Anonimato y privacidad práctica en internet

Fran Brizzolis

A tod@s los grandes profesionales y amateurs de la ciberseguridad que, desde el primer momento, confiaron en mí, me acogieron, me apoyaron, y me enseñaron, aun sabiendo que siempre sería un curioso, y eterno aprendiz.

Gracias a tod@s por tanto.

Índice de contenidos

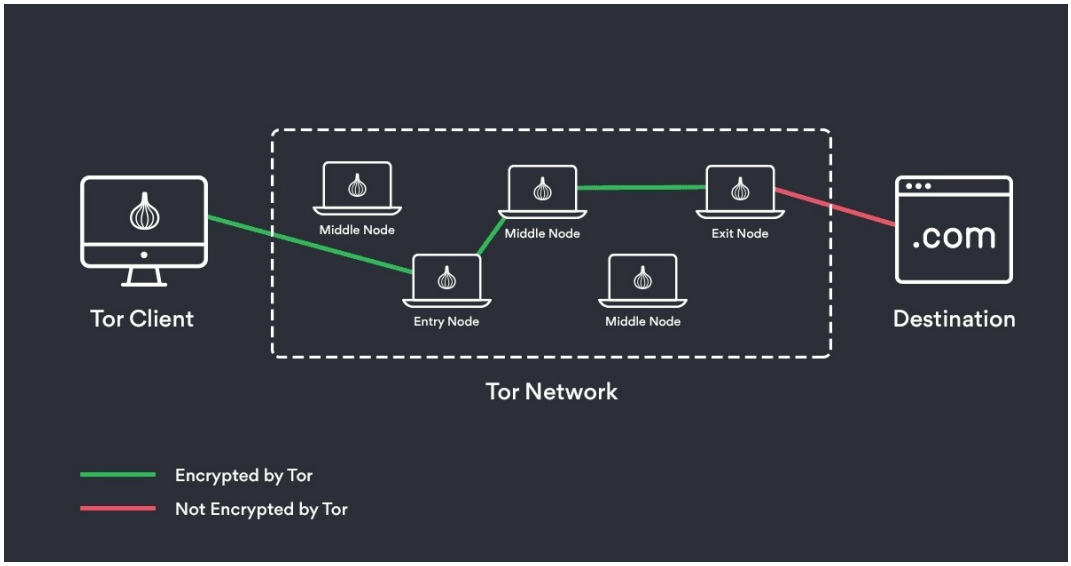
1. Introducción a la comunicación segura - TOR, HTTPS, SSL

Si estás leyendo esto, probablemente seas un usuario de la DarkNet, o simplemente, un friki de la ciberseguridad, ya que son términos poco usados en otros ámbitos. Tor proporciona un grado de anonimato “suficiente” utilizando un AES de 128 bits (estándar de cifrado avanzado). Se ha debatido si la NSA puede descifrar este código, y la respuesta es: **SÍ**.

Por eso, nunca debes enviar nada por Tor que no te resulte cómodo compartir con todo el mundo, a menos que estés utilizando algún tipo de **cifrado PGP,** del que hablaremos más adelante.

La comunicación desde el ordenador a internet depende de un **nodo de entrada** que, básicamente, "ingresa el ordenador" a la red Tor. Este nodo de entrada se comunica con el ordenador, y dicho nodo de entrada conoce la dirección IP.

El nodo de entrada pasa la solicitud cifrada al **nodo de retransmisión**. El nodo de retransmisión se comunica con el nodo de entrada y el nodo de salida, pero no conoce la dirección IP del ordenador. El **nodo de salida** es donde la solicitud se descifra y se envía a Internet. El nodo de salida no conoce la IP del ordenador, sólo la IP del nodo de retransmisión. El uso de este modelo de 3 nodos hace que sea más difícil, **pero no imposible**, correlacionar la solicitud con la dirección IP original.



El problema surge, obviamente cuando se ingresa texto sin formato en TOR, porque cualquiera puede configurar un nodo de salida. El FBI puede

configurar un nodo de salida, la NSA o cualquier otro gobierno extranjero, o cualquier persona malintencionada que desee robar información. No debemos introducir datos confidenciales en ningún sitio web, especialmente al acceder a ellos a través de TOR. Si alguno de los nodos de la cadena está en peligro, y las personas que están a cargo de esos nodos comprometidos tienen la capacidad de descifrar la solicitud, es mejor que no haya nada delicado.

Entonces, ¿qué podemos hacer para arreglar esto? Afortunadamente, ahora tenemos más y más servidores que ofrecen algo llamado “servicios ocultos”. Se pueden reconocer fácilmente estos servicios por la dirección “.onion”.

Estos servicios ofrecen lo que se llama cifrado de extremo a extremo. Lo que hacen es quitarles el poder a los nodos de salida comprometidos, y volver a ponerlos en sus manos. El servidor web del servicio oculto ahora se convierte en el nodo de salida, lo que significa que el sitio web que estás visitando es el que descifra el mensaje, no un nodo de salida aleatorio ejecutado por un atacante potencial.

Debemos recordar que, el nodo de salida tiene la clave para descifrar la solicitud. El nodo de salida puede ver lo que se está enviando en texto claro una vez que lo descifran. Por ello, si estamos introduciendo el nombre y la dirección en un campo, el nodo de salida tendría nuestra información. Si estamos colocando una tarjeta de crédito, una cuenta bancaria, nuestro nombre real, incluso nuestra información de inicio de sesión, estamos comprometiendo nuestra identidad.

Otro paso que podemos dar, es visitar sitios web que usan algo llamado **HTTP Secure**. Podemos saber si el sitio web que se está visitando utiliza HTTP Secure con el prefijo al comienzo de la dirección. Si vemos **https://**, entonces el sitio web está utilizando HTTP Secure.

Lo que hace es encriptar las solicitudes para que solo el servidor pueda descifrarlas, y que nadie "escuche" nuestra comunicación, como un nodo de salida de Tor comprometido. Esta es otra forma de encriptación de extremo a extremo. Si alguien interceptara la solicitud a través de HTTP Secure, verían datos encriptados y tendrían que trabajar para descifrarlos.

Otra razón por la que debemos usar **HTTPS** siempre que sea posible es, que los nodos maliciosos de Tor, pueden dañar o alterar los contenidos que pasan a través de ellos de manera insegura, e inyectar malware en la conexión. Esto es más fácil cuando se envían solicitudes en texto plano, pero HTTPS reduce esta posibilidad.

