Prólogo por Mikko Hypponen

Este empieza hablando de que Kevin Mitnick comienza describiendo un encuentro con un viejo amigo, con quien se reencuentra después de varios años, estos hablan de recuerdos antinguos antes de Kevin se convirtiera en un hacker famoso, en si de lo que se hablan ellos es de como la tecnología ha evolucionado y cómo esto ha impactado la privacidad personal.

Capítulo 1: "Vuestra Contraseña Puede Ser Agrietada!"

El capítulo empieza hablando de que Jennifer Lawrence fue una de varias celebridades que experimentaron un fin de semana de Día de Trabajo difícil en 2014, cuando se filtraron imágenes privadas, muchas de ellas desnudas, a través de un caso conocido como "theFappening". Este incidente expuso vulnerabilidades en la seguridad de las cuentas de iCloud de las celebridades, que habían sido accedidas sin autorización, lo que llevó a una gran especulación sobre una posible brecha en los sistemas de Apple. Sin embargo, Apple negó cualquier fallo en su seguridad, afirmando que las cuentas habían sido comprometidas a través de ataques dirigidos a usuarios. Herramientas como Elcomsoft Phone Breaker y iBrute facilitaron el acceso no autorizado a las cuentas, permitiendo a los atacantes obtener datos personales valiosos. Una de las herramientas que se habla en este capitulo es EPPB, esta herramienta se utilizaba para acceder a cuentas de iCloud. Para acceder a esas cuentas, accedieron a bases de datos para recopilar la información de usuarios. Luego habla de otra herramienta que también se hizo uso para conseguir contraseñas, que fue el iBrute. Este era un código en línea que aún sigue público en GitHub y se utilizó para conseguir credenciales de iCloud, entre otras. También habla de cómo un forense digital pudo acceder a hacer una copia de seguridad de una cuenta de iPhone y conseguir todos los datos de esta. Luego habla de ejemplos de robo de cuentas de iCloud, como un hombre que intentó hacer eso (Ryan Collins), pero fue pillado y enviado a la cárcel. También menciona el ejemplo que pasó en Sony Diversion, donde Michael Lynton puso una contraseña muy fácil y los atacantes pudieron acceder al sistema. Además, en este capítulo se menciona la herramienta oclHashcat, que agrieta contraseñas utilizando gráficos de apalancamientos. También se habla de la herramienta John the Ripper para conseguir contraseñas. Luego da casos donde, a partir de la herramienta John the Ripper y oclHashcat, los ciberdelincuentes pudieron acceder a grandes empresas e incluso a bancos. También se habla de la encriptación y desencriptación de archivos. En resumen, este capítulo enfatiza la principal importancia de tener una buena contraseña, y aun así, pueden acceder a tus datos. También habla de lo que es el 2FA, que es una medida de seguridad que añade una capa adicional de protección al proceso de inicio de sesión, como por ejemplo en Gmail, donde al iniciar sesión también te pide que introduzcas el código que te han enviado al SMS del móvil.

Capítulo 2: "Quién Más está Leyendo Vuestro Email?"

