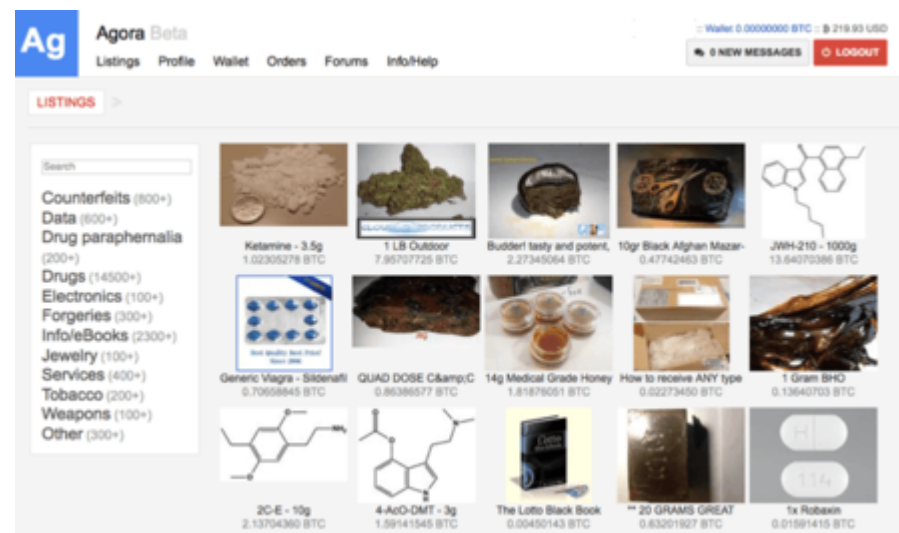




La web profunda de TOR es un entorno que se encuentra en constante cambio y los servicios ocultos que consultamos un día, al otro día pueden dejar de funcionar por muchos motivos, ya que no hay que olvidar que la mayoría son mantenidos por voluntarios en la red y no son servidores dedicados. Por este motivo, algunos de los sitios en la web profunda pueden modificar su direccionamiento y en esta web no existe un Google, Yahoo o similar que indexe dichos contenidos continuamente.

Muchos de los servidores pueden ser simples maquinas virtuales levantadas expreso para compartir de forma pública una determinada información, pero al y como aparecen desaparecen, a excepcion de aquellas que mantienen una estructura de negocios y servicios poco lícitos que se abonan con el dinero digital por excelencia (los bitcoins).

¿Dónde encuentro enlaces .onion?



Una de las puertas de entrada a la darknet es The Hidden Wiki, una wiki que sirve de directorio para encontrar otros servicios ocultos de Tor. Como muchas otras "páginas invisibles", la *Hidden Wiki* cambia de vez en cuando de pseudo-dominio, pero su URL actual se puede encontrar fácilmente en Google. Hay

otras wikis, que se diferencian de la Hidden Wiki por ser más o menos restrictivas que ésta respecto a la pornografía infantil (un problema que divide a la darknet, con una buena parte de la comunidad persiguiendo este tipo de enlaces).

Están la Liberty Wiki, All You're Wiki y The Uncensored Hidden Wiki. También hay muchas páginas (dentro y fuera de deep web) que no son wikis pero mantienen una lista actualizada de enlaces ".onion". Por eso la deep web tiene sus propios buscadores. Los dos más conocidos son "Torch", que tiene indexadas webs .onion de todo tipo; y "Grams", que buscará lo que le pidas en varias tiendas del mercado negro (los darknet markets).

Luego está el *bot* Harry71, una araña web que rastrea toda la deep web y mantiene actualizada una lista de enlaces pública, con estadísticas del uptime de las páginas.

¿Qué son los bitcoins?

El Bitcoin es la moneda "de curso legal" en la deep web. Es dinero inconfiscable y anónimo, pero incluso usando bitcoins hay que tomar muchas precauciones para que no puedan seguirte el rastro.

La dirección en la que un usuario recibe una transferencia de bitcoins es completamente anónima. El "problema" es que las transacciones con bitcoins son públicas. Por eso, alrededor de las webs de compraventa han ido creciendo servicios de blanqueo de bitcoins y mezcladores de bitcoins, para dificultar que —siguiendo las transacciones en la cadena de bloques— se puedan relacionar tus bitcoins con tu persona.

¿Qué es un mezclador de bitcoins? Son empresas como BitMixer, BitBlender, Tor Wallet... Lo que hacen es justamente eso: mezclar tus bitcoins con otros y reenviar bloques equivalentes a las direcciones que especifiques. Los honorarios de estos servicios son un porcentaje fijo del total a blanquear (en el caso de Bitmixer, un 0,5%). En algunas tiendas de la deep web, los mezcladores van integrados en el proceso de compra.

¿Pero qué se puede comprar en la deep web?

Visto todo lo que hay a la venta en la deep web, uno se pregunta cómo pueden funcionar las tiendas de compraventa. El mercado negro de la darknet se sostiene sobre cuatro pilares:

1) PGP ¿Hay alguna forma de ser más anónimo que estando en una red descentralizada y que hace casi imposible rastrear tu IP? Sí, cifrando todas tus comunicaciones con PGP, o mejor dicho "GPG" —su versión open source. Es el método preferido de los traficantes de droga, que ofrecen su clave pública al usuario durante la transacción. Además, no se usa el correo electrónico (la mayoría de las tiendas sólo te piden una contraseña y un pin para registrarte).

2) Bitcoins Todo lo que se ve en la darknet puede comprarse, incluso las cosas mas ilegales.

3) Los sistemas de reputación Al igual que en eBay, tu reputación como vendedor es lo que te da validez en los mercados de la darknet. Las valoraciones se pueden encontrar en las propias tiendas, en foros de la deep web e incluso en Reddit. Los usuarios advierten a otros de las estafas y dejan reviews muy completas de los vendedores fiables y sus productos. Los vendedores nuevos pueden introducirse en el mercado enviando muestras ("samples") gratuitas o a precio de coste para que los compradores puedan legitimarlo con su feedback.

4) Escrow y Multisig Escrow Si no existiera el Escrow, no habría forma de protegerse contra las estafas. Todos los grandes mercados ofrecen este servicio: el dinero queda depositado en manos de los administradores de la tienda durante el proceso de compra, y no pasa al vendedor hasta que el producto se envía al comprador. Las tiendas cobran un porcentaje pequeño (alrededor de un 0,5%) por utilizar Escrow, además de un sistema de disputas si hay algún problema. Algunos vendedores te ofrecen un descuento si te saltas este mecanismo. El Multi-Signature Escrow (o Multisig) es una alternativa en la que el dinero del comprador está retenido en una dirección de Bitcoin firmada tanto por él como por el vendedor. De esta forma, son los involucrados los que arbitran sobre el dinero

¿Y cómo te llega lo que has comprado?

Si el producto que compras es físico y tangible, especialmente si es ilegal, hay varios métodos para recibirlos por correo postal para los más osados, pero pierdes todo el tratamiento de confidencialidad anteriormente realizado.

Y luego están los "*métodos de discreción*" de los vendedores. Como puede ser camuflar el paquete para que parezca que viene de una tienda conocida (un cartón de Amazon, por ejemplo); o esconder el producto en otro objeto, un clásico. Que finalmente recibas el paquete no significa que te hayas librado de un seguimiento del paquete ya que hay veces que la policía sabe lo que contiene, pero deja que continúe el proceso de entrega para poder investigar esa vía de tráfico ilegal, por lo que salvo que tengamos la certeza de que estamos adquiriendo algo lícito es mejor no tentar a la suerte ni incumplir la ley.