Sin embargo, conviene saber que HTTPS también puede ser más vulnerable, en función de la fortaleza de la clave utilizada para encriptarlo.

Cuando visitamos un sitio web usando HTTPS, estamos encriptando la solicitud usando su clave pública, y la están descifrando usando la clave privada. Así es como funciona la criptografía. Se proporciona una clave pública a quienes desean enviar un mensaje cifrado, y el único que puede descifrar es el que tiene la clave privada.

Desgraciadamente, muchos sitios web de hoy todavía usan claves privadas de sólo 1.024 bits de longitud, algo que hoy en día ya no es suficiente. Por lo tanto, debemos asegurarnos de averiguar qué nivel de cifrado utiliza el sitio web que estamos visitando, para asegurarnos de que estamos utilizando como mínimo 2.048, o como recomendación 4.096 bits. Incluso hacer todo esto puede no ser suficiente, porque podemos tener otro problema.

¿Qué sucede si el servidor web se ha visto comprometido? Quizás nuestros nodos TOR estén limpios, tal vez hayamos utilizado HTTPS para todas las solicitudes, pero el servidor web del sitio que estamos visitando, ha podido verse comprometido.

2. ¿Cómo usar PGP?

Otro paso que deberíamos seguir, especialmente cuando nos comunicamos con otros usuarios de **Silk Road**, es mediante el cifrado PGP. Esto no siempre es posible, como en los casos en los que se inicia sesión en un sitio web, se rellena un formulario, se inicia una sesión en el correo electrónico, etc.

Debemos considerar que cualquier tipo de información que se introduzca en un sitio web utilizando texto sin formato, posiblemente se verá comprometida. Por eso, nunca debemos poner ningún dato sensible, en cualquier formato de texto plano.

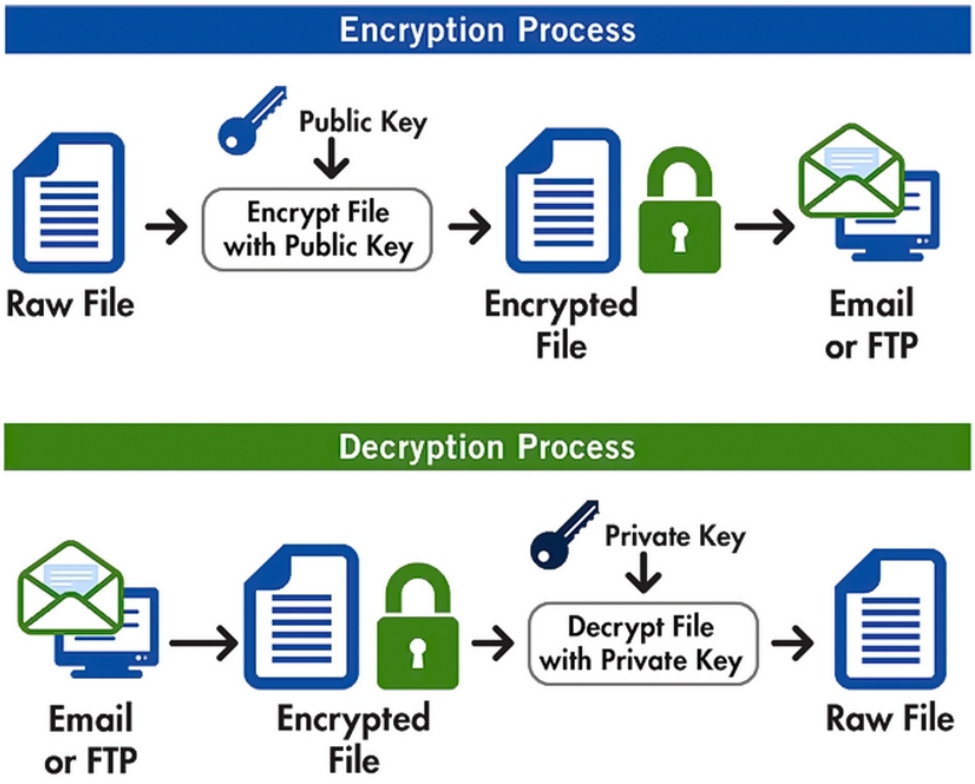
PGP usa un método de encriptación muy fuerte llamado **criptografía híbrida**. PGP significa **Pretty Good Privacy**, y se utiliza para encriptar, descifrar y firmar textos, correos electrónicos, archivos, directorios y particiones de discos completos y para aumentar la seguridad de las comunicaciones por correo electrónico.

Para los usuarios más técnicos, PGP utiliza una combinación en serie de hash, compresión de datos, criptografía de clave simétrica y finalmente, criptografía de clave pública. Para los usuarios menos técnicos, el proceso de cifrado de mensajes mediante PGP es el siguiente: Se crea una clave privada y una clave pública. La clave pública es la clave que se les da a las personas que desean que se les envíen mensajes encriptados.

La clave privada la guarda de forma privada. Esta clave privada es la única clave que puede descifrar mensajes que anteriormente estaban cifrados con nuestra clave pública.

Esto se llama criptografía, y fue diseñado para que cualquiera que intercepte nuestro mensaje no pueda descifrar el mensaje sin la clave privada. **Incluso nosotros mismos, si perdemos la clave privada, no hay un método de recuperación de clave.** Pudiendo considerar dicho mensaje cifrado de por vida.

Entonces, ¿cómo usamos PGP? Antes de llegar a eso, deberíamos conocer un sistema operativo live, que hace que el uso del cifrado y descifrado PGP sea muy fácil. Un sistema operativo live es un sistema operativo que puede ejecutarse sobre un sistema operativo actual.



Por ejemplo, si somos un usuario de Windows, tenemos 2 opciones. Podemos descargar el sistema operativo live, grabarlo en un CD o DVD y luego iniciar el ordenador desde ese DVD o CD. Esto asegurará que el ordenador funcione como si tuviera este sistema operativo instalado en el ordenador. Sin embargo, si quitamos el CD o DVD y reiniciamos, el ordenador arrancará normalmente. También puede usar una unidad USB para realizar esta misma función.

En segundo lugar, podemos ejecutar este sistema operativo live en lo que se llama una máquina virtual. Los beneficios de esto son que podemos ejecutar Windows simultáneamente mientras ejecutamos este otro sistema operativo y podemos cambiar fácilmente de uno a otro sin reiniciar el ordenador.