De lo que habla este capítulo es de la importancia del correo electrónico, este empieza diciendo los tipo de correo electrónico que hay es decir las diferentes compañías que proporcionan servidores de correo como por ejemplo Outlook de Microsoft, Gmail de Google... También añade la importancia que tienen estos, toda la privacidad ,etc...
El primer caso que pone es cuando Stuart Diamond usuario de Yahoo busco viajes a Dubai, i al dia siguiente le llegaron correos sobre hoteles... Es decir esta persona acepto las cookies y le apareció publicidad en su correo, añade la importancia de dar permisos a las páginas web a nuestro datos, como inicio de sesión en páginas… Luego habla de que mucha gente denuncio a Yahho ya que le preocupaba de que pudieran meterse en su intimidad, al final denunciaron a Yahoo por entrar en la intimidad de los usuarios que tenían una cuenta de correo suya. A partir de lo que hico Yahoo todas las otras compañías dejaron de hacer esto ya que no le interesaba que los denunciaran por incumplir una ley, tengo que añadir que a día de hoy eso ya no funciona así todas las compañías controlan lo que buscas, haces… Luego habla de que aun que borres correos electrónicos de tu bandeja de entrada la información se queda guardada en los servidores.
Luego habla de la encriptación simétrica para la transferencia de archivos, pone el ejemplo que en una empresa de EEUU se transmitía los mensajes de forma cifrada para que no pudieran coger los datos de este, para la encriptación de mensajes utilizaron la herramienta PGP ya que es la más popular para la encriptación de mensajes por correo electrónico. También habla del creador Phil Zimmermann y también de la actualización de la herramienta que paso a ser GPG esta es de código abierto. Luego habla de un ejemplo en la NASA de Edward Snowden, al revelar información sensible de la NSA, necesitaba establecer una comunicación segura y anónima con periodistas como Laura Poitras. Utilizó su cuenta de correo en Lavabit, consciente de que los emails pueden ser interceptados en su recorrido. Para asegurar su privacidad, recurrió a Micah Lee de la Electronic Frontier Foundation, buscando compartir su clave pública de PGP para encriptar la comunicación. Sin embargo, en un descuido, olvidó incluir su clave en su mensaje, lo que obligó a Lee a enviarle un email.Ya que la información era demasiado sensible para ser compartida por correo convencional, crearon cuentas de email. Para hacerlo de forma segura, utilizaron a Micah Lee, quien los ayudó a establecer confianza entre ellos al usar el pen digital de la clave publica de Poitras publicada en Twitter. Entonces se transmitieron los mensajes, archivos cifrados...
Del siguiente ejemplo que habla es de la discusiones entre Correa del Norte y EE.UU. También añade que para para lograr un verdadero anonimato digital, es crucial gestionar la información que se revela a través de direcciones IP, hardware y software, y considerar el uso de proxies o remailers anónimos. Además de esto habla de la web oscura de Internet "Dark Web", como haceder a esta mediante el navegador Tor y todas las cosas que esta contiene como contenido pornografico datos personales de gente, drogas, etc... y como crearte una cuenta en esta también lo dice. En resumen este capitulo habla de muchos temas de lo que es la privacidad del correo hasta del Dark Web.

Capítulo 3: Wiretapping 101

El tercer capítulo habla de que nuestra sociedad estamos a toda hora con el móvil, este explica como están todos los móviles conectados entre si, mediante torres que lo que hacen es compartir señal… Luego explica que para proteger nuestra identidad de nuestro móvil se hace mediante el IMSI que es el numero que tiene la tarjeta SIM del móvil. De lo que habla después es de cuando usas tu teléfono, este se conecta a la torre de movil más cercana, lo que permite que tus llamadas y datos se manejen sin problemas, incluso mientras te mueves. Luego añade de que cada teléfono tiene su propia señal, la cual queda almacenada. Así las autoridades pueden disponer de información sobre el desplazamiento en relación con los usuarios. El registro de la señal de una sola torre puede mostrar que un dispositivo estaba presente, pero el manejo de las señales de varias torres permite realizar triangulaciones exactas de la geolocalización de un usuario. Luego de lo que habla es de que para proteger tu privacidad y evitar ser rastreado a través de tu teléfono, es fundamental considerar diversas estrategias. Al firmar un contrato con un proveedor de servicios móviles, se requiere proporcionar datos personales, como tu nombre y número de seguro social, lo que aumenta tu vulnerabilidad. Una alternativa más discreta es utilizar un teléfono de prepago, que puedes adquirir con efectivo y sustituir periódicamente. Lo que pasa es que es importante tener en cuenta que, aunque estos dispositivos tengan un nivel de privacidad, no garantizan el anonimato total. Las autoridades pueden rastrear el uso del IMSI vinculado al dispositivo, y los patrones de llamadas pueden revelar conexiones importantes. Este capitulo explica el caso de Pat Barbaro, un narcotraficante que utilizó varios teléfonos de prepago en un intento de ocultar su identidad. Pero al final la policia lograron rastrear sus comunicaciones a través de patrones de uso. También menciona el protocolo de señalización SS7, que es clave para la conexión de las llamadas, el cual puede ser aprovechado por un atacante para interceptar y manipular las llamadas incluso a través del pequeño operador de telecomunicaciones. Ademas tambien aborda el tema PFS este es un sistema que usa una encriptación ligeramente diferente tono para cada llamada…

