Capítulo 3
Black Market

1. Introducción

Tener en cuenta el Black Market en un plan global de seguridad informática se ha convertido en una obligación para cualquier empresa que se quiera proteger, asegurar sus activos y su sostenibilidad económica, sin olvidar a sus clientes y su imagen. Por supuesto, este capítulo no pretende invitarlo a participar en este Black Market vendiendo o comprando el contenido que se comercializa (bases de datos pirateadas, identidades digitales usurpadas, etc.). Nuestra misión es permitirle ser un observador atento de este Black Market 2.0 de lo ilícito.

El objetivo de este capítulo es explicar por qué es fundamental vigilar este entorno y ayudarlo a descubrir qué es el Black Market: ¿por qué no se debe confundir con la Dark Web/Deep Web? Qué se puede encontrar en él, cómo funciona, qué se vende y adquiere, y cómo orquestar un seguimiento eficaz en este extraño entorno informático.

2. Deep Web, Dark Web, Darknet y Black Market

En cuanto empezamos a hablar del Black Market, se mezcla el vocabulario, su ubicación geográfica digital y su presencia imaginaria o no. No es raro leer que el Black Market se esconde en la Deep Web o que los piratas comercializan sus productos en una Dark Web oculta en una *darknet* que protege su negocio. Si en la forma este atajo puede parecer lógico, al final estamos a mil kilómetros de la realidad.

En 2024, según el FBI, la facturación global de los mercados negros digitales habría superado los 8.000 millones de dólares, para todas las plataformas. Solo Hydra Market (Rusia, cerró en 2022) gestionó 1.300 millones de dólares al año. El sitio BreachForums, gestionado por franceses, solía generar entre 50.000 y 60.000 € al mes. Sigue activo, pero en enero de 2026 se filtró públicamente la base de datos completa del foro (unos 324.000 usuarios), lo que provocó una crisis de confianza en este sitio en la comunidad criminal.

En primer lugar, no hay nada peligroso o perturbador en la Deep Web. Se trata ni más ni menos de datos que no se referencian en la Web. Por ejemplo, una base de datos que administra su sitio web, un blog que es solo para su familia, los correos electrónicos que envía y recibe, el foro que necesita credenciales de inicio de sesión para acceder a su contenido, etc. Todo esto no tiene que estar referenciado. Los motores de búsqueda que recorren la web con sus robots (*spider*) no tienen la posibilidad de catalogarlos para encontrarlos con la primera petición. En definitiva, estos datos están en la Deep Web.

Antes de empezar nuestra visita por el Black Market y su utilización en el entorno de una política de vigilancia, echemos un vistazo rápido a las diferentes capas de la Web. En primer lugar, la más conocida, la Web "común", la Clear Web. Facebook, Twitter y YouTube forman parte de ella. Está a unos segundos usando cualquier motor de búsqueda del mundo.

A continuación, la Web de superficie. También es fácil de acceder, pero hay más contenido "underground" como Reddit, jetable.org (permite crear una dirección de correo electrónico con una duración temporal limitada) o simplemente bases de datos SQL, el host de su blog, la intranet de su empresa, etc. Con respecto a la darknet, existe la misma confusión. La darknet es una red de comunicación de persona a persona (*friend-to-friend*). No hay nada peligroso o ilegal al respecto. Pero su uso con fines maliciosos perturba su comprensión. Es parecido a decir que un automóvil es peligroso porque hay personas que lo utilizan en un atraco a un banco.

En tercer lugar, la Bergie Web, el vínculo entre la Web y la Deep Web. Por ejemplo, aquí nos encontramos con The Pirate Bay. El motor de búsqueda de TPB dirige a los usuarios a la Deep Web, donde se encuentran los enlaces torrent. Los foros anónimos 4chan o los servidores FTP también forman parte de ella.

La cuarta capa, la Web profunda, la famosa Deep Web, donde hay varios subniveles más, incluido el que nos interesa en este capítulo, es decir, el de los markets y autoshops del Black Market.

Un mundo en constante evolución, creando "profesiones" del mal. Por ejemplo, los "*Initial Access Brokers* (IAB)". Estos especialistas venden acceso a redes corporativas, un preludio a ataques de ransomware o la posibilidad de acceder sin límite a datos de la empresa. Luego está el "*Ransomware-as-a-Service*" (RaaS). Estamos hablando de alquiler de kits de ransomware, incluyendo soporte técnico. Grupos como Lockbit, desmantelado en 2025, habían atraído a decenas de clientes a este alquiler de herramientas pirata durante 5 años. La venta de documentos falsos, aunque no sea nueva, está atrayendo a cada vez más estafadores KYC. La aparición de documentos "digitales" falsos generados por IA para superar controles de identidad, se está volviendo más profesional. Los dos últimos son ejemplos de estos hackers de "nuevas profesiones" piratas y hay otros por descubrir en ZATAZ.COM: la exfiltración de APIs. El hacker especializado roba y vende claves API (OpenAI, AWS, Google, etc.) para uso fraudulento. Por último, " IA scam": robo de identidad de audio/vídeo mediante IA generativa para extorsionar a seres queridos (deepfake voice, etc.).