Ambos métodos tienen sus pros y sus contras. Las ventajas de ejecutar un arranque de live CD son, que reducen el riesgo de que el ordenador se vea comprometida por virus, malware y keyloggers que dependen de las vulnerabilidades de Windows para ejecutarse.

La razón por la que os recomiendo **Tails** es porque ya tiene instaladas muchas de las características de seguridad que necesitamos para mantener el anonimato. Algunos usuarios no están contentos con Tails, pero realmente es un gran sistema operativo cargado con funciones de seguridad. Muchos de los que hablaremos en esta serie sobre seguridad.

Hay muchos tutoriales sobre cómo cargar Tails en Virtual Box, así que no entraremos en muchos detalles, asegúrate de ejecutar **Virtual Box** y Tails desde una unidad USB o tarjeta SD. Sugeriría un dispositivo USB, que por razones que explicaré más adelante. Pero básicamente cuando Virtual Box se ejecuta directamente en el disco duro, crea un disco duro virtual que se utiliza como un disco duro temporal mientras Tails se está ejecutando.

Una vez que se cierra Tails, esta unidad virtual se eliminará, pero no se elimina permanentemente. Como sabemos por el poder de las herramientas de recuperación y el análisis forense, los archivos eliminados son fácilmente recuperables con las herramientas adecuadas.

Por ahora, simplemente mantén la máquina virtual y las colas desactivadas del disco duro y cárgalo en una unidad USB o en una tarjeta SD.

Lo mismo ocurre cuando se inicia el ordenador directamente en Tails desde un DVD o dispositivo USB. El disco duro se usará para almacenar los archivos utilizados por Tails, así que asegúrate de que los archivos guardados o accedidos usando Tails se realicen desde un dispositivo USB o tarjeta SD, de lo contrario serán recuperables.

La mejor opción es usar una Máquina Virtual y ejecutar todo en una memoria USB. Mantén fuera del disco duro real todo cuanto sea posible. Es posible triturar archivos para que sean irrecuperables, pero es mucho más fácil hacerlo en una unidad flash de 16 GB, que en un disco duro de 1 TB.

3. Usar PGP en TAILS

Bien, ahora supongamos que tenemos Tails funcionando. Vamos a aprender cómo usar PGP dentro de Tails. Lo primero que debemos hacer es crear nuestra propia clave personal, que consiste en la **clave pública**, que se puede entregar a las personas o publicar en sus perfiles en línea.

Como se mencionó anteriormente, esta es la clave que las personas utilizan para cifrar los mensajes que envían. La clave personal también consta, además de la clave pública, de la **clave privada** que puede usar para descifrar los mensajes cifrados con la clave pública de PGP.

A continuación, y una vez creada, debemos guardar la clave privada en una unidad USB secundaria o tarjeta SD. Si está ejecutando Tails desde una unidad USB, debe usar una unidad independiente para almacenar la clave. Nuevamente, **nunca almacene las llaves privadas en el disco duro, manténgalas FUERA del ordenador.**

Si se pierde la clave privada, nunca podrá recuperarla, incluso si se crea otra clave personal con la misma contraseña. Cada clave privada es única para el momento en que se creó y, **si se pierde, se pierde para siempre.**

Una vez que se haya hecho esto, se habrá guardado la clave personal para usarla en el futuro una vez que reinicie Tails. Recordando que Tails no está instalado en el disco duro, por ello cada vez que se reinicia Tails se pierden todas las claves que pudiese tener. Al guardar las llaves en una unidad USB o tarjeta SD, se pueden importar para usarlas cada vez que se reinicie Tails.

Ahora, deberemos aprender a cifrar y descifrar mensajes con la clave. Bueno, afortunadamente, Tails ya ha hecho un tutorial sobre cómo cifrar y descifrar mensajes.

4. Encriptación completa del disco duro y sus archivos

Ahora que hemos descubierto PGP, recordamos de nuevo que usar PGP siempre que sea posible es muy, muy importante. Una de las *trampas* que pusieron a Silk Road es que algunos de los administradores, incluido el propio **Ross**, no siempre se comunicaban utilizando el cifrado PGP. Una vez que Ross fue arrestado, tenían acceso a los servidores y los portátiles, y todo lo que no estaba encriptado, estaba abierto pudiendo ser revisado.

La mayoría de los usuarios de Silk Road creen que Ross había almacenado información personal sobre algunos de los administradores y moderadores en el ordenador en texto plano, lo que se utilizó para realizar 3 arrestos más de usuarios de Silk Road.

Una de las razones por las que se sugiere que se guarden las llaves PGP y otros datos confidenciales en una tarjeta SD es que si llega ese día en que está comprometido y se recibe un golpe en su puerta, tenemos tiempo para deshacernos de una Tarjeta SD o unidad USB rápidamente. Aún mejor, si tenemos una tarjeta micro SD que se conecta a un adaptador SD, podemos incluso esconderla.

Nuestro siguiente tema nos lleva a algo llamado **Whole Disk Encryption** o **Full Disk Encryption**. A partir de ahora nos referiremos a él como FDE (Full Disk Encryption). Tails tiene una función FDE incorporada, que es otra razón por la que es muy recomendable el uso de Tails. Tiene muchas de estas características para protegerte.

Esencialmente FDE protegerá la unidad, ya sea SD o USB, de las personas que pueden venir a buscarnos algún día. El método en el que lo hace es formatear la unidad y reescribir el sistema de archivos de forma cifrada, de modo que sólo pueda acceder a ella quien tenga la contraseña.

Si olvidamos la contraseña, al igual que pasa en **PGP**, no podremos recuperarlo. La única opción es formatear el disco y comenzar de nuevo. ¡Así que asegúrate de recordarlo! Y por favor, por el amor de Dios, **nunca guardes la frase de contraseña en el disco duro.**

5. Usa PGP cuando te comuniques con otros en la DarkNet

La trituración de archivos es extremadamente importante, este es el motivo de que sea el próximo tema. Si eliminamos un archivo del ordenador, sólo estamos eliminando el lugar donde se encuentra en la unidad. Todavía está en la unidad real, sólo se han eliminado los datos de ubicación.

Si utilizamos una herramienta de recuperación de archivos, podemos recuperar virtualmente cualquier archivo que se haya eliminado recientemente. La trituración de archivos combate esto sobrescribiendo archivos en su lugar. La idea es que, en lugar de eliminar la ubicación del archivo, debemos sobrescribir el archivo con datos aleatorios para que no se puedan recuperarse.

