PALABRAS CLAVE / KEY WORDS

Tor / Delito informático / Redes informáticas / Tecnología.

Tor / Computer crime / Computer networks / Technology.

RESUMEN / ABSTRACT

La red Tor es un lugar dentro de internet del que se ha hablado mucho. Con este artículo pretendemos hacer una explicación accesible y detallada de su funcionamiento indicando por qué es tan empleada, segura, pero como todo sistema no es infalible.

Como veremos a continuación desmitificaremos los usos principales de la red Tor y también recogeremos algunos de los servicios ilícitos que podemos encontrar dentro de la misma.

The Tor network is a place within the internet that has given plenty to talked about. With this article we intend to make an accessible and detailed explanation of its operation indicating why it is so used, safe, but like any system is not infallible.

As we will see below, we will demystify the main uses of the Tor network and we will also collect some of the illicit services that we can find within it.

Comencemos diferenciando entre la *Deep Web* y la *Dark Web*. Mientras que la *Deep Web* es todo aquel contenido de las bases de datos y otros servicios web que por una razón u otra no se encuentran indexados, es decir accesibles desde los motores de búsqueda convencionales, la *Dark Web* es la cifrada en los servidores Tor. Ni la web profunda ni la oscura pueden ser indexadas, pero siendo un poco más técnico, los portales que engloba la *Dark Web* son los sitios que utilizan el protocolo de servicio conocido como *Tor Hidden*, es decir, es una colección de sitios web que son públicamente visibles, pero ocultan las direcciones IP de los servidores en los que están alojados. Esto hace que puedan ser visitados por cualquier usuario de la red, sin embargo, dificulta mucho ver quién está tras los sitios. Casi todos los sitios de la llamada *Dark Web* camuflan su identidad utilizando la herramienta de cifrado de Tor.

El 20 de septiembre de 2002 nació este ambicioso proyecto por Roger Dingledine, Nick Mathewson y Paul Syverson, que había sido financiado por el Laboratorio de Investigación Naval de los Estados Unidos para finalmente pasar a ser patrocinado al año siguiente por la *Electronic Frontier Foundation* (organización de defensa de libertades civiles en el mundo digital) hasta el año 2005. Actualmente el proyecto Tor se encuentra en manos de *The Tor Project* como una organización sin ánimo de lucro orientada a la investigación y a la educación desde Massachusetts liderado por Roger Dingline.

Su principal objetivo era utilizar las conexiones entre ordenadores y variar las rutas de los mismos para poder proteger la identidad de los usuarios y que así no se pueda analizar la información que envía un usuario para poder llegar hasta él, es decir, hasta su IP. Su uso más habitual es que sea utilizado para lograr el mayor grado de privacidad posible durante la navegación web en internet, sin embargo, sin estar diseñado para ello, se descubrió que dificulta considerablemente la labor a determinados programas que censuran o vigilan el acceso que se realiza a cierto tipo de contenido.

Pero, ¿cómo funciona la red Tor, también conocida como "enrutado cebolla"? A diferencia del modelo de enrutado que seguimos tradicionalmente para conectarnos a internet que es directo (el cual obviamente es el más rápido) el sistema *onion routing*, que como hemos visto fue diseñado de cara a proteger las informaciones de la marina, cambia su enrutamiento para tratar de garantizar tanto la privacidad de la información como el anonimato. El enrutado tradicional sigue un orden muy sencillo, ordenador, router, enrutador ISP (router de nuestro proveedor de internet) y servidor del lugar al que queremos acceder. Mientras que el enrutado *onion* no solo pasa por varios nodos (puntos de intersección, conexión o unión de

varios elementos informáticos) aleatorios, también cifra por capas de forma asimétrica todos y cada uno de los router por los que pasa, es decir que, si pasa por tres router, solo el "router a" podrá descodificar el cifrado del "router b" y solo el "router b" podrá descodificar el "router c". El proceso se repite hasta que acabe hasta el último nodo, esto no hace al sistema infalible. Hay formas como el analizado de tiempos, es decir si el "ordenador A" ha enviado el paquete de datos a las 17:19:05:3:120

más tarde el "ordenador B" recibe otro paquete y se repite el patrón de la latencia más veces, la probabilidad de que el "ordenador A" esté conectado con el "ordenador B" aumenta. Es necesario, del mismo modo, que el nodo final sea el único capaz de leer el paquete de datos, por lo que hay que cifrar el mensaje original. No obstante, es cierto que las redes Tor son de las que a día de hoy más pueden garantizar un nivel extremadamente alto de privacidad.