Los mercados se han vuelto "uberizados" con sistemas de valoración de vendedores/compradores, garantías de devolución de dinero, servicio postventa, devolución de efectivo e incluso campañas promocionales (Black Friday, etc.).

3. Black Market, entre lo visible y lo invisible

El Black Market intenta permanecer en este espacio de invisibilidad, o eso podríamos pensar a primera vista. Esta Web invisible apareció por primera vez en el vocabulario informático en 1994, en boca de la escritora Jill H. Ellsworth. El Black Market opera en la Deep Web, y más específicamente en la Dark Web, siendo la propia Dark Web parte de la darknet. La darknet incluye todas las actividades digitales organizadas por un número limitado de personas que no necesariamente evolucionan en la Dark Web. La Dark Web requiere necesariamente la visualización de páginas web. ¿Complicado?

La Dark Web es una pequeña parte de lo que se esconde en la Deep Web en forma de páginas web accesibles usando herramientas como Tor, Freenet, IP2, etc.

La Dark Web no se referencia usando un motor de búsqueda; al menos normalmente. Hablaremos de eso más adelante en estas páginas. Por lo tanto, en la darknet encontramos, por ejemplo, correos electrónicos cifrados de pirata a pirata o tiendas del Black Market. Tiendas que, para sobrevivir, deben evolucionar en la Dark Web, el único lugar donde pueden existir.

En resumen, si tuviéramos que decirlo de una manera sencilla, el Black Market no es más que una tienda que ofrece datos pirateados, como bases de datos robadas en un sitio web infiltrado, clones de tarjetas bancarias, documentos administrativos falsos (desde nóminas hasta permisos de conducir y otras facturas falsas), estupefacientes, manuales de usuario y software dedicado a la piratería informática en forma de páginas web. En las tiendas más extremas, se pueden adquirir armas y municiones. Por supuesto, la idea es que esto suceda de la forma más anónima posible.

Hay varios "tamaños" de Black Market. La tienda más sencilla está a cargo de una sola persona. Se llama "autoshop". Este espacio ofrece un tipo específico de producto: drogas, documentos falsos, etc. El "marketplace" reúne varios "autoshops" como podría hacerlo un centro comercial en cualquier hipermercado que encontramos en nuestras ciudades. La diferencia es que los centros comerciales del Black Market solo venden productos ilegales.

4. Funcionamiento

Un portal del Black Market funciona como las tiendas que encuentras en la web: productos, clientes, vendedores y transacciones financieras. Para dar fe de su fiabilidad los sistemas de clasificación se muestran como en eBay. Durante su vigilancia, el hecho de que a un vendedor se le acredite un determinado número de ventas, con clientes satisfechos, debería hacerle fijarse con detenimiento en la autenticidad de los datos que vende. Es fiable si su porcentaje de satisfacción supera el 80%. Las notas de los compradores darán fe de su eficacia y de la calidad de los productos: ¿las bases de datos contienen datos inéditos? ¿El contenido es interesante? ¿Velocidad de entrega? Etc.

Las "tiendas" más conocidas incluso ofrecen garantías. ¿Los datos bancarios que se compran no funcionan? Se organizan reembolsos y/o sustituciones. A los vendedores que tratan de proporcionar información y productos desactualizados no les va a ir nada bien porque el Black Market es un entorno criminal que trabaja con muchos intermediarios, cuyos principales actores son los llamados "escrows".

¿Cuál es la misión del escrow? Es un intermediario que controla y verifica la transacción entre el vendedor y el comprador. Recibe el dinero y paga el importe al vendedor una vez que el comprador ha recibido el producto. El escrow recibe un porcentaje del precio establecido (entre el 2 y el 10%, en función de la tienda). En otras palabras, el vendedor tiene todas las de perder en caso de haya problemas. Un tercero, escrow o tienda, que retiene el dinero de una transacción se denomina "exit scam". También hay robots escrow. Median entre un comprador y un vendedor y, por lo tanto, se supone que evitan las estafas. El scrow "automático multi-sig" controla que cada transacción esté firmada con una clave privada para bloquear los intentos de exit scam.

Dependiendo del nivel de confianza, es posible encontrar Finalize Early (FE): se trata de un vendedor conocido y reconocido, por lo que recibe el dinero antes de que se reciba el pedido.

Los pagos se realizan principalmente en forma de monedas virtuales como Bitcoin, XMR o Ethereum. Por el lado de la comunicación, los más profesionales del Black Market imponen el cifrado de las conversaciones entre interlocutores, ya sea con un sistema propietario o mediante claves PGP.