Hay mucho debate sobre si se puede sobrescribir un archivo una vez, o si se necesita hacerlo varias veces. Supuestamente, la NSA recomienda 3 veces, el Departamento de Defensa de Estados Unidos recomienda 7 veces, y un documento antiguo de un hombre llamado Peter Gutmann escrito en los 90 se recomienda 35 veces. Personalmente, creo que entre 3-7 veces es suficiente, y varias personas creen que 1 sola vez hará el trabajo.

El razonamiento detrás de esto es que algunas personas creen que el disco puede perder algunos archivos la primera vez que los escribe y para ser más completos, debe hacer múltiples pasadas. Haz lo que te parezca más cómodo, pero incluso creo que 3 pases serían suficientes, aunque no pasaría nada si de vez en cuando ejecutaras 7 pases y simplemente dejarlo durante la noche.

Estos programas pueden eliminar los archivos de la Papelera de reciclaje, eliminar los archivos temporales de Internet e incluso borrar el espacio libre en disco para asegurarnos de que todo está limpio. Siempre necesitas pensar, ¿tengo algún material sensible en mi disco duro? Si es así, tal vez debas destruir el espacio libre en el disco. Al vaciar la Papelera de reciclaje, siempre debemos usar una trituradora. Cuando sólo borras menos de 1 GB a la vez, podemos hacer fácilmente 7 pasadas rápidamente.

Para poner esto en perspectiva, el líder de un grupo llamado nombre **LulzSec Topiary** ha sido excluido como parte de su sentencia de utilizar cualquier tipo de aplicación de trituración de archivos por si el FBI quiere controlarlo, puedan hacerlo. La trituración de archivos mantiene los archivos borrados, realmente eliminados.

Algunas aplicaciones de trituración de archivos que podemos usar son: **dban, fileshredder o priform.**

6. Vulnerabilidades JavaScript y eliminación de metadatos personales en archivos

Antes de comenzar a eliminar metadatos dañinos de sus archivos, quiero hablar sobre otra vulnerabilidad a nuestras capacidades de exploración llamada JavaScript.

A mediados de 2013, una persona en Irlanda brindaba alojamiento a personas que hospedaban servicios "ocultos", incluida una plataforma segura de correo electrónico llamada **Tor Mail**. Lo arrestaron por un cargo relacionado con la pornografía infantil y confiscaron todos sus servidores.

Ya fuera que estuviera o no relacionado con pornografía infantil, las autoridades terminaron inyectando JavaScript malicioso en los servidores para que los usuarios visitaran ciertos sitios, y al hacerlo, este código malicioso se ejecutaría en sus servidores y revelaría información sobre sus computadoras a las autoridades. Le sugiero que lea el siguiente artículo para obtener más información al respecto.

Dicho esto, es posible que deseemos deshabilitar JavaScript en los navegadores, especialmente cuando visitamos ciertos sitios web de las **DarkNet** que podrían verse comprometidos algún día. Muchos usuarios se niegan a visitar el sitio web original de **Silk Road** y los foros con JavaScript habilitado porque las autoridades probablemente han podido inyectarlo con JavaScript malicioso para identificar a los usuarios.

En Tails, el navegador se llama **Iceweasel** y cuando Tor se ejecuta en Windows, usa **Firefox**. Ambos navegadores pueden deshabilitar JavaScript utilizando el mismo método. Abrid una ventana y escribid el siguiente comando en la barra de direcciones, "**about: config**" y haced clic en el botón que dice "Tendré cuidado, lo prometo".

Esto abrirá una serie de configuraciones que incluyen una barra de búsqueda en la parte superior. Buscamos JavaScript en la barra de búsqueda y sus dos entradas, "**JavaScript.enabled**" y **“browser.urlbar.filter.JavaScript**". Clic derecho sobre ellos y clic en "Alternar", verá el valor cambiado a falso. Si deseáis habilitar JavaScript nuevamente, simplemente haced clic en Alternar nuevamente y veremos que el valor vuelve a ser verdadero.

Recordemos que, cada vez que reiniciemos Tails tendremos que hacer esto de nuevo, así que tengamos el hábito de hacerlo todo el tiempo. Nunca se sabe cuándo nuestro sitio web favorito podría verse comprometido.

Tras ver la importancia de JavaSript, pasamos a los metadatos. Hay una pequeña historia famosa sobre un hacker online llamado **w0rmer** que tomó fotos de su novia y las publicaría en línea en un **defacement** de una página web. Lo que olvidó, o no sabía, era que las **fotos tomadas con el iPhone y otros teléfonos inteligentes guardan las coordenadas GPS de donde se tomó la imagen y la almacenan en los metadatos de la imagen.**

¡Necesitamos eliminar estos metadatos! Afortunadamente, Tails tiene una solución para esto. Tened en cuenta los formatos actualmente compatibles. En términos de imágenes, jpg, jpeg y png. Pero MAT no es perfecto, y yo no confiaría en él, por lo que una buena idea sería **NO** subir nunca fotos nuestras o de nuestra pareja online, especialmente si estamos alardeando de un hack cometido.

7. Precauciones generales de seguridad al publicar online

Hablaremos a continuación sobre buenas prácticas al usar Tor, Tails y otros servicios de la **DarkNet**.

En primer lugar, es muy recomendable utilizar múltiples identidades online para diferentes cosas. Si eres es un comprador y un vendedor en Silk Road, es posible que desees tener inicios de sesión separados para esto. Y luego posiblemente un tercer inicio de sesión para los foros. O si quieres ser parte de otro mercado, entonces quizás deberías tener un cuarto acceso.

Bueno, Tails tiene otro buen programa ofrecido por Tails que se llama **KeePassX**. Cuando tenemos varios inicios de sesión, es difícil hacer un seguimiento de todos ellos, por lo que podría ser una buena idea mantenerlos todos en 1 documento cifrado con una contraseña segura.

Nunca debemos usar apodos o ubicaciones, o cualquier otra cosa que relacione la vida online con la pública. Otra precaución que debemos adoptar son nuevas formas de movernos. Si generalmente eres una persona desordenada, que comete los mismos errores de gramática, o los mismos errores de ortografía todo el tiempo, debes saber que esto puede usarse para identificarte.

Siempre debemos verificar todo lo que publiquemos públicamente o en privado, porque las autoridades siempre encontrarán maneras de relacionarnos con ello.

Con **Ross Ulbricht**, encontraron una publicación anterior que publicó en un foro cuando comenzó Silk Road preguntando a la gente si habían oído hablar de un mercado llamado Silk Road.

