EXPLORING THE DARK WEB



SECRETS FROM AN EX HACKER

By Faisal .j

EXPLORANDO

LA DARK WEB

SECRETO DE UN EXHACKER

Faisal .J

Página de derechos de

Explorando la Dark Web: Secreto de un Ex-Hacker

Copyright © 2025 por Faisal .J

Todos los derechos

Ninguna parte de este libro puede ser copiada,

de cualquier forma—electrónica, mecánica, fotocopiado u otras—sin el permiso escrito previo del autor, excepto para citas breves en reseñas o investigaciones.

Aviso legal

Este libro es para fines informativos y educativos solo. El autor **no promueve, respalda, o incita a actividades ilegales.** Los lectores son responsables sus propias acciones y deben cumplir con todas las leyes aplicables. El contenido se basa en investigaciones y experiencias personales y se proporciona “tal cual” sin garantías de ningún tipo. Algunas imágenes en este libro fueron generadas por IA o obtenidas de investigaciones en línea. El texto ha sido editado usando herramientas de gramática asistidas por IA para mayor claridad. Aunque se ha hecho todo lo posible para garantizar la exactitud, los temas de ciberseguridad evolucionan y cierta información puede quedar desactualizada.

Publicación independiente,

Para consultas o permisos, contacte a:

faisaljalvi0509@gmail.com

Patreon: Apoya mi trabajo y contenido

ÍNDICE

Capítulo 1 – Introducción a la Darknet.....2
Capítulo 2 – Acceso a la Darknet.....10
Capítulo 3 – Lista de Enlaces Ocultos .....18 Capítulo 4 – Acceso Seguro a la Dark Web..... 28 Capítulo 5 – Puntos Brillantes en la Darknet..... 41 Capítulo 6 – Revelando el Internet Oculto..... 51 Capítulo 7 – Cómo Usar Tor ..... 63 Capítulo 8 – Dark Web para OSINT..... 73 Capítulo 9 – Explicación de VPNs..... 80

Capítulo 10 Impacto de en la

Capítulo 1

INTRODUCCIÓN A LA DARKNET

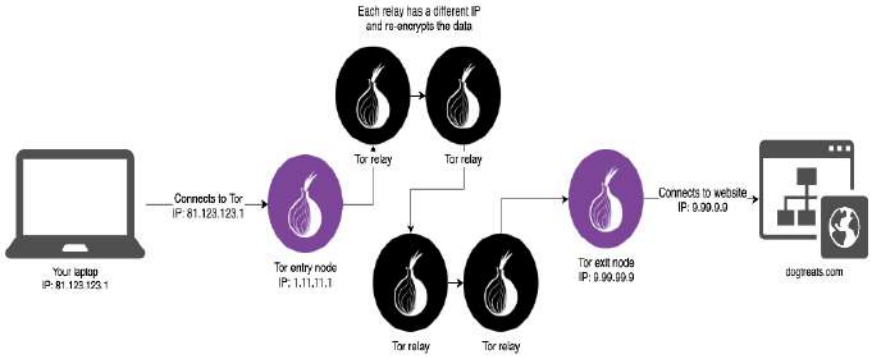
📜❝ **"La Darknet no es un lugar que visitas—es un submundo sombrío donde el secreto es la supervivencia."**

Internet tiene un lado que la mayoría de la gente nunca ve...

TOR (The Onion Router)

A diferencia de la navegación web tradicional, donde tu dispositivo al servidor de un sitio web, TOR redirige tu

conexión a través de múltiples capas cifradas, rebotando tu solicitud entre diferentes servidores en todo el mundo. Este proceso garantiza que tu identidad permanezca oculta, haciéndola casi imposible.



La Primera Capa: Punto de Entrada

Tu viaje hacia la red TOR empieza cuando te conectas al nodo de entrada (Servidor 1). Este nodo recibe la dirección IP de tu dispositivo pero no sabe a dónde pretendes ir. Simplemente cifra tu solicitud y la reenvía a otro servidor en la red.

La Segunda Capa: Nodos TOR

Una vez dentro de la red TOR, tu solicitud se mueve a través de nodos de retransmisión (Servidor 2). Estos actúan como intermediarios, asegurando que ningún servidor único conozca tanto tu identidad como tu destino. Los nodos intermedios manejan datos cifrados, lo que significa que no pueden ver ni alterar tu solicitud. Solo saben qué nodo les envió datos y a dónde enviarlos a continuación.

La Tercera Capa: Nodo de Salida

Tu solicitud finalmente llega al nodo de salida (Servidor 3), el relé final antes de conectarse al sitio web real que deseas visitar. Este nodo descifra la última capa de cifrado y completa la solicitud. Sin embargo, el nodo de salida todavía no sabe quién es el remitente original: solo ve el relé TOR anterior, manteniendo el anonimato del usuario.

El destino final: servidor web

Por fin, tu solicitud llega al servidor web que aloja el contenido al que quieres acceder. Desde la perspectiva del sitio web, la solicitud se origina desde el nodo de salida, no desde tu dispositivo real. El sitio no tiene forma de rastrearla hasta ti, asegurando la privacidad total.

Cómo viajan los datos de forma segura a través de TOR

Cada pieza de información enviada a través de TOR está envuelta múltiples capas de cifrado. El proceso funciona de la siguiente

1. Tus datos son cifrados antes de salir de tu dispositivo.
2. El nodo de entrada lo cifra de nuevo y lo envía al primer relé.
3. Cada nodo de relé elimina una capa de cifrado antes de pasarlo hacia
4. Solo el nodo de salida ve la solicitud final pero no conoce al
5. Este método de cifrado en capas garantiza que nadie nodo individual conozca tanto la fuente como el

destino, lo que lo hace prácticamente imposible de la conexión.

Accediendo a la Darknet con TOR

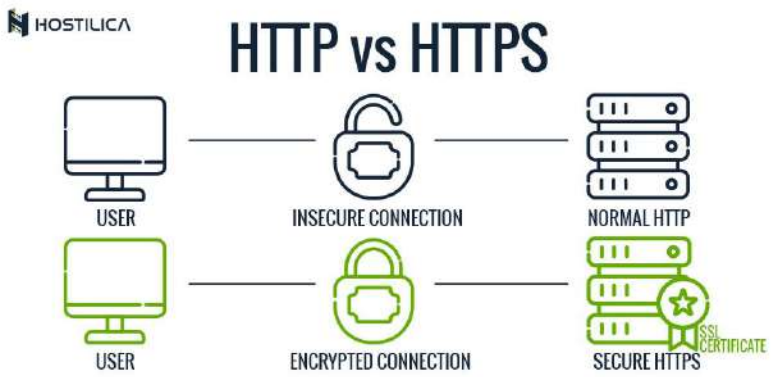
Aunque TOR se puede usar para navegar sitios web normales, su propósito es acceder. sitios onion, servicios ocultos que existen solo dentro de la red TOR. Estos sitios no pueden ser encontrados a través de buscadores regulares y requieren conocimiento directo de sus direcciones. Navegar por la Darknet a través de TOR puede ser lento, ya que cada solicitud debe viajar a través de múltiples relés. Además, algunos sitios web bloquean a los usuarios de TOR para prevenir el acceso anónimo. Sin embargo, a pesar de estas limitaciones, TOR sigue siendo una de las herramientas más efectivas para proteger la privacidad en línea y evadir la censura.



HTTP vs. HTTPS

Protocolo de Transferencia de Hipertexto (HTTP) Por delante de la la abreviatura HTTP se ve en la parte superior desde la barra de direcciones del navegador. El enlace no está encriptado. Los hackers lo tienen fácil para interceptar, manipular y leer

la información. El navegador TOR pone fin a HTTP conexiones. Después de introducir una dirección HTTP, el navegador solicita una edición HTTPS cifrada de la página web. HyperText Transfer Protocol Secure (HTTPS) La URL va precedida de HTTPS y también suele aparecer un pequeño candado para significar la seguridad de su relación. Para aumentar la seguridad de las conexiones HTTP, se añadió el certificado SSL. Las computadoras que se comunican entre sí acuerdan un secreto frecuente que los fabricantes de TOR consideran que HTTP es tan inseguro que, mecánicamente, añaden un certificado a cada enlace HTTP, transformándolo así en una conexión HTTPS.



¿Está totalmente protegido su consumidor con TOR?

El navegador TOR y programas similares crean las avenidas tomadas de la información anónima. Por otro lado, la información enviada a través de él no está necesariamente protegida. Por ejemplo, la información de inicio de sesión, datos de tarjetas de crédito o direcciones podrían extraerse al ingresar datos en un formulario web incluso cuando

TOR está utilizado. Además, el anonimato de TOR

la comunicación también puede eliminarse si una persona accede a este navegador TOR, que también podría ser manipulado como cualquier otra aplicación. Exactamente lo mismo se aplica, obviamente, a los servidores desde donde TOR envía usuarios o sobre qué páginas de la Deep Web se guardan. El navegador TOR dirige una solicitud a través de varios nodos. Desde la perspectiva del nodo de destino, esta solicitud llega a la República Checa.

Dos opciones para TOR

Aunque TOR es la forma más conocida de anonimizar el tráfico,

no es el único protocolo que puede garantizar el anonimato de los usuarios de la deep web. Hornet (Highspeed Onion Routing Network) El sistema de anonimización desarrollado por investigadores del University College London y ETH Zurich es comparable a TOR en rendimiento, pero funciona más rápido. I2P (Invisible Internet Project) I2P, por otro lado, funciona, en principio, como una red privada virtual, y por lo tanto es distinto de TOR y Hornet.

¿Cuál es la brecha entre Darknet y Deep Web?



En la mayoría de las redes de habla alemana más populares, las frases Darknet y Deep Internet se usan como sinónimos. De hecho, Darknet y Deep Internet no son en absoluto equivalentes, ya que el Darknet es solo una pequeña parte de Internet. Figurativamente, podríamos imaginar la Web así: la Web normal, que podemos buscar con Google y compañía, es la punta del iceberg. La parte bajo el agua que solo podemos ver con medios específicos es la Deep Web. Y el Darknet es el fondo del iceberg flotando en el océano. Para ver las áreas del iceberg bajo la superficie, se necesita un "equipo de buceo" especial: el navegador TOR. Para entrar de Internet al Darknet, se requiere más. Mientras que la red visible —es decir, la Web reconocible, visible y dirigida por motores de búsqueda— es accesible con un navegador típico, la web profunda opera oculta bajo la capa superior de la red. Para acceder a las páginas de la Deep Internet se requiere protección, el sistema TOR, que implica anonimato al navegar. La única clave de acceso a la Web es un

software específico y la configuración adecuada del

¿Quién está utilizando la darknet?



El anonimato es especialmente interesante para dos clases: En la por un lado, hay personas que desean la seguridad de la Deep Web debido a sus propias comunicaciones. Hablan de información y datos sensibles y deben temer por sus vidas o las de los informantes si no intercambian datos bajo la seguridad de Internet. Este grupo involucra a los oprimidos o disidentes, miembros de la oposición de naciones dirigidas por dictadores o periodistas y denunciantes. A lo largo de la Deep Web, la Anonimización ayuda a los periodistas a proteger sus recursos. Por ejemplo, los activistas de la Primavera Árabe han logrado obtener estaciones de redes sociales en todo el sistema TOR y difundir información sobre la revolución. Denunciantes como Edward Snowden, además, utilizan Internet para entregar datos sensibles al público en general. Esta clase original se protege de efectos no deseados y la persecución al visitar la Web. Y el siguiente grupo también utiliza el anonimato de la Deep Web para escapar de lo negativo.

efectos y escapar de la persecución. Este grupo consta de individuos cuyas acciones en la Web observable darían lugar muy rápidamente a quejas, penalidades y encarcelamiento.

Darknet incluye foros, tiendas e intercambios en plataformas para bienes y servicios que están prohibidos o sujetos a regulaciones estrictas.

Capítulo 2

ACEDIENDO A LA DARKNET



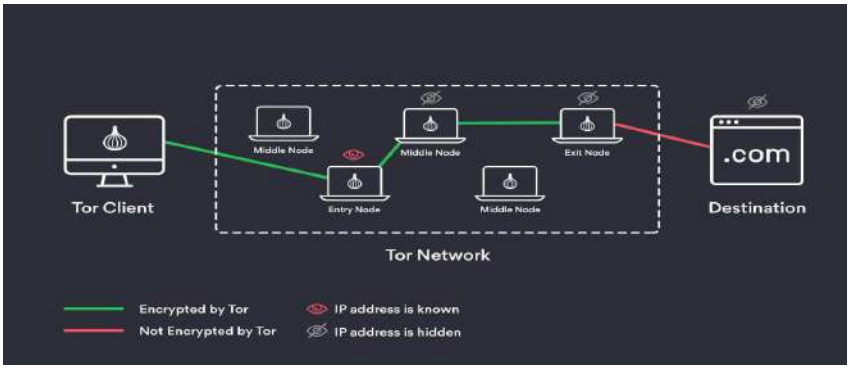
“ "Más allá de la web indexada yace un abismo digital, donde el conocimiento y el peligro van de la mano."

La Darknet no es solo un rincón oculto: es todo un mundo subterráneo digital.

Internet se ha convertido en una parte fundamental de operar empresa. Ya sea comprobando correos electrónicos, manteniéndose al tanto de noticias de la industria o accediendo

diariamente de diversas maneras. Pero ¿realmente entendemos trabaja, incluso a un nivel básico? Antes de adentrarse en la darknet y la web oscura, es importante entender primero la estructura de Internet.

El término "Internet" es la abreviatura de un un sistema que conecta múltiples redes informáticas. Esta interconexión permite a los dispositivos comunicarse entre sí, formando la vasta red global que usamos hoy. Internet, cuando se escribe con mayúscula para distinguirlo de otras internetworks, es el ejemplo más conocido. Conecta miles de millones de dispositivos en todo el mundo a través de protocolos estandarizados que permiten un intercambio de datos sin problemas. Aunque navegar por sitios web es la forma más común en que las personas utilizan Internet, no es el único método de comunicación. El correo electrónico, la mensajería instantánea y las transferencias de archivos (FTP) son otras formas en las que la información se comparte a través de esta red. Es esencial señalar que Internet y la Web no son lo mismo. La Web (o World Wide Web) es solo una forma de acceder a la información en Internet. En términos simples, Internet es la infraestructura, mientras que la Web es un servicio que funciona sobre ella.

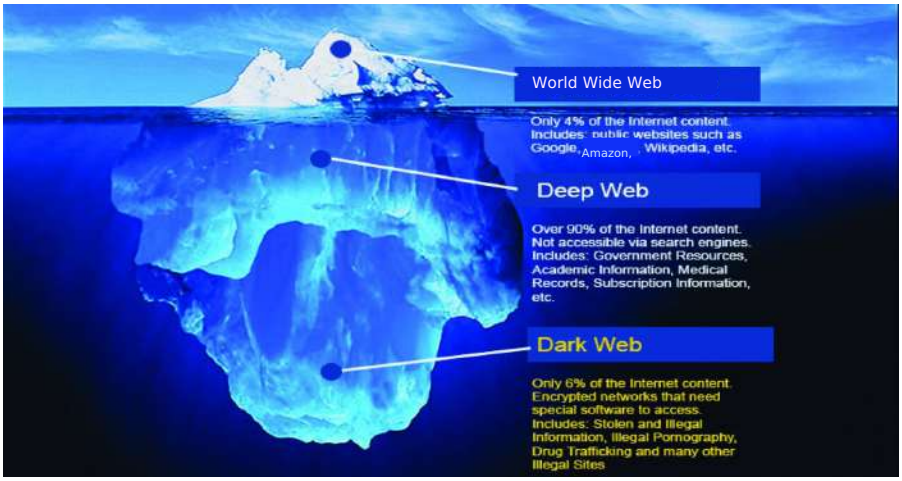


La Internet de Superficie

Los sitios web que visitamos a diario representan solo una pequeña todo Internet. Esta porción, conocida como la web de superficie, incluye todos los sitios accesibles públicamente que motores de búsqueda como Google y Yahoo pueden indexar y mostrar en los resultados de búsqueda. Aunque las estimaciones varían, los expertos coinciden en que la web de superficie representa solo alrededor del 4% de todo el contenido en línea. Si tienes curiosidad sobre cómo rastrean e indexan las páginas web los motores de búsqueda, la guía integral de Google ofrece una excelente visión general.

Más allá de la Superficie

Más allá de la web de la superficie se encuentra el vasto, mundo web profunda y el darknet, que en conjunto componen el 90% restante del contenido en línea.



