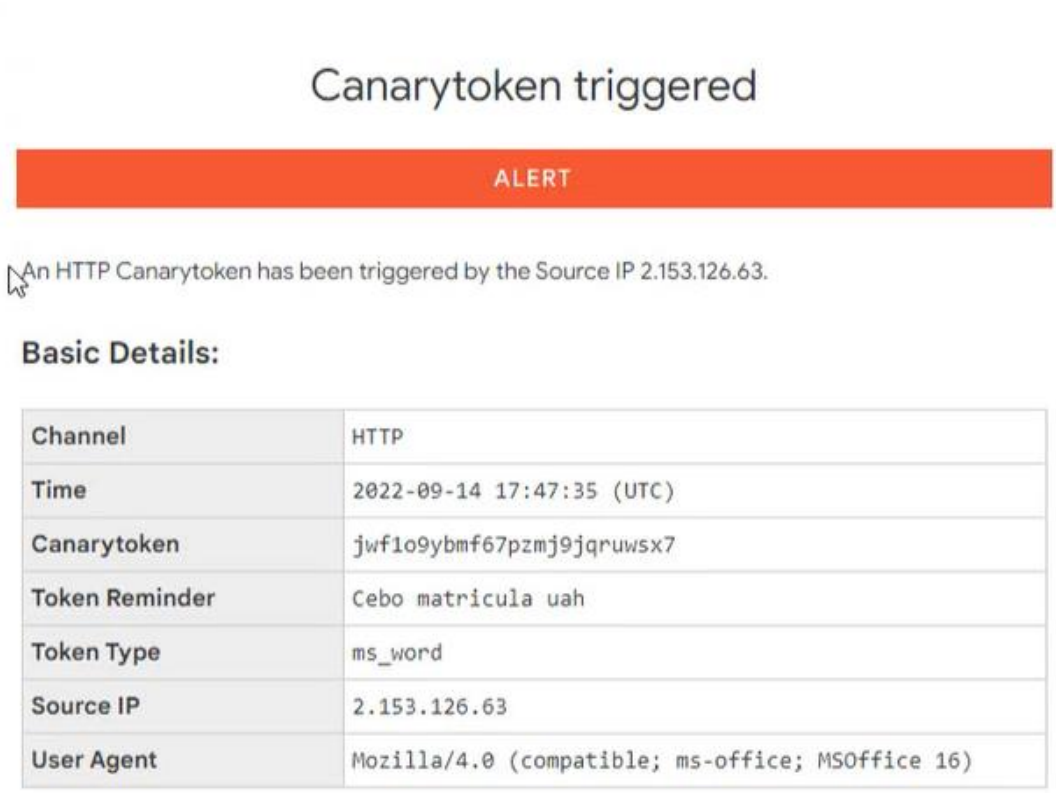


Archivo de creación propia

Es un documento Word con el logo de la Universidad de Alcalá. No se aprecia nada que pueda levantar sospechas. No hace falta decir que esto es un ejemplo, las personas que realmente se dediquen a la realización de este tipo de ataques, serán mucho más minuciosos a la hora de editar los documentos, para que, al recibirlo la víctima, no exista ningún tipo de duda acerca del origen del mismo. También es normal que el atacante use una cuenta de correo por ejemplo, robada del dominio de una empresa concreta, o una temporal a la que haya hecho spoofing para que aparezca por ejemplo como el correo real de la Agencia tributaria.

Una vez que la víctima lo abre, el atacante recibe un correo con la siguiente información:

Figura 16. Datos reales de conexión



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 2.153.126.63.

Basic Details:

Channel	HTTP
Time	2022-09-14 17:47:35 (UTC)
Canarytoken	jwf1o9ybmf67pzmj9jqruwsx7
Token Reminder	Cebo matricula uah
Token Type	ms_word
Source IP	2.153.126.63
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Archivo de creación propia

En el apartado Source IP tenemos la IP real de la víctima, que, usando herramientas de localización de IP, por ejemplo, podremos localizar. A continuación, veamos la IP que Tor le había dado a la víctima:

Figura 17. IP de Tor de la víctima

Archivo de creación propia

Comparando las dos, confirmamos que la que le llega al atacante es la real del equipo de la víctima.

6.3. DESANONIMIZACIÓN CON PROGRAMAS (TorBot)

Existen varios métodos para poder identificar las IP reales de los usuarios y servicios de TOR. En este caso, hablaremos de una herramienta en desarrollo de inteligencia de código abierto (OSINT) TorBot, basada en el lenguaje de programación Python.