Obviamente, este es un viejo truco utilizado por las personas que tratan de difundir la conciencia sobre un nuevo proyecto suyo. Más tarde se identificó diciendo que estaba buscando programadores y dio su dirección de correo electrónico privada en el mismo foro con el mismo nombre.

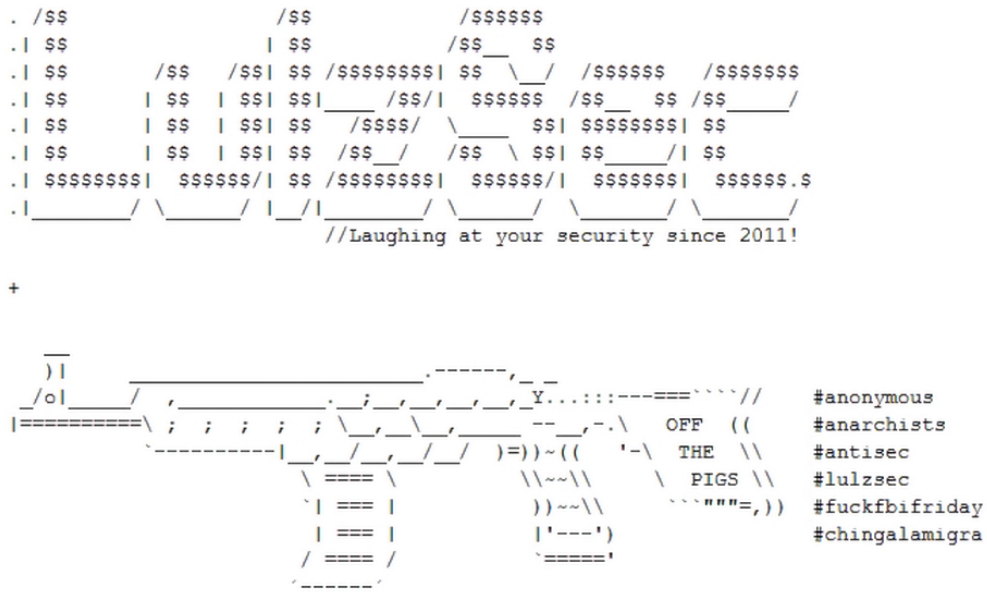
Si siempre escribes mal las mismas palabras, si siempre utilizas los mismos términos de argot, escribes en mayúscula las mismas palabras, usas una cierta cantidad de períodos después de un etc. o siempre usas la misma cantidad de…

Todas estas cosas dan una sospecha razonable y es más fácil atribuir las cosas a alguien. Una vez que te tienen bajo su radar, solo te costará un par de errores ¿Entiendes?

Piensa en el tiempo que usa el ordenador. ¿Es fácil correlacionar la zona horaria según el momento en que te conectas? ¿O es más aleatorio? ¿Tiene patrones que son predecibles? Siempre piensa en estas cosas cuando publiques online. Siempre piensa en qué tipo de personalidad estas presentando sobre el nombre online.

Espera que cada palabra que escribas online sea leída por las autoridades. Para ellos, esto es mucho más fácil que rastrear a los señores de la droga en las calles. Se sientan en una oficina y leen mensajes en un foro e intentan establecer conexiones. No subestimes a las autoridades.

Siempre trata todo como si estuviese comprometido, siempre trata a todos como si estuviesen comprometidos y nunca pienses que alguien va a ir a la cárcel por ti. Si alguien se puede evitar 10-20 años al delatarte, lo hará en un instante.



El ejemplo perfecto es **Sabu** de **LulzSec.** Después de que fuera arrestado y se enfrentase a 112 años en la cárcel, le hicieron un trato para que delatara a sus amigos, y que terminó con múltiples arrestos de los mismos. Incluso las personas que son tus amigos, llegado el caso, te darían la espalda cuando se tratara de su libertad.

8. Datos EXIF

Olvidé mencionar arriba, cuando hablábamos de metadatos, que cuando se trata de fotos, hay otro riesgo involucrado llamado **datos EXIF**, esta es otra forma de metadatos específicamente relacionados con las imágenes y que, además, no pueden ser eliminados correctamente por la herramienta **Metadata Anonymisation Toolkit,** mencionada anteriormente.

Los datos EXIF nos muestran información relevante sobre el formato de archivo de imagen intercambiable, y afectan a los archivos JPG, JPEF, TIF y WAV. Por ejemplo, una foto tomada con una cámara habilitada con GPS puede revelar la ubicación exacta y el momento en que se tomó, y el número de identificación único del dispositivo, todo esto se hace de manera predeterminada, a menudo sin que el usuario lo sepa.

En diciembre de 2012, el programador anti-virus **John McAfee** fue arrestado en Guatemala mientras huía de una supuesta persecución en Belice, que comparte una frontera.

La revista Vice había publicado una entrevista exclusiva con McAfee "en marcha" que incluía una foto de McAfee con un vicepresidente tomada con un teléfono que había etiquetado geográficamente la imagen. Los metadatos de la foto incluían coordenadas GPS para ubicar a McAfee en Guatemala, fue capturado dos días después. **Para evitar esto, sólo toma fotos que usen PNG, porque no almacenan datos EXIF.**

O podemos descargar una herramienta haciendo una búsqueda rápida online para ver qué datos EXIF pueden contener las fotos antes de subirlas. Ten mucho cuidado con los archivos que cargues online, porque nunca se sabe qué tipo de datos dañinos se pueden adjuntar en ellos. Es útil usar Tails, pero siempre considera todo lo que pongas online como una posible prueba para usar en tu contra y siempre prepárate para el día en que las autoridades lleguen a nuestra puerta.

9. Necesito un abogado, captura e interrogatorio

¡Hablemos claro!

Todos somos humanos y cometemos errores. Desafortunadamente, sólo necesitamos cometer un error, y nos aplicaran la ley. Quizás esperen a que hagas algo más serio antes de que te atrapen, pero si te equivocas y sienten

que vales la pena, con raras excepciones puedes esperar que te atrapen sin importar dónde vivas.

¿Debería tener a mano un teléfono de abogado de emergencia? La respuesta es: **Sí.**

Una vez arrestado, pueden confiscar tu dinero basándose en la suposición de que está relacionado con las actividades ilícitas. Por ellos, necesitamos tener un abogado pagado por adelantado. De esta forma, en el desafortunado caso de que recibamos una visita de las autoridades, tendríamos abogado.