LA DARKNET - LA DARK WEB La Web Profunda

La web profunda consiste en contenido que no se puede

accedidos directamente a través de motores de búsqueda estándar como Google o Yahoo. Ejemplos de contenido de la web profunda incluyen sitios que requieren credenciales de inicio de sesión (como portales de correo electrónico o banca), sitios web no enlazados que requieren una URL directa para acceder y bases de datos que restringen intencionalmente los rastreadores de motores de búsqueda. De hecho, una gran mayoría del contenido de la web profunda existe en bases de datos que albergan información sensible o estructurada. Muchas bases de datos de la web profunda tienen sus propias funciones de búsqueda internas, lo que permite a los usuarios recuperar información almacenada en ellas. Las bases de datos gubernamentales, registros personales y catálogos de bibliotecas son solo algunos ejemplos de repositorios de la web profunda. Algunas de estas bases de datos son accesibles sin credenciales de inicio de sesión, pero otras requieren autenticación de usuario. Tomemos, por ejemplo, la Denver Property Taxation and Assessment

Sistema. Este sistema permite a los usuarios buscar información de turbas de evaluación y detalles fiscales al ingresar una

Navegadores para la Dark Web

Más allá de la web profunda se encuentra la darknet, una red oculta construida sobre Internet. A diferencia de la web profunda, que es accesible con las credenciales adecuadas, la darknet requiere herramientas y software especializados, como complementos de cifrado o protocolos de red específicos para acceder. No puedes simplemente introducir una URL de darknet en un navegador web común. Así como Internet es una interred que conecta computadoras a nivel mundial, las darknets funcionan como redes aisladas diseñadas para el anonimato. Aquí hay algunas conocidas

ejemplos:

- Tor (The Onion Router): una red descentralizada de servidores operados por voluntarios que ayudan a ocultar la ubicación y la actividad de navegación de los usuarios. En lugar de establecer conexiones directas, los usuarios se comunican a través de una serie de túneles cifrados.
- **I2P (Proyecto de Internet Invisible):** Una red diseñada para asegurar comunicaciones privadas, evitando el rastreo y la vigilancia.
- Freenet: una plataforma de igual a igual que permite a compartir archivos, navegar por sitios 'gratuitos' anónimos y participar en conversaciones seguras.
- **Zero Net:** Una red descentralizada que funciona de manera similar a las darknets, utilizando tecnología

Los sitios en la red Tor suelen terminar en. onion



Tor emplea el enrutamiento de cebolla, donde los datos pasan por múltiples nodos de retransmisión cifrados antes de llegar a su destino final. Cada retransmisor solo desencripta una capa de cifrado a la vez, lo que garantiza que ningún único retransmisor conozca tanto la identidad del remitente como el destinatario final. Otros darknets utilizan métodos de cifrado similares para mantener la privacidad y el anonimato.

¿Quién usa la darknet y por qué?



La mayoría de las discusiones sobre la darknet se centran en lo actividades. Aunque la darknet ofrece anonimato para

usuarios legítimos, como periodistas, activistas o individuos viviendo bajo regímenes opresivos, también atrae a empresas criminales. A continuación se muestran algunos de los usos ilícitos más comunes: comercio de drogas y sustancias ilegales: los mercados de la darknet facilitan transacciones anónimas de drogas y sustancias controladas.

Falsificación: Documentos de identidad falsos, dinero falsificado que a menudo se vende en foros de la darknet. Vendedores de datos robados: detalles de tarjetas de crédito, números de Seguro Social y otros datos personales se venden para uso fraudulento.

Comercio de Armas de fuego y otras armas ilegales son vendidas en los mercados negros de la darknet. Servicios de hackeo: hackers de sombrero negro ofrecen sus servicios por encargo, explotan vulnerabilidades de seguridad e intercambian datos robados.

Gambling: Algunos sitios de juego de la darknet operan fuera **regulaciones**

comunicación terrorista: los grupos extremistas pueden usar la para reclutamiento, intercambio de información y coordinación.

Servicios de asesinato a cambio de dinero: aunque a menudo u oposiciones de las fuerzas del orden, algunos sitios de la darknet afirman ofrecer servicios de asesinato por encargo.

Contenido explícito Desafortunadamente, la darknet conocida por alojar sitios involucrados en contenido ilícito e inquietante. Aunque la darknet proporciona herramientas de privacidad útiles para denunciantes y disidentes políticos, sigue siendo un punto crítico de actividad criminal. Las agencias de seguridad en todo el mundo monitorizan activamente los mercados y foros de la darknet para
rastrear operaciones

.....
.....

Capítulo 3

LISTA DE ENLACES OCULTOS



“"La clave para navegar por la Dark Web no es la curiosidad, sino la precaución y preparación."

Cada acción deja rastro, a menos que sepa cómo encubrir tus huellas.

⚠ DARKNET: POR FAVOR SE CAUTELoso!

Como en cualquier lugar de la vida, necesitas aportar una Parte escepticismo al emplear la Darknet. Donde no es posible la censura ni la vigilancia, también descubrirás un

muchos personajes sombríos. Sin embargo, no solo se negocian áreas para armas o drogas!

El sitio web más popular en la Dark Web

Sorprendentemente, uno de los sitios más visitados de la Dark
La versión Onion de Facebook. Esta versión especial de Facebook permite a los usuarios acceder a la plataforma de forma anónima, evitando la censura en países donde está restringida, como China e Irán. Proporciona una manera segura para que las personas se conecten con el mundo manteniendo la privacidad.



Cómo encontrar información: motores de búsqueda de la Dark Web

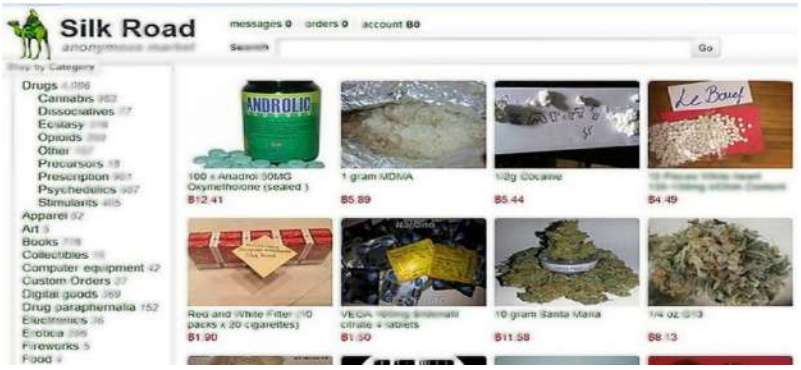
Debido a que los sitios web en la Dark Web a menudo quedan fuera
mantener un registro de enlaces que funcionen puede ser difícil. A diferencia de la web superficial, donde Google indexa eficientemente los sitios web, la Dark Web requiere motores de búsqueda especializados.



Anteriormente, Grams era el motor de búsqueda de referencia, a el "Google de la Dark Web". Sin embargo, desde entonces ha desaparecido. Una alternativa más nueva y confiable es Torch, uno de los motores de búsqueda de la Dark Web más grandes, indexando miles de sitios .onion.



Varios directorios también ayudan a los usuarios a



Servicios de correo de la Red Oscura: Comunicación segura

La comunicación en la Red Oscura suele estar cifrada, y varios proveedores de correo operan estrictamente dentro de este espacio. Uno de estos servicios es Tor Box, que permite a los usuarios enviar y recibir mensajes de forma segura. Sin embargo, Tor Box solo funciona dentro de la Red Oscura, lo que significa que los correos no pueden enviarse ni recibirse desde proveedores de correo regulares como Gmail o Yahoo.

Red Oscura vs. Web superficial: ¿Cuál es la diferencia?

La mayoría de los usuarios de Internet solo interactúan con la Web parte visible de Internet que incluye motores de búsqueda, redes sociales y sitios de noticias. Más allá de ello se encuentra la Deep Web, que consiste en contenido no indexado como expedientes médicos, bases de datos privadas y trabajos académicos. La Red Oscura es una pequeña porción de la Deep Web que requiere herramientas especiales, como Tor, para acceder.

Reflexiones finales: Mantente a salvo en la Red Oscura

Adentrarse en la Red Oscura requiere precaución.

Aunque ofrece herramientas y recursos valiosos de privacidad, también alberga riesgos potenciales, incluidos estafas, sitios de phishing y software malicioso. Para mantenerse seguro: use siempre Tor con una VPN para mayor seguridad. Nunca revele información personal. Evite descargar archivos desconocidos.

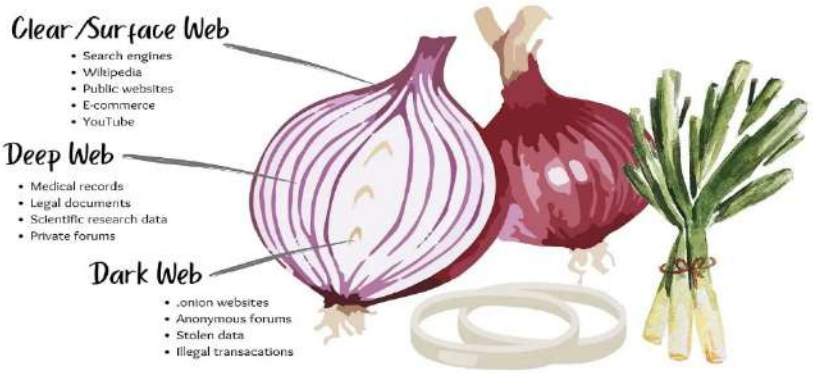
✅

✅

✅

✅ Utilice directorios y motores de búsqueda confiables de la

✅ Tenga en cuenta posibles estafas y servicios falsos.

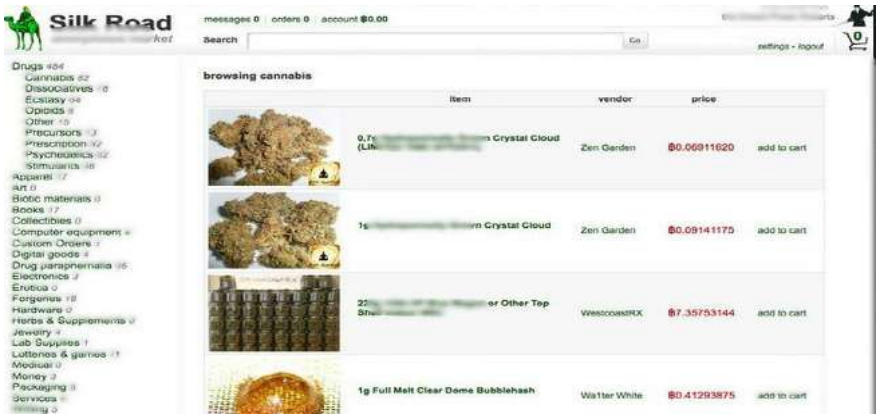


Al seguir estas buenas prácticas, los usuarios pueden explorar la Web mientras minimiza los riesgos. Ya sea que busque privacidad, investigue información oculta o simplemente tenga curiosidad sobre esta red subterránea, el conocimiento y la precaución son sus mejores aliadas.

Casos infames de esta Dark Web

Cuando la mayoría de las personas piensa en la web oscura, vienen a la mente, a menudo aquellos que han acaparado titulares por sus actividades ilícitas. Muchos de estos sitios web o redes operan en áreas legalmente grises o abiertamente ilegales. Sin embargo, no todos los mercados de la dark web son necesariamente ilícitos. Uno de los ejemplos más conocidos fue el mercado Silk Road. Lanzado en 2011, Silk Road se convirtió en famoso por facilitar el comercio de bienes ilegales, incluidos narcóticos, documentos falsificados y armas de fuego. Fue uno de los primeros mercados de la dark net en operar con Bitcoin,

aprovechando su anonimato para las transacciones. Sin embargo, el sitio fue incautado y cerrado por el FBI en 2013, y su fundador, Ross Ulbricht, fue sentenciado a cadena perpetua.

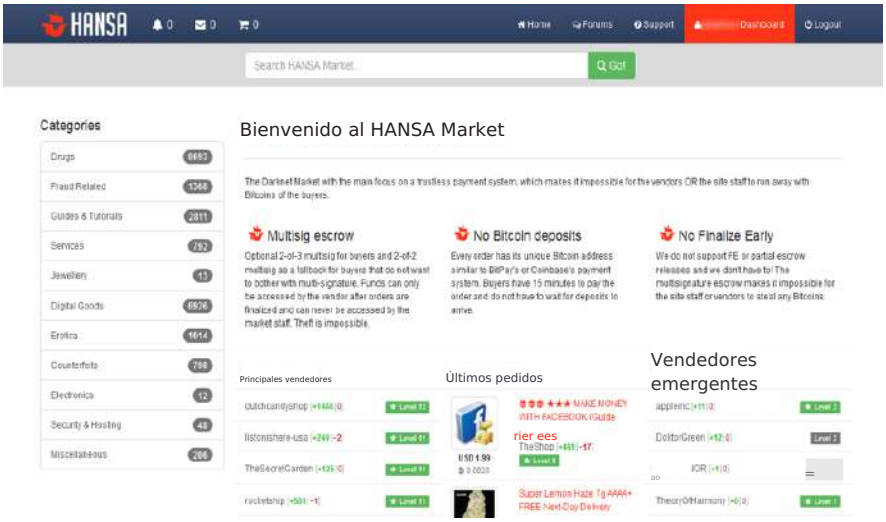


Alpha Bay (2014–2017)

Uno de los mercados de la web oscura más grandes tras Silk causa de su desaparición, Alpha Bay facilitó la venta de drogas ilícitas, herramientas de hacking e información financiera robada. Fue cerrado por el Departamento de Justicia de EE.UU. en 2017, lo que llevó al arresto de su fundador, Alexandre Cazes, quien más tarde fue encontrado muerto en su celda.

Hansa Market (2015–2017)

Este mercado ganó popularidad después de Alpha Bay's cierre, pero en un giro dramático de los acontecimientos, fue secretamente tomado por la policía holandesa en 2017. Las autoridades operaron el sitio durante un mes, recopilando datos de los usuarios antes de cerrarlo.



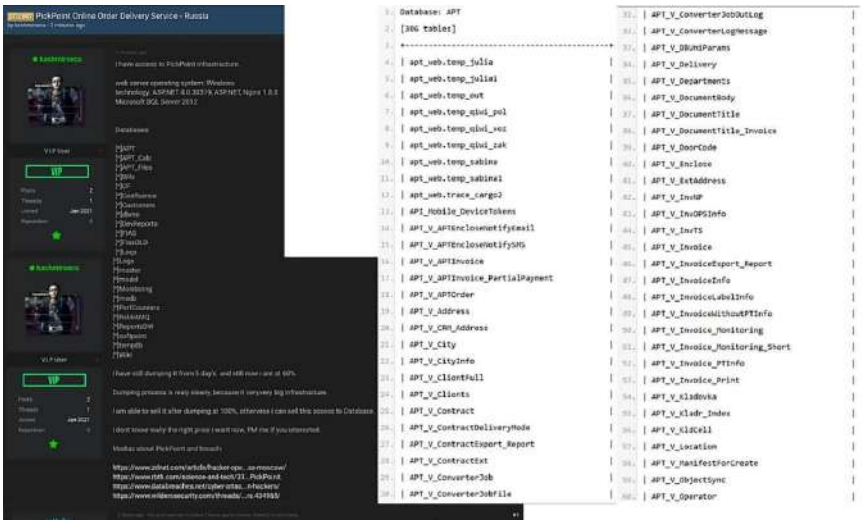
Wall Street Market (2016–2019)

Otro mercado significativo de la dark web, facilitó comercio ilegal antes de ser incautado por Europol en 2019. Sus administradores fueron arrestados y se confiscaron millones de dólares en criptomonedas.



Dark Market (2021)

Este fue uno de los mercados ilegales más grandes en la dark con casi 500.000 usuarios. Fue desmantelado por las autoridades alemanas en una operación coordinada que involucró a varios países. Aunque estos mercados suelen estar vinculados a actividades ilegales, la dark web en sí no es completamente ilegal. También es utilizada por periodistas, activistas y denunciantes para comunicarse de forma segura. Por ejemplo, organizaciones de medios como The New York Times y



Razones para usar o evitar la dark web

Además de las compras y ventas prohibidas, existen razones válidas por las que uno puede estar interesado en utilizar la dark web. Las personas dentro de sociedades cerradas y que enfrentan una censura intensa pueden usar la dark web para comunicarse con personas fuera de la sociedad. Incluso las personas en sociedades abiertas pueden tener cierto interés en utilizar la dark web,

especialmente en lo que respecta a las investigaciones

la recopilación de datos continúa aumentando a nivel mundial. No es difícil suponer por qué podría ser la situación: la web oscura ofrece un cierto grado de seguridad de la individualidad que Internet de superficie no ofrece. Los criminales que buscan proteger sus identidades para evitar la detección y la captura se han sentido atraídos por el aspecto de la web oscura. Debido a esto, no es sorprendente que varios hackeos notables y violaciones de información estén vinculados con la web oscura de una u otra manera.