El principal objetivo de esta herramienta es recopilar datos abiertos de la Dark Web, apoyándose en una serie de algoritmos de minería de datos.

Si bien esta herramienta por sí sola no logra desanonimizar usuarios, combinandola con diferentes técnicas de las que se habla en el trabajo, sería posible obtener los datos reales de una conexión.

6.3.1. Funcionamiento básico

TorBot es un crawler —robots que inspeccionan páginas web de una forma automatizada— al que el usuario le pasa una URL del tipo ".onion", y este saca todas las URLs —enlaces— relacionadas a ella, en caso de estar activa. El código que se ejecuta es el siguiente:

Figura 18. Código que ejecuta TorBot

```
 URLs = input(url)
while(URLs is not empty) do
    dequeue url
    request page
    parse for Links
    for(link in Links) do
        if (link islive && link is not visited) then
            add link to URLs
    store page content
```

Extraído de la bibliografía [15].

Tras introducir la URL, el crawler irá buscando webs relacionadas y proporcionará la IP de esa URL, lo que facilita el proceso de desanonimización de los servicios de la red Tor.

6.3.2. Configuración y utilización

Torbot es una herramienta que requiere de una configuración concreta y depende de una serie de programas, por lo que habrá que seguir una serie de pasos para poder ejecutarla correctamente.

Antes de ejecutar la herramienta hay que asegurarse que Tor se ha iniciado, por ello es necesario abrir una consola y ejecutar el comando [15]:

- `sudo service tor start`

De igual manera asegurarse de que TORRC, un archivo de texto que contiene las instrucciones de configuración que marcan cómo ha de comportarse Tor, está configurado a SOCKS_PORT localhost:9050. [16]

Normalmente esta última configuración suele venir por defecto, si no es así se puede configurar usando un editor de texto y cambiando las propiedades de SOCKS_PORT, para ello habría que abrir un terminal y ejecutar el siguiente código:

- `sudo nano /etc/tor/torrc`

Por último, instalar TorBot Python [15]:

- `pip3 install -r requisitos.txt`

Estos programas se encuentran en la carpeta del proyecto de git, en un archivo de texto llamado requisitos.txt.

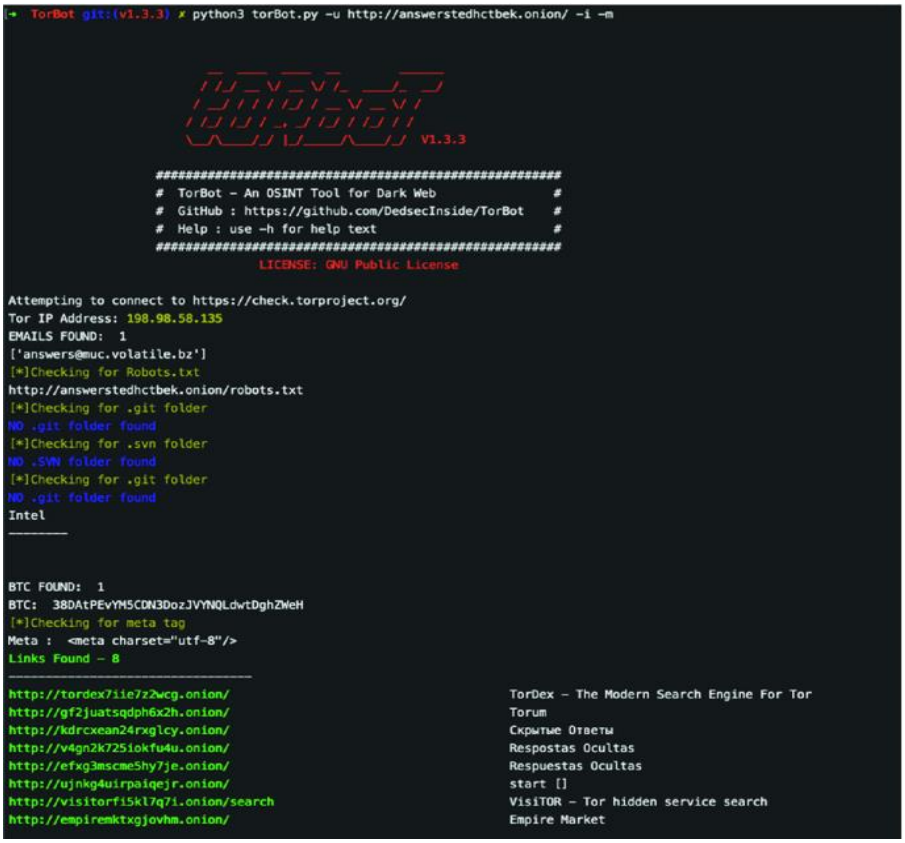
Una vez instalado y configurado, para lanzarlo habría que introducir en la consola lo siguiente [15]:

- `python3 torBot.py`

Finalmente, una vez abierto se nos mostrará la pantalla de inicio, donde usando el comando `python3 torBot.py -u [URL],` podremos buscar la información que buscamos de una URL en concreto [15,16].

