Deep Web: El Lado Más Oscuro de Internet

en los albores de la era digital nació un universo oculto Más allá de lo que nuestros ojos pueden ver más allá de los muros brillantes de nuestros populares motores de búsqueda existe un mundo vasto subterráneo y en constante cambio Este es un mundo donde la libertad de información desafía las reglas donde lo inalcanzable se convierte en accesible y donde lo que permanece oculto se revela Este es el mundo de la Deep web un espacio infinito de información no indexada no regulada y en gran parte inexplorada un iceberg digital cuya punta apenas se vislumbra en nuestro uso diario de internet acompáñanos en este viaje donde nos sumergiremos en la profundidad de este océano digital conoceremos su estructura su origen su evolución y desvelaremos los secretos que alberga en su profundidades Pero recuerda el viaje a las profundidades no está exento de peligro Bienvenidos a bajo la superficie una Odisea en la Deep web gamesphone es una página la cual ofrece claves de software OEM baratas y completamente legales las cuales son 100% oficiales y pueden ser activadas en línea en esta ocasión a través del enlace que os compartimos en la descripción de este vídeo podréis adquirir múltiples productos al mejor precio entre ellos claves de producto para la suite de Microsoft Office claves de activación para Windows 10 y Windows 11 y también van del products a un precio bastante asequible Cabe destacar que en este caso no se necesitan cupones de descuento dado que tras acceder a la página con el enlace que os compartimos ya dispondréis del descuento directamente aplicado en la página para adquirir el producto recordad que simplemente tenéis que añadirlo al carrito darle a tramitar pedido y proceder ya al pago posteriormente proporcionando los datos correspondientes gracias a casefam por patrocinar este vídeo y ahora continuemos con el vídeo de hoy para entender completamente la historia y la esencia de la Deep web debemos retroceder en el tiempo hasta los primeros días de internet a principios de los años 60 durante la Guerra Fría el departamento de defensa de los Estados Unidos comenzó a trabajar en un proyecto llamado arpanet una red de Comunicaciones descentralizada y robusta diseñada para sobrevivir a un ataque nuclear este proyecto sin saberlo plantaría las semillas de lo que hoy conocemos como internet a medida que la tecnología y las necesidades evolucionaron esta red de ordenadores empezó a expandirse llegando a universidades laboratorios de investigación y más tarde ahogares y empresas pero mientras esta evolución acontecie una gran parte de la información en estas redes no era accesible al público general esta información que yacía envases de datos en directorios ftp en intranets privadas y más constituía una gran web profunda la cual no podía ser rastreada o indexada por los motores de búsqueda tradicionales y así sin saberlo mientras la parte visible de internet crecía y se popularizaba también lo hacía esta inmensa masa de información oculta a lo largo de los años el término Deep web se popularizó para describir esta vasta porción de la red un lugar que alberga tantos conocimientos invaluables como rincones oscuros y secretos Pero que es exactamente la Deep web cómo está estructurada cómo se accede a ella y sobre todo Qué secretos alberga en sus profundidades para responder a estas preguntas vamos a sumergirnos en este océano digital explorando sus rincones más recónditos y descubriendo lo que se esconde bajo la superficie imaginemos internet como un inmenso océano de información la superficie de este océano lo que podemos ver y acceder fácilmente es lo que llamamos la web superficial Esta es la parte de Internet que la mayoría de nosotros usamos a diario es justamente donde se encuentran nuestras redes sociales sitios de noticias tiendas online y donde los motores de

búsqueda como Google indexan y buscan información pero debajo de esta superficie en las profundidades de este océano digital yace La Deep web aquí encontramos la información que los motores de búsqueda convencionales no pueden o no quieren indexar estos datos no son necesariamente secretos o ilícitos simplemente están fuera del alcance de los motores de búsqueda y en las partes más profundas de este océano encontramos lo que se conoce como la Dark web Esta es una pequeña parte de la Deep web que ha sido intencionalmente ocultada y es inaccesible a través de los navegadores web estándar las redes de la target web como Thor y 2p y freinet utilizan cifrado y capas de redireccionamiento para garantizar la privacidad y el anonimato atrayendo a una variedad de usuarios desde activistas y periodistas hasta criminales ahora que hemos establecido que es la Deep web Y cómo está estructurada exploremos sus orígenes Cómo ha evolucionado a lo largo de los años y qué tipo de actividades se llevan a cabo en sus profundidades nuestra travesía nos lleva de vuelta a la década de los 90 Cuando internet comenzó a tomar forma como la conocemos hoy