En 2015, como ejemplo, se robó un tesoro de información de

salió de Ashley Madison, un sitio que afirmaba ofrecer a las parejas una forma de engañar a sus cónyuges. La información robada apareció en la web oscura, donde luego fue recuperada y compartida con el público en general. En 2016, la entonces fiscal general de Estados Unidos, Loretta Lynch, advirtió que las ventas de armas que ocurren a través de Internet oscuro se estaban volviendo más frecuentes, ya que permitía a compradores y vendedores evadir regulaciones. Ilegal

la pornografía es otra ocurrencia relativamente común en el la web

Capítulo 4

ACCESO SEGURO A LA DARK WEB



“"El anonimato es una espada de doble filo— protégete antes de aventurarte hacia los rincones invisibles de Internet."

———————

Conocer los riesgos antes de ingresar puede marcar la diferencia entre seguridad y exposición. Internet que navegas diariamente representa solo una pequeña fracción de la vasta World Wide Web. Según estimaciones, la web contiene casi 500 veces más contenido que lo que

Google indexa en sus resultados de búsqueda. La parte de

eso a lo que los motores de búsqueda como Google pueden “surface web”, mientras que la parte no indexada por búsquedas se conoce como la “deep web” o la “web invisible.”

Comprendiendo la Deep Web

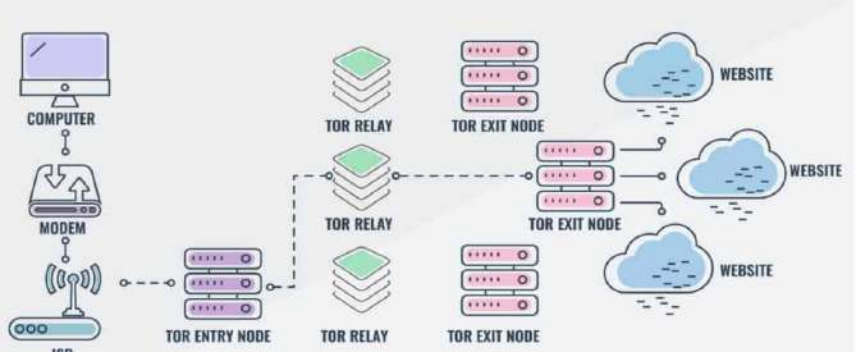
Mucho de la deep web permanece oculto simplemente porque la los usuarios no requieren acceso a ella. Muchos de sus contenidos se almacenan en bases de datos que Google no indexa o del rastreo está restringido. Ejemplos incluyen revistas académicas, expedientes judiciales, perfiles privados de redes sociales, documentos almacenados en servicios en la nube y contenido dentro de aplicaciones móviles. Aunque estos recursos existen en línea, no son accesibles automáticamente a través de los motores de búsqueda.



⚠Advertencia: Tu proveedor de servicios de Internet (ISP) puede

Una parte significativa de esta guía se centra en el anonimato redes como Tor, que permiten a los usuarios acceder a la dark web. Sin embargo, los proveedores de servicios de Internet (ISPs) pueden detectar cuando alguien está usando Tor, ya que las direcciones IP de los nodos de Tor son públicas.

Para mantener la privacidad, los usuarios pueden utilizar una VPN o —nodos alternativos que no están listados públicamente. Para los usuarios de Tor basados en EE. UU., a menudo se recomienda usar una VPN, ya que ofrece mejor velocidad y fiabilidad. Debido a cambios recientes en las leyes de EE. UU., los proveedores de servicios de Internet (ISP) pueden recopilar y vender datos de los usuarios, incluida la historia de navegación.



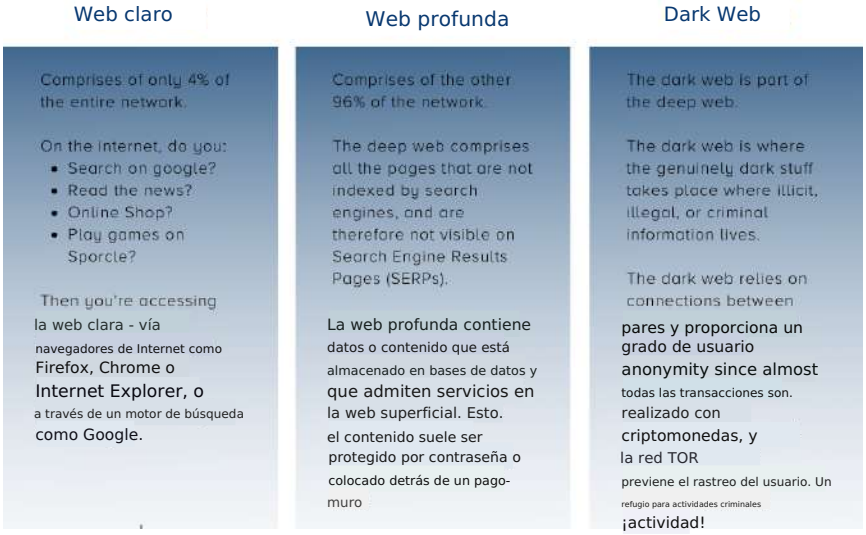
Deep Web vs. Dark Web: la deep web a menudo se confunde con la dark web, también conocida como la darknet o web negra. En términos simples, la deep web consiste en todo el contenido en línea que no está indexado por los motores de búsqueda. A diferencia de la dark web, no requiere herramientas especializadas para acceder; los usuarios solo deben saber dónde mirar.

Biblioteca Virtual El primer índice web, funcionando más como un directorio que como un motor

Surf wax: Indexa feeds RSS (aunque su funcionalidad puede estar limitada

Ice Rocket: Busca en blogs y Twitter para la deep web contenido.

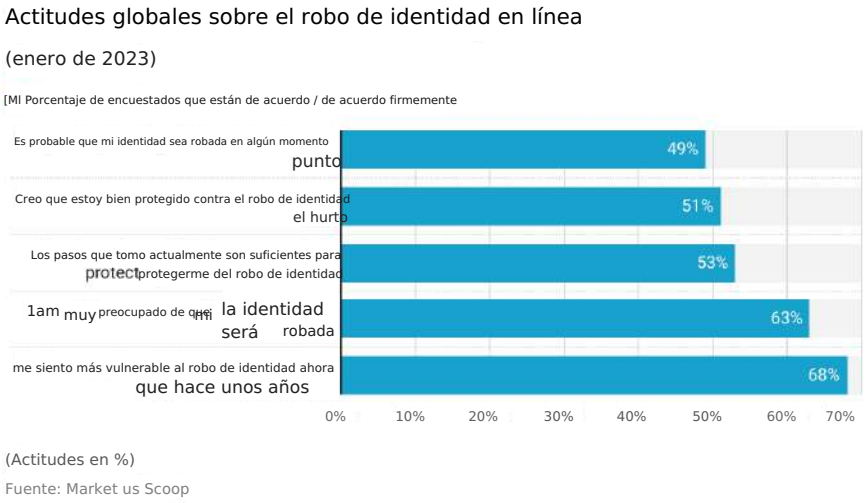
Por ejemplo, los registros legales se pueden encontrar en archivos, mientras que los documentos académicos están disponibles en bases de datos de investigación. Los usuarios también pueden refinar las búsquedas utilizando tipos de archivo específicos, como PDF o hojas de cálculo de Excel, mediante operadores como "filetype: PDF" en las consultas de búsqueda.



La Dark Web: Anonimato y Riesgos

La dark web es una pequeña subsección de la web profunda que intencionalmente oculta. A diferencia de la web profunda, el contenido de la dark web requiere herramientas especializadas, como el navegador Tor, para acceder. A menudo, la dark web se asocia con actividades ilegales, como mercados de drogas, armas y información financiera robada. Sin embargo, también se utiliza para fines legítimos, como foros privados, comunicación anónima y denuncias seguras. Una de las características definitorias de la dark web es su énfasis en el anonimato. Los usuarios pueden operar sin ser rastreados por

corporaciones o gobiernos, siempre que tomen las medidas medidas de seguridad. Periodistas, activistas y denunciantes, incluyendo a Edward Snowden, han utilizado la web oscura para compartir información sensible. La filtración de datos de Ashley Madison, por ejemplo, fue publicada por primera vez en un sitio accesible solo a través de Tor.



Cómo acceder de forma segura a la Dark Web

La dark web es descentralizada, al igual que la web superficial, con servidores distribuidos en todo el mundo. La forma más segura de acceder a ella es a través de la red Tor (The Onion Router). Las direcciones de la dark web suelen terminar en “.onion” en lugar de dominios comunes como ".com" o ".org", lo que indica que solo son accesibles a través de Tor.

Pasos para acceder a la Dark Web:

Descargar e instalar el navegador Tor: la forma más segura para navegar por la dark web es a través del navegador Tor, que es

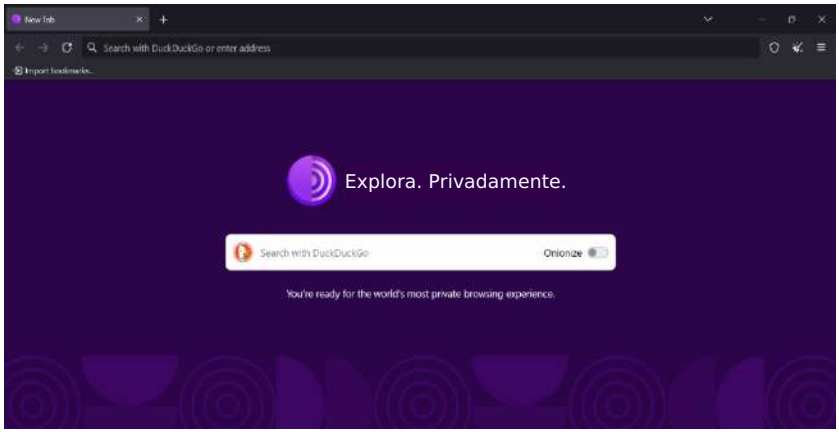
basado en Firefox y enruta el tráfico a través de múltiples relés cifrados.

Asegúrate de descargar desde la fuente oficial

Para evitar malware, siempre descarga el navegador Tor desde su sitio web oficial.

Evita navegadores Tor de terceros

Oficialmente, el navegador Tor está disponible para Windows, Mac, y Linux. Usar navegadores basados en Tor de terceros en otras plataformas puede presentar riesgos de seguridad.



Al seguir estas precauciones, los usuarios pueden navegar por la web de forma segura mientras minimizan los riesgos asociados a las herramientas de anonimato en línea.

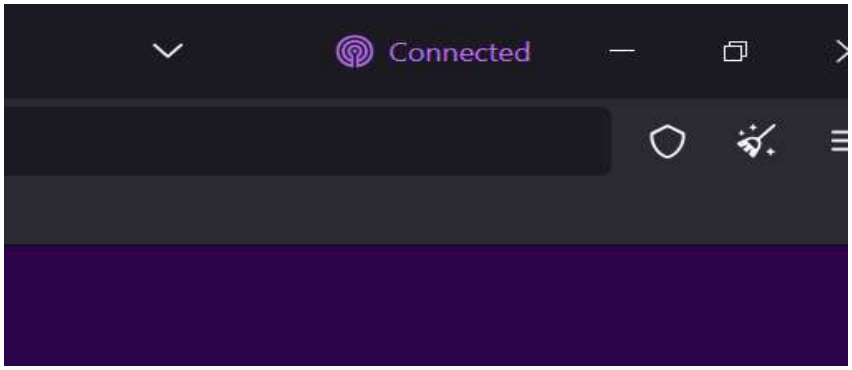
Accede a la dark net en Android usando Tor Browser (ACTUALIZACIÓN)

El navegador Tor oficial está actualmente disponible en Android. Puedes obtenerlo fuera de The Play Store o de las descargas de Tor

página web. Al momento de escribir, Tor Browser para Android alpha, y también requiere que configures Orbot como requisito

Navegando por la Web oscura

Ahora puedes navegar con seguridad por sitios de la dark net y wikis, pero si planeas hacer algo más largo que eso, querrás dar varios pasos. Es decir, configurar correo electrónico cifrado usando una dirección de correo nueva, con un seudónimo, establecer una wallet de Bitcoin anónima, deshabilitar JavaScript en Tor Browser, explorar proveedores y mucho más.



Encontrar sitios .onion es tu primer reto, ya que no aparecerán en los resultados de búsqueda de Google. No puedes simplemente buscar en Google "Silk Road" y esperar aterrizar en la web oscura. Sin embargo, algunos motores de búsqueda de la dark web indexan sitios .onion, incluyendo Onion.City, Onion.to y Not Evil. Si buscas bienes específicos, especialmente medicamentos y narcóticos, puedes usar Grams.

Reddit también puede ser un recurso valioso para navegar por La web oscura. Subreddits como /r/deep web, /r/onions y /r/Tor pueden ayudar. Además, los directorios de wikis ocultos pueden ayudar a acotar su búsqueda. El anonimato y la seguridad son cruciales al navegar por la web oscura. Aunque su ISP y las autoridades pueden no ser capaces de ver sus actividades en la red Tor, pueden detectar que está usando Tor, lo que puede levantar sospechas. De hecho, una reciente decisión de la Corte Suprema de los EE. UU. declaró que meramente usar Tor podría considerarse causa probable para que las fuerzas del orden investiguen cualquier computadora en el mundo. Otra precaución crítica es asegurar que sus URLs .onion sean precisas. Estas URL suelen consistir en una serie aleatoria de letras y números. Dado que HTTPS se usa raramente en la web oscura, los certificados SSL no pueden verificar la legitimidad del sitio. Siempre confirme una URL de al menos tres fuentes diferentes antes de usar un sitio de la web oscura. Una vez verificada, guárdela en una nota encriptada— el navegador Tor no almacena en caché las URL. De lo contrario, corre el riesgo de caer víctima de estafas como mezcladores de Bitcoin falsos. Para mayor seguridad, se recomienda encarecidamente usar una VPN.

VPN sobre Tor vs. Tor sobre VPN

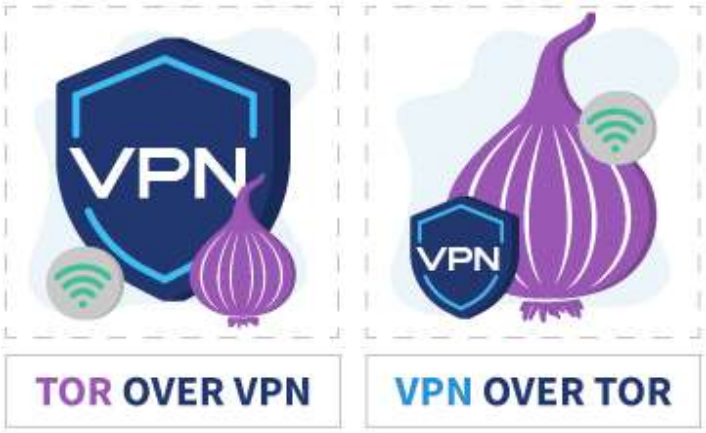
Una VPN cifra todo el tráfico de Internet que viaja hacia y desde dispositivo y lo enruta a través de un servidor de su elección. Cuando se combina con Tor, mejora la seguridad y el anonimato. Aunque tienen un objetivo similar, Tor da prioridad al anonimato, mientras que

una VPN se centra en la privacidad. Combinar ambos reduce el el orden en que se usan marca una diferencia significativa.

Tor sobre VPN

Si te conectas a una VPN primero y luego usas el navegador Tor, estás empleando Tor sobre VPN, el método más común. En esta configuración:

Tu ISP sólo ve tráfico VPN cifrado y no will saber que estás usando Puedes acceder a sitios onion. normalmente. Sin embargo, este método requiere confianza en tu proveedor de VPN, que puede ver que estás usando Tor y puede conservar registros de metadatos, incluso si no puede ver el contenido de tu tráfico Tor. Elegir un VPN sin registros es crucial. Algunos VPN, como NordVPN, ofrecen funcionalidad integrada de Tor sobre VPN, lo que te permite acceder a Tor sin usar el navegador Tor. Sin embargo, otros navegadores pueden seguir filtrando datos identificativos. Tor sobre VPN no protege a los usuarios de nodos de salida maliciosos de Tor. Dado que los nodos de Tor son operados por voluntarios, algunos pueden intentar interceptar datos.



VPN sobre Tor

Menos común pero recomendado por el Proyecto Tor oficial, El VPN sobre Tor funciona de

1. El tráfico de Internet primero pasa por Tor, luego a través de la VPN.
2. El proveedor de VPN no ve tu dirección IP real.
3. La VPN te protege de nodos de salida maliciosos de Tor.
4. Solo unos pocos proveedores de VPN, como AirVPN y BolehVPN, soportan VPN sobre Tor. Sin embargo, no son conocidos por tener altas velocidades.

Tor sobre VPN es mejor para acceder a sitios .onion, mientras VPN sobre Tor es ideal para evitar nodos de salida maliciosos de Tor. Algunos argumentan que VPN sobre Tor es más seguro ya que mantiene el anonimato durante el proceso, suponiendo que la VPN se pague de forma anónima. Aunque el Proyecto Tor desaconseja VPN sobre Tor, ambos métodos son más seguros que usar Tor solo.