Podemos concluir que Tor es un *software* que implementa el "enrutado cebolla" para el usuario básico, instalándolo en un ordenador, se enlaza a un proxy local (ordenador que interactúa como intermediario entre otros dos). Lo que hace peculiar al servidor proxy de Tor es su enrutado a través de la red Tor, utilizando este como una puerta de acceso anónima desde la que podemos realizar un acceso desde cualquier programa de ordenador que soporte proxy's. Pero no estaremos completamente en el anonimato, si el programa que empleamos utiliza nuestra IP en los datos que envía, siendo así todo el cifrado que realicemos no habrá valido para nada, por tanto, el proyecto Tor recomienda el uso del navegador Tor, debido a que este navegador ya viene preparado para no enviar absolutamente ningún dato de identificación.

QUIÉN EMPLEA LA RED TOR

La red Tor es utilizada en todo el mundo por gente que necesita

Tor es un software que implementa el "enrutado cebolla" para el usuario básico, instalándolo en un ordenador.

tener comunicaciones seguras incluyendo periodistas que hablan con sus fuentes que desean permanecer en el anonimato hasta activistas que son perseguidos por sus países como contrarios al régimen, voluntarios de ONG e incluso usuarios que desean acceder a servidores bloqueados por su ISP o gobierno.

La red es también empleada para servicios ocultos. Se trata de un servicio que crea varios puntos de introducción en múltiples nodos de red notificando a una base de datos qué nodos son. Cuando el cliente en cuestión quiere conectarse a uno de esos nodos la dirección es un punto de encuentro estando conectado con una clave única, estableciéndose de esta forma una conexión entre el cliente y el servicio.

Planteados de esta forma los servicios ocultos permiten conectarnos a correos y chats sin tener en cuenta el conocimiento exacto de su dirección, empleando para ello intermediarios y circuitos Tor totalmente anónimos. Siendo así prácticamente imposible rastrear quién fue el emisor del correo, ya que ni siquiera el propio servidor del correo sabe el ordenador con el que estaba comunicándose.

DELITOS EN LA *DEEP WEB*

Cualquier herramienta, al igual que un cuchillo de cocina se utiliza para cocinar pero se le puede dar mal uso para apuñalar a alguien, la red Tor se emplea, aunque no en su mayoría, para cometer numerosos ilícitos. Entre los más graves que se pueden encontrar tras una profunda investigación, enumeramos los siguientes.

El contrato de sicarios está a la orden del día, no es fácil encontrarlos ya que, según numerosos foros en los que se comparten opiniones y experiencias con otros internautas, la gran mayoría son falsos, pero el hecho es que hay un gran conjunto que ofrece los mas variopintos servicios. Suelen pertenecer a Europa y Asia central (los que se pueden confirmar como auténticos, ya que como cualquier comercio en la red existen vetos, comentarios y demás publicaciones que aseveran la veracidad de su “oficio”), suelen estar definidos tanto por méritos como por sus objetivos, fiabilidad y su consecuente variación del precio. Por regla general, este varía en función de las condiciones sociales y capacidades del individuo, es decir, en caso de contratar el asesinato de un político o jefe de una gran empresa, o por otro lado, una persona con una formación militar amplia, el precio se disparará. Hay que indicar que muy pocos de estos asesinos han sido descubiertos. El caso más famoso que se ha revelado a la información pública fue el francés de iniciales A.J., arrestado en Bulgaria, que ofrecía sus servicios en la *Deep Web* para acabar siendo rastreado por la Interpol. El resultado fue su puesta en libertad por falta de pruebas debido a la inconexión de su persona con los asesinatos. Comentarios en numerosos foros hacen pensar que los asesinos más eficaces y reales solo actúan por re-

comendación de alguien que ha sido cliente.

