DARK WEB IN TEN MINUTES

Una guía rápida sobre cómo mantenerse anónimo usando la red TOR



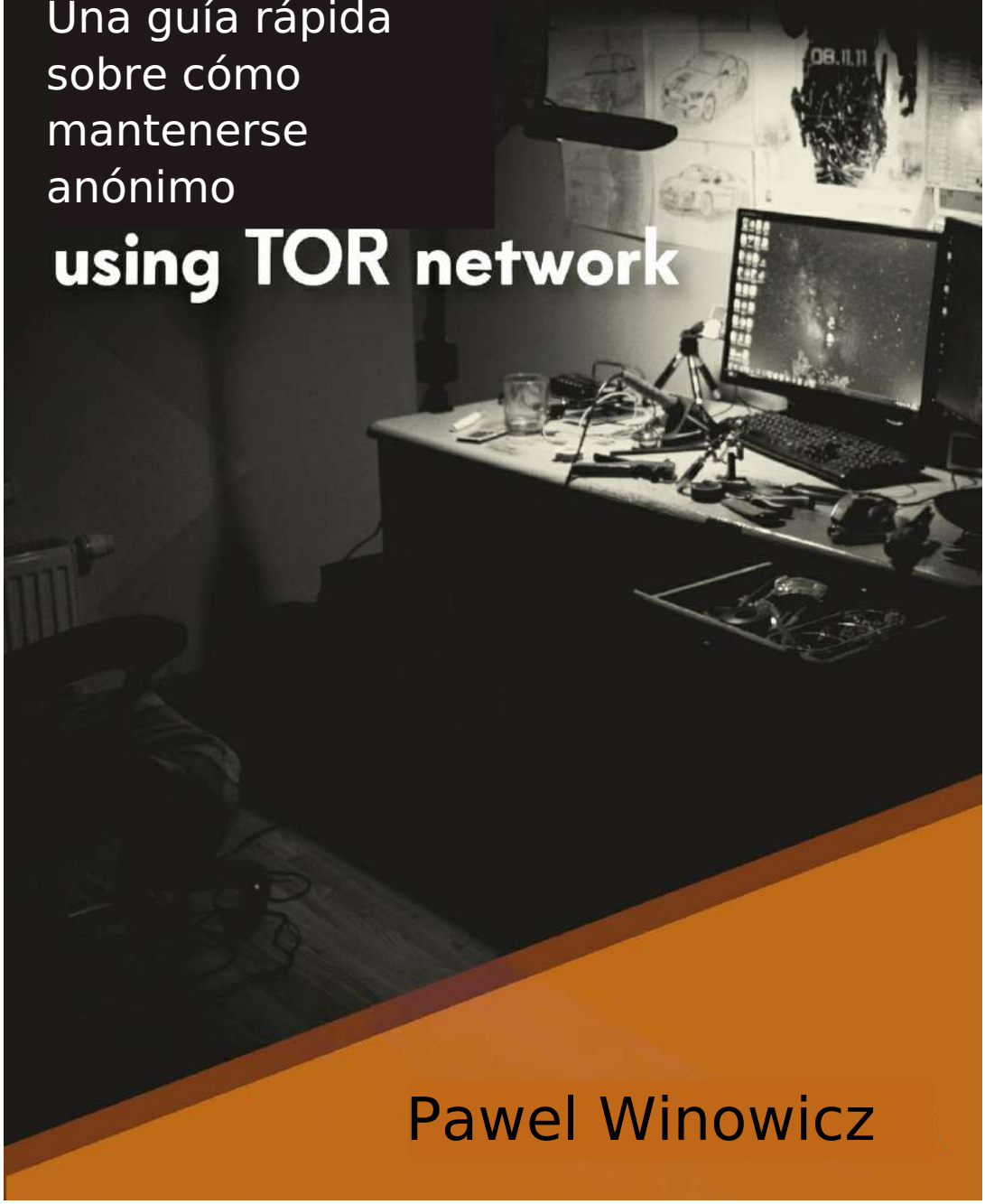
Pawel Winowicz

LA RED OSCURA

IN DIEZ MINUTES

Una guía rápida sobre cómo mantenerse anónimo

using TOR network



Pawel Winowicz

DARK WEB EN 10 MINUTOS

UNA GUÍA RÁPIDA PARA SER ANÓNIMO USANDO TOR RED

por Paweł Winowicz

Autor libro Dark Web en 10 minutos Una guía rápida sobre cómo permanecer anónimo usando la red TOR © 2020, Paweł Winowicz Autoeditado theselfpublisher@zohomail.eu