Capítulo 4: Si no Encriptas, eres Unequipped

En el cuarto capítulo se habla del caso de Daniel Lee. Este caso se inicia cuando la policía arresta a un supuesto traficante de drogas por el que no tenían clave en su teléfono. La policía examina el teléfono y encuentra un mensaje que coincidía con una transacción anterior entre Lee y una persona de su contacto denominada Z-Jon. Para suplantar la identidad de Lee, los agentes respondieron al mensaje de Z-Jon y arrestaron. El capítulo también habla del caso de Tom Brady el jugador de la NFL este caso lo acusan con balones desinflados, cuando acusaron a Tom, este decidió cambiar su teléfono y destruir el anterior. Lo que supuso que le sancionaran cuatro partidos en la NFL, aunque fue anulada por un juez. La liga no pudo recuperar los mensajes, en si lo que es imporatante para recuperar mensajes es hacer copias de seguridad de los datos en la nube, ya que los proveedores de servicios a menudo no retienen esa información y así podrian haberlo pillado. En este capitulo tambien se habla del software Norton Diskreet, que este prometía alcanzar un nivel de seguridad de 56 bits pero sólo utilizaba 30 bits. También se habla de las aplicaciones de mensaje Facebook, Snapchat e Instagram… estas han sido potencialmente vulnerables a ataques de intermediarios, y la mayoría de las aplicaciones no incorporan encriptación de los datos almacenados esto se significa que los proveedores, o potenciales hackers, tienen acceso a mensajes antiguos.

Capítulo 5: Ahora Me Veo, Ahora Tú no

Este capitulo empieza hablando de que en abril de 2013, Khairullozhon Matanov, un taxista de Quincy, Massachusetts, cenó con los hermanos Tamerlan y Dzhokhar Tsarnaev, que más tarde serían identificados como los autores del atentado en el Maratón de Boston entonces los arrestaron. Lo que quiere decir que las autoridades pueden utilizar el historial de navegación en investigaciones, incentivando el uso de modos de navegación privados para encontrar información de gente. Luego habla de cuando navegas por Internet, los sitios web pueden utilizar encriptación mediante el protocolo HTTPS para proteger la comunicación, lo que asegura que los datos viajan de forma segura entre tu dispositivo y el servidor del sitio pero tu proveedor de servicios de Internet (ISP). También añade que navegadores como Chrome, Firefox y Safari permiten navegación privada, evitando que se guarde tu historial, pero no protegen totalmente tu privacidad, ya que los ISPs y algunos sitios pueden rastrear tu actividad. También habla de herramientas como HTTPS Everywhere, un complemento para navegadores, pueden forzar el uso de conexiones seguras. Este capitulo habla de los certificados de seguridad de sitios web y añde que es importante desactivar la geolocalización en tu navegador para evitar que sepan donde estas. También habla de que puedes ocultar tu dirección IP usando el navegador Tor o un proxy, aunque no todos los sitios aceptan estas conexiones, y algunos proxies gratuitos pueden ser inseguros o estar llenos de anuncios añade que es importante usar HTTPS para encriptar tus actividades, especialmente cuando usas proxies. Luego habla de lo que es compartir cuenta en iCloud y del caso de Monroe, quien, al conectar su cuenta de iCloud con la de su prometida, terminó exponiendo memorias que preferiría mantener privadas, además este capitlo también habla del caso de Michele Catalano entre otros ejemplos…