A continuación, hablaremos sobre qué hacer en caso de ser interrogado.

Básicamente. Mantén la boca cerrada. Las autoridades van a probar todo tipo de tácticas para que admitas la culpabilidad de los crímenes de los que te acusan. Es probable que usen el policía bueno, el policía malo contigo. Primero le dirán que quieren ayudarlo, y que buscan a los grandes. Sólo necesitan tu ayuda para alejar a los grandes. No escuches esto, una vez que admitas ser culpable, puedes despedirte de tu libertad.

En segundo lugar, si te niegas a cooperar, la actitud cambiará a policía malo. Ellos dirán: *"Muy bien, ¿no quieres cooperar? Traté de ayudarte, pero ahora vas a tener un montón de problemas. ¿Tienes alguna idea de a qué tipo de cargos te enfrentas? Te van a encerrar por un largo tiempo, a menos que empieces a hablar"*.

Intentarán asustarte para que admitas tu culpa. De nuevo, mantén la boca cerrada y continúa solicitando un abogado. Nunca hables sin un abogado presente y nunca hagas nada que no tengas que hacer legalmente. Si tienes derecho a permanecer en silencio, entonces utiliza ese derecho. Sé que hay algunas circunstancias en las que no tienes ese derecho, pero a menos que sea así, es mejor que te mantengas callado.

Tercero, abandona la actitud. No discutas con los policías sobre que el hecho en cuestión no tiene nada contigo, o algo por el estilo. Actúa asustado, ansioso y confundido. Actúa como si no tuvieras idea de lo que está pasando y que tienes miedo de tu vida. Dile a la policía que te están asustando y que quieres ver a tu abogado porque no sabes de qué se trata. Necesitan pruebas y pruebas sólidas para acusar de un delito.

Intentarán correlacionar las publicaciones realizadas en los foros, los números de teléfono llamados, tal vez un paquete enviado al hogar, todas las formas de comunicación, transferencias bancarias, etc., hasta que encuentren la manera de vincularte con el delito. Te están acusando. Pero la evidencia más grande siempre será la disposición a admitir la culpa por una pena menor.

Cuando Sabu descubrió que se enfrentaba a 112 años en una prisión federal, rápidamente contó todo, y comenzó a trabajar para las autoridades. Una vez más, habla con tu abogado, descubre las pruebas en tu contra y sólo responde las preguntas que tu abogado te recomiende que respondas, y respóndelas de la manera en que tu abogado te aconseje que las responda.

Trata de ser lo más honesto posible con tu abogado. Tu abogado no puede, y no compartirá ninguna admisión de culpa que tengas con los fiscales, esto se llama privilegio de abogado-cliente.

10. Combinando TOR con una VPN

¿Debería usar una VPN con TOR? ¿Debo usar TOR para conectarme a una VPN, o usar una VPN para conectarme a TOR?

Permítanme decir, en primer lugar, que cuando se navega por Internet sin TOR, probablemente deberíamos estar utilizando una VPN, independientemente de si estamos utilizando TOR o no. Debemos asegurarnos de que la VPN también usa alguna forma de encriptación.

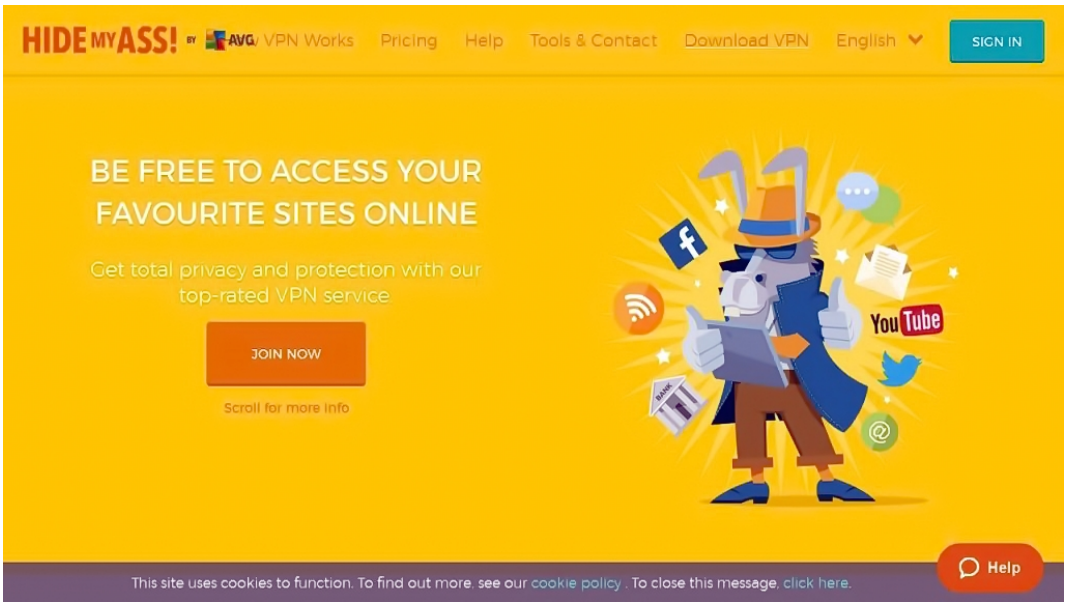
Todas las redes, pero especialmente las redes wifi públicas, son vulnerables al análisis del tráfico. Si combinamos esto con el hecho de que algunos proveedores de servicios de Internet controlan tu actividad hasta cierto nivel, podemos ver por qué podría ser una buena idea usar siempre un método cifrado para usar Internet. Por lo menos, para proteger la información personal cuando introduzcamos datos de tarjetas de crédito, nombres de usuario y contraseñas, así como, otros datos personales online. De nuevo, especialmente si estamos usando una red wifi pública.

Elegir una VPN que use al menos un cifrado de 128 bits como TOR es una buena práctica, y detendrá a la mayoría de los espías. Pero si puedes obtener encriptación de 256 bits, mucho mejor. Antes de entrar en la cuestión de si deberíamos usar una VPN junto con TOR, quiero advertirte brevemente sobre cómo debería usar una VPN.

Si vais a utilizar una VPN para cualquier tipo de lucha de libertad, aseguraros de que vuestra VPN no guarda los registros. Esto es realmente mucho más difícil de lo que pueda parecer. Muchos proveedores de VPN alegarán no mantener registros de su actividad para poder ganarte como cliente, porque tienen que competir con los demás proveedores.