Todos los derechos reservados. Ninguna parte de esta publicación puede reproducirse, almacenarse en un sistema de recuperación, almacenarse en una base de datos y / o publicada en cualquier forma o por cualquier medio, electrónico, mecánico, fotocopiado, grabación o de cualquier otra manera, sin el permiso previo por escrito del editor.

Esta guía no pretende fomentar actividades ilegales en Internet, sino concienciar a los usuarios sobre cómo pueden proteger su privacidad. No me hago responsable de ninguna acción inmoral o ilegal tomada por mis lectores.

INTRODUCCIÓN

Para empezar, me gustaría plantear algunos temas básicos relacionados con la Dark Web, que aparecerán con frecuencia en este libro. Antes de comenzar la práctica, vale la pena aprender un poco de teoría para entender mejor los principios que

rigen esta capa mística de Internet.

RED INFORMÁTICA PROFUNDA Y DARK WEB, ¿QUÉ SON?

Antes de pasar a discutir qué es un navegador TOR, cómo usarlo y cómo llegar a las capas más profundas de Internet con él, necesitamos entender exactamente qué es la Deep Web y la Dark Web. Estos dos conceptos suelen

estar
confundidos.

¿Qué es la Deep Web?

En pocas palabras, es una capa de Internet a la que no podemos acceder desde un normal navegador, o necesitamos los permisos apropiados para hacerlo.

Las cosas que oculta este rincón de Internet incluyen bases de datos gubernamentales, informes médicos, información sobre usuarios de varios sitios web,

contenido de la nube, videos privados en YouTube, etc.

La mayoría de las estadísticas muestran que el usuario promedio de Internet puede acceder a solo el 4% de la información contenida en Internet. Toda la red a menudo se compara con una gran glaciar, donde solo una parte sobresale por encima del océano

superficie. En este caso, el océano es la Deep Web.

¿Qué es Dark Web? La Dark Web es una pequeña parte de la Deep Web, de tamaño comparable a la superficie Web. Las páginas de la Dark Web están diseñadas para que los usuarios puedan acceder a ellas. Sin embargo, se necesitan herramientas especiales como el navegador TOR para ello. La mayoría de la información que podemos encontrar sobre esta capa son informes de su naturaleza criminal. Pero no es cierto que la Dark Web solo sea utilizada por delincuentes. Muchos de los usuarios que encontramos aquí simplemente valoran su privacidad y, por alguna razón, quieren ocultar su identidad al mundo.

No olvidemos que los gobiernos de algunos países son opresivos con sus ciudadanos y limitan su libertad de expresión en Internet. En este caso, usar la Dark Web puede ser la única forma de sortear la censura.

En la Dark Web podemos encontrar foros que agrupan a muchos activistas de los derechos humanos. y defensores de países donde se violan esos derechos.

Crimen y Dark Web

El navegador TOR, requerido para navegar esta parte de Internet, garantiza anonimia y una sólida protección de nuestra privacidad. Esto crea condiciones ideales para el desarrollo del crimen. Podemos encontrar muchos sitios que ofrecen mercaderías ilegales, desde drogas, armas o tarjetas de crédito robadas hasta pasaportes falsos, tarjetas de identidad y licencias. Aunque algunos vendedores cumplen el contrato y envían lo pedido, la mayoría de los sitios están gestionados por estafadores. La forma de pago preferida en la Dark Web es Bitcoin, lo que da al criminal una mayor certeza de que no descubriremos quién es y de dónde viene.