Capítulo 6: Cada Clic de Ratón Haces, Seré Mirar Te

El capítulo seis habla de cómo la información que buscamos en Internet se guarda en diferentes páginas web. Muchas de estas páginas, como WebMD, no cuidan bien nuestra información. Por ejemplo, si buscas "pie de atleta", esa búsqueda puede ser vista por otros, como tu proveedor de internet o empresas grandes como Google y Facebook. Habla de que un estudio dice que el 91% de los sitios de salud comparten datos con otras compañías que los usan para hacer publicidad. También dice que hay empresas como Experian y Axioma que recopilan y venden datos personales. Además, explica cómo funciona el DNS, que ayuda a los navegadores a cargar las páginas web. Esto muestra que nuestra información puede estar en peligro. También añade que los navegadores pueden contar cosas sobre nosotros, como qué versión del software usamos o qué tan grande es nuestra pantalla... Luego habla de la Fundación de Frontera Electrónica que esta tiene una herramienta llamada Panopticlick.com. También se habla de trucos como los píxeles invisibles y JavaScript, que siguen a los usuarios sin que ellos lo sepan. Para protegerse, sugieren usar máquinas virtuales, bloquear ventanas emergentes y poner extensiones como NoScript, que evitan que se ejecuten scripts y sigan a la gente. Pero esto puede hacer que algunas páginas no funcionen bien. Además también añade que las cookies guardan información nuestra para rastrear lo que hacemos en línea y ayudarnos a ser identificados en diferentes sitios. También este cápitulo habla del termino llamado fingerprinting.

Capítulo 7: Paga Arriba o Más!

El capítulo siete empieza de que alguna persona estaba bajando pornografía infantil y haciendo amenazas al vicepresidente Joe Biden. Luego lo que paso es que la policía se confundió y fue a la casa equivocada por un lío con las direcciones IP y esto muestra que las conexiones Wi-Fi pueden ser inseguras. Luego habla del caso de Barry Vincent Ardolf, este trata de que este había sido denunciado por su vecino, porque usó el router inalámbrico de su vecino para crear cuentas en línea a su nombre y causarle problemas. También se añade en este capitulo que muchos routers que te dan las compañías de internet vienen con configuraciones que pueden ser peligrosas si no se protegen bien, por eso, es importante que los usuarios actualicen el software de sus routers, cambien el nombre de la red (SSID) y ajusten las configuraciones de seguridad para protegerse de los intrusos. También se habla de la seguridad de las redes Wi-Fi ya que esta es muy importante porque lo que hagan otros puede afectar al dueño de la red. Aunque la ley suele proteger a los dueños de no ser responsables por cosas ilegales que hagan otros en su conexión, hay que tener cuidado. Además, la encriptación WEP ya no sirve porque es muy fácil de romper, así que se recomienda usar WPA o WPA2, que son más seguras, pero actualmente esta la WPA3 en curso. Añade de que cuando activas WPA2, todos los dispositivos que se conecten deben usar el mismo tipo de encriptación. También hay que crear contraseñas fuertes, de al menos quince caracteres, y se puede usar una opción llamada "whitelisting" para permitir solo a dispositivos específicos que se conecten a la red, usando sus direcciones MAC. Aunque esto da más seguridad, los hackers aún pueden encontrar formas de entrar. También se habla del WPS, que este es una función para conectar dispositivos fácilmente, pero no es segura y se puede atacar fácilmente. Por eso, es mejor desactivar WPS y usar contraseñas fuertes para mantener la red de casa segura y evitar que gente no autorizada entre.

Capítulo 8: Cree Todo, Confía en Nada

El capítulo empieza hablando sobre cómo ha cambiado la forma en que nos comunicamos y lo difícil que es mantener nuestra privacidad hoy en día. Añade que los teléfonos fijos nos ofrecían más intimidad, pero ahora, usar Wi-Fi gratis en lugares como cafeterías puede ser muy peligroso. Muchas personas se conectan automáticamente a estas redes sin leer las advertencias, lo que puede hacer que su información personal se filtre. También añade que los dispositivos a veces se conectan a redes guardadas sin que nos demos cuenta, y podríamos elegir una red falsa, lo que facilita que los hackers roben información. Por eso, si necesitamos hacer cosas importantes, es mejor usar datos móviles en lugar de Wi-Fi público y asegurarnos de que nuestras conexiones estén seguras. También se recomienda usar protocolos como HTTPS o SFTP para proteger lo que enviamos por Internet. También habla el uso de VPN (red privada virtual) esta es útil porque crea un "túnel" seguro para que nuestra información viaje sin que otros la vean. Sin embargo, el proveedor de la VPN aún puede saber de dónde venimos, así que no somos completamente anónimos. También en este capitulo se habla del caso David Petraeus que este para enviar mensajes privados uso la carpeta de borradores en una cuenta de correo compartida para enviar mensajes a su biógrafo.