Una vez ejecutamos el programa, e introducimos alguna dirección URL para analizar, TorBot mostrará la siguiente ventana:

Figura 19. Interfaz de TorBot



Extraído de la bibliografía [17]

Existen distintos comandos, entre ellos el manual, que mostraría lo siguiente [15]:

```
usage: torBot.py [-h] [-v] [--update] [-q] [-u URL] [-s] [-
m] [-e EXTENSION]
                 [-l] [-i]

optional arguments:
  -h, --help            Show this help message and exit
  -v, --version         Show current version of TorBot.
  --update                Update TorBot to the latest stable
version
  -q, --quiet           Prevent header from displaying
  -u URL, --url URL       Specifiy a website link to crawl,
currently returns links on that page
  -s, --save            Save results to a file in json format
  -m, --mail            Get e-mail addresses from the crawled
sites
  -e EXTENSION, --extension EXTENSION
```

```
                          Specifiy      additional      website
extensions to the
                          list(.com or .org etc)
  -l, --live                Check if websites are live or not
(slow)

  -i, --info                 Info displays basic info of the
scanned site (very slow)`
```

Con esta herramienta no sólo podemos obtener el estado del enlace, o la IP de Tor, también podemos obtener una breve descripción de la web para saber en qué mercado se mueve.

6.4. DESANONIMIZACIÓN POR CORRELACIÓN DE TRÁFICO

Este tipo de ataque es uno que se ejecuta de una forma más pasiva.

El objetivo del atacante es el escuchar o monitorizar el tráfico entre nodos, para que, una vez recopilados una serie de datos, en concreto el tamaño de los paquetes y sus tiempos, a través de una serie de herramientas o estadísticas pueda desanonimizar a los usuarios o víctimas.

En este tipo de ataques, son muy frecuentes los falsos positivos y la baja tasa de precisión, por lo que para llevar a cabo uno con un resultado concluyente es necesario ejecutar este ataque de una forma prolongada y continuada en el tiempo, para recopilar el máximo de información posible y poder correlacionar los datos de la forma más precisa posible [18].

A continuación, se pasará a ver cuáles son las principales métricas usadas en los algoritmos de correlación de tráfico:

- **Información Mutua:** Esta métrica mide la dependencia entre dos variables aleatorias. Se puede utilizar para cuantificar la correlación de las características de los flujos. Por ejemplo, las características de tráfico de una comunicación saliente dependen de las características de flujo de su correspondiente entrada (ingreso y egreso de datos). Esta métrica requiere de flujos largos para ser efectiva ya que, necesita reconstruir y comparar las distribuciones empíricas de las características de flujo objetivo [18].

- **Correlación de Pearson:** El coeficiente de correlación de Pearson, es una medida de la correlación lineal entre dos variables continuas o conjuntos de datos. A diferencia de la métrica de Información Mutua, esta no necesita reconstruir la distribución empírica de los flujos a analizar y por lo tanto se puede aplicar en datos de menor tamaño [18,19].

- **Similitud Coseno:** Esta métrica mide la similitud angular de dos variables aleatorias. Cada variable constituye un vector dentro de un espacio, y la métrica determina su similitud basándose en el coseno del ángulo que forman [18,20].