Las transacciones de BitCoin son completamente anónimas y la conexión entre cliente y vendedor está efectivamente encriptada. Sumando el hecho de que intentamos comprar mercancías ilegales, se facilita aún más engañarnos. No iremos a la policía y no diremos: - Sr. Policía, quería comprarme un paquete de cannabis y un pasaporte falso, pero me defraudaron. Incluso si intentamos comprar algo perfectamente legal allí, no podemos estar seguros de que el vendedor.

será honesto. El mejor consejo que puedo darte es abandonar cualquier transacción.

mientras estás en la Dark Web.

NAVEGADOR TOR

TOR (The Onion Router) es un navegador gratuito y de código abierto diseñado para la comunicación anónima y sin censura. El nombre TOR proviene del enrutamiento de cebolla desarrollado por dos empleados del Laboratorio de Investigación Naval de EE.UU. El objetivo era proteger las comunicaciones de las agencias gubernamentales estadounidenses. El desarrollo posterior del enrutamiento de cebolla fue asumido por DARPA (Defense Advanced Research Project Agency) en 1997, implementándolo para el uso del Ejército de EE.UU. Las primeras versiones del navegador basadas en el enrutamiento de cebolla se lanzaron en 2002. En 2004, el código de TOR fue entregado bajo una licencia libre a Roger

Dingledine y Nick Mathewson, quienes continuaron desarrollando el proyecto TOR.

¿TOR ofrece anonimato total?

Sí, siempre y cuando hagamos todo lo posible por no revelar nuestra identidad ni el dispositivo que estamos usando. Cualquier revelación de usuarios de TOR resulta de su descuido o

ignorancia. Solo basta con abrir el archivo descargado de la Dark Web a través de un navegador diferente a TOR y nuestra ubicación real ya no es anónima.

Configuración de seguridad

El navegador TOR ofrece tres niveles de protección para el usuario: estándar, más seguro y el más seguro.

1. Estándar: todas las funciones del navegador y de los sitios web están habilitadas, esto garantiza la funcionalidad completa de los sitios web. Utilice la configuración estándar solo

al navegar por sitios conocidos y de confianza. 2. Más seguro: desactiva funciones potencialmente peligrosas de los sitios web. Algunas fuentes o símbolos pueden no funcionar correctamente y los contenidos multimedia como clips de audio y video solo se inician con un clic. Además, los scripts de Java están desactivados en todas las páginas que no sean HTPS. 3. El más seguro: permite que los sitios web utilicen solo sus funciones básicas. Los scripts en todas las páginas, incluso las que tienen protocolo HTTPS, no se inician. Muchas páginas serán

no funcionales en este modo.

ENVÍO EN CEBOLLA

Este nombre se deriva de la forma en que los datos se transmiten a través de la red TOR. En la red de cebollas, los mensajes se envían con capas de cifrado, similar a las capas de la cebolla. El paquete de información enviado por el usuario no llega directamente al destinatario. Este paquete debe viajar a través de varios ordenadores seleccionados al azar en la red. Los datos se cifran inicialmente y luego se envían a través de una serie de nodos de la red llamados routers de cebolla. El remitente de la información durante una llamada de este tipo permanece anónimo porque cada intermediario solo conoce la ubicación de los nodos anteriores y siguientes. Hay información más detallada disponible en el sitio web oficial del proyecto TOR

https://www.torproject.org/

TAILS - EL SISTEMA OPERATIVO CREADO PARA

LA PRIVACIDAD

Tails es un sistema operativo gratuito, de código abierto y en tiempo real, enfocado en proteger la privacidad de sus usuarios. ¿Qué es un sistema en vivo? Es un sistema operativo que funciona directamente desde una memoria USB o CD/DVD y se carga en la RAM del ordenador. Dicho sistema no utiliza disco duro y, por lo tanto, no tiene conexión con los datos almacenados en nuestro ordenador. Cuando apagas dicho sistema, todos los archivos temporales, contraseñas guardadas, cookies y cualquier otra cosa que pueda dejar rastro en

nosotros se eliminan.

En el caso de Tails, el espacio vacío restante en la memoria USB se utiliza como espacio de disco. Esto nos permite guardar archivos, por ejemplo presentaciones o imágenes creadas con el software incluido. Tails nos permite elegir qué archivos o configuraciones de programas son importantes para nosotros y los guarda en un espacio cifrado, por lo que no tenemos que preocuparnos por perderlos. Todos los demás datos se eliminan cuando el

sistema se apaga, de modo que no quedan rastros.