durante este periodo la Deep web existía principalmente en las bases de datos de las universidades en los registros gubernamentales y en las intranets de las empresas esta información era difícilmente accesible para el usuario común y no estaba indexada por los motores de búsqueda con el tiempo a medida que internet se expandía también lo hacía la Deep web sin embargo no fue hasta la década de los 2000 con el lanzamiento del proyecto Thor que la Deep web comenzó a tomar forma en la mente pública Thor que significa de onion router es una red que permite el anonimato y la privacidad en línea al redireccionar el tráfico de internet a través de una serie de servidores voluntarios esta red dio lugar a la Dark web la sección más escondida de la Deep web la Deep web y la Dark web son escenarios de una amplia gama de actividades alguna de estas son completamente legales y legítimas por ejemplo periodistas y activistas utilizan la Dark web para protegerse mientras informan sobre gobiernos autoritarios o para evitar la censura también es utilizada para proteger la privacidad personal y evitar el seguimiento en línea pero como Suele suceder con cualquier tecnología la Deep web también tiene un lado oscuro debido a su naturaleza anónima se ha convertido en Un refugio para actividades ilícitas el comercio de drogas la venta de armas y datos robados y una serie de otros crímenes han encontrado un hogar en la Dark web la Deep web es en muchos sentidos un reflejo de la sociedad misma es un lugar de contraste donde los mejores y los peores aspectos de la humanidad pueden manifestarse en su forma más pura a medida que seguimos explorando sus profundidades es importante recordar la complejidad de este vasto océano digital Thor que como ya sabéis significa de onion router es una red distribuida de servidores llamados nodos o relés que permite a los usuarios navegar por internet de forma anónima su nombre justamente el router cebolla proviene de su enfoque en las capas de cifrado para entender cómo funciona Thor primero Debemos entender un poco sobre cómo funciona internet normalmente cuando te conectas a un sitio web tu ordenador hace una petición directa a los servidores de ese sitio este proceso es rápido y eficiente pero también revela tu dirección IP y por lo tanto te ubicas en aproximada e identidad al sitio web y a cualquiera que esté observando la transmisión Thor aborda este problema utilizando una red de servidores también conocidos Como nodos para enmascarar tu identidad Cuando te conectas a través de Thor tu petición no va directamente al sitio web en lugar de eso es cifrada y enviada a través de una serie de nodos en la red Thor cada nodo solo sabe de dónde vino la petición Y a dónde la está enviando pero no puede ver todo el recorrido de la petición la petición es como una cebolla con cada nodo pelando una capa de cifrado solo el último nodo conocido como el nodo de salida puede ver la petición final y la envía al sitio web de destino pero

incluso este nodo no conoce tu ubicación original ni tu identidad cuando el sitio web responde los datos vuelven por la misma ruta cifrados en cada paso del camino hasta que finalmente vuelven a ti a lo largo de todo este proceso tu identidad y tu ubicación permanecen ocultas en cada paso se añade una nueva capa de cifrado como las capas de una cebolla cada nodo solo descifra una capa para revelar la ubicación del próximo nodo en la red esto significa que ningún nodo individual sabe tanto a la Fuente original como el destino final de los datos proporcionando un alto grado de anonimato es importante mencionar que los nodos de Thor están distribuidos por todo el mundo y son mantenidos por voluntarios cada uno contribuye a la robustez y el anonimato de la red sin embargo también plantea una serie de desafíos y riesgos ya que no todos los nodos pueden ser confiables Thor no solo protege la privacidad del usuario al ocultar su ubicación y hábitos de navegación sino que también permita acceder a sitios web que están alojados en la misma red conocidos Como sitios onion o punto onion estos sitios no son accesibles a través de los navegadores web tradicionales y conforman una parte importante de lo que conocemos como la Dark web Aunque Thor es un poderoso instrumento de anonimato no es completamente impenetrable un ejemplo de estos son los nodos de salida malintencionados en la red Thor el último nodo por el que pasa tu información antes de llegar a su destino es lo que se conoce como un nodo de salida Si un actor malicioso controla este nodo puede ver y en teoría Modificar el tráfico que pasa a través de él Aunque no podrán rastrear la información hasta tu ubicación exacta pueden ver a Qué sitios web estás accediendo otro posible riesgo es lo que se conoce como un ataque de correlación de tráfico en este escenario si un único actor controla tanto el primer nodo de la red Thor el nodo de entrada como el último nodo el nodo de salida podrían correlacionar los patrones de tráfico y potencialmente identificar a