Capítulo 9: No Tienes Ninguna Intimidad? Coge Encima Lo!

El capítulo nueve habla de John McAfee, quien hizo un programa antivirus. Él se tuvo que ir a esconder en Belice ya que lo culparon de vender droga... También habla de que su vecino fue muerto por culpa suya, McAfee escribió de su vida en un blog. Pero, una foto en su blog mostró dónde estaba por los datos ocultos que tiene la foto. Esto hizo que lo atraparan y mandaran de vuelta. Esto muestra que atraves de una foto podemos obtener datos (Escenografia). Luego se habla de los metadatos EXIF de las imágenes digitales pueden contener información sensible, como la ubicación exacta. Investigaciones han demostrado que la combinación de reconocimiento facial entre otras cosas… También habla que las empresas como Google y Apple utilizan el reconocimiento facial en sus aplicaciones, pero esto presenta riesgos de privacidad, ya que los gobiernos pueden usar estas imágenes para identificar a manifestantes o sospechosos, pero esto corre un riesgo muy grande ya que si alguien coge una fotografia tuya podria hacer uso de ella. También habla que las redes sociales permiten a las empresas usar tus datos personales sin compensación, lo que complica la eliminación de contenido.

Capítulo 10: Te Puede Correr pero No Esconder

Este cápitulo empieza hablando de que si llevas tu teléfono contigo a todas partes, aunque esté en modo avión, estás siendo vigilado por tu servidor de servicios (ISP). Este rastreo de datos también se utiliza en investigaciones policiales, como en EE.UU., donde los registros de ubicación se usaron para vincular sospechosos con robos. Además, Google y Apple almacenan tus ubicaciones a menos que configures lo contrario, y dispositivos como relojes inteligentes y rastreadores de actividad siguen recopilando información sobre ti, compartiéndola con las empresas, lo que facilita que otros reconstruyan tu rutina y tus relaciones personales. También añade que la tecnología moderna ha ampliado los desafíos a la privacidad, desde drones que capturan imágenes de alta resolución hasta sistemas de reconocimiento facial en tiendas o también en el ámbito comercial, las tiendas utilizan capturadores de señal y reconocimiento facial para personalizar experiencias, rastrear a clientes y detectar posibles ladrones. En este cápitulo se habla del caso de Moshe Greenshpan este hombre es un desarrollador del software de Churchix, que permite a iglesias usar reconocimiento facial para monitorear la asistencia de congregantes, identificar a quienes asisten irregularmente e incentivar las donaciones.

Capítulo 11: Hey, KITT, no Comparte Mis Investigadores

Este capítulo empieza hablando que Charlie Miller y Chris Valasek controlaron un Jeep Cherokee a alta velocidad desde una distancia remota, utilizando métodos de hacking, por seguridad a la gente que tenia ese coche se lo quitaron y le rembolsaron el dinero que este costaba. También habla de que los taxis (Uber) comenzaron a utilizar datos de GPS, permitiendo a las empresas rastrear ubicaciones de recogida y entrega, así como detalles de los pagos. Este capítulo habla un estudiante llamado Anthony Tockar que demostró que era posible desanonimizar esta información combinándola con datos públicos y fotografías de paparazzi. Utilizando el número de medallón de los taxis visibles en fotos, logró identificar a celebridades y sus trayectos en Nueva York. Además, los sistemas de transporte público están implementando tecnologías como NFC para facilitar los pagos, lo que también podría poner en riesgo la privacidad del usuario. Además este capítulo habla de la tecnología ALPR permite a las autoridades escanear placas a alta velocidad, almacenando información sobre los movimientos de los vehículos, incluso en situaciones donde los conductores no están bajo sospecha. También habla sobre Slas políticas de privacidad de Tesla ya que esta ecopila una amplia variedad de datos del vehículo, incluyendo el número de identificación, información de velocidad, uso de la batería, y detalles del sistema eléctrico y de seguridad. Esto se puede hacer tanto de manera presencial como a través de acceso remoto, lo que permite a Tesla rastrear la ubicación y el estado del vehículo en tiempo real. En si de lo que habla este capítulo es que hoy en dia puees hackera un coche y conducirlo de forma remota.