Cómo funciona: más profesional que nunca

Los sitios "piratas" se están volviendo cada vez más profesionales. Interfaces de usuario con un diseño comparable al de plataformas como Amazon o Vinted. Tiendas personalizables, chat online, gestión de carritos, recomendaciones, plugins de Telegram/Discord. Pagos reforzados por la generalización de Bitcoin, XMR (Monero, estrella del anonimato), Ethereum. Algunos sitios pirata todavía cobran por compras a través de cupones de Amazon o Apple. Más fácil de blanquear, pero más difícil de manejar. Desde 2023, adopción parcial de stablecoins (USDT, USDC) para evitar la volatilidad.

La proliferación de escrows automáticos multisig (verificación multiclave) permite asegurar las transacciones piratas. La tendencia a la plataforma apareció en 2024. Algunos Black Markets incluso ofrecen APIs para los vendedores.

Pongamos fin al cambio masivo hacia la mensajería cifrada (Telegram o Signal) para contactos, entrega de datos o servicio postventa. Telegram, tras la detención por parte de Francia de su cofundador, vio cómo las autoridades "capturaban" a decenas de hackers. El 28 de agosto de 2024, Pavel Durov fue acusado de unos quince delitos, puesto bajo control judicial en Francia (prohibición de salir del país, obligación de presentarse dos veces por semana ante la policía y fianza de varios millones de euros). Fue liberado en 2025. Los investigadores acusan a Telegram, y por tanto a su fundador, de permitir que contenido ilegal (pornografía infantil, drogas, blanqueo de capitales, etc.) circule libremente en su plataforma y de no proporcionar los datos solicitados cuando los solicitaron.

Desde entonces, Telegram ha respondido. Global 2024: 893 solicitudes a Telegram, con 2.072 usuarios implicados. Último trimestre de 2024: 673 solicitudes del sistema judicial francés para 1.386 usuarios. Esto significa que el 75% de las consultas y perfiles objetivo lo han sido durante los últimos tres meses de 2024. El aumento del **30%** refleja un contexto posterior al arresto, marcando un punto de inflexión para Telegram en Francia.

5. ¿La tiendas son anónimas?

Se puede poner en contacto con las tiendas del Black Market usando muchos métodos: por cooptación, enlaces que pasan de mano en mano, etc. El más sencillo, y el que se ha convertido en tendencia, es un buscador que permite encontrar información o un producto concreto, escribiendo una consulta en Yahoo!, Qwant o Google. El sitio Black Market puede tener la forma de un foro o simplemente una tienda con ofertas, precios y botones de compra. Tenga cuidado con los foros. En general, se trata de nidos de víboras, cuando no simplemente de estafas puras y duras. Sin embargo, el Black Market usando Google no es imposible, aunque arriesgado e ilegal. Volveremos sobre esto un poco más adelante en este capítulo.

La gran mayoría de estas tiendas operan a través de direcciones en .onion. .onion indica **una dirección anónima accesible a través de la red Tor**.

Entienda que una URL en forma de "dirección.onion" no funcionará en Internet usando su navegador habitual, como Chrome, Edge, etc. Esta dirección .onion solo se puede leer desde la red Tor, sus proxies y navegador dedicado, Tor Browser. La dirección generada para continuar en Tor es aleatoria, aunque es posible darle un significado para conocer su destino. Un espacio .onion ofreció durante un tiempo la posibilidad de adquirir nombres de dominio .onion. Se vendieron varios millones de direcciones en bitcoins como freakbug-fpaynode.onion (Freak Bug-F Paynode), que se vendió por 5 bitcoins, es decir, más de 7000 €.

En cuanto a Tor, es una gran herramienta ofrecida por Tor Project, Inc (https://es.wikipedia.org/wiki/.onion). Tor significa *The Onion Router*. Es una red informática descentralizada que utiliza millones de ordenadores en todo el mundo para servir como nodos de conexión. Conclusión: Tor permite ocultar el rastro del usuario o del sitio web .onion visitado. Dado que las comunicaciones están encriptadas, Tor permite anonimizar el origen de las conexiones TCP. Es una herramienta genial utilizada por cientos de periodistas, blogs que abogan por la libertad de expresión o simples internautas que no quieren que los rastreen el marketing y los rastreadores de los gigantes de Internet, con Google a la cabeza.

Los diseñadores de las tiendas Black Market también aprovechan este anonimato para evitar la localización de sus servidores. Un servidor puede estar alojado con un host perfectamente identificado y completamente legal. Las tiendas también se pueden ocultar a través de Ip2, Freenet, pero Tor y .onion siguen siendo mayoría, porque el acceso es más fácil. El sistema Tor también permite a estas tiendas del Black Market "proteger" a sus visitantes, ya que no aparece la IP de conexión de compradores/vendedores. Eso sí, tenga cuidado con este detalle de la anonimización.