También existen páginas virtuales que muestran vídeos de contenido gore, de hecho hay foros para que todo tipo de gente comparta vídeos de asesinatos. Uno de los más famosos que existieron llevaba por título "Tres hombres y un martillo" (*Three guys and one hammer*), de los *Maniacos de Dnepropetrovsk*. Las grabaciones que surgieron del fondo de la *Deep web* en 2007 fueron llevadas en poco tiempo a la superficie. En el vídeo se observa cómo Viktor e Igor Sayenko Suprunyuck, durante unos siete minutos golpean repetidamente a un anciano con un martillo para terminar perforándolo finalmente con un destornillador. Ambos fueron arrestados y condenados a cadena perpetua en 2009. Existen numerosos casos similares, como la pornografía italiana, en las cuales las mujeres son escalpadas con vida.

Entre todos los vídeos que pueden encontrarse, sin duda el más deleznable es la pornografía infantil. Es más frecuente de lo que debería, encontrar enlaces a páginas sin la más mínima estructura en la que se puede hallar este tipo de pornografía que, al menos dentro de los chats que los contienen, llenos de comentarios de desaprobación e insultos al creador del sitio, hace que al menos se tenga la esperanza de que, aunque existen esos monstruos, no es el grueso de usuarios de la *Deep web*.

Hace casi diez años el director Tom Six, conocido por ser el impulsor de programas como *Gran Hermano*, creó lo que se ha conocido durante mucho tiempo como la película de terror más grotesca jamás creada *El ciempiés humano* (*Human Centipede*). Su argumento, un médico alemán secuestra tres turistas a los cuales une quirúrgicamente de la boca al ano creando así el ciempiés humano. Tras el éxito de la operación comienza a entrenarlo. Esto tan solo es una película, pero la realidad una vez más enmudece ante los experimentos que se pueden encontrar en este lugar, foros de intercambio de informes de experimentos realizados con seres humanos que incluso carecen de sentido como la implantación de las piernas de una cabra en un ser humano. Normalmente afirman que estos experimentos son realizados en beneficio de la ciencia y solo utilizando como sujetos de prueba a mendigos tratando de reducir su culpabilidad. Se denota en sus comentarios en los foros sus elevados conocimientos en medicina, así como la gran seguridad que tienen funcionando bajo una vigilancia masiva ya que, ante el más mínimo indicio de seguimiento, el sitio es completamente eliminado y borrado. Estos sitios no suelen estar en funcionamiento más de 24 horas, lo que no hace más que demostrar la inversión realizada, así como una estructura y organización durante estas acciones.

La realidad una vez más enmudece ante los experimentos que se pueden encontrar en este lugar, foros de intercambio de informes de experimentos realizados con seres humanos que incluso carecen de sentido.

Durante el año 2003 en Alemania se editó una noticia que conmocionó al mundo. Un caníbal confesó ante un tribunal ha-

ber sido el autor de la muerte y posteriormente haber comido a una persona a petición de la propia víctima. Conocido como *el caníbal de Rothenburg* indicó que conoció a la víctima por internet. La investigación de los organismos policiales de Alemania llegó a una serie de foros de la *Deep web* cuyo tema era el canibalismo. Estas páginas fueron utilizadas y siguen existiendo ejemplos de este tipo en las cuales se encuentran vídeos, fotos y testimonios, tanto de los propios caníbales como de sus víctimas, quienes de una forma totalmente voluntaria se prestan a ser comidas por estos primeros.