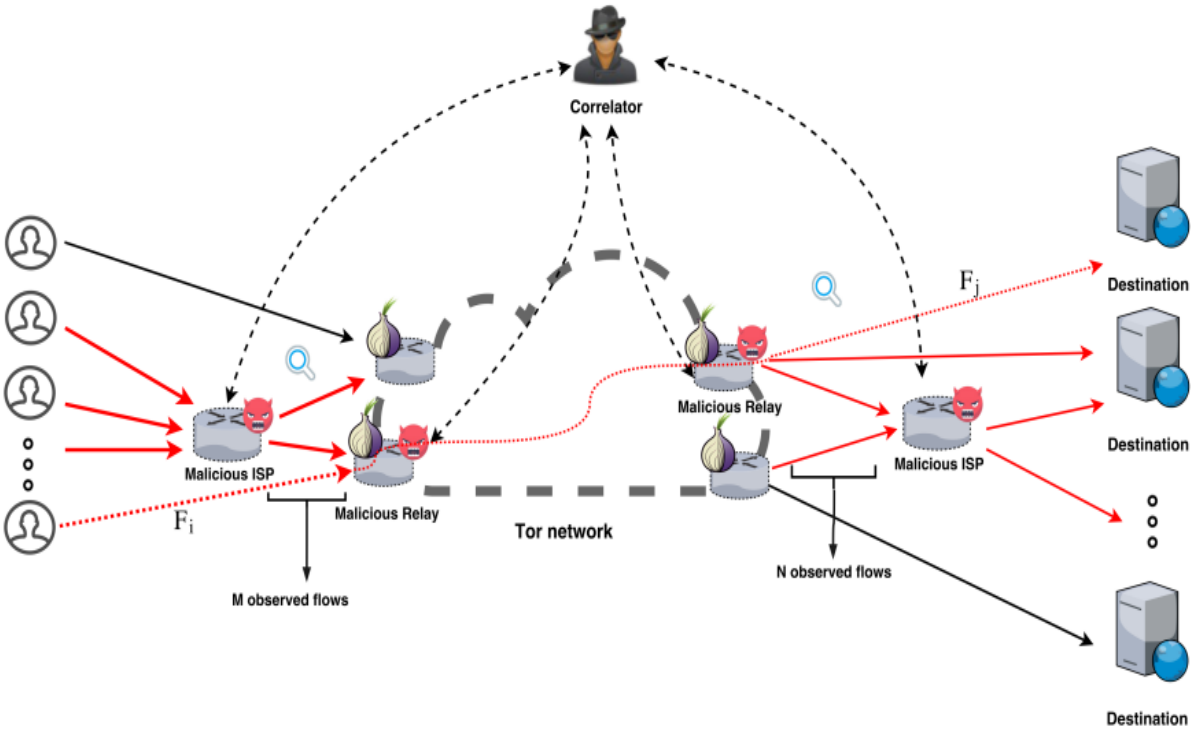
- **Correlación de Spearman:** El coeficiente de correlación de Spearman evalúa la independencia entre dos variables. En una relación independiente, las variables tienden a cambiar a la vez, pero no necesariamente a un ritmo constante. Esta métrica no se centra en los datos sin procesar, sino en los valores jerarquizados de cada variable [18,21].

La correlación de tráfico es el pilar fundamental utilizado en una amplia gama de ataques estudiados contra sistemas de anonimato como Tor. Para llevar a cabo un ataque de este tipo, el atacante necesita interceptar ciertos fragmentos de datos entrantes y salientes de la red de Tor. Si el atacante es capaz de monitorizar el tráfico entrante y saliente de una conexión, aplicando algoritmos de correlación a esos segmentos, sería capaz de desanonimizar a quien está tras esa conexión [18].

Para incrementar las posibilidades de éxito, el atacante deberá incrementar la longitud de los segmentos que es capaz de interceptar, y para ello existen dos formas principales de hacerlo. La primera consiste en que el atacante controle o lance un gran número de nodos bajo su mando, y que grabe las características del tráfico que pasa por ellos. El segundo método es controlar o “pinchar” sistemas autónomos (ASes) o Puntos Neutros (IXPs), y grabar las características de su tráfico que pasa por la red TOR [18].

La Figura 20 muestra un escenario típico de ataques de correlación de tráfico:

Figura 20. Escenario ataques de correlación de tráfico



Extraído de la bibliografía [18].

Este escenario muestra una red, con X flujos de ingreso e Y flujos de salida. La relación entre los flujos no se puede detectar utilizando el contenido de los paquetes debido a su encriptación.

El objetivo del atacante es identificar los pares de flujos asociados, a través de la comparación de datos como el tamaño de los paquetes y sus tiempos, proporcionados por sus nodos maliciosos y sus proveedores de servicios de internet (ISPs) “pinchados”. Una vez cuenta con los datos y usando algoritmos de correlación como los previamente mencionados, el atacante podría desanonimizar la conexión.

6.4.1. Sistema DeepCorr

DeepCorr es un sistema desarrollado por la Universidad de Massachusetts Amherst.

Es un sistema de correlación de tráfico basado en algoritmos de deep learning.