I2P

I2P (Proyecto de Internet Invisible) es una alternativa anónima red de Tor. A diferencia de Tor, I2P no puede acceder a Internet regular; solo puede alcanzar servicios ocultos dentro de la red I2P. No admite sitios .onion, ya que opera en una red separada, usando "respites" en su lugar.



Aunque es menos popular y más complejo de configurar, I2P ventajas sobre Tor: es más rápido y más fiable gracias a su avanzado sistema de enrutamiento peer-to-peer. No se apoya en un directorio centralizado para la información de enrutamiento.

Freenet

Al igual que I2P, Freenet es una red descentralizada punto a punto que no permite el acceso a Internet estándar. En su lugar, los usuarios solo pueden acceder al contenido cargado en el almacén de datos distribuido de Freenet. A diferencia de I2P y Tor, alojar contenido no requiere un servidor dedicado. Una vez cargado, el contenido permanece en Freenet mientras siga siendo popular.



Freenet ofrece dos modos de conexión:

Modo darknet: Los usuarios se conectan solo con pares de creando redes privadas y anónimas. Modo de red abierta: los usuarios se conectan automáticamente a pares aleatorios y utilizan unos pocos servidores dedicados para el enrutamiento. Freenet es relativamente fácil de usar. Después de la instalación, funciona a través de una interfaz de navegador. Sin embargo, por razones de seguridad, se recomienda usar un navegador separado del habitual para mantener el anonimato.

Buscadores y la Deep Web

Google y Bing dominan el mercado de motores de búsqueda, con Google posee alrededor del 92% y Bing alrededor del 3%. Indexan automáticamente grandes cantidades de datos, pero no cubren todo. Muchos sitios web se ocultan deliberadamente de los motores de búsqueda, formando lo que se conoce como la Deep Web.

¿Es ilegal la Darknet?

No, la darknet en sí no es ilegal. Es simplemente una parte de Internet sin censura ni regulación. Es utilizada por activistas, periodistas e investigadores, pero también por delincuentes. Su anonimato lo convierte en una espada de doble filo. La darknet sigue siendo uno de los últimos bastiones de la libertad de expresión, permitiendo que las personas se comuniquen sin temer la vigilancia. Sin embargo, también ofrece una plataforma para mercados ilegales, foros de hacking y contenido ilícito. Para quienes exploran la dark web, el conocimiento, la precaución y las medidas de seguridad son esenciales para mantenerse seguros.

Capítulo 5

LUMINARIOS EN EL DARKNET



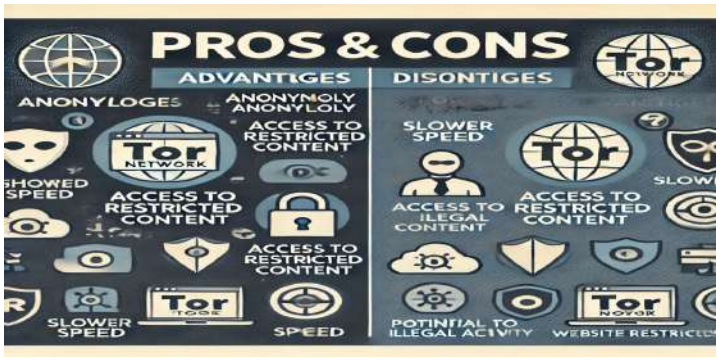
“"No todo lo que está en las sombras es siniestro—a veces, las luces más brillantes brillan donde menos se esperan."

La Darknet no es solo un lugar para criminales—denunciantes, investigadores y activistas también dependen de él. La Darknet no es solo un centro para contenido ilegal o cuestionable. Aunque indudablemente alberga mercados criminales, foros de malware y otras actividades subterráneas, también contiene algunos sitios web y comunidades legítimos. Para ser claros, la darknet sigue siendo un espacio de alto riesgo y no regulado. No deberías simplemente descargar un navegador Tor y empezar a explorar sin entender los riesgos. Según TechRepublic, la darknet alberga entre 10,000 y 100,000 sitios web, mientras que la red Tor tiene aproximadamente dos millones de usuarios activos en todo el mundo. Algunos de estos usuarios participan en actividades ilícitas, pero muchos simplemente buscan

anonimato mientras navegas por la red de superficie o contribuyes comunidades legítimas y valiosas de la dark

10 Puntos brillantes en el Darknet

El Darknet no es solo un centro para el ciberdelito, también hay mundo oculto de sitios útiles e incluso fascinantes. Cuando la mayoría de las personas oyen “darknet”, piensan en actividades ilegales: mercados negros, foros de hacking y contenido perturbador escondido en las sombras de Internet. Y sí, esas cosas existen. Pero el darknet no es solo oscuridad y pesimismo. Sorprendentemente, hay muchos lugares legítimos, informativos y hasta divertidos escondidos en las profundidades de Tor. Ya sea juegos anónimos, periodismo sin censura o investigación académica, este rincón misterioso de Internet tiene puntos brillantes que vale la pena conocer.



1. The Chess – Juega Partidas de Ajedrez Anónimas

Imagina un lugar donde puedas jugar ajedrez contra sin nombres de usuario, sin chat y completamente anónimo. Eso es exactamente lo que ofrece The Chess. Tú creas

una cuenta temporal y puede jugar partidas de ajedrez

Hay un pequeño foro donde los usuarios discuten

Sin embargo, la mayor desventaja es que el sitio parece sacado directamente de Windows 95, funcional, pero muy anticuado.



2. Investigación académica – Acceso gratuito al conocimiento

La educación debería ser gratuita, ¿verdad? La Darknet tiene recursos controvertidos pero útiles para la investigación académica. Sci-Hub es una herramienta de darknet bien conocida

miles de artículos académicos. Sin embargo, es cuestionable. Una alternativa más ética es el American Journal of Freestanding Research Psychology (AJFRP)—la primera revista académica de acceso abierto hospedada en la darknet. A diferencia de Sci-Hub, esto es completamente legal, ya que los autores envían voluntariamente su propio trabajo.



3. ProPublica – Periodismo sin censura

En países donde el gobierno censura las noticias,

acceder a la verdad puede ser peligroso. Ahí es donde entra la versión darknet de ProPublica. ProPublica es una plataforma de periodismo de investigación ganadora del Premio Pulitzer. Las personas en regiones censuradas pueden leer noticias independientes de forma segura, sin dejar huellas digitales. A diferencia de los sitios de noticias habituales, ProPublica no rastrea tus datos.

"No queremos que nadie sepa que nos visitaste

ni qué leíste." **de Mike Tiga's**



4. Secure Drop – Refugio seguro para denunciantes

Te has preguntado alguna vez cómo los denunciantes filtran

a los periodistas? Secure Drop es la respuesta. Es ampliamente utilizado por grandes medios como The Washington Post, The New Yorker, Vice Media y Forbes. Secure Drop no registra direcciones IP ni almacena datos del navegador, garantizando la máxima seguridad para quienes envían información confidencial. Incluso los EE. UU.

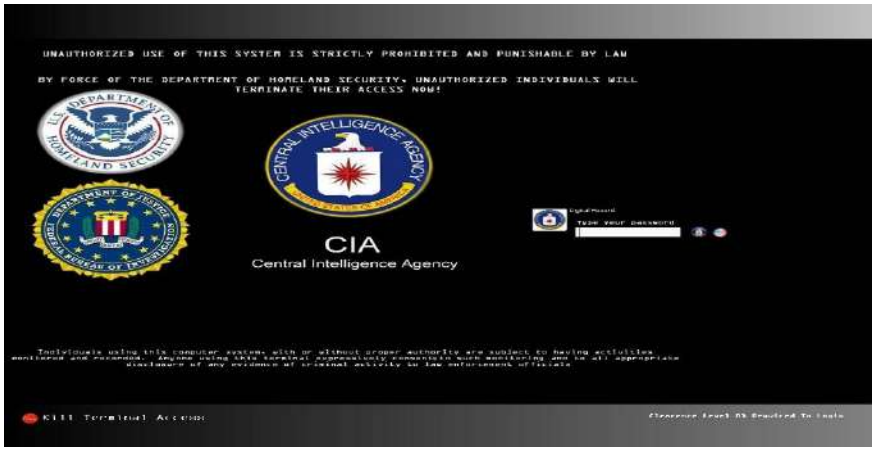
el gobierno lo está probando para vulnerabilidad de seguridad informes.

Qué hace SecureDrop



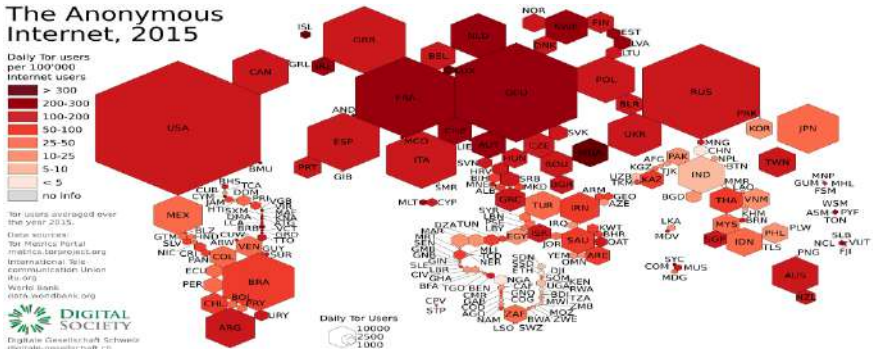
5. El sitio oculto de la CIA

Sí, incluso la CIA tiene un sitio web darknet. Es un simple formulario de contacto donde las personas pueden enviar información de forma anónima. La agencia garantiza "cuidar cuidadosamente toda la información que proporcionas, incluida tu identidad." Aunque no es una plataforma de inteligencia completa, es una de las presencias gubernamentales más sorprendentes en la darknet.



6. Tor Metrics – ¿Quién realmente usa Tor?

¿Crees que la darknet es solo para delincuentes? El 60% del uso de completamente legal. Tor Metrics es un sitio web de datos públicos que rastrea cuántas personas usan Tor en todo el mundo y para qué fines. La censura política sigue siendo una de las principales razones por las que las personas recurren a Tor, mientras que muchos periodistas, investigadores y usuarios cotidianos confían en él para la privacidad en línea.



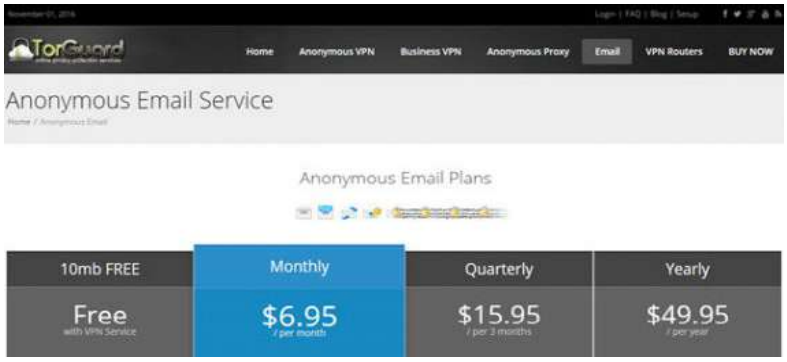
7. Túneles IIT – Exploración Urbana de la Vida Real

Muy profundo bajo el Illinois Institute of Technology (IIT) se misterioso red de túneles subterráneos abandonados. Un usuario de darknet pasó meses explorando estos túneles y publicó fotos y mapas en línea. Nadie sabe exactamente por qué fueron construidos: unos dicen que eran para tuberías de vapor, mientras que otros creen que eran puntos de acceso secretos para la universidad. Este descubrimiento ha generado tanto fascinación como teorías de conspiración.

8. Servicios de correo anónimo – Privacidad primero

En un mundo donde Google, Yahoo y Outlook rastrean todo, los proveedores de correo darknet ofrecen un enfoque

alternativa. Una de las más conocidas es Proton Mail, desarrollado por científicos del MIT y CERN. Proton Mail ofrece cifrado de extremo a extremo, y a diferencia de los proveedores de correo habituales, no requiere ningún dato personal para crear una cuenta.



9. Búsqueda sin anuncios – Sin seguimiento, Sin anuncios

¿Odias los anuncios en línea? DuckDuckGo es un motor de que:

1. No rastrea a los
2. No guarda el historial de
3. No tiene

A diferencia de Google, DuckDuckGo no venderá tus datos. No es solo para la darknet: también puedes usarlo en la web



10. Tor Kittenz – La parte más adorable de la Darknet

Creas o no, alguien hizo un sitio web solo para Tor que era solo una galería de fotos de gatos. Tenía un diseño retro de los años 90, y aunque ya no existe, fue uno de los pocos sitios de la Darknet puramente saludables, demostrando que no todo en los rincones ocultos de la web es siniestro.



Reflexiones finales: La Darknet no es solo crimen y caos

Sí, hay lugares peligrosos en la darknet. Pero, como hemos visto, también hay partes positivas y útiles—

herramientas educativas, comunicación segura, e incluso simples diversión como jugar al ajedrez o compartir fotos de gatos. La curiosidad es buena, pero la seguridad es lo primero. Si alguna vez decides explorar, asegúrate de usar medidas de seguridad adecuadas y mantenerte en sitios de confianza.

⚠ NOTA IMPORTANTE:

Nunca intentes acceder a sitios onion a través de un navegador navegador web. Si eliges explorar la darknet, hazlo con precaución, usando medidas de seguridad adecuadas.

Capítulo 6

REVELANDO INTERNET OCULTO



“"Tor no es solo una herramienta—es una puerta de anonimato, para mejor o peor."

Ya sea que busques privacidad o secreto, entender Tor es el primer paso

La World Wide Web, en su esencia, es una red de computadoras que se comunican entre sí. La Computadora A solicita información a la Computadora B, y la Computadora B devuelve los datos. Estos datos pueden ser una página web, un anuncio, un cálculo casi cualquier cosa. Cada computadora involucrada en este intercambio tiene un único

identificador conocido **dirección IP (Protocolo de Internet).** Estas direcciones se ven algo así: 29.75.148.222. Dado que las direcciones IP son difíciles de recordar, a menudo se reemplazan por nombres de dominio. Por ejemplo, cuando escribes **"facebook.com"** tu Proveedor de Servicios de Internet (ISP)

traducen ese dominio a la dirección IP correspondiente de el servidor de Facebook. Facebook luego responde entregando los datos solicitados a tu computadora. Este método de comunicación se aplica a todas las áreas de Internet, incluyendo la deep web y la dark web. La diferencia entre estas y la web regular radica en cuánto se puede encontrar fácilmente el contenido.

La Deep Web vs. la Surface Web

Cuando buscas en Google Facebook, CapitalOne o TSN, recibes resultados indexados—estos son ejemplos de la web de superficie. Cualquier cosa que aparezca en los resultados de un motor de búsqueda forma parte de esta web indexada. Sin embargo, no todo el contenido es searchable. Por ejemplo, conversaciones privadas de WhatsApp, correos electrónicos personales, portales bancarios o incluso anuncios clasificados en ciertos sitios web no son accesibles a través de motores de búsqueda tradicionales. Esta porción in searchable de Internet es lo que llamamos la deep web. La deep web también contiene una gran cantidad de datos que se generan constantemente por máquinas—tales como registros del sistema, informes de monitoreo de salud y comunicaciones del servidor. La mayoría de esta información no es interesante para el usuario promedio. De hecho, la web de superficie searchable representa solo alrededor del 10% de Internet en su totalidad, mientras que la deep web representa el 90% restante.

