PARTE 1.

Principalmente la dark web está compuesta por páginas con unos enlaces muy determinado y particulares a los que no se pueden acceder por un motor de búsqueda cualquiera como el de Windows o el software necesario.

Si la Deep Web es el 90% de Internet, la Dark Web ocuparía únicamente el 0,1% de ella. Es una porción de Internet intencionalmente oculta a los motores de búsqueda, con direcciones IP enmascaradas y accesibles sólo con un navegador web especial. La Dark Web por lo tanto forma parte de la Deep Web, pero son cosas diferentes.

Dentro de la Dark Web encontramos las dark nets que conforman esta, se suele definir la Dark Web como una zona no indexable por buscadores convencionales, lo que quiere decir que no puedes encontrar sus páginas en Google, Bing y demás buscadores. Pero hay alguna excepción, redes específicas como TOR o I2P que se alojan esas páginas. Las Dark net son las redes ocultas, mientras que la dark web se puede utilizar para referirse dos cosas, se puede utilizar para referirse al contenido (webs oscuras) y también se puede utilizar para referirnos a todo lo relacionado a el resto.

**TOR**, una red de anonimización que tiene también su propia Darknet, y es básicamente a la que suele referirse todo el mundo cuando habla de ellas.

Por ejemplo, dentro de la dark net podemos encontrar páginas alojadas en ella en las que se produzcan asesinatos, se vendan drogas, animales exóticos, tráfico de armas etc… están las Red Rooms, esas supuestas páginas en las que puedes ver o participar en una tortura o asesinato.

Para entender qué es la Dark Web tienes que entender cuatro conceptos diferentes: Clearnet, Deep web, Dark web y Darknet. El más fácil de entender es el de la Clearnet, que es el Internet tal y como lo conoces, las páginas que encuentras en Google y otros buscadores accesibles para todo el mundo.

El 90% del contenido de la red no es accesible a través buscadores. Eso es una parte de la Deep Web, que engloba toda la información a la que no puedes acceder públicamente. Puede tratarse de páginas convencionales protegidas por un paywall.

PARTE 2.

TOR (The Onion Router) es un proyecto de software libre y de código abierto que permite a los usuarios navegar por Internet de forma anónima y protegida. Fue creado para proteger la identidad y la privacidad de los usuarios en entornos donde la vigilancia y la censura son comunes

La red Tor se compone de una serie de nodos (también llamados “routers”) distribuidos por todo el mundo. Cuando un usuario accede a la red Tor, su tráfico se enruta a través de tres nodos aleatorios (también conocidos como “routers de cebolla” o “onion routers”) en la red. Cada nodo encripta y desencripta el tráfico, dificultando la capacidad de terceros para rastrear la fuente del tráfico y la identidad del usuario.

La red TOR sigue una serie de pasos;

Entrada: El usuario inicia sesión en la red Tor mediante un cliente Tor (como Tor Browser) y especifica la dirección IP del sitio web que desea visitar.

Nodo de entrada: El tráfico se envía a un nodo de entrada (Nodo 1) en la red Tor, que encripta el tráfico y lo envía a otro nodo aleatorio.

Nodo intermedio: El tráfico pasa a través de un nodo intermedio (Nodo 2), que también encripta y desencripta el tráfico, antes de enviarlo a otro nodo aleatorio.

Nodo de salida: Finalmente, el tráfico llega a un nodo de salida (Nodo 3), que desencripta el tráfico y lo envía al sitio web especificado.

Salida: El usuario recibe la respuesta del sitio web, sin que se pueda rastrear su identidad ni la dirección IP original.

La red Tor utiliza protocolos de encriptación como TLS (Transport Layer Security) y SSH (Secure Shell) para proteger el tráfico en tránsito.

PARTE 3.

La NSA y el GCHQ han utilizado proyectos para atacar y "desanonimizar" a usuarios de Tor. Sin embargo, no lo han conseguido con el 100% de usuarios ni han logrado atacar a usuarios específicos: por el contrario, lo que hacen es "poner trampas" y ver quién cae. Tampoco han roto la seguridad y cifrado de Tor, los ataques se dirigen más bien a otros programas que use el objetivo para "colarse" en su ordenador.