¿Qué es exactamente Tails?

Tails es un sistema operativo muy sencillo, completamente funcional y seguro. Tiene un navegador TOR integrado, correo electrónico Thunderbird que cifra los mensajes que enviamos, LibreOffice, programas de gráficos como GIMP e InkScape, y la aplicación OnionShare con la que podemos compartir archivos y carpetas en la red TOR. Además, aquí encontrarás todas las herramientas como un calendario,

Calculadora, bloc de notas y muchos otros. El navegador incorporado nos ofrece varios complementos que se pueden activar en cualquier momento y configurarse libremente.

NoScript es una extensión que, cuando se activa, bloquea cualquier script que se inicie al abrir la página. Estos pueden ser animaciones, sonidos, anuncios que dirigen a sitios externos, enlaces infectados con malware o archivos de seguimiento. Sin embargo, muchos sitios no funcionan correctamente con los scripts desactivados, así que si confiamos en un sitio, podemos aumentar gradualmente sus privilegios hasta poder usarlo con facilidad.

uBlock es una extensión de código abierto gratuita que bloquea todos los anuncios (incluidos los infectados) y nos da la capacidad de filtrar y bloquear el contenido de nuestra elección.

HTTPS Everywhere es un complemento que obliga a las páginas web a operar en un HTTPS más seguro y cifrado.

conexión. Si un sitio web no admite dicho protocolo, puede ser bloqueado.

CÓMO DESCARGAR Y USAR TAILS?

1. Prepara una memoria USB con una capacidad de al menos 8 GB. 2. Ve al sitio oficial de Tails y descarga la imagen USB. 3. Descarga uno de los programas gratuitos para crear unidades flash BOOTABLES como Rufus. 4. Conecta la memoria USB a tu computadora. 5. Ejecuta el programa para crear medios booteables, introduce la ruta a la imagen USB y luego selecciona el medio en el que quieres instalar el sistema. Confirma la configuración y espera a que el programa termine. (Nota: esta acción eliminará todos los datos de la memoria USB). 6. Cuando el programa termine, reinicia tu computadora y espera a la pantalla de la computadora o de la placa base del fabricante. Cuando aparezca, haz clic varias veces en el botón responsable de iniciar el menú de arranque. Probablemente será una de las teclas F1 a F12; esta información se puede encontrar en la parte inferior de la pantalla de carga mencionada anteriormente. 7. En el menú de arranque, selecciona el medio de almacenamiento USB y espera a que el sistema se cargue. 8. Después de un tiempo verás una ventana donde puedes cambiar el idioma, la zona horaria y el tipo de teclado. Personalmente, siempre dejo la configuración predeterminada: menos personalización, menos información sobre ti.

En la pestaña "más opciones" podemos encontrar configuraciones como suplantación de dirección MAC y conexión a un servidor proxy (Habilitar el servidor proxy es útil cuando provienes de un país donde la internet está filtrada y censurada.)

¿Qué es la suplantación de dirección MAC?

Además de la dirección lógica, es decir, IP, las tarjetas de red también tienen sus

dirección física inalterable - MAC. La opción mencionada anteriormente cambiará la dirección MAC de nuestra tarjeta de red a una falsa. Esto te dará aún más anonimato.

Encontrarás todos los detalles sobre Tails en su sitio web oficial.

https://tails. boum. org/

¿POR QUÉ DEBERÍA USAR UNA UNIDAD FLASH BOOTABLE Y NO UNA MÁQUINA VIRTUAL?

Aparte del método que describí arriba, hay otra forma de ejecutar tal sistema sin usar una unidad flash. Esto se puede hacer mediante una máquina virtual, que es un emulador de hardware real. La parte de disco y memoria se asigna a dicha máquina virtual y, a partir de ahora, se puede usar como una computadora completamente diferente. Sin embargo, este método conlleva mucho riesgo; un hacker eficiente puede llegar a lo que está por encima de la máquina virtual, hablando un lenguaje más técnico, que es

su host y luego acceder a nuestro dispositivo real y robar nuestros datos.