La Deep Web vs. la Dark Web

Las personas a menudo usan los términos "deep web" y "dark

de manera intercambiable, pero son bastante diferentes. La dark web es una pequeña parte de la deep web, como una capa oculta debajo de la ya escondida deep web. A diferencia de la deep web general, que incluye contenido no indexado pero normal, la dark web está diseñada intencionadamente para el anonimato y requiere herramientas especializadas para acceder. Debido a que la dark web permite a los usuarios ocultar sus identidades, ha ganado reputación como un centro de actividades ilegales. Sin embargo, sus orígenes no son tan siniestros como se podría pensar. Antes de que internet se volviera popular, los primeros usuarios en línea participaban en

discusiones anónimas a través **Internet Relay Chats (IRC).** Algunas de las actividades delictivas actuales en la dark web pueden rastrearse hasta esas comunidades. Dicho esto, no todo en la dark web es ilegal. Muchas personas la utilizan por razones legítimas, como los denunciantes que necesitan proteger su identidad o individuos que viven en países donde la censura en internet restringe el acceso a la información. A diferencia de la deep web, a la que se puede acceder si tienes un enlace directo, la dark web requiere un navegador especializado. Incluso si un usuario encuentra un enlace a un sitio de la dark web, no puede

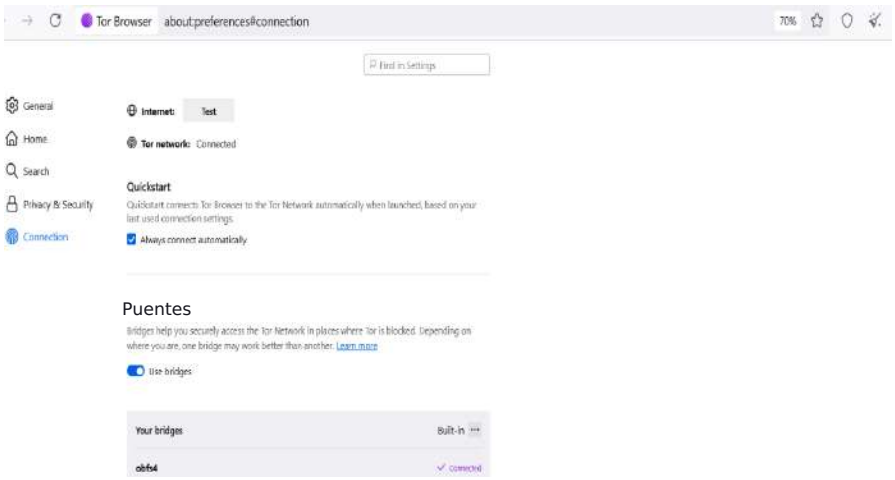
acceder a él a través de navegadores **Chrome o** tradicionales como Firefox.

Es importante señalar que, aunque la metáfora del iceberg se usa comúnmente para describir internet, donde la web superficial es la punta, la deep web está debajo y la dark web es

aún más profundo—esto no es totalmente exacto. En realidad, diferentes secciones existen uno al lado del otro en el mismo espacio, ocultas a plena vista en lugar de existir en compartimentos digitales separados.

Accediendo a la Dark Web: el papel de Tor

El mercado más infame de la web oscura fue Silk Road, que fue cerrado por el FBI en noviembre de 2014. ¿Qué hizo que Silk Road fuera un sitio web "oscuro"? Para acceder a sitios de la dark web, los usuarios deben usar un navegador especializado llamado Tor. Tor parece como cualquier otro navegador, pero ofrece anonimato a través de un método conocido como enrutamiento en cebolla.



El nombre "Tor" en sí significa "The Onion Router" (Enrutador de el enrutamiento funciona haciendo rebotar el tráfico de internet del usuario a través de múltiples computadoras, conocidas como nodos o relés, antes de llegar al destino final. Cualquier computadora que ejecute Tor

el software puede actuar como un nodo. Al pasar por múltiples capas de cifrado, se vuelve casi imposible rastrear la fuente original de la solicitud. Sin embargo, este proceso hace que la navegación sea extremadamente lenta. Mientras que los usuarios de Tor pueden visitar sitios web normales como lo harían en Chrome o Firefox, los sitios de la dark web tienen extensiones de dominio únicas que terminan en “.onion” en lugar de “.com”. Estos sitios solo pueden ser accedidos a través del navegador Tor.

Los orígenes de Tor: ¿Quién lo creó?

Contrario a la creencia popular, Tor no fue desarrollado por o ciberdelincuentes. De hecho, fue creado por el gobierno de EE. UU. El concepto de onion routing fue financiado por primera vez por la Oficina de Investigación Naval de EE. UU. en 1995 y luego mejorado con el apoyo de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) en 1997. La tecnología finalmente se lanzó al público en 2002.

¿Se puede hackear Tor? ¿Es realmente segura la anonimidad?

Tor en sí es altamente seguro, y hackear el algoritmo es considerado casi imposible. Sin embargo, ningún sistema es completamente infalible. Si las fuerzas del orden o los ciberdelincuentes quieren rastrear a alguien que usa Tor, no atacan la tecnología en sí, sino que apuntan al error humano.



Por ejemplo, durante la Segunda Guerra Mundial, la Enigma de la máquina fue descifrada no por fuerza bruta sino mediante una comprensión de los patrones y comportamientos humanos. También existen vulnerabilidades en la forma en que opera Tor. Aunque el navegador protege a los usuarios de ser rastreados directamente, no evita que descarguen malware accidentalmente que podría revelar su identidad. Además, los nodos de salida de Tor —donde el tráfico encriptado sale de la red— pueden ser monitoreados, exponiendo potencialmente la actividad de los usuarios.

¿Por qué es importante la información sobre la Deep Web y la Dark Web?

Dado que la Deep Web y la Dark Web ofrecen anonimato, tienen se han convertido en puntos de interés para actividades ilegales. Sin embargo, estas áreas ocultas también proporcionan inteligencia valiosa para expertos en ciberseguridad, las fuerzas del orden y las corporaciones. Por ejemplo, la deep web contiene foros no indexados donde las personas pueden incitar al discurso de odio, coordinar amenazas o discutir actividades ilegales como el hurto y el consumo de drogas. De manera similar, sitios de paste como Pastebin suelen usarse para compartir datos filtrados. la dark web eleva la actividad ilegal a otro nivel. Aunque muchos sitios

son estafas, otros funcionan como mercados para drogas, datos datos, servicios ilegales y cosas

7 Formas en que el Mundo Oculto de la Darknet está evolucionando

La darknet ya no está tan escondida como antes. Lo que alguna parte secretiva de Internet que ahora es más accesible. Hoy, cualquier persona con habilidades técnicas básicas puede descargar un navegador Tor y comenzar a explorar, a menudo usando criptomonedas para el anonimato. Pero con más accesibilidad vienen mayores riesgos. Los cibercriminosos usan la darknet para vender narcóticos, datos robados y servicios ilegales. Las agencias de aplicación de la ley han intensificado su represión. Ross Ulbricht, el fundador del infame mercado Silk Road, cumple ahora dos cadenas perpetuas más 40 años por tráfico de drogas y lavado de dinero. Incluso dentro de la darknet, las cosas están cambiando.



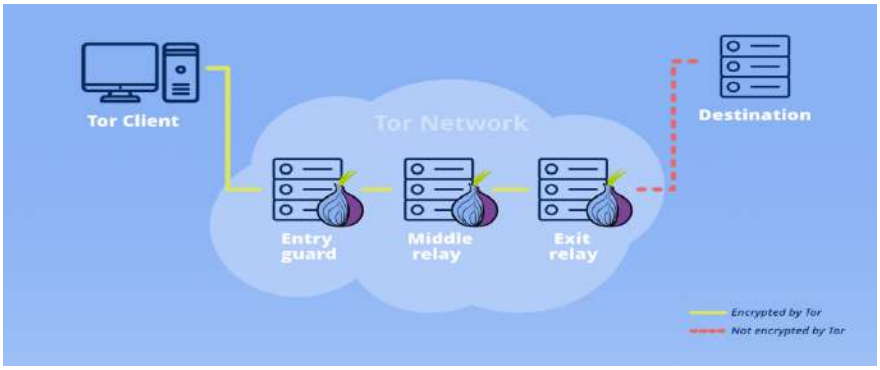
1. La batalla no ha terminado

A pesar de su creciente visibilidad, la darknet sigue siendo un campo de batalla. Más allá de los mercados conocidos y los casos ampliamente reportados, el verdadero peligro se encuentra en los rincones difíciles de alcanzar de internet: foros ocultos, salas de chat cifradas y filtraciones de datos secretas. Para las empresas, esto representa una amenaza creciente para la ciberseguridad. Los estudios indican que los riesgos ocultos están creciendo rápidamente, y muchas organizaciones desconocen cómo se está circulando su información sensible dentro de estas redes secretas.



2. La darknet se extiende más allá de Tor

Muchas personas creen erróneamente que la darknet se limita a sitios accesibles a través del navegador Tor. Sin embargo, la darknet va más allá de los sitios .onion. "La darknet es cualquier espacio en línea que no está fácilmente disponible para el público", explica Andrei Barysevich de Recorded Future. Algunos centros de la darknet son anteriores a Tor y continúan funcionando utilizando protocolos alternativos como I2P, GNU net y Riffle.



3. Las amenazas empresariales están aumentando

La darknet no es solo para la venta de drogas ilícitas. También cibercriminales que venden herramientas y servicios que apunten específicamente a las corporaciones. Un estudio de Bromium encontró un aumento del 20% en los listados de la darknet que representan amenazas para las empresas entre 2016 y 2019. Estos incluyen:

1. Malware dirigido
2. Servicios de ataques DDoS específicos para
3. Datos corporativos
4. Kits de phishing de

Muchos de estos vendedores son altamente secretos; el 70% de los solo se comunican a través de canales

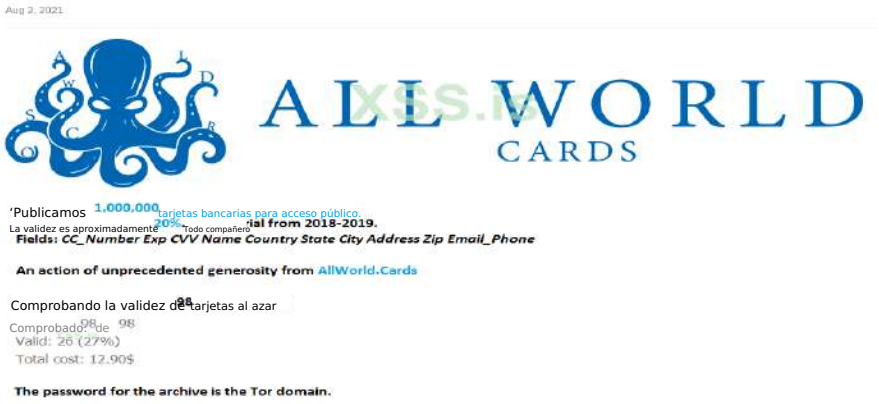
4. Las tendencias del ciberdelito reflejan las amenazas empresariales

La actividad en la darknet a menudo refleja tendencias en la amenazas de ciberseguridad. Una preocupación creciente son los ataques de whale (whaling), donde se apuntan a ejecutivos de alto perfil mediante ingeniería social. Un informe de IBM X-Force de 2019 reveló que

El 13% de todos los ciberataques involucraron compromiso de (BEC) o caza de

5. Las identidades digitales robadas se venden en masa

En 2019, los ciberdelincuentes comenzaron a vender identidades identidades. Estas incluyen: 1. credenciales de inicio de sesión bancarias y de redes sociales 2. cookies web y huellas dactilares del navegador 3. huellas dactilares de canvas HTML5 Los precios van de $5 a $200 por identidad, lo que facilita a los ciberdelincuentes hacerse pasar por individuos como nunca.



6. El acceso a la red corporativa está a la venta

Investigadores de Bromism descubrieron que muchos ofrecen acceso de puerta trasera a sistemas corporativos, con al

60% de proveedores que venden acceso no autorizado a múltiples redes de perfil.

7. La propiedad intelectual está en riesgo

Cuando los investigadores de Bromism preguntaron a un vendedor acceder a tres grandes corporaciones, se les ofreció:

1. Acceso a cuentas de
2. Servicios de extracción de datos
3. Herramientas de
4. Los precios oscilaban entre 1.000 y 15.000 dólares



Conclusión

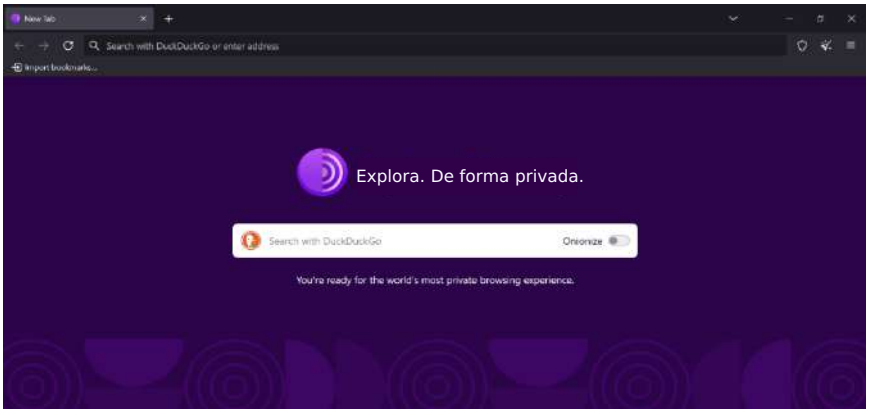
La web superficial es a lo que la mayoría de las personas accede indexada por los motores de búsqueda. La deep web es mucho más grande e incluye contenido no indexado pero mayormente inofensivo. La dark web es una parte pequeña pero significativa de la deep web, diseñada para el anonimato y a menudo asociada con actividades ilegales.

Si la dark web es conocida por sus mercados criminales, también se utiliza

La información de la dark web es crucial para la ciberseguridad, las fuerzas del orden y otras organizaciones que buscan prevenir actividades ilegales. Entender estas distinciones ayuda a separar los hechos de la exageración mediática. No todo en la dark web es criminal, pero sigue siendo un lugar donde chocan los riesgos de seguridad y el anonimato.

Capítulo 7

CÓMO USAR TOR



“"La privacidad es un derecho, pero solo aquellos que dominan el herramientas del anonimato pueden realmente reclamarlo."

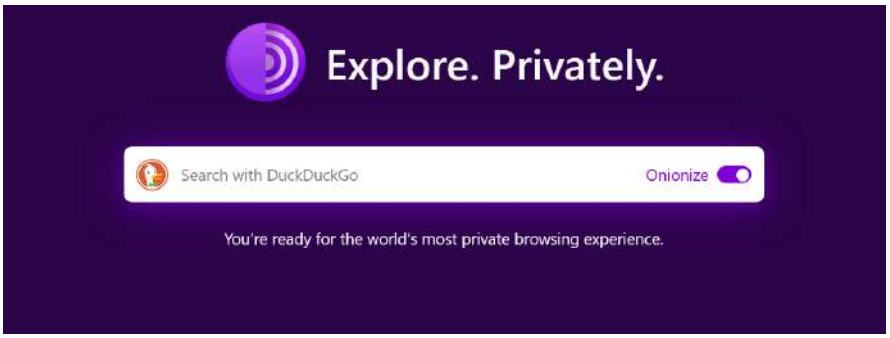
Saber cómo configurar Tor correctamente es la diferencia entre estar oculto y estar expuesto. Recientemente, Boing Boing compartió un artículo sobre algunos bibliotecarios en Massachusetts que han comenzado a usar el software Tor en todas las computadoras públicas para anonimizar la actividad de navegación de sus usuarios. Los bibliotecarios están haciendo esto como una postura contra la vigilancia gubernamental descontrolada y las empresas que rastrean a los usuarios en línea para crear perfiles de marketing dirigidos. Es una iniciativa intrigante y una postura sólida para la privacidad del usuario. Afortunadamente, no es necesario ir a una biblioteca para usar Tor. Conectarse a la red Tor desde tu propio ordenador es rápido y fácil, gracias al navegador Tor, fácil de usar, del Proyecto Tor.

¿Qué es Tor?

Tor es una red global operada por voluntarios. Cada voluntario ejecuta un "relé", que es simplemente un ordenador que ejecuta software que permite a los usuarios conectarse a Internet a través de la red Tor.

Antes de llegar a Internet público, Navegador Tor se conecta a varios relés diferentes, asegurando tu actividad

anonimizado a lo largo del camino, lo que hace que sea casi rastrear tu ubicación e identidad. Aunque Tor ha ganado reputación por usarse para comprar productos ilícitos en línea, el software tiene muchas aplicaciones legítimas. Activistas que esconden su ubicación de gobiernos opresivos y periodistas que se comunican con fuentes anónimas son solo dos ejemplos.



Si, como los bibliotecarios de Massachusetts, no tienes ninguna intención nefaria, Tor sigue siendo una excelente herramienta para mantener tu navegación privada de tu Proveedor de Servicios de Internet (ISP), anunciantes y la recopilación de datos gubernamentales pasiva. Sin embargo, si agencias como la NSA decidieran dirigirse activamente a tu navegación, esa sería una historia completamente diferente.

Comenzando

La forma más fácil de usar Tor es descargando el Tor Navegador. Esta es una versión modificada de Firefox, combinada con otro software que te conecta a la red Tor.

Algunos usuarios prefieren verificar el instalador para asegurarse haber descargado la versión correcta y sin manipular. Si solo quieres mantener tu navegación privada, puedes usar el Modo de Incógnito de Chrome, la Navegación Privada de Firefox o el modo InPrivate de Microsoft Edge. Aunque estos evitan que otros vean tu historial de navegación, no evitan que tu ISP rastree los sitios que visitas. Si quieres navegar por la web de forma completamente anónima, Tor Browser es lo que necesitas.