un usuario la fuerza del orden y las agencias de seguridad por ejemplo han utilizado estas vulnerabilidades para infiltrarse en la Dark web y rastrear actividades y legales han llegado por ejemplo a operar sus propios nodos para recolectar información sin embargo esto no significa que un usuario de Thor este automáticamente en riesgo tomar precauciones adicionales como el uso de servicios de VPN o la navegación cuidadosa puede ayudar a mitigar estos riesgos a pesar de estos posibles riesgos Thor sigue siendo una herramienta poderosa para aquellos que buscan proteger su privacidad en línea y acceder a la libre información en internet es un recordatorio de que aunque las herramientas y tecnologías pueden ayudarnos a navegar por la Deep web de manera segura nuestra seguridad y privacidad en línea dependen finalmente de nuestros conocimientos y nuestro comportamiento Aunque a menudo se habla de la Deep web y la Dark web como lugares misteriosos y siniestros en realidad contienen una amplia gama de contenido como mencionamos anteriormente la Deep web Incluye todo lo que los motores de búsqueda convencionales no pueden o no quieren indexar además la Deep web también contiene una gran cantidad de recursos académicos y científicos como bases de datos de bibliotecas archivos de revistas y conjuntos de datos de investigación también hay foros de discusión privados y comunidades que prefieren mantenerse fuera de la vista del público general muchas empresas y organizaciones de hecho utilizan la Deep web para alojar intranets privadas y bases de datos de clientes Esto no es coña sin embargo cuando nos adentramos en la Dark web la naturaleza del contenido puede cambiar drásticamente debido a su anonimato y privacidad la Dark web se ha convertido en un mercado para una variedad de actividades ilícitas pero la gran pregunta por qué los vastos recursos de la Deep web están ocultos a los motores de búsqueda convencionales qué es lo que hace que estos tesoros de información permanezcan invisibles a los ojos de Google Bing y otros buscadores que usamos a diario para entender esto

debemos mirar cómo funcionan los motores de búsqueda los motores de búsqueda como Google usan lo que se llaman crawlers o spyders que son programas de Software que rastrean la web siguiendo enlaces de una página a otra y recopilando información sobre estas páginas para que puedan ser buscadas más tarde sin embargo hay muchas páginas en la web que estos crawlers no pueden alcanzar algunas páginas están protegidas por contraseñas o son de pago algunas son bases de datos que requieren una entrada de búsqueda específica para generar una página y otras están en la red Store y requieren software especial para acceder a ella estas son todas partes de la Deep web así que aunque puede parecer que la web que vemos a través de nuestros motores de búsqueda es inmensa en realidad sólo estamos rascando la superficie la gran mayoría de la información en la está escondida en las profundidades de la Deep web accesible solo a aquellos que saben cómo encontrarla pero Cuán grande es realmente la Deep web la verdad es que es difícil de cuantificar algunas estimaciones sugieren que la Deep web podría ser hasta 500 veces más grande que la web superficial la parte que podemos ver con nuestros motores de búsqueda convencionales Pero estos números solo pueden dar una idea aproximada ya que la naturaleza oculta de la Deep web hace que sea difícil de medir ahora si nos aventuramos Más allá de la Deep web y nos adentramos en la oscuridad de la Dark web el tamaño se vuelve aún más difícil de precisar a pesar de ser famosa por su contenido ilícito y sombrío la Dark web en Sí es bastante pequeña comparada con la totalidad de la Deep web sin embargo el tamaño de la Dark web no debe subestimarse especialmente en términos de los peligros potenciales Aunque es una herramienta valiosa para preservar la privacidad y eludir las censura la Dark web también alberga una variedad de actividades ilegales como hemos comentado desde la venta de drogas y armas hasta la distribución de contenido ilegal además la Dark web es un hervidero de ciberdelincuencia es un lugar donde los cibercriminales pueden comprar y vender malware explotar vulnerabilidades de seguridad y llevar a cabo una serie de estafas en línea navegar por la Dark web puede poner a los usuarios en riesgo de ser Víctimas de estos criminales finalmente Aunque la Deep web y la Dark web pueden proporcionar privacidad también pueden amenazarla los datos personales robados incluyendo números de tarjetas de crédito se compran y venden a menudo en la Dark web pero Cómo llegan estos datos a la Dark web en primer lugar bueno a menudo es el resultado de las violaciones de datos donde los cibercriminales penetran en las defensas de una empresa y roban información de sus usuarios los datos robados luego pueden ser vendidos en la Dark web para obtener un beneficio el valor de los datos varía por ejemplo los datos bancarios y los números de tarjeta de crédito suelen