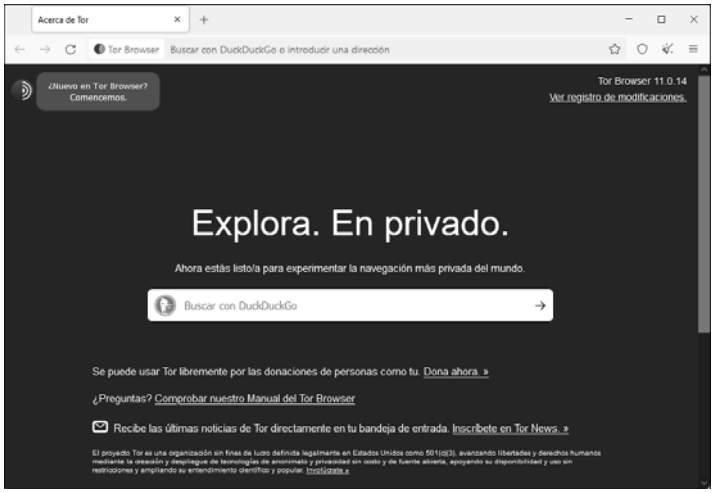
Aunque la imprescindible Electronic Frontier Foundation (EFF), fundación que trata de proteger la privacidad en Internet, ofrece Tor como solución para asegurar sus conexiones, la experiencia ha demostrado que la herramienta no es infalible (https://www.torproject.org/). La investigadora informática Sarah Jamie Lewis, inició el proyecto OnionScan. Su misión: ayudar a encontrar e informar de las vulnerabilidades y bugs descubiertos en Tor. OnionScan (https://github.com/s-rah/onionscan) digitaliza automáticamente vulnerabilidades y errores comunes que pueden bloquear la capacidad de ser anónimo usando Tor. "**La privacidad es importante. Aunque algunas personas usan Tor para hacer cosas ilegales, hay muchos sitios privados y blogs de política alojados en la Dark Web, y los propietarios deben poder estar seguros**". (http://www.extremetech.com/internet/226106-onionscan-tests-dark-web-sites-to-see-if-they-really-are-anonymous).

6. Cómo se utiliza Tor

Para configurar su vigilancia y visitar los espacios que se ofrecen en el Black Market, pasando a través de direcciones .onion, es imprescindible la instalación de Tor y el uso de Tor Browser. Las siguientes secciones detallan cómo instalarlo y usarlo.

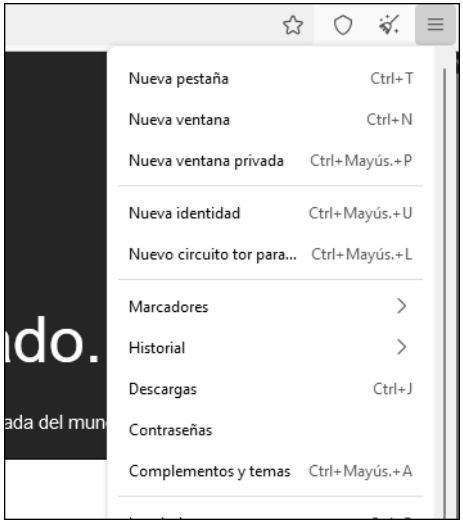
6.1 Instalación

La instalación es sencilla. Después de descargar Tor desde el sitio web oficial https://www.torproject.org, solo necesita instalarlo en su ordenador siguiendo el procedimiento que ofrece el software.



6.2 Configuración de la seguridad

- En las tres líneas horizontales que se encuentran en la parte superior derecha del navegador, configure su Tor Browser.



6.3 Verificación de la dirección IP

Puede verificar su dirección IP haciendo clic en el enlace **Comprobar la configuración de la red Tor**. El enlace http://www.mi-ip.com/localizar-direccion-ip.php permitirá comparar su dirección IP real con su dirección IP una vez que Tor se esté ejecutando en su conexión. Las dos direcciones IP deben ser diferentes al conectarse a través de Tor.

6.4 Navegación

Para navegar en Tor, es suficiente con introducir la URL .onion o web en la barra del navegador. Los sitios web recibirán la dirección IP ofrecida por Tor y no su dirección IP oficial. En la parte superior derecha del menú representado por tres líneas horizontales, puede crear reglas para los sitios que desea visitar, porque prevenir ciertas consultas limita el riesgo de espionaje entre el usuario y su punto de conexión. Esto reduce considerablemente las posibilidades de interceptación.

6.5 Cambio de dirección IP

Pulsando en **Nueva identidad** y **Nuevo circuito Tor**, cambia la dirección y los nodos Tor que estaba utilizando.