Usando Tor Browser: Paso a Paso

Instalar y Configurar Tor Browser

Comienza descargando e instalando Tor Browser. Una vez que la instalación esté completa, haz clic en Finalizar, y Tor se iniciará por primera vez. Se te presentará un cuadro de diálogo de configuración que controla cómo te conectas a la red Tor. Por lo general, puedes hacer clic en el botón Conectar, pero si usas un proxy para conectarte a Internet, deberás hacer clic en el botón Configurar para introducir tus configuraciones.

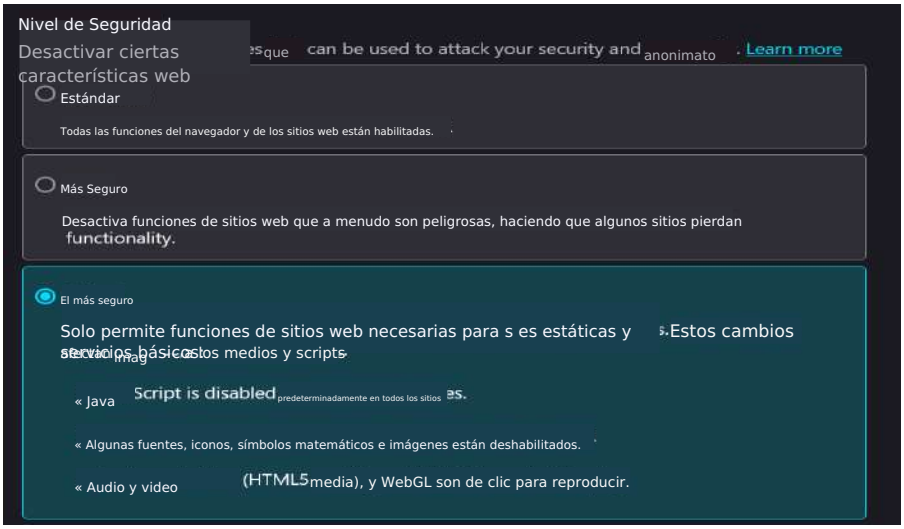
Conéctate a Internet con Tor

Puede haber una leve demora mientras Tor configura el conexión a la red a través de relés. El navegador te informará que la conexión inicial puede tardar unos minutos. Una vez que la conexión esté establecida, Tor Browser se abrirá y estará listo para usar. Dado que Tor utiliza el mismo código subyacente que Firefox, si has utilizado Mozilla’s

el navegador de antes, debería sentirse bastante familiar. Incluso no has usado Firefox, encontrarás la interfaz de Tor muy similar a la de otros navegadores como Edge, Chrome y Safari.

Elige tu nivel de seguridad

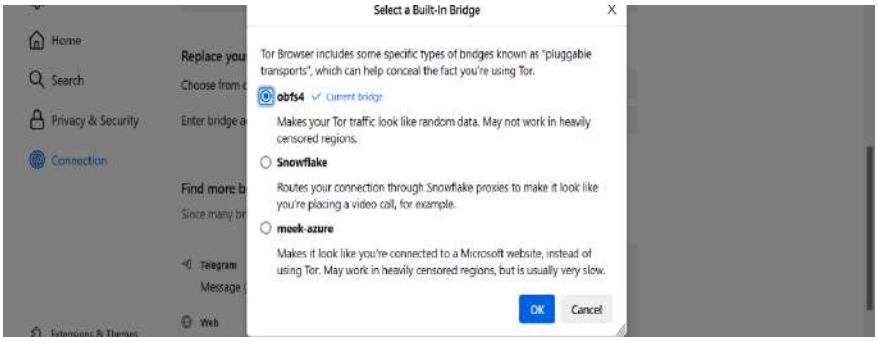
Antes de empezar, es importante señalar que usar Tor involucra un equilibrio entre privacidad/seguridad y comodidad. Por defecto, la seguridad está configurada en Estándar, que sigue siendo mucho más segura que otros navegadores. Para mejorar la seguridad, haz clic en el símbolo de la cebolla junto a la barra de direcciones y selecciona Configuración de Seguridad. Usa el control deslizante de Nivel de Seguridad para ajustar tu nivel de protección preferido.



Cambia tus hábitos de navegación

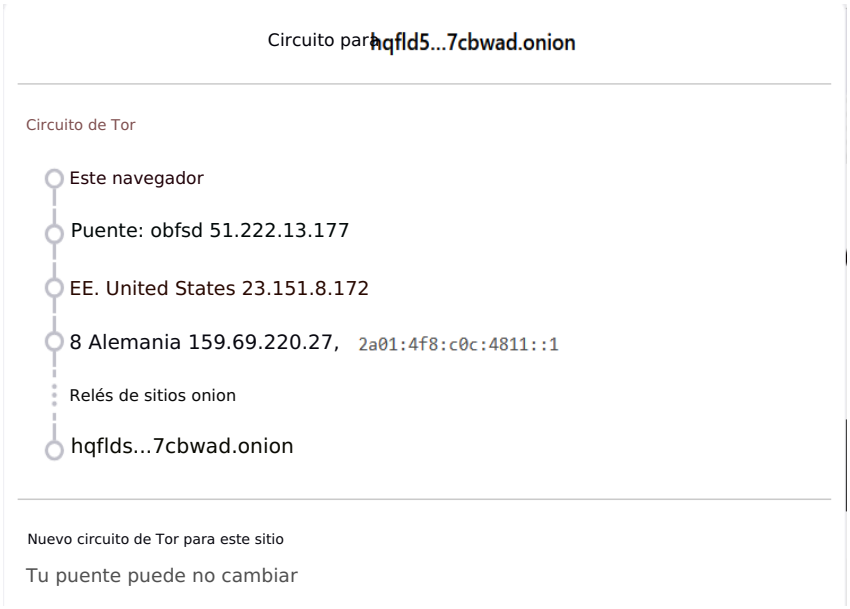
Para sacar el máximo partido a Tor, deberás ajustar algunos de hábitos de navegación. El primer cambio es el motor de búsqueda

uso. En lugar de depender de Google o Bing, se recomienda utilizar Disconnect.me, un motor de búsqueda que evita que los rastreadores supervisen tu actividad. Puedes usarlo con Bing, Yahoo o DuckDuckGo. Además, se recomienda evitar instalar extensiones del navegador, ya que podrían comprometer tu privacidad filtrando información.



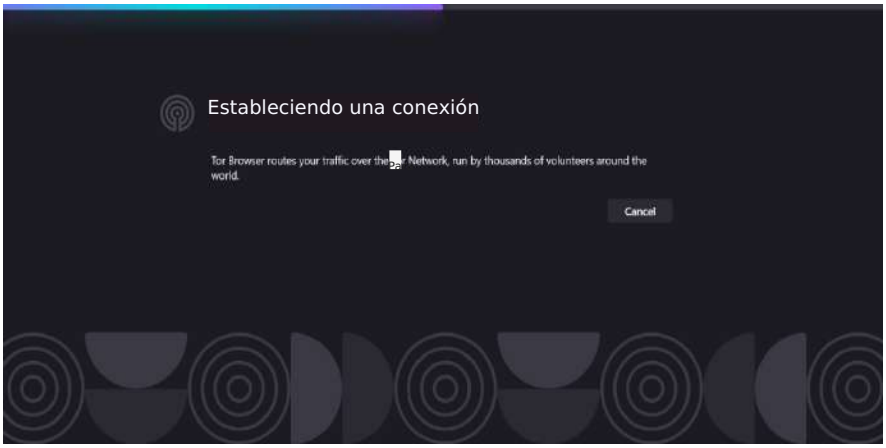
Entiende los Circuitos de Tor

Al navegar por Internet, Tor mantiene tus actividades seguras al evitar conexiones directas a sitios web. En su lugar, tu conexión se reenvía entre varios nodos de la red Tor, cada salto anonimizando tu identidad. Este proceso dificulta enormemente que un sitio web rastree quién eres y dónde te encuentras, pero también contribuye a velocidades de navegación más lentas. Si experimentas un rendimiento significativamente lento o una página deja de responder, puedes iniciar un nuevo circuito de Tor haciendo clic en el icono de menú (hamburguesa) y seleccionando la opción ‘Nuevo circuito de Tor para este sitio’. Esto obligará a Tor a encontrar una nueva ruta hacia el sitio.



Crear una Nueva Identidad

La opción “Nuevo Circuito” solo se aplica a la pestaña actual. Si quieres un nivel aún más alto de privacidad, puedes hacer clic en el icono de menú y seleccionar ‘Nueva Identidad’, lo que cerrará y reiniciará Tor con una nueva dirección IP. Cuando te conectas a un sitio a través de Tor, es posible que veas una advertencia emergente de que un sitio web en particular está intentando rastrearte. Con qué frecuencia aparecen estas advertencias depende de los sitios que visitas y de la configuración de privacidad que hayas elegido.



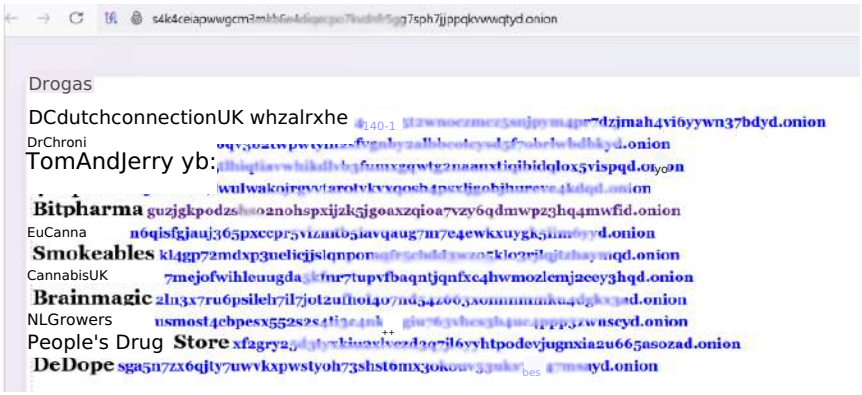
Usar HTTPS

Para mantenerse seguro y anónimo en línea, es esencial usar HTTPS en lugar de las versiones HTTP de los sitios web. El navegador Tor viene con la extensión HTTPS Everywhere preinstalada, que redirigirá automáticamente a la versión segura de cualquier sitio, si está disponible. Sin embargo, presta siempre atención a la barra de direcciones para una protección adicional. Si estás conectado a un sitio seguro, verás un candado verde. Si no está presente, haz clic en el icono “i” para obtener más información.

Acceder a sitios .onion

La forma más segura de navegar por la web a través de Tor es .sitios .onion, también conocidos como servicios ocultos de Tor. Estos sitios web no pueden ser indexados por motores de búsqueda y para acceder a ellos debes conocer la dirección exacta. Existen varios directorios .onion disponibles para ayudarte a encontrar dichos sitios, pero procede con precaución. Es fácil topar con sitios que ofrecen

contenido ilegal, venta de artículos ilícitos o promoción de actividad.



Prueba Tor sobre VPN

Para una capa adicional de privacidad, considera conectarte a un VPN antes de iniciar el Navegador Tor. El VPN no podrá ver tu actividad dentro de Tor, y añade el beneficio de evitar que cualquier relay de Tor vea tu dirección IP real. También evita que tu ISP sepa que estás usando Tor, lo cual puede ser útil si Tor está bloqueado en tu región.



Conclusión

No existe una única red de anonimato que haga todo.
Para garantizar un anonimato eficaz, debes combinar varias

herramientas. Aunque consigas usar las tres redes correctamente, todavía queda mucho por aprender. Cada red tiene un propósito único. Hay muchas más herramientas que pueden trabajar con estas redes para proporcionar una funcionalidad aún mayor, incluyendo tunelización SSH avanzada y configuración, VPN personales y numerosas utilidades de línea de comandos. Cuando se usan juntas, estas herramientas pueden lograr mucho más de lo que la mayoría de los usuarios puede hacer con software simple basado en GUI. Las redes de anonimato hoy en día son similares a Internet a principios de la década de 1990, un «reino de hackers» que trabajan hacia un futuro mejor.

Capítulo 8

RED OSCURA WEB PARA TU OSINT



“"En las profundidades de la Red Oscura, la inteligencia no es hallada, sino revelada."

Las fuerzas del orden, los periodistas y analistas utilizan OSINT técnicas para rastrear actividades ocultas.

¿Estás rastreando filtraciones de información sobre la Oscura? ¿Internet?

Cuando tu trabajo es proteger a las personas y los recursos, la Internet (o Darknet) se convierte en un área crítica para explorar. La información de Darknet juega un papel crucial en la seguridad y la inteligencia de amenazas. El equipo de Echoes ha desarrollado una herramienta OSINT, Beacon, para buscar en la red oscura de forma eficiente. Con Beacon, puedes filtrar a través de los vastos y a menudo desorganizados datos para extraer organización inteligencia relevante para tu significativa.



La solución - Un motor de búsqueda oscuro

Beacon es una herramienta avanzada de búsqueda en la red múltiples fuentes, que incluyen sitios web, repositorios de código y bases de datos. Desarrollado por Echoes, líder en descubrimiento de datos, Beacon ofrece inteligencia estructurada de la red oscura. A diferencia de Echoes, que se centra en datos en tiempo real, Beacon se especializa en datos históricos, brindando a los usuarios una visión más profunda de la información oculta.



Usando el procesamiento del lenguaje natural (NLP), Beacon entidades clave de datos de la web oscura, como nombres,

organizaciones, números de teléfono y números de seguro social.

Al crear un grafo de conocimiento interno, Beacon permite a los analistas rastrear información a través de varias plataformas, incluidas las redes sociales y foros subterráneos.

¿Cómo puede usar esta información?

Los datos organizados de la red oscura permiten a los analistas sobre posibles amenazas. Por ejemplo:

Protección de la Identificar direcciones de correo violaciones, filtraciones clasificadas o productos

Seguridad Detectar información filtrada, correos hackeados y cuentas de redes sociales comprometidas. Prevención de pérdidas minoristas: rastrear productos vendidos ilegalmente e identificar vendedores no autorizados.

Seguridad Corporativa: datos Descubrir violaciones de NDA y

Seguro y Cumplimiento Legal: Monitorear información para mitigar responsabilidades legales y gestionar crisis de relaciones públicas. Prevención de Fraude Financiero: Detectar tarjetas de crédito filtradas, contraseñas reutilizadas y datos bancarios comprometidos. Rastreo de cibercrimen: Comprender actividades subterráneas e identificar amenazas emergentes.

Revelando Internet Oscura

Beacon simplifica datos de la red oscura estructurando grandes de información no filtrada. Esta herramienta de OSINT identifica rápidamente inteligencia valiosa en las profundidades de la web oscura, ayudando a los profesionales a mantenerse por delante de posibles amenazas. Los ciberdelincuentes explotan frecuentemente las vulnerabilidades de la red oscura, distribuyendo software traqueteado como versiones maliciosas del Tor Browser. Estos navegadores modificados se han utilizado para robar más de 40 000 USD en Bitcoin. Los delincuentes crean sitios web engañosos que imitan la página oficial de Tor Browser, engañando a los usuarios para que descarguen versiones infestadas de malware.

Cómo operan los ciberdelincuentes en la web oscura

Dominios maliciosos: los ciberdelincuentes crean sitios web falsos "topolect [.] org" para engañar a los usuarios y que descarguen navegadores troyanizados. Estrategias de distribución: difunden malware a través de mensajes de spam en foros rusos, promoviendo actualizaciones falsas de Tor.

Manipulación de Los delincuentes usan motores de tácticas de optimización (SEO) para colocar sus páginas maliciosas más alto en los rankings de búsqueda. Ingeniería social: mensajes falsos afirman que usar su versión de Tor garantizará anonimato y eludir la censura gubernamental.

Inyección de El navegador Tor trojanizado inyecta JavaScript malicioso que rastrea a los usuarios y roba datos sensibles.