Los clientes tenderán hacia los proveedores que no ofrecen conservan datos de identificación. Pero, este reclamo no siempre es el caso real, y os mostraré un ejemplo.

Existe un conocido proveedor de VPN llamado **HideMyAss** que anteriormente afirmaba no mantener registros de sus usuarios. Lamentablemente, cuando se vió con una orden judicial del gobierno en el Reino Unido, entregaron pruebas de un presunto hacker de **LulzSec** que ayudó a su arresto.



Un hombre muy inteligente que utiliza el manejo online **The Grugq**, dijo que cuando luchas por la libertad online, nadie va a ir a la cárcel por ti, algo 100% correcto. Cuando se trata de eso, ningún proveedor de VPN va a arriesgarse a ir a la cárcel para proteger a un suscriptor que paga 20€ al mes.

No importa lo duras parezcan, no importa cuánto pretendan cuidar de proteger a sus clientes, cuando se enfrenten con la opción de renunciar o ir a la cárcel, siempre elegirán la libertad.

Otra cosa a tener en cuenta, es el uso de una VPN para ocultar tu actividad de Internet del proveedor de servicios de Internet. Esto también puede ocultar el hecho de que se está utilizando TOR, lo que puede hacer sospechar cuando las autoridades comienzan a pedirles a los ISP que proporcionen datos sobre sus usuarios.

Esto puede o no ser relevante, ya que muchas personas usan TOR y podremos argumentar que hay muchas razones legítimas para usar TOR.

Pero es solo otro factor para despertar sospechas que pueden o no entrar en juego y deben ser consideradas.

Si eliges utilizar TOR sobre una VPN, los beneficios son que estarías otra vez, ocultando a tu ISP el hecho de que estás usando TOR. Además, tu VPN sólo podrá ver que se está conectando a nodos TOR y que está enviando datos encriptados. La VPN no podrá ver qué datos está enviando a través de TOR a menos que lo descifren, recuerda, toda la información retransmitida a través de TOR está encriptada.

Las desventajas, por supuesto, como ya mencioné, son que los proveedores VPN pueden o no, registrar todo lo que haces en forma de metadatos o incluso contenido si tienen la capacidad de almacenamiento, y mantener esos registros a mano durante mucho tiempo. En este caso, no es mejor que conectarse a TOR a través de un ISP.

Otra cosa que debe mencionarse a aquellos que usarán VPN cuando no usen TOR, pero también usarán VPN cuando usen TOR es, recordar cuándo y cuándo no están conectados a su VPN. A veces las conexiones VPN se pueden desconectar inesperadamente, y es posible que ni siquiera os deis cuenta de ello. Si la razón por la que estáis utilizando una VPN es para ocultar la actividad TOR del ISP, recordad que, si vuestra VPN cae, el ISP comenzará a ver tráfico TOR.

O tal vez, te olvides de que estás conectado a tu VPN y terminéis indicando tu dirección en Google Maps para encontrar direcciones en algún lugar. Bueno, ¿adivina qué hace Google con todos los datos introducidos en su sistema? **Siempre lo conservan, y probablemente lo mantengan indefinidamente.**

Entonces, si un día la NSA nos identifica en la red TOR ocupando una gran cantidad de nodos, usando el análisis de tráfico para identificarlo en función del análisis estadístico, nos vinculará a nuestra dirección IP VPN.

En este punto, es probable que le pidan a la VPN que entregue datos sobre sus usuarios, pero si la VPN se niega a cumplir porque no están sujetos a la ley de un determinado país, pueden consultar algunos de los sitios web de mayor monitorización, para ver si navegamos y usamos esa dirección IP para cualquier otra cosa online. Comprobarán los registros de Google, Yahoo, Facebook, Twitter, Netflix y otras compañías de recopilación de grandes volúmenes de datos para ver quién ha estado usando esa dirección IP para conectarse a sus servidores.

Si accidentalmente introducimos la dirección en Google cuando nos conectamos a esa VPN, somos sospechosos. Así que siempre debéis tener esto muy en cuenta. **El hecho de estar detrás de una VPN no significa que no se pueda rastrear por un error humano.**

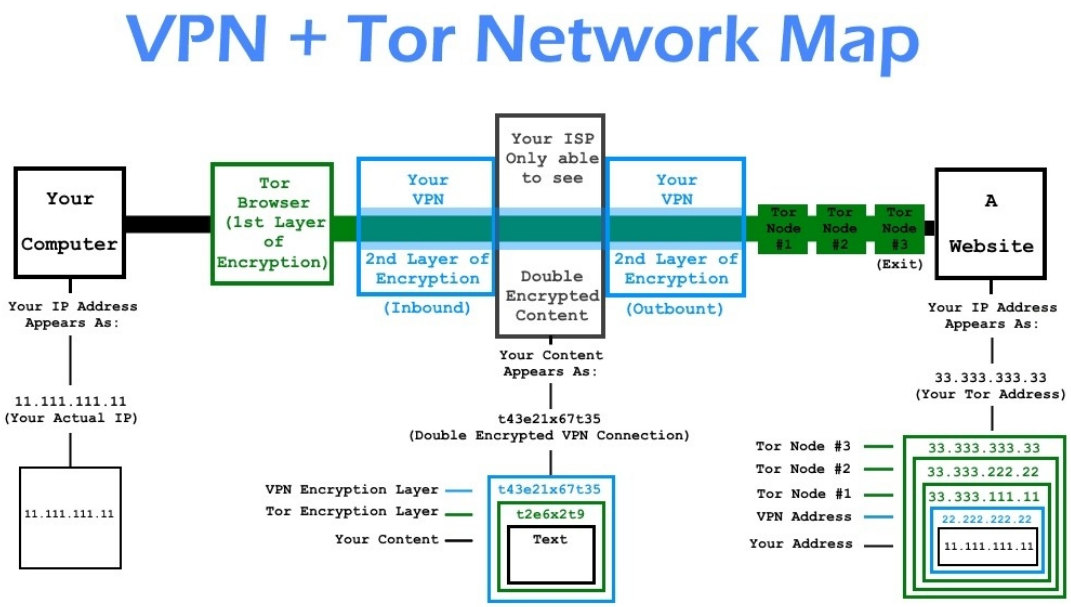
Los beneficios de TOR son que obtenéis una identidad nueva cada vez que os conectáis. Este puede ser o no, el caso de nuestra VPN, así que por favor verificad y aseguraros de cómo y cuándo estáis conectados.