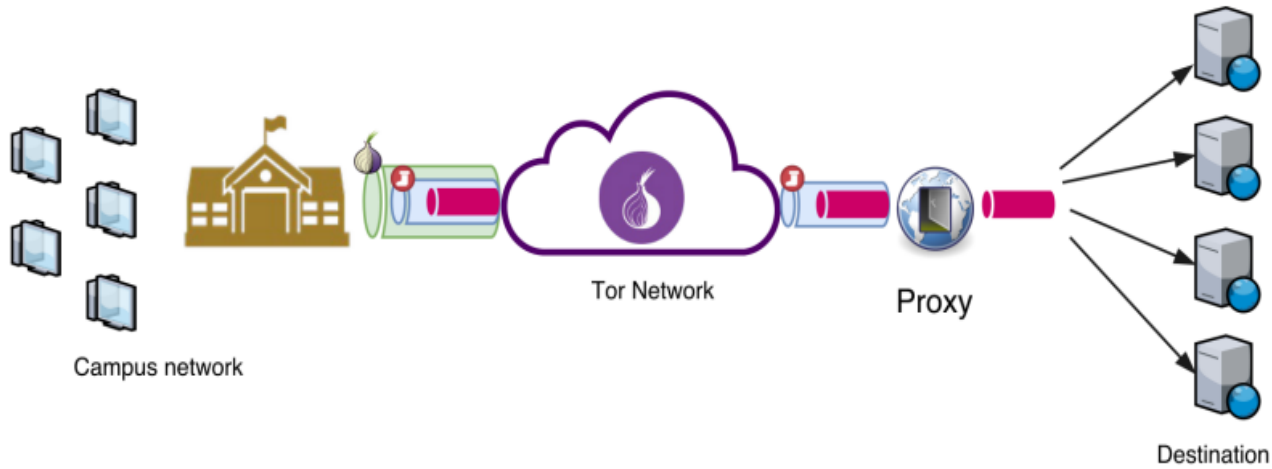
De igual manera que las otras métricas, realiza la correlación de flujos basándose en la información relevante de sus paquetes, tiempos y tamaño. La ventaja de este tipo de algoritmo frente a los convencionales es su capacidad de trabajar con datos no procesados. DeepCorr toma datos no procesados como entrada, y los utiliza para la obtención de características del flujo más complejas [18].

Este sistema utiliza redes neuronales convolucionales (CNN), ya que las características de los flujos de red se pueden transformar en series temporales, y las CNNs son bien conocidas por su rendimiento con series temporales [18].

Según indican sus creadores, entrenan dicho algoritmo usando un gran conjunto de pares de flujos que crearon en TOR, entre los que se encuentran pares asociados y pares que no lo están. (Los que están asociados corresponden a la misma conexión, y los no asociados a conexiones arbitrarias) [18].

A continuación, el modelo usado en sus experimentos:

Figura 21. Modelo usado en experimentos con DeepCorr



Extraído de la bibliografía [18]

Se utilizaron varios clientes de Tor ejecutándose dentro de diferentes máquinas virtuales para generar y recoger el tráfico. Utilizaron Tor para buscar el top 50.000 de webs de Alexa, y capturar los flujos de entrada y salida de dichas conexiones [18].

También se usaron 1.000 circuitos de Tor aleatorios buscando diversos sitios web, con lo que se vio que cada circuito encontraba aproximadamente unos 50 sitios [18].

Recopilaron el tráfico en dos pasos: Primero recopilaron el tráfico durante dos semanas, y después, tras tres meses de inactividad volvieron a recopilar durante un mes, para así comprobar el aprendizaje de su algoritmo [18].

6.5. SEGUIMIENTO ENTRE DISPOSITIVOS. DESANONIMIZACION DE USUARIOS DE TOR MEDIANTE BEACONS SONOROS.

Este tipo de ataque se centra en rastrear a un usuario a través de múltiples dispositivos a la vez. En este caso, esto es posible gracias a balizas o beacons, en concreto a uBeacons, balizas de ultrasonidos.

Las balizas o beacons, son pequeños dispositivos de bajo consumo que están basados en la tecnología Bluetooth. Estos emiten una señal que identifica unívocamente a un dispositivo, esta señal puede ser recibida e interpretada por otros dispositivos, como, por ejemplo, Smartphones, y proporcionan datos como por ejemplo la distancia a la que se encuentran. Esta tecnología se encuentra presente, por ejemplo, en la geolocalización de dispositivos [22].