Comprender la Deep Web, la Dark Web y la Darknet

Internet consta de múltiples capas:

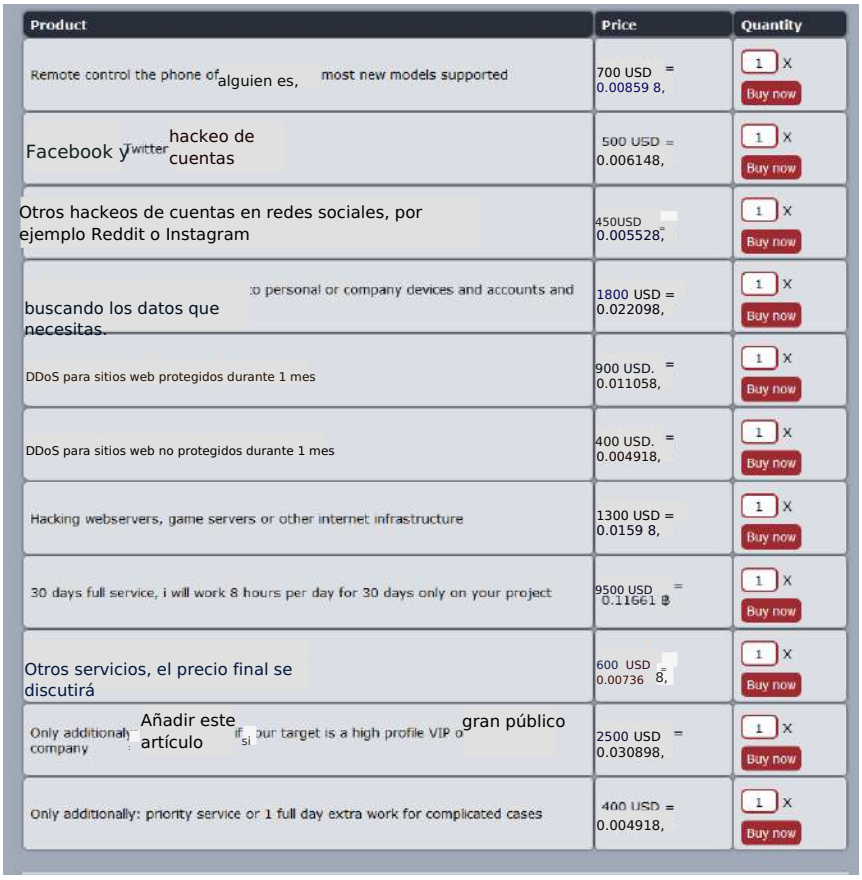
Surface Web: La parte visible de la web indexada por motores de búsqueda como Google (p. ej., Facebook, Wikipedia, sitios de noticias). Esto constituye solo un 4-6% de la web total.

Dark Web: Una red encriptada accesible mediante software como Tor, utilizado para la comunicación anónima y servicios ocultos.

Darknet: Un subconjunto de la dark web, que facilita actividades como el comercio de drogas y mercados

¿La Darknet es solo para delincuentes?

Aunque la web oscura tiene una reputación notoria, también sirve para fines legítimos. Denunciantes, periodistas y activistas la usan para proteger sus identidades de regímenes opresivos. Gobiernos y profesionales de ciberseguridad la aprovechan para la obtención de inteligencia y el análisis de amenazas. Sin embargo, la presencia de mercados ilegales, como el infame Silk Road, subraya la necesidad de una vigilancia y medidas de seguridad.



Product	Price	Quantity
Remote control the phone of alguien es, most new models supported	700 USD = 0.00859 8,	1 X Buy now
Facebook y Twitter hackeo de cuentas	500 USD = 0.006148,	1 X Buy now
Otros hackeos de cuentas en redes sociales, por ejemplo Reddit o Instagram	450USD 0.005528,	1 X Buy now
buscando los datos que necesitas. :o personal or company devices and accounts and	1800 USD = 0.022098,	1 X Buy now
DDoS para sitios web protegidos durante 1 mes	900 USD. = 0.011058,	1 X Buy now
DDoS para sitios web no protegidos durante 1 mes	400 USD. = 0.004918,	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.0159 8,	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.11661 ฿	1 X Buy now
Otros servicios, el precio final se discutirá	600 USD = 0.00736 8,	1 X Buy now
Only additionally company Añadir este artículo if si our target is a high profile VIP o gran público	2500 USD = 0.030898,	1 X Buy now
Only additionally: priority service or 1 full day extra work for complicated cases	400 USD = 0.004918,	1 X Buy now

Beacon equipa a los profesionales con una poderosa herramienta información crucial oculta en la deep web. Ya sea para seguridad corporativa, prevención de fraudes o cibercrimen investigación, la inteligencia OSINT estructurada es esencial para mantenerse por delante en la era digital.

Capítulo 9

TODO SOBRE VPN

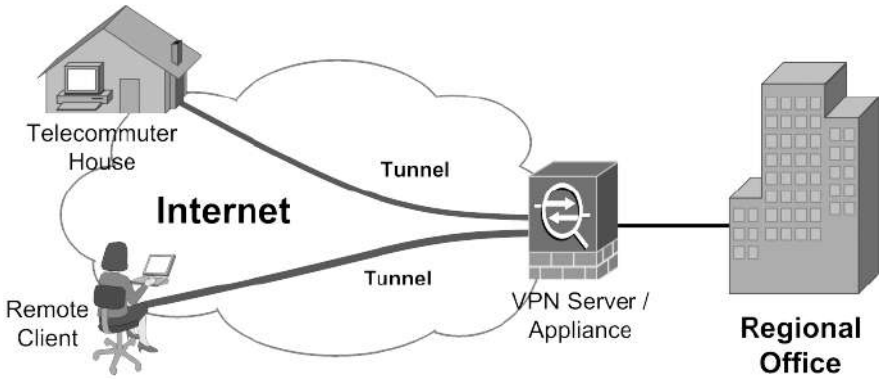


“"A VPN es tu primer escudo en lo digital campo de batalla—úsalo sabiamente."

No todos los VPN son iguales; elegir el correcto puede hacer o deshacer tu anonimato.

Una Red Privada Virtual (VPN) te proporciona en línea anonimato y privacidad al crear una red privada sobre una conexión pública a Internet. Las VPN ocultan tu protocolo de

(IP) dirección, haciendo casi indistinguibles tus actividades en línea intraceable. Lo más importante, los servicios VPN establecen conexiones encriptadas y seguras para ofrecer una mejor privacidad que un punto de acceso Wi-Fi compartido.



¿Por qué necesitaría un servicio VPN?

Navegar por la web o realizar transacciones en una red Wi-Fi no la red significa que podrías exponer tu información personal y tus hábitos de navegación. Por eso, una Red Privada Virtual (VPN) debería ser obligatoria para cualquiera preocupado por la privacidad y la seguridad en línea. A menos que estés conectado a una red Wi-Fi privada que requiera una contraseña, cualquier dato enviado durante tu sesión podría quedar expuesto a oyentes que usen la misma red. Las VPNs protegen tu correo electrónico, compras en línea o pagos de facturas cifrando tu conexión y manteniendo anónita tu actividad en línea.



Cómo una VPN protege tu dirección IP y privacidad

Las VPN crean un túnel de información entre tu red local

Las VPN crean un túnel de información entre tu red local y un nodo de salida ubicado a kilómetros de distancia, haciendo parecer que estás en una ubicación diferente. Esta ventaja permite libertad en línea, como acceder a tus sitios web o aplicaciones favoritas mientras estás en movimiento. Las VPN usan cifrado para proteger los datos cuando se envían a través de una red Wi-Fi, haciéndolos ilegibles para los hackers. Esto es especialmente importante cuando se utiliza una red Wi-Fi pública, ya que evita que cualquiera en la misma red escuche tu actividad en línea.



Privacidad de la VPN: ¿Qué oculta una VPN?

Una VPN puede ocultar mucha información que podría poner en tu privacidad. Aquí hay cinco ejemplos:

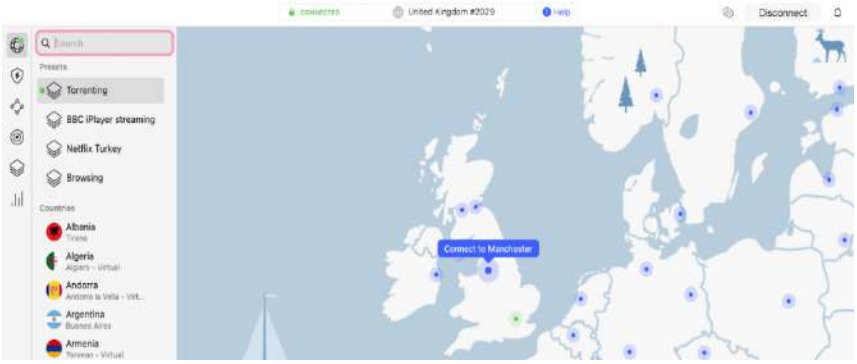
1. Tu historial de navegación

Tu ISP y el navegador pueden rastrear lo que haces en línea. Sin una VPN, tu historial de navegación podría venderse a anunciantes. Con una VPN, tus actividades en línea quedan



2. Tu dirección IP y ubicación

Cualquier persona que obtenga tu dirección IP puede determinar tu y ubicación. Una VPN ayuda a ocultar tu dirección IP real, manteniendo tu actividad de navegación anónima.



3. Tu ubicación para ver contenido en streaming

Los servicios de streaming a veces restringen el contenido según la ubicación. Una VPN te permite acceder a contenido como si estuvieras en tu país de origen, eludiendo estas restricciones.

4. Tus dispositivos

Una VPN protege tus dispositivos (portátil, tableta, teléfono de hackers, especialmente cuando estás conectado a redes Wi-Fi públicas.



5. Tu actividad en Internet para mantener la libertad en la red

Una VPN evita que tu ISP supervise tu actividad en línea y ayuda a proteger tu libertad para navegar con privacidad.



¿Cómo ayuda una VPN a salvaguardar contra el robo de identidad?

El robo de identidad sucede cuando los ladrones roban datos úsenlo para actividades fraudulentas. Una VPN ayuda a proteger su información cifrándola, creando un túnel seguro para sus datos que los ciberdelincuentes no pueden acceder.

Qué debe buscar en los servicios de VPN?

Al buscar una VPN, considere sus necesidades y prioridades. ¿Quiere navegar de forma anónima, proteger sus datos en Wi-Fi público o acceder a contenido desde casa mientras viaja? Aquí hay algunas cosas que buscar en una buena VPN:

Cómo seleccionar una VPN

Estas son preguntas para hacer al elegir un proveedor de

1. ¿Respetan su privacidad?

Asegúrese de que el proveedor de VPN tenga una política de no no rastrean sus actividades en

2. ¿Usan los protocolos de cifrado más recientes?

Busque VPN que utilicen OpenVPN, que ofrece una mayor seguridad que los protocolos antiguos

3. ¿Cuáles son los límites de datos?

Asegúrese de que la VPN proporcione un ancho de banda adecuado imponga límites de datos que podrían

4. ¿Dónde se encuentran los servidores?

Verifica si el proveedor de VPN tiene servidores en los países a los quieres conectarte.

5. ¿Puedes instalarlo en varios dispositivos?

Verifica si la VPN te permite usarla en múltiples dispositivos a la vez, como teléfonos, tabletas y

	ExpressVPN	NordVPN	IPVanish	TunnelBear	CyberGhost	Access
Simultaneous Connections	3	©	10	s	B	B
Number of Servers	1.700	4,873	1.000 +	350 +	2.700	3,252
Servers across the Globe (countries)	148	62	60+	20	60	37
Number of IP addresses	15.000	5,000	40.000+	n/a	n/a	n/a
Switch	✓	V	V	V	V	V
No Registros Potey	V	V	V	V	V	V
Free Version	✗	✗	✗	✓	✗	✗
Bitcoin payment	V	V	X	V	V	V
jurisdicción	British Islas Vírgenes	Panamá	Estados Unidos	Canadá	Rumanía	Estados Unidos.

6. Glosario VPN

Comprender la terminología VPN puede ser complicado, así que glosario de términos



Capítulo 10

IMPACTO DE SEGURIDAD



“"La Darknet desafía el propio tejido de la ciberseguridad—donde la innovación y las amenazas evolucionan de la mano."

A medida que la ciberseguridad se fortalece, la Darknet encuentra nuevas formas de adaptar un interminable juego del gato y el ratón.

Para no confundir con toda la deep web, la darknet es una colección de miles de sitios que no pueden accederse por medios comunes y no están indexados por motores de búsqueda como Google o Yahoo. En otras palabras, la darknet es una superposición de redes que requieren herramientas y aplicaciones específicas para su acceso. La historia de la darknet precedente a la década de 1980, con el término utilizado inicialmente para describir computadoras en ARPANET que estaban ocultas y programadas para recibir mensajes sin responder ni reconocer nada, quedando así indetectables o "a oscuras". Desde entonces, "darknet" se ha convertido en un término paraguas que se refiere a secciones ocultas de Internet o redes deliberadamente ocultas a la vista pública.

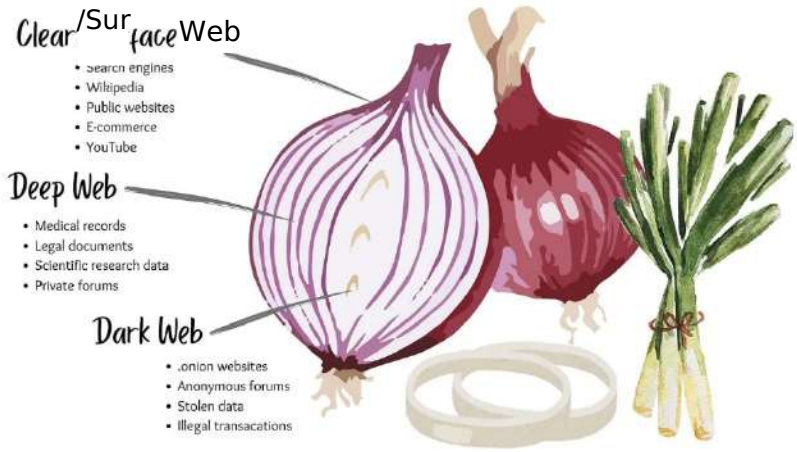


Paradójicamente, el desarrollo de la darknet puede ser crédito al ejército de EE. UU. La forma más común de acceder a la darknet es mediante herramientas como la red Tor. Las técnicas de enrutamiento utilizadas por Tor fueron desarrolladas a mediados de los años 90 por matemáticos e informáticos en los EE. UU.

Laboratorio de Investigación Naval para proteger la inteligencia de comunicaciones en línea.

USO Y ACCESO

Las aplicaciones de la darknet son tan diversas como Internet El propio, incluyendo servicios de correo electrónico, redes sociales, intercambio de archivos, sitios de noticias y comercio electrónico. Acceder a él requiere software especializado, configuraciones o permisos, a menudo utilizando protocolos e interfaces de comunicación no estándar. Actualmente, dos de las formas más conocidas de acceder a la darknet son a través de redes superpuestas: Tor e I2P.



Tor, abreviatura de "The Onion Router" (El enrutador

para mantener a los usuarios anónimos. Al igual que las capas de una cebolla, los datos están envueltos en múltiples capas de cifrado. Cada capa revela otro relé hasta que la última capa envía los datos a su destino. La información se envía de forma bidireccional, lo que significa que los datos se transmiten de ida y vuelta a través del mismo túnel.

En cualquier día, más de un millón de usuarios están activos en red. I2P, o el Proyecto de Internet Invisible, fue diseñado para compartir archivos entre usuarios. Encapsula datos en varias capas,

similar a un diente de ajo, agrupando los datos de varios usuarios para evitar la descifrado y el análisis. Transmite datos a través de un túnel unidireccional.

¿QUÉ HAY ALLÁ?

Como se mencionó anteriormente, la darknet aloja sitios de plataformas de comercio, servicios de correo electrónico y soluciones de hosting. Si bien muchos de estos servicios son alternativas legítimas a las plataformas principales, una parte significativa está asociada con actividades ilegales debido a su carácter anónimo. Desde la década de 1990, los ciberdelincuentes han utilizado la darknet como un espacio para comunicar, coordinar, y ahora incluso



Uno de los servicios de darknet más comunes es el correo el cual ha visto un aumento drástico en su uso, coincidiendo con el auge del ransomware. Los ciberdelincuentes a menudo

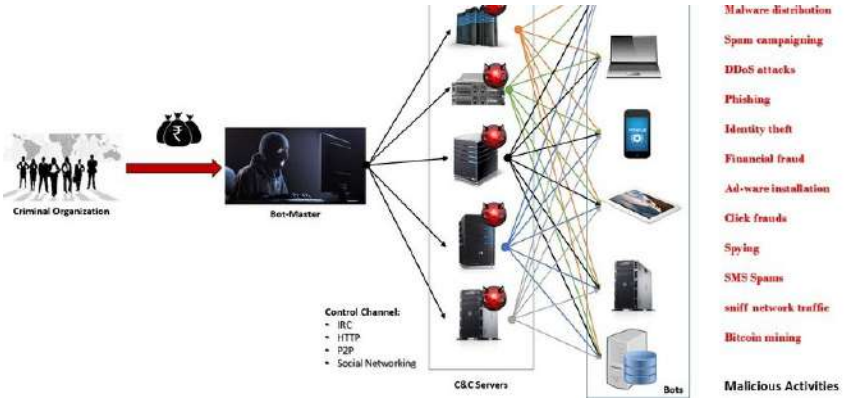
utilice estos servicios de correo electrónico para ejecutar ataques la detección por parte de las autoridades. Otro servicio crítico es el hospedaje en darknet. Así como la computación en la nube es utilizada por las empresas para la infraestructura de TI, los ciberdelincuentes aprovechan el hospedaje en darknet para sitios ilícitos, mercados de comercio electrónico y servicios de DDoS por encargo. Sin embargo, estos servicios de hospedaje suelen ser inestables, ya que las fuerzas del orden o hackers vigilantes pueden derribarlos por razones políticas, ideológicas o éticas. Los foros también sirven como lugares de encuentro donde hackers y delincuentes intercambian conocimientos, planifican ataques y refinan técnicas de ciberataques. Estos foros incluyen discusiones especializadas en varios idiomas y pueden estar asociados con grupos de hacking específicos, vectores de ataque o movimientos ideológicos.