Capítulo 12: El Internet de Vigilancia

Este capítulo empieza hablando que los dispositivos del hogar han adquirido una mayor inteligencia gracias a la tecnología, y da el ejemplo de un termostato (Nest), este se puede controlar desde el móvil. Lo que pasa es que algunos investigadores han descubierto que estos dispositivos presentan fallas de seguridad. Por ejemplo, si alguien tiene acceso físico a un termostato, puede modificar su software y evitar que envíe información a Google. Entonces esto es peligroso ya que muchos dispositivos, como cámaras y luces inteligentes, pueden ser hackeados y utilizados para llevar a cabo ataques cibernéticos. Otro ejemplo son los monitores de bebé entre otros…
Además, los sistemas de seguridad del hogar, que antes funcionaban con cables, ahora operan a través de Internet, lo que facilita su instalación pero también los hace más vulnerables a ataques. Los hackers pueden interrumpir las señales entre los dispositivos, provocando que las alarmas se activen sin motivo o desactivando sistemas de seguridad. Para protegerse, es fundamental utilizar contraseñas seguras y desconectar dispositivos como webcams cuando no están en uso.

Capítulo 13: Cosas Vuestro Jefe no Te Quiere para Saber

Este capitulo empieza hablando de la preocupación por la privacidad ya que esta no solo se limita a la vigilancia del gobierno, sino que también se extiende a los entornos laborales, donde los empleadores utilizan tecnologías de rastreo como GPS en dispositivos corporativos para supervisar a sus empleados. Para proteger su intimidad, los empleados deben ser conscientes de que todo lo que se realiza en redes corporativas pertenece a la empresa y evitar realizar actividades personales en dispositivos laborales. Además, es aconsejable cerrar sesión en sus computadoras cuando se ausentan y usar dispositivos personales para asuntos privados. La preocupación por la privacidad se extiende más allá de la vigilancia gubernamental hacia los entornos laborales, donde los empleadores utilizan tecnologías como el GPS para rastrear a sus empleados y recopilar datos sobre su ubicación. También habla de que muchas empresas controlan el uso de Internet, las pulsaciones de teclas y los correos electrónicos, lo que plantea serias preocupaciones sobre la privacidad personal. Para salvaguardar su intimidad, los empleados deben ser conscientes de que su actividad en redes corporativas pertenece a la empresa y evitar realizar actividades personales en dispositivos laborales, así como cerrar sesión en sus computadoras cuando se ausenten. Da el ejemplo de Cui este utilizó métodos como ondas de radio, aprovechando la capacidad de los teléfonos móviles y otros dispositivos para captar vibraciones y emitir datos a través de antenas no diseñadas para registrar datos. También explica de uso de hotspots falsos en oficinas entre otras cosas…

Capítulo 14: Obteniendo el anonimato Es Trabajo duro

De lo que habla este capítulo es que Kevin fue detenido en Colombia y Durante cuatro horas, estuve en una sala privada, mientras los agentes revisaban su equipaje, que contenía varios dispositivos electrónicos y herramientas de seguridad relacionadas con una conferencia sobre seguridad. Lo que el hizo para proteger su privacidad, fue limpiar mis dispositivos de información sensible, utilizar encriptación robusta, y transferir datos a servicios en la nube, asegurándose de que la eliminación de datos fuera realmente segura y efectiva. El Aprendío la importancia de tener un respaldo físico de sus dispositivos y de ser consciente de la vulnerabilidad de mis aparatos, como el iPhone, al conectarlos a otros equipos. Tras esta experiencia, el ajusto mis protocolos de seguridad, manteniendo copias de seguridad actualizadas y evitando el acceso directo a mis dispositivos sin la debida protección.