Las uBeacons, emiten señales de entre 18000Hz y 20000Hz, una frecuencia inaudible para una persona adulta. Estas señales se dividen en trozos más pequeños, de unos 75Hz aproximadamente, y a cada trozo se le asigna una letra del alfabeto. Cada señal tiene una duración aproximada de 4 segundos, y son una codificación de entre 4 y 6 caracteres, donde se incluye el ID de la baliza que se lanza [22].

Estas señales pueden ser interceptadas, por ejemplo, por el asistente de voz de un smartphone, si se encuentran a un rango aproximado de 40 metros desde dónde se emiten [22].

Esta tecnología es muy potente y por ello se le pueden dar diversos usos, en este caso veremos cómo se puede utilizar para desanonimizar usuarios de la red Tor entre otras.

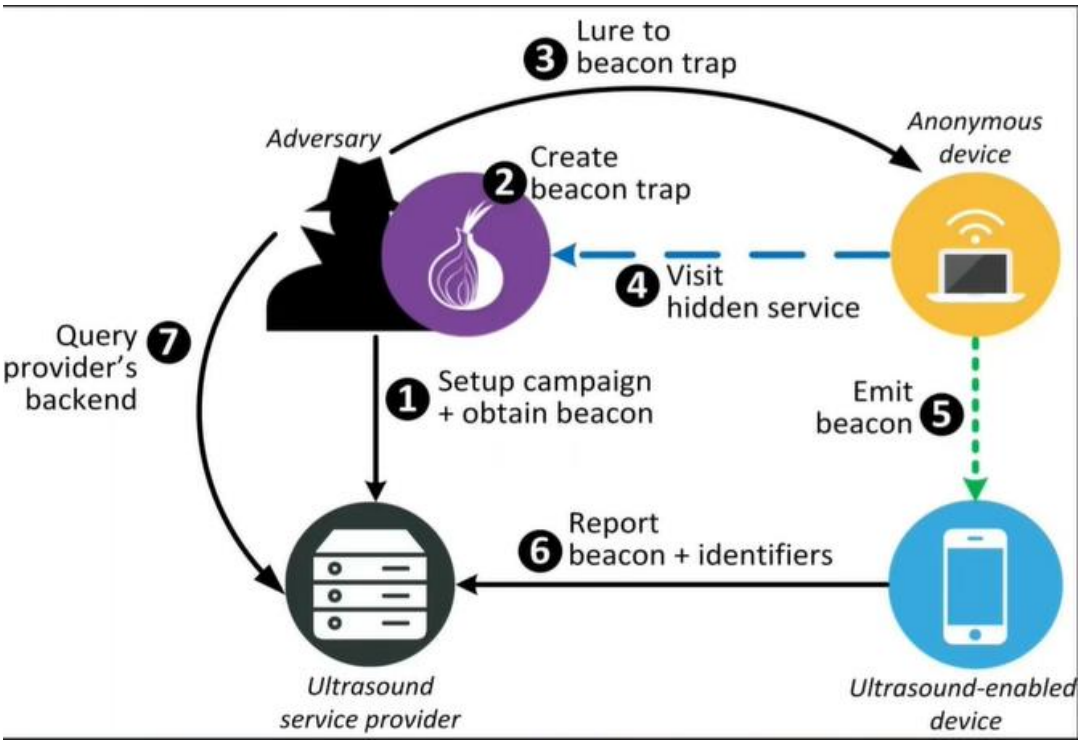
Para ello, es necesario la creación de archivos cebo o portales web trampa, ya que en estos se podría meter dicha baliza sonora. Independientemente de que la víctima tome medidas como usar Whonix —sistema operativo—, si al abrir un sitio o un archivo este reproduce la baliza sonora, pese a que la víctima haya cerrado el sitio, el ataque ya habrá sido lanzado [23].

Si un dispositivo inteligente capta la señal, los datos de transmisión de dicha señal serán traspasados directamente junto con las coordenadas y la dirección IP, aunque también se pueden recibir datos como lista de contactos, SMS, Wifi usados, número de teléfono, etcétera [23].

En la Figura 20 se pueden ver una serie de pasos que el atacante seguiría a la hora de ejecutar este tipo de ataque.

1. En primer lugar, el atacante empieza una campaña para obtener beacons.
2. En segundo lugar, prepara un sitio web con el beacon trampa.
3. A continuación, incita al usuario a visitar dicho sitio.
4. El usuario carga los recursos del sitio, incluyendo el beacon.
5. Se lanza la señal.
6. Si su smartphone cumple los requisitos de tener el framework necesario para captar el beacon, lo captura.
7. El atacante “invoca” al proveedor de servicios de internet que esté usando el smartphone en ese momento y le pregunta por la IP y otros datos como geolocalización.