tener un precio alto los datos de identidad como los números de seguro social y los detalles del pasaporte también son valiosos incluso algo tan simple como una dirección de correo electrónico puede tener un valor para los spammers y los fishers es por eso que es tan importante proteger nuestra información personal el uso de contraseña fuerte y única la autenticación de dos factores y el cuidado con los correos electrónicos y los sitios web sospechosos son solo algunas de las maneras en que podemos proteger nuestros datos y mantenernos a salvos de las amenazas de la Deep web y la Dark web el dinero es el nexo que mueve la Dark web pero no estamos hablando de dinero en efectivo o transferencias bancarias ordinarias en este entorno clandestino la moneda de elección es digital las criptomonedas la criptomoneda más conocida y la más usada en la Dark web es el bitcoin bitcoin y otras criptomonedas son populares por una serie de razones en primer lugar las criptomonedas proporcionan un nivel de anonimato Aunque todas las transacciones de bitcoin están registradas en un blockchain público las identidades de las personas detrás de estas transacciones pueden

ser difíciles de rastrear especialmente si se toman precauciones adicionales existen criptomonedas como monero y zcash que ofrecen aún más privacidad ocultando completamente la Fuente el monto y el destino de las transacciones estas criptomonedas Por ejemplo están ganando bastante popularidad en la Dark web Pero cuánto dinero se mueve realmente en la Dark web es difícil de determinar con precisión debido a su naturaleza clandestina sin embargo se estima que solo en los mercados ilícitos se pueden mover cientos de millones de dólares cada año Y recuerda esto es solo una fracción de toda la actividad de la Dark web sin embargo es importante recordar que aunque las criptomonedas ofrecen cierto grado de anonimato no son completamente impenetrables las agencias de aplicación de la ley han desarrollado herramientas para rastrear transacciones de criptomonedas y han tenido éxito en rastrear actividades ilícitas en la Dark web quizás después de todo lo que hemos explorado te preguntas Cómo puede ingresar a la Deep web aunque te recomendamos encarecidamente que procedas con precaución vamos a explicar cómo se hace el primer paso es descargar e instalar un navegador especializado en privacidad como Thor el navegador Thor oculta tu identidad cifrando y rebotando tu conexión a través de varios servidores o nodos alrededor del mundo una vez instalado deberás ajustar las configuraciones de seguridad según tus necesidades Thor ofrece diferentes niveles de seguridad que puedes elegir desde el nivel estándar hasta el nivel más seguro que deshabilita todas las secuencias de comandos y solo permite el acceso a una fracción de la web con Thor podrás acceder a sitios web de la Deep web que terminan en punto onion un sufijo que indica que el sitio web se encuentra en la red torp sin embargo es vital recordar que la seguridad en la Deep web y la Dark web no está garantizada aunque Thor ofrece un alto grado de privacidad no es infalible existen riesgos tanto legales como de seguridad asociados con el acceso a la Deep web y a la Dark web recordad que la actividad ilegal sigue siendo ilegal independientemente de donde ocurra si decides explorar la Deep web asegúrate de tener una seguridad informática robusta un antivirus actualizado un firewall sólido y otras medidas de seguridad son esenciales Y recuerda nunca compartas información personal o financiera A menos que estés seguro de la seguridad del sitio y la legalidad de la transacción Aunque Thor puede proporcionar un alto grado de anonimato no es perfecto existen varias formas en las que un atacante podría intentar desenmascarar la dirección IP de un usuario de Thor como mencionamos antes Thor protege el anonimato de los usuarios cifrando su tráfico y enviándolo a través de una serie de nodos antes de llegar a su destino final sin embargo una vez que el tráfico llega al último nodo conocido como nodo de salida es descifrado y enviado al sitio web destino esto significa que el operador del nodo de salida puede ver el tráfico que sale de su nodo en teoría si una entidad como una agencia de seguridad controlara un número suficiente de nodos de salida Podría tener una visión significativa del tráfico de la red Thor claro controlar múltiples nodos de salida no es una tarea sencilla requiere recursos significativos y tiempo sin embargo algunas entidades especialmente las agencias gubernamentales de seguridad podrían tener los recursos para hacerlo aún así existen mecanismos de defensa y supervisión en la red Thor para detectar y mitigar este tipo de actividad es por eso que es esencial utilizar siempre conexiones seguras como https incluso a navegar con Thor una conexión segura cifra tus datos de tal manera que incluso si alguien puede ver tu tráfico no podrán entender lo que estás enviando o recibiendo uno de los malentendidos más comunes sobre Thor es que al usarlo tu ordenador se convierte en un nodo que cifra y reenvía el tráfico de otros usuarios bueno Esto hay que desmentirlo esto no es cierto en realidad los nodos de Thor son servidores operados por voluntarios en todo el mundo cuando usas Thor para navegar por la web tu tráfico se cifra y pasa por varios de estos relés o