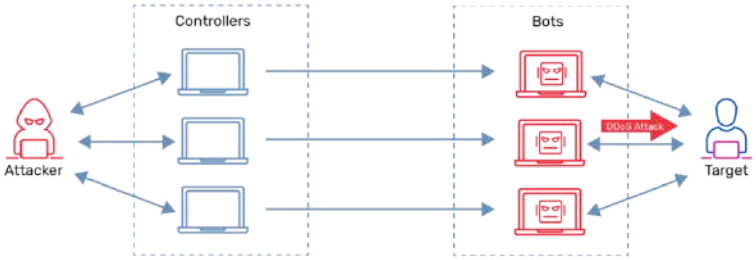
Finalmente, al igual que la web de superficie, la darknet tiene tales como Candle y Torch, que permiten a los usuarios encontrar y navegar por varios foros, sitios web y mercados.

UNA TIENDA DIGITAL

Quizás el aspecto más preocupante de la darknet es el auge de los sitios de comercio electrónico que facilitan el ciberdelito. Estas plataformas han ganado una inmensa popularidad en los últimos años debido a la creciente disponibilidad de servicios de alquiler de DDoS por encargo y de botnets, que permiten a usuarios no técnicos lanzar ataques cibernéticos sofisticados.



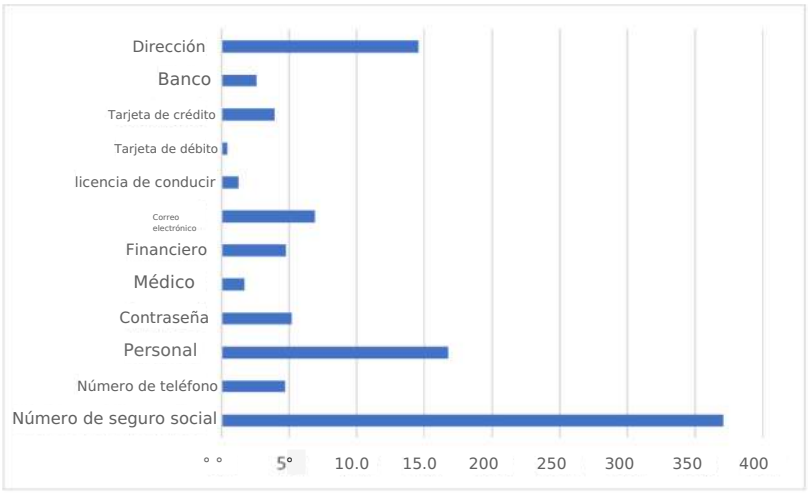
Muchos ofrecen interfaces intuitivas y interfaces que hacen lanzar un ataque es tan simple como realizar un pedido en línea. Un ejemplo es Putin Tresser, un servicio de alquiler de DDoS que ofrece varias opciones de ataque, herramientas para evadir detección e incluso soporte al cliente. Otro ejemplo es la botnet Jex, descubierta en 2018, que ejemplifica el crecimiento de los servicios de alquiler de botnets.



Los precios de estos servicios oscilan desde tan solo 100 $ hasta miles de dólares, dependiendo de factores como la cantidad de vectores de ataque, tamaño del ataque (Gbps/Tbps) y la demanda del mercado. Similar a servicios de botnets y DDoS, los modelos de ransomware-as-a-service permiten a los usuarios lanzar ataques con un esfuerzo mínimo, simplemente seleccionando una cantidad de rescate y personalizando la nota de rescate antes de implementar malware.

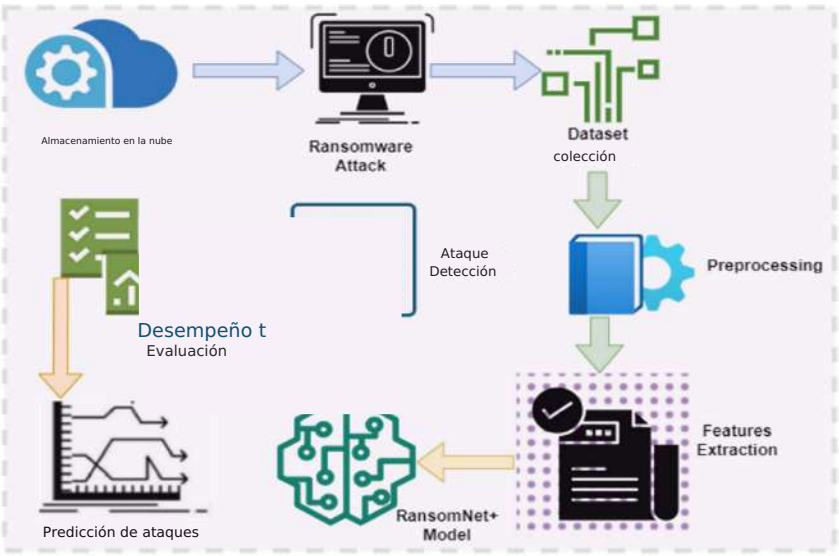


Los servicios de hackers a sueldo también están ampliamente pueden pagar por servicios que van desde piratear cuentas de correo y redes sociales hasta diseñar malware personalizado



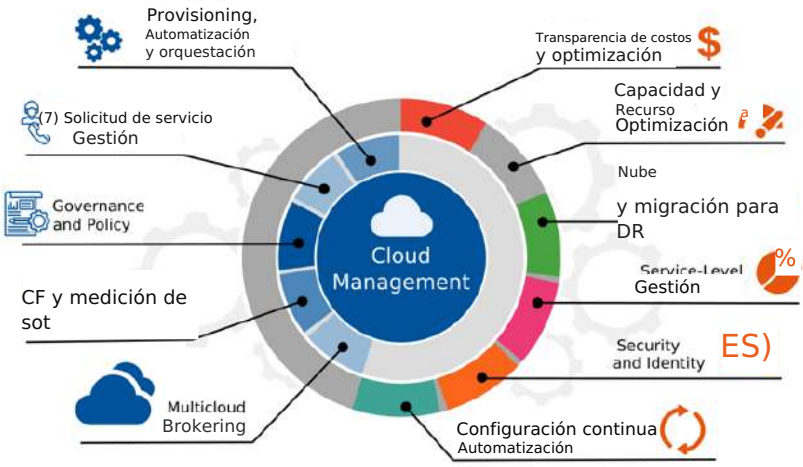
¿PUede LA NUBE PROTEGER CONTRA EL RANSOMEWARE?

El ransomware cifra los archivos de las víctimas y exige un secuestro para la descifrado. Aunque el almacenamiento en la nube proporciona una alternativa conveniente y rentable a las copias de seguridad fuera del sitio, no está inherentemente protegido contra ataques de ransomware. Una de las mayores ventajas de la nube es su infraestructura de seguridad. Aunque los proveedores de la nube son objetivos de alto perfil, invierten mucho en medidas de ciberseguridad para protegerse contra ataques. Para defenderse del ransomware en entornos en la nube, las empresas deben comprender el modelo de responsabilidad compartida de la computación en la nube.



La forma más rápida de protección contra ransomware en la nube

Usar la nube para copias de seguridad es efectivo, pero en lugar de confiar en un único proveedor de nube, utilizar varias nubes simultáneamente puede mejorar la seguridad y minimizar los riesgos— sin aumentar significativamente los costos. Un plan dedicado de ciberseguridad y recuperación ante desastres es crucial al aprovechar la nube. Al evaluar su postura de ciberseguridad base, puede identificar vulnerabilidades y mitigar amenazas de forma más eficaz. Tomarse el tiempo para categorizar sus aplicaciones ayuda a determinar los Objetivos de Tiempo de Recuperación (RTOs) y los Objetivos de Punto de Recuperación (RPOs), lo que conduce a una estrategia de recuperación ante desastres más enfocada. Nuestro equipo de expertos se especializa en soluciones de respaldo, recuperación ante desastres y ciberseguridad, asegurando una transición a la nube sin contratiempos.



¿USENET es parte de la Deep Web?

Los términos Deep Web, Dark Web y frases similares tienen se han discutido ampliamente en los medios. Estndose, el colectivo de hackers Anonymous ha derribado varios sitios de la Dark Web involucrados en actividades ilícitas. Esto ha despertado curiosidad sobre la Deep Web y cómo se diferencia de USENET.

Comprendiendo la indexación

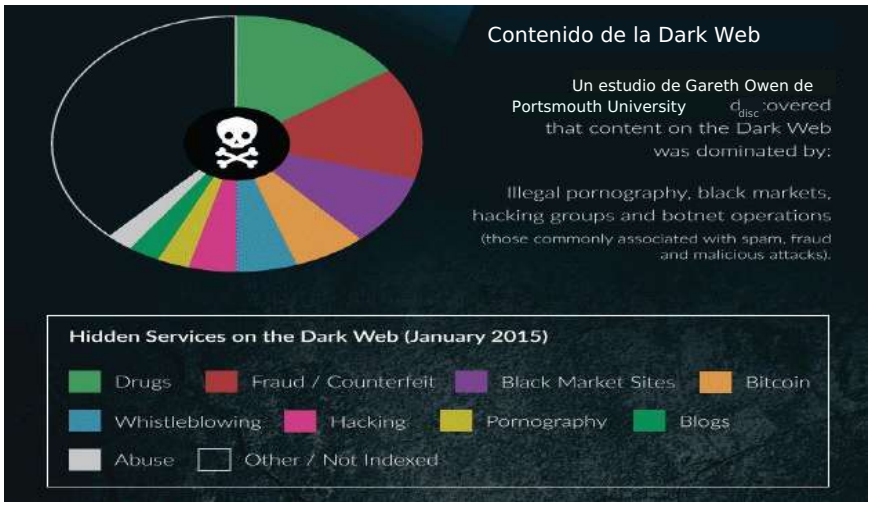
Puede que hayas encontrado términos como "motor de búsqueda optimización" (SEO), que implica técnicas para hacer que los sitios web sean más fáciles de encontrar por los motores de búsqueda. Los sitios web se indexan cuando los motores de búsqueda los encuentran a través de enlaces o envíos directos. Sin embargo, algunos sitios nunca se indexan, formando lo que se conoce como la Dark Web. En contraste, USENET funciona de manera diferente. No requiere indexación por motores de búsqueda porque opera como una red distribuida de grupos de noticias en lugar de sitios web tradicionales.

No todo lo no indexado es sinistro

Muchas sitios no indexados existen por razones legítimas.

páginas de investigación, bases de datos internas y portales web privados pueden no estar destinados a un descubrimiento público. Además, sitios web abandonados, olvidados por sus creadores, también pueden convertirse en parte de la Dark Web. Si bien algunos sitios de la Dark Web facilitan actividades ilegales, encontrarlos por accidente es altamente improbable.

USENET, por otro lado, es una plataforma transparente diseñada para compartir información más que para ocultarla. Aunque alberga un vasto archivo de discusiones, sigue siendo un recurso abierto y accesible.



Protegiendo su computadora de amenazas cibernéticas

Muchas personas se preocupan por la vigilancia gubernamental,

comparten voluntariamente sus datos personales en las redes sociales. Plataformas como Facebook, Instagram y Twitter recopilan

cantidades de datos de usuario, a menudo haciéndolos fácilmente anunciantes—y actores potencialmente



Los ciberdelincuentes pueden extraer esta información, revelar tu ubicación y hábitos. Incluso más allá de las redes sociales, tu actividad en línea se rastrea constantemente. ¿Alguna vez enviaste un correo a un amigo sobre planes de vacaciones, solo para encontrar anuncios de viaje inundando tu bandeja de entrada? Eso es porque empresas como Google analizan tus correos electrónicos y hábitos de navegación para servir anuncios dirigidos. Para mejorar la privacidad, considera usar extensiones de navegador **DoNotTrackMe** y **Self-Cookies de** Estas herramientas limitan el rastreo evitar que las empresas recolecten datos excesivos.

Riesgos de seguridad a nivel empresarial

Si bien la seguridad personal es importante, las empresas riesgos mayores. Violaciones de datos recientes en grandes minoristas como Home Depot y Target han comprometido millones de detalles de tarjetas de crédito. A menudo, los hackers no evitan directamente los firewalls, sino que explotan errores humanos mediante correos de phishing,

proveedores de terceros comprometidos, o incluso empleados conectar unidades USB infectadas. Los ciberdelincuentes también operan en la Dark Web, vendiendo datos robados y herramientas de hacking. Acceder a estos mercados requiere navegadores especiales como Tor, lo que los hace difíciles de rastrear.Para mitigar los riesgos, las empresas deben invertir en auditorías de ciberseguridad, pruebas de penetración y capacitación de empleados. Ignorar estas medidas hasta después de una violación puede conllevar consecuencias devastadoras.

El peligro de las actualizaciones de software no verificadas

Cada día recibes indicaciones para actualizaciones de tu teléfono, ordenador e incluso dispositivos inteligentes. Pero ¿alguna vez te preguntas qué se está instalando? Los actores maliciosos pueden disfrazar malware como actualizaciones legítimas, permitiendo que secuestren cámaras, micrófonos y datos sin el conocimiento del usuario. ¿La lección? Nunca confíes ciegamente en una actualización. Verifica siempre la fuente antes de instalar nuevo software.



La creciente amenaza del cibercrimen

El cibercrimen, junto con las crisis de salud global y el terrorismo, una de las mayores amenazas para la sociedad moderna. Sin embargo, muchas empresas dudan en invertir en medidas de seguridad robustas hasta que se convierten en víctimas. Las actualizaciones de firewall, antivirus

suscripciones, y la capacitación en seguridad deben verse como esenciales inversiones en lugar de gastos opcionales.

Educar a los empleados en prácticas seguras de Internet, incluidas la reconocimiento de estafas de phishing y evitar redes no confiables, puede reducir significativamente las vulnerabilidades de seguridad. En una era en la que los datos son tan valiosos como la moneda, las medidas proactivas de ciberseguridad ya no son opcionales: son una necesidad.



Pensamientos finales

La web profunda y la dark web son espacios vastos y complejos mucho más allá de su reputación como centros de cibercrimen. Aunque alojan muchas actividades ilícitas, también brindan herramientas valiosas para la privacidad y las comunicaciones seguras. Para los profesionales de ciberseguridad e inteligencia de amenazas, monitorear la darknet es esencial. Ayuda a identificar credenciales filtradas, posibles ciberataques y amenazas emergentes antes de que escalen. Sin embargo, navegar por este mundo oculto requiere precaución, conciencia y la protección adecuada.

medidas. Al comprender la estructura de la deep web y la dark web, las personas y las organizaciones pueden tomar decisiones informadas, ya sea proteger datos, prevenir amenazas cibernéticas o aprovechar redes anónimas con fines éticos.

.....

AGRADECIMIENTOS

Escribir este libro ha sido un viaje inolvidable, lleno con largas noches, investigaciones interminables y momentos de duda. A veces me cuestioné si tenía la energía para seguir, pero mi fascinación por el mundo oculto de la dark web me seguía atrayendo. La curiosidad es una fuerza implacable, y este libro es un testimonio de la necesidad de explorar, cuestionar y descubrir lo que yace bajo la superficie. Estoy profundamente agradecido a los expertos en ciberseguridad, hackers éticos y exploradores digitales que, consciente o inconscientemente, me han inspirado a seguir aprendiendo. A las comunidades en línea que desafiaron mi comprensión, gracias por empujarme a profundizar más.

Y lo más importante, para ti, el **lector.** Ya sea que es decir, si recogiste este libro por curiosidad, una sed de conocimiento o un deseo de entender el lado invisible de Internet, te aprecio más de lo que las palabras pueden expresar. Escribir un libro es una cosa, pero que alguien se tome el tiempo para leerlo es lo que realmente lo hace provechoso. Gracias por ser parte de este viaje. Mantente curioso, mantente seguro y nunca dejes de explorar.

Faisal .J

SOBRE EL AUTOR

Muhammad Faisal es un investigador y escritor de Lahore, Punjab, Pakistán, con un profundo interés en **ciberseguridad, la privacidad y las capas ocultas de internet. A través de una extensa investigación independiente, explora temas digitales complejos y los presenta de manera accesible para los lectores.**

Cuando no está escribiendo, disfruta aprender sobre **tecnologías emergentes** y mantenerse al día con las últimas tendencias en

Apoya mi trabajo

Si encontraste este libro valioso y te gustaría apoyar mi investigación y futuros escritos, puedes contribuir a través de

Patreon:

patreon.com/MuhammadFaisal0317

¡Tu apoyo es muy apreciado!

Para consultas, no dudes ponerte en contacto por correo **faisaljalvi0509@gmail.com**