Figura. 22. Modelo de escenario de ataque con uBeacons



Extraído de la bibliografía [24]

Siguiendo estos pasos el atacante puede identificar al usuario de su sitio trampa e incluso saber dónde vive, con quién habla por el móvil, o su registro SMS [23].

6.5.1. Defensas

Frente a este tipo de ataque la mejor defensa es desconectar los altavoces, a ser posible, a nivel de cable para lograr el máximo anonimato.

También es buena idea apagar los dispositivos inteligentes o usar dispositivos orientados a la seguridad [24].

6.6. TIMING ATTACK.

Este tipo de ataque se centra en gobiernos que buscan cibercriminales que aparecen periódicamente por la red, y que realizan actividades cortas como por ejemplo la transmisión de datos.

Para poder llevar a cabo este ataque, se necesita disponer de programas que registren y rastreen los inicios y cierres de sesión de usuarios. Una vez se lleve unos días realizando el seguimiento de la víctima, se pasará a usar los sistemas OSA (actividades de búsqueda operativa). Dichos sistemas de espionaje están a disposición de la mayoría de los países, en el caso de Rusia, el sistema usado es el SORM [25].

En el supuesto caso de saber que el ciberdelincuente se encuentra en España, por ejemplo, se necesitaría averiguar qué y cuántos usuarios se han conectado a la red Tor en ese país y por cuánto tiempo.

Una vez extraídos los datos de su última conexión y de su última desconexión, se podría sacar el número de usuarios conectados y desconectados a Tor en España en el mismo rango horario que el objetivo.

Tras varias veces de realizar el mismo análisis, el círculo se irá estrechando y por tanto seríamos capaces de detectar el lugar de acceso a la red del ciberdelincuente [25].

Cabe destacar que cuanto más frecuente sea el acceso y cuanto menor sea el número de usuarios en ese momento, el ataque será más rápido.

6.6.1. Defensas

Un método efectivo contra este ataque es el cambiar de punto de acceso a internet desde el que te conectas con cierta frecuencia, y de esta forma “marear” al analista de datos, para que de esta forma sea más difícil ubicarte [25].

Difícil pero no imposible ya que de igual manera sería posible triangular tu posición y de esa forma estrechar el área de búsqueda.

7. CONCLUSIONES

La red es un lugar inmenso que ofrece una infinita variedad de contenidos. No todos esos contenidos están al alcance de un usuario estándar ya que, mucho no está indexado por los buscadores convencionales o es contenido al que no es legal tener acceso, como por ejemplo sitios relacionados con actividades terroristas, cibermercados negros, etcétera.

A este contenido se puede acceder a través de herramientas como Tor, quienes además de darte acceso, protegen tu identidad. Si bien Tor garantiza un alto grado de anonimato, este no es absoluto ya que, como se ha visto, existen varios métodos para identificar a los usuarios que utilizan las diversas redes de anonimato.

Estas técnicas son ejecutables por cualquier usuario con un cierto nivel de conocimientos técnicos, aunque al llevar a la práctica uno de los ataques en un entorno controlado, es cierto que algunos son bastante sencillos ya que existen herramientas que se encargan de la parte técnica del ataque. Es por esto que hay ataques a medida para cada ciberdelincuente, ya tenga un mayor o menor nivel de conocimientos técnicos, y dichos ataques pueden ser utilizados por estos ciberdelincuentes en beneficio propio. Por razones como esta también es bueno saber cómo defenderse de las mismas o minimizar los riesgos al navegar por redes de anonimato.

Conocer estas técnicas de desanonimización podría ser de utilidad a las fuerzas de seguridad para poder poner a disposición judicial a aquellos que realizan un uso indebido de este tipo de herramientas.

También para personas que utilicen dichas redes de anonimato, con fines lícitos, para que sepan como poder defenderse de posibles ataques y hacer que la utilización de herramientas como Tor sea segura para ellos.