nodos antes de llegar a su destino final si decides convertirte en un operador de relé de Thor eso significa que estás donando algo de ancho de banda de tu conexión a internet para ayudar a los usuarios de Thor a mantener su privacidad y seguridad pero este es un proceso voluntario y requiere una configuración deliberada simplemente usar Thor para navegar por la web no convierte tu ordenador en un relé habiendo aclarado que al usar Thor no te conviertes automáticamente en un nodo de la red puedes estar preguntándote Cómo funcionaría si decidieras convertirte voluntariamente en uno como hemos mencionado si te conviertes en un operador de relé estás donando parte de tu ancho de banda de internet para ayudar a otros usuarios de Thor Pero qué significa eso exactamente ya hemos visto que cuando alguien Envía una solicitud a través de Thor esa solicitud se cifra varias veces y luego se envía a través de una serie de nodos en cada nodo se elimina una capa de cifrado antes de reenviar la información al siguiente nodo es un poco como pelar una cebolla no de ahí el nombre original de Thor de onion router o el router cebolla Como operador de tu nodo tu nodo recibiría tráfico de Thor cifrado de otro nodo tu nodo luego descifraría una capa de ese tráfico antes de reenviarlo al siguiente relé o nodo en la cadena o al destino final si tú nodo es un nodo de salida es importante tener en cuenta que aunque estás manejando el tráfico Como operador de un relé no puedes ver la información que contiene todavía está cifrado y tú solo estás quitando una capa de ese cifrado no tiene forma de saber quién envió la información o cuál es su contenido la excepción a esto es si operas un nodo de salida como mencionamos anteriormente los nodos de salida son los que envían el tráfico a su destino final en internet en este punto el tráfico ha sido completamente descifrado y por lo tanto es visible para el operador del nodo de salida ahora algunos de vosotros podéis estar pensando no podría convertirme en un nodo de salida en la red Thor la respuesta corta es sí puede pero es importante entender la responsabilidades y posibles riesgos que esto conllevaría primero configurar un nodo de salida no es excesivamente complicado desde un punto de vista técnico necesitas una buena conexión a internet un ordenador dedicado que pueda estar en línea todo el tiempo y debes estar dispuesto a seguir las guías de configuración disponibles en la página web de Thor sin embargo ser operador de un nodo de salida puede tener implicaciones legales como mencionamos antes en un nodo de salida el tráfico ha sido completamente descifrado antes de llegar a su destino final en internet esto significa que si alguien está utilizando Thor para actividades ilegales ese tráfico podría pasar a través de tu nodo de salida en algunos casos esto ha llevado a los operadores de nodos de salida a tener problemas legales aunque estén simplemente ayudando a la redstore por lo tanto si estás pensando en convertirte en un operador de nodo de salida es importante que te informes bien y consideres hablar con un abogado que esté familiarizado con las leyes de tu país sobre privacidad y seguridad en internet a lo largo de este vídeo hemos navegado Juntos por las aguas desconocidas y a menudo malentendidos de la Deep web y la Dark web hemos desentrañado su historia estructura y hemos destapado la tecnología que la sustenta hemos explorado los secretos que oculta y los peligros que presenta nos hemos adentrado en el mundo de Thor la red que facilita el anonimato y la privacidad en la web una herramienta que en manos adecuadas puede ser un Baluarte contra la censura y un defensor de la libertad de expresión pero también hemos visto La otra cara de la moneda hemos visto cómo esta misma tecnología puede ser utilizada para actividades ilegales desde el comercio de datos hasta el mercado negro hemos aprendido que incluso el anonimato tiene sus límites y que la seguridad Nunca es absoluta En definitiva la Deep web y la Dark web son reflejos de la dualidad inherente a la tecnología y a la naturaleza humana son lugares donde la libertad de expresión puede florecer pero también donde pueden prosperar

las actividades delictivas lugares de sombras pero también de luz espacios de misterio pero también de conocimiento al final del día la tecnología Es una herramienta y como todas las herramientas su impacto depende de cómo se utilice la Deep web y la Dark web nos plantean preguntas difíciles sobre la privacidad la seguridad y el equilibrio entre ambas no hay respuesta sencillas pero Esperamos que este vídeo haya arrojado algo de luz sobre estas partes ocultas de la web y te haya dado algo en lo que pensara