LAS REGLAS A SEGUIR SI QUIERES PERMANECER ANÓNIMO

1. Utiliza el sistema instalado en el pendrive en lugar de usar una máquina virtual. Como mencioné antes, el uso de una VM puede revelar información sobre tu hardware real. 2. No proporciones ningún dato real ni información que pueda llevar a tu identidad. Esto no solo aplica a cuestiones obvias como tu nombre o edad, sino incluso a cosas como tus colores favoritos, comida, marcas de ropa o autos. Cuando estés en la Dark Web, tu objetivo debe ser claro: nada debe destacar. ¿Usas TOR? ¡Genial! Pero no personalices este navegador, sería otro elemento que comprometería tu anonimato. 3. No uses el navegador en modo de pantalla completa. Los programas ajustan el tamaño de su ventana a la resolución del monitor y la configuración de la tarjeta gráfica. Estos son otros datos que pueden acercar a terceros a nuestra identidad. 4. Al usar foros, utiliza un apodo que nunca hayas usado antes, lo mejor es nombrarte de la manera más abstracta posible. Gran Comepan300, JaleaDeLaVerdad_17, etc. Piensa un momento y crea un apodo que no usarás fuera de la Dark Web. 5. Si vas a dejar algún comentario en sitios web de la Dark Web, primero escríbelo en un bloc de notas y luego pega el contenido creado en el comentario. Esto te ayudará a evitar keyloggers o programas que registran todo lo que escribes con el teclado. Sí, si es tarea del sitio recopilar dichos datos, este método no cambiará nada. Sin embargo, si el sitio está infectado por malware, esto nos ayudará a evitar situaciones desagradables como filtraciones de nuestro contenido a

sitios web externos.

6. Al usar la red TOR, no inicies sesión en tus cuentas reales en ningún sitio como Facebook, YouTube, Instagram, etc. Tal acción revela inmediatamente tu identidad, a pesar de todas las capas de seguridad que tengas. 7. Usa el modo más seguro del navegador TOR y utiliza todos los complementos predeterminados disponibles siempre que sea posible. 8. Si tienes una cámara web o micrófono, desconéctalos mientras navegas por la Dark Web. Si usas un portátil que tiene estos dispositivos integrados, puedes taparlos con un trozo de cinta adhesiva. Puede sonar tonto, pero vale la pena protegerte de todas las formas posibles. 9. No instales extensiones adicionales en el navegador, las básicas son

suficientes.

CÓMO USAR EL TOR NAVEGADOR?

Lo primero que debemos hacer después de instalar Tails y activar TOR

el navegador es ingresar la verificación de dirección. torproject. org en la barra de búsqueda.

Esta dirección lleva al sitio web oficial del proyecto TOR, que verifica si nuestro navegador está configurado correctamente y es capaz de conectarse a la red TOR. El siguiente paso en nuestro recorrido por la Dark Web debería ser visitar el Hidden Wiki. Es un conjunto de sitios web, ordenados por categorías, accesibles solo desde el navegador TOR. El Hidden Wiki es una especie de centro de servicios disponibles en la

la web oscura.

Como advertencia: el 99% de las páginas que encuentras aquí no están de ninguna manera controladas por el contenido que subes, por lo que puedes encontrarte con cosas realmente perturbadoras.

Los sitios web que visitas usando el navegador TOR pueden cargarse mucho más lento debido a la ruta que debe seguir la conexión. Esto no se aplica a todos los sitios, pero puede ocurrir en algunos.

vale la pena ser paciente.

RESUMEN

La regla básica que debes seguir si quieres mantenerte anónimo en línea es mantenerte callado y usar el sentido común. No funcionarán capas de seguridad ni cifrado si no sigues las reglas mencionadas anteriormente en mi tutorial.

Finalmente, me gustaría agradecerte por leer mi libro corto. Espero que esto sea un buen comienzo para ti en la protección de tu privacidad. Si quieres, puedes dejar una reseña, seguramente me ayudará en el desarrollo posterior.

Si tienes alguna pregunta o sugerencia, estoy aquí para ayudar.

Mi dirección de correo electrónico: theselfpublisher@zohomail.eu