8. BIBLIOGRAFÍA

[1] G.Owen, N.Savage, “Empirical Analysis of Tor Hidden Services”, IET Information Security, Vol. 10, pp. 113-118, Septiembre 2015, Disponible: https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/iet-ifs.2015.0121

[2] Tor Project, “Historia”, Disponible: https://www.torproject.org/es/about/history/

[3] J. S. Hernández Cuenca, “Red de anonimización Tor y cibermercados negros”, Trabajo de Fin de Máster, Universidad Oberta de Cataluña, Barcelona, diciembre 2018, Disponible: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/91329/6/jshernandezcTFM0119memoria.pdf

[4] Universidad Veracruzana, “Conocimientos Generales Tor”, Disponible: https://www.uv.mx/infosegura/general/conocimientos_tor-3/

[5] R.Silva, “Así funciona Tor”, El País, Junio 2014, Disponible: https://elpais.com/elpais/2014/06/06/media/1402080096_135619.html

[6] Wikipedia, “Tor (red de anonimato)”, Disponible: https://es.wikipedia.org/wiki/Tor_(red_de_anonimato)

[7] Derechos digitales, “Torifícate”, Disponible: https://tor.derechosdigitales.org/torificate/p1.3/

[8] Cloud Center Andalucía, “Deep Web y Dark Web: qué son y principales diferencias”, Disponible: https://www.cloudcenterandalucia.es/blog/deep-web-dark-web-que-son-y-principales-diferencias/

[9] Centribal, “Diferencia entre Deep Web, Dark Web y Surface Web”, Disponible: https://centribal.com/es/diferencia-entre-deep-web-dark-web-y-surface-web/

[10] R.Jansen, F. Tschorsch, A. Johnson, B. Scheuermann,”The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network”, en NDSS Symposium 2014, Disponible: https://www.ndss-symposium.org/wp-content/uploads/2017/09/05_4_0.pdf

[11] Tor Project, “New Tor Denial of Service Attacks and Defenses”, Disponible: https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses/

[12] Cyber Yoth, “Internet privacy and security course”, cap. 73, Disponible: https://book.cyberyozh.com/deanonymization-tor-users-through-bait-files/

[13] Whonix, “Why does Whonix uses Tor”, Disponible: https://www.whonix.org/wiki/Why_does_Whonix_use_Tor

[14] FBI, “‘PlayPen’ Creator Sentenced to 30 years”, Disponible: https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

[15] Derecho de la Red, “TorBot - Herramienta de OSINT para la Dark Web”, Disponible: https://derechodelared.com/torbot-herramienta-osint-dark-web/

[16] TorProject, “Se supone que tengo que editar mi “torrc”. ¿Qué significa esto?, Disponible: https://support.torproject.org/es/tbb/tbb-editing-torrc/

[17] P. S. Narayanan, R. Ani, A. T. L. King, “Inventive Communication and Computational Technologies”, Lecture Notes in Networks and Systems book series, vol. 89, pp. 187-195, Enero 2020.

[18] M. Nasr, A. Bahramali, A. Houmansadr, “DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning”, en ACM SIGSAC Conference on Computer and Communications Security (CCS ’18), Octubre 15–19, 2018, Toronto, ON, Canada, pp. 1962-1976, Disponible: https://dl.acm.org/doi/pdf/10.1145/3243734.3243824

[19] Kent State University, “SPSS Tutorials: Pearson Correlation”, Disponible: https://libguides.library.kent.edu/SPSS/PearsonCorr

[20] Graph Everywhere, “Algoritmo de similitude coseno”, Disponible: https://www.grapheverywhere.com/algoritmo-de-similitud-de-coseno/

[21] MiniTab, “Una comparación de los métodos de correlación de Pearson y Spearman”, Disponible: https://support.minitab.com/es-mx/minitab/18/help-and-how-to/statistics/basic-statistics/supporting-topics/correlation-and-covariance/a-comparison-of-the-pearson-and-spearman-correlation-methods/

[22] The Valley, “Qué son los Beacons y cuál es su potencial”, Disponible: https://thevalley.es/blog/que-son-los-beacons-y-cual-es-su-potencial/

[23] Cyber Yoth, “Internet privacy and security course”, cap. 69, Disponible: https://book.cyberyozh.com/cross-device-tracking-deanonymization-users-tor-vpn-proxy-using-sound-beacons/

[24] Media CCC, “Talking Behind Your Back. On the Privacy & Security of the Ultrasound Tracking Ecosystem”, en 33C3: Works for me, 2016, Disponible: https://media.ccc.de/v/33c3-8336-talking_behind_your_back#t=1449

[25] Cyber Yoth, “Internet privacy and security course”, cap. 70, Disponible: https://book.cyberyozh.com/timing-attack-how-special-services-deanonymize-users-messengers/