Capítulo 15: El FBI Siempre Coge Su Hombre

En este capítulo empieza hablando de que en octubre de 2013, Ross William Ulbricht, conocido como "Dread Pirate Roberts" (DPR), fue arrestado en la biblioteca del Parque del Glen en San Francisco mientras operaba el sitio web de drogas "Carretera de Seda". A pesar de sus intentos de anonimato, como usar Wi-Fi público y Tor, un agente del IRS, Gary Alford, descubrió su identidad al rastrear menciones anteriores del sitio en chats en línea. Alford encontró que Ulbricht había utilizado su dirección de correo electrónico personal en varias ocasiones, lo que vinculó directamente su identidad con DPR. La situación culminó cuando el FBI lo arrestó mientras estaba conectado al sitio, capturando evidencia crucial que selló su destino. También habla de que en 2015, el investigador Ben Caudill anunció un dispositivo llamado ProxyHam, que permitiría ocultar la ubicación real del usuario, pero su presentación fue cancelada y las unidades destruidas, aunque la idea de un dispositivo similar probablemente seguiría existiendo. ProxyHam es un dispositivo que permite acceder a Internet de forma remota, utilizando un transmisor de Wi-Fi que puede estar a una milla de distancia, conectándose a través de una antena dongle en un ordenador a hasta 2.5 millas. Esto significa que, en el caso de Ross Ulbricht, el FBI podría haberlo observado desde fuera de la biblioteca del Parque del Glen mientras él se encontraba en otro lugar. Aunque tales dispositivos pueden ser útiles para quienes viven en países opresivos al ocultar la geolocalización, el investigador Ben Caudill canceló su presentación sobre ProxyHam en DEF CON, posiblemente debido a preocupaciones legales sobre el acceso no autorizado a redes. Luego, Samy Kamkar desarrolló ProxyGambit, que utiliza tráfico celular inverso, permitiendo que los usuarios se conecten desde cualquier parte del mundo. La web está dividida en la Web de Superficie, la Web Profunda y la Web Oscura; esta última es donde operan sitios como Carretera de Seda, inaccesibles a través de navegadores normales y no indexados por motores de búsqueda. También habla del acceso a la Web Oscura esta se realiza a través de Tor, que oculta la ubicación del usuario al enrutar las solicitudes a través de múltiples servidores. Sin embargo, existían especulaciones de que la NSA y otras agencias podrían rastrear a los usuarios en la Web Oscura a través de nodos de salida, observando patrones de actividad que podrían vincular a los usuarios con sus solicitudes.

Capítulo 16: Mastering el Arte de Invisibilidad

Este capítulo detalla que para alcanzar una verdadera invisibilidad en línea, es crucial establecer una identidad completamente distinta de la real. Esto implica conseguir un dispositivo específico solo para actividades anónimas, como un portátil de bajo costo, preferiblemente con Windows o Linux, que no esté asociado a cuentas personales y que se adquiera en efectivo para evitar rastreos. La instalación de software como Tor y Tails es vital para navegar de manera segura y anónima. Además, se aconseja no utilizar el portátil anónimo en casa o en la oficina para prevenir que el proveedor de servicios registre la dirección MAC del dispositivo. La clave es mantener una separación clara y emplear múltiples capas de seguridad, ya que el riesgo de ser rastreado es alto si se ignora algún detalle. Para lograr un anonimato total en línea, es esencial seguir un enfoque metódico que incluya la compra de un portátil y otros dispositivos anónimos. Primero, se deben adquirir tarjetas de regalo prepagadas sin revelar la identidad, preferiblemente a través de un tercero para evitar cámaras de vigilancia. Es importante evitar tarjetas recargables que requieran información personal. Se recomienda utilizar una red Wi-Fi pública, asegurándose de cambiar la dirección MAC cada vez que se conecte, y evitar el uso del dispositivo anónimo en casa para prevenir la vinculación con registros de proveedores de servicios. Además, se sugiere obtener un hotspot personal de manera similar, evitando siempre usar dispositivos personales en la misma ubicación. Finalmente, es crucial crear cuentas de correo electrónico anónimas utilizando servicios que no requieran verificación de identidad, y convertir las tarjetas de regalo en Bitcoin para mantener la privacidad. Además este capitulo habla sobre temas de criptomonedas.