Uno de los negocios más perturbadores que se pueden encontrar sin duda en esta red son las conocidas como esclavas sexuales que son convertidas en muñecas. Jamás se ha conseguido encontrar ningún fabricante ni su origen, no solo porque sus transacciones se realicen en bitcoins sino por el excesivo recelo con el que se realizan. A diferencia de otros lugares de la *Deep web*, los comentarios en el foro y en los chats son mínimos, escasas entradas, no se aprecia un número que pudiéramos considerar normal o en la media del resto de páginas que existen dentro de la *Dark web*, esto puede ser simplemente porque es un negocio que de por sí, causa pánico al oír de qué se trata. Por una determinada cantidad a los niños se les transforma en *Doll Maker*, niños entre los 8 y 10 años comprados en países de pobreza extrema, para posteriormente, en centros clandestinos de cirugía, transformarlos en simples muñecos que no pueden presentar resistencia alguna a las perversiones de sus compradores. Sus extremidades son amputadas y sustituidas por implantes de silicona, al igual que sus dientes, que se cambian por piezas de goma tras una extirpación de sus cuerdas vocales. El proceso en sí visto como intervención quirúrgica debe durar semanas y solo se realiza una vez que la muñeca ha sido encargada. Dependiendo de las características el precio puede oscilar en una horquilla entre 40.000 y 700.000$. Este "producto" se entrega con un manual que indica cómo alimentar y llevar a cabo otros tipos de mantenimientos para la supervivencia básica, pues se convierten en un objeto completamente dependiente del comprador. Este caso surgió a la luz de la parte más oscura de la *Dark web* a foros más en la superficie mediante una historia llamada "Juguetes Lolita: esclavas sexuales". Un miembro anónimo del sitio 4chan, lo destapó publicando la dirección y la forma de contactar con el creador. Con el aumento del número de visitas, el autor que respondía al alias *Pussymonster* prefirió des-

mantelar su sitio web mostrando una limpieza y un trabajo con una habilidad tal que fue imposible seguir su rastro de ninguna manera.

EL MERCADO NEGRO

A pesar de todas las cosas escabrosas mencionadas antes, lo cierto es que la mayor parte del mercado de la *Dark web* son simplemente productos tales como armas o drogas. La posibilidad de encontrar drogas ilegagales es de lo más variada pues se ven desde tabaco de contrabando hasta heroína, pasando por cocaína y cannabis entre otros. Existe para este cometido uno de los buscadores más famosos de la *Deep web*, conocido como Grams, con una interfaz muy similar a la de Google. Uno de los mercados con mayor relevancia ha sido Agora, el más completo y concurrido desde la caída de Silk Road en 2013, tras la detención de su líder, Ross Ulbricht. Sin embargo, este nicho de mercado fue cubierto rápidamente tanto por Agora como por otros cientos de páginas. El estado de los servidores es muy variable, sobre todo por las cuestiones de cifrado y en función de las entradas y compras que reciban, es muy complicado mantener una estabilidad de servicio en estas condiciones. Su método de compra no varía de unas páginas a otras, el vendedor expone fotografías de sus productos y el precio, y en función de la convicción que se muestre en comentarios por compras previas de otros usuarios, se ve el nivel de fiabilidad de la página, incluso existen aquellos en lo que se miden por un nivel de estrellas como se utilizan en otros lugares de internet.

Otro negocio en auge son las cuentas robadas, los robos de tarjetas de crédito e incluso credenciales de videojuegos, todos funcionan de una forma similar.

Existen numerosos lugares donde ciudadanos ilegales en el lugar en que residen pueden obtener tanto pasaportes como otros documentos falsificados, cuya validez es difícil comprobar hasta una vez adquirido el producto en cuestión, así que puede tratarse de un simple *scam* (término con el que se conoce este tipo de estafas en jerga informática). Uno de los que más visitas recibe es FakeID con una gran lista de precios, productos y packs de varios documentos, como DNI, pasaporte, carné de conducir… por ejemplo el pasaporte español tiene un precio de 550€ hasta un pack por 900€ con el que obtener todos los documentos como ciudadano americano.

Otro negocio en auge son las cuentas robadas, los robos de tarjetas de crédito, venta de armas e incluso credenciales de videojuegos, todos funcionan de una forma similar.

Podemos concluir, por tanto, que la *Deep web* no es un sitio en el que el grueso de sus páginas sean para cometer irregularidades, pero que sin embargo los que hay son los más graves que se pueden hallar, pero no dejan de ser más que unas pocas manzanas podridas en una cesta de increíble tamaño. ■

BIBLIOGRAFÍA

Manual Tor Browser
The Hidden Wiki
Torchan
Silk-Road
https://www.torproject.org/
https://www.genbeta.com/