La NSA quiere saber quién y que está haciendo en Internet en todo momento, y Tor se lo pone difícil. Todas las técnicas de análisis están enfocadas a saber quién está detrás de cada petición de Tor, para o bien añadir esos datos a sus registros o bien efectuar más ataques sobre el objetivo posteriormente.

La primera parte consiste en distinguir si una petición a una página web viene de la red Tor o de un usuario normal. No es un paso difícil: Tor deja muchas huellas que hace que su detección sea sencilla. Por ejemplo, TorButton no desvela el número de compilación de Firefox que estás usando. Lo hace por motivos de privacidad, y porque no pasa nada si se detecta una petición Tor: lo que de verdad importa es que no se pueda distinguir entre varios usuarios Tor.

El otro tipo de técnicas de análisis se basan en estudiar la red Tor. La primera es sencilla de entender: la reconstrucción de circuitos.

Si la NSA controla todos los nodos de un circuito, podría vigilar por dónde va el paquete, desde que lo envía el usuario original hasta que sale a Internet. Sin embargo, controlan un número muy bajo de nodos, de tal forma que la probabilidad de que un paquete visite sólo los nodos de la NSA es ínfima, lo que hace la reconstrucción de circuitos casi imposible.

También existe el análisis de tiempos, que es igualmente simple. Por ejemplo, pueden detectar que cuando un paquete entra a la red Tor, sale otro a los 300 milisegundos en otra parte del mundo hacia el ordenador de nuestro amigo Bob. Si se repite mucho ese patrón de latencia, es muy posible que ese tráfico de Tor esté originado por Bob.

PARTE 4.

El caso Snowden, la filtración de documentos clasificados por Edward Snowden, un excontratista de inteligencia de la Agencia de Seguridad Nacional (NSA) de Estados Unidos, revelando programas de vigilancia masiva y espionaje llevados a cabo por la NSA y otras agencias de inteligencia estadounidenses. Estas filtraciones, que comenzaron en junio de 2013, expusieron la escala y la naturaleza de la vigilancia estatal, generando un debate público sobre la privacidad y los límites de la autoridad gubernamental.

Hechos clave;

* En 2013, Edward Snowden, entonces empleado de la NSA, comenzó a filtrar documentos clasificados a periodistas y organizaciones de derechos humanos, revelando programas de vigilancia como PRISM, Upstream y Boundless Informant.
* Estos programas permitían a la NSA recopilar y analizar grandes cantidades de datos de comunicaciones electrónicas, incluyendo correos electrónicos, llamadas telefónicas y datos de internet, sin necesidad de un mandato judicial o una orden de autorización específica.
* Las filtraciones también revelaron la cooperación entre la NSA y otras agencias de inteligencia, como el FBI y el Departamento de Defensa, en la recopilación y análisis de datos.
* Snowden se exilió en Rusia después de que Estados Unidos lo acusara de espionaje y violación de la Ley de Espionaje.

En mi opinión Aunque Snowden violó la ley al filtrar documentos clasificados, su motivación fue ética y su acción puede ser vista como una forma de proteger la sociedad de la opacidad y la arbitrariedad del poder estatal

PARTE 5.

He encontrado referencias sobre algunos países;

Alemania: La agencia de inteligencia alemana, la Bundesverfassungsschutz (BfV), transfiere de manera sistemática datos personales de residentes en Alemania a la NSA, la CIA y otros siete miembros de la Comunidad de Inteligencia de Estados Unidos a cambio de otras informaciones y software de espionaje.

Revelaciones sobre la red de vigilancia mundial (2013-2015): Los documentos filtrados por Snowden revelaron que la NSA interceptó comunicaciones electrónicas de ciudadanos alemanes, incluyendo al entonces canciller Gerhard Schröder, sin autorización judicial ni parlamentaria.

Reino Unido: En 2013, se descubrió que la agencia de inteligencia británica, GCHQ, había estado interceptando comunicaciones de ciudadanos británicos y extranjeros, incluyendo a líderes políticos y periodistas, sin autorización judicial ni parlamentaria.

Francia: En 2015, se reveló que la agencia de inteligencia francesa, DGSE, había estado recopilando datos personales de ciudadanos franceses y extranjeros, incluyendo a líderes políticos y periodistas, sin autorización judicial ni parlamentaria.