11. Montando una sesión de TOR sobre una VPN

Los beneficios de hacerlo son los siguientes. Eres más anónimo con tu VPN en caso de mantener registros, o si haces algo que no debes con la VPN, y un sitio web o servidor toma nuestra dirección IP VPN.

En el caso de que esto suceda, incluso si la VPN logra mantener registros de todo lo que hacemos, sólo pueden identificarnos como un usuario de TOR anónimo, siempre y cuando, *no hayamos comprado el servicio como un idiota con nuestra tarjeta de crédito o cuenta de Paypal*.

Si usamos Bitcoin y nos aseguramos de que el camino de **Bitcoin no sea fácil de rastrear**, deberíamos estar protegidos. Algunos sitios web bloquean que los usuarios de TOR se conecten a sus sitios web o servidores, al usar nuestra VPN para aparecer como nodo de salida, estamos ocultando nuestra actividad con TOR del sitio web visitado y, con suerte, omitiendo dichos filtros.



Otra ventaja, es que, si nuestra conexión VPN cae, su caída será nuestra dirección IP TOR en lugar de nuestra dirección IP real. Y finalmente, si pasamos a través de un nodo de salida TOR comprometido, nuestra información permanecerá encriptada a través del protocolo de cifrado de la VPN hasta que llegue al nodo de salida de la VPN.

Esto es bueno si está pasando por un nodo de salida comprometido, pero no olvide que la VPN podría estar registrando todo lo que está haciendo de todos modos. **¡No confíes en nadie que tenga acceso a tus datos no cifrados! ¡NUNCA!**

Algunas de las desventajas de hacer las cosas de esta manera, como se ha mencionado anteriormente, es que nuestro ISP sabe que estamos utilizando TOR, cuándo y durante cuánto tiempo. Esto puede o no importarnos, pero es sólo algo a considerar. En segundo lugar, no podremos visitar sitios web de servicios ocultos.

¿Recuerdas aquellos sitios ".onion" de los que hablamos al principio? Debemos estar conectado a la red TOR para visitar esos sitios web de servicios ocultos.

Pero estoy conectado a TOR ¿no? Sí, lo estamos, pero nuestro método final de comunicación con Internet no proviene de la red TOR, proviene de nuestra VPN. Y nuestra VPN probablemente no está bien configurada para usar TOR. Para que podamos conectarnos a los **Hidden Sevices**, debemos estar conectados directamente a TOR, o usar una VPN para conectarnos a TOR.

TOR debería ser siempre nuestro nodo final de conectividad para visitar sitios web ".onion".

La elección depende de nosotros, y cada persona en cada estado, provincia y país tendrá diferentes motivos para querer usar VPN -> TOR o TOR -> VPN, o simplemente TOR, o simplemente VPN. Cualquiera que sea la elección que hagamos, debemos tener en mente todas las cosas mencionadas.

Ninguno de estos métodos nos salvará si ingresamos algo que nos identifique online. No inicies sesión en tu cuenta de Facebook con nuestra VPN. No revises el correo electrónico ni busques una dirección cercana en Google usando la VPN. De hecho, aléjate de Google por completo a menos que sea absolutamente necesario.

Hay otros dos motores de búsqueda que no almacenan información sobre sus usuarios.

1. **DuckDuckGo.**

Tienen una URL de clearnet y una URL de servicios ocultos para ambos tipos de usuarios.

- duckduckgo.com
- 3g2upl4pq6kufc4m.onion - Ten en cuenta que el espejo de Hidden Services no es HTTPS

2. **StartPage.**

Este servidor tampoco almacena ninguna información sobre sus usuarios.

- startpage.com

Antes de continuar, quiero volver al tema de cómo elegir una buena VPN. Cuando busquemos un proveedor de VPN, lo más probable es que encontremos dos protocolos para elegir. Tendremos que averiguar cuál utiliza nuestro proveedor de VPN antes de registrarnos con ellos. **PPTP** y **OpenVPN**. En este momento, recomiendo encarecidamente evitar PPTP, quedándonos con los proveedores de **OpenVPN**.

Como podemos ver, PPTP utiliza un cifrado más débil, de 128 bits frente a 160 bits a 256 bits para OpenVPN. Ofrece seguridad básica frente a un alto nivel de seguridad utilizando algo llamado certificados digitales.

Esto es básicamente una forma de asegurarnos de que los datos que llegan, se envíen de forma segura desde nuestro proveedor VPN, y no sean inyectados por terceros malintencionados, porque los datos entrantes y salientes se firman utilizando certificados especialmente obtenidos, similares a mostrar nuestro ID para entrar en un área restringida.

El único inconveniente es que la configuración de **OpenVPN** puede ser un poco difícil para los usuarios menos técnicos, pero hay muchos tutoriales online para configurar proveedores de OpenVPN, y nuestro proveedor de VPN probablemente también nos ayude a configurarlo.

PPTP ha sido abandonado por aquellos que exigen el más alto nivel de seguridad, por lo que recomendaría evitarlo. Una tercera opción para los proveedores de VPN es **L2TP/IPsec**, pero muchos usuarios creen que también ha sido comprometida por la NSA debido a sus niveles más débiles de cifrado y también debemos evitarla. **Debemos usar OpenVPN.**

Por último, si deseamos saber cómo conectarnos a TOR a través de una VPN. Si estamos utilizando OpenVPN, es realmente simple. Asegúrate de estar conectado a la VPN, verifica tu dirección IP en cualquier sitio web como **WhatIsMyIpAddress** para asegurarnos que haya cambiado. Luego, abrimos

TOR o TAILS y comenzamos a usar TOR y ya estaríamos conectados a TOR a través de una VPN.

Conectarse a una VPN por TOR es más complicado, ya que OpenVPN reconfigura las rutas de la red para que TOR no pueda ejecutarse en el mismo host. Actualmente solo los usuarios de Windows pueden usarlo.

12. Conexión TOR -> VPN para usuarios de Windows

Después de una larga búsqueda, hemos encontrado una forma de conectar TOR -> VPN. No es perfecta, y algunos pueden no estar de acuerdo con hacer las cosas de esta manera, pero funciona y se muestra como una opción, pero *sólo funciona para los usuarios de Windows* en este momento.

Ya os he hablado anteriormente sobre la combinación de VPN y TOR, donde encontraréis las razones por las que deberíais hacerlo, y algunas de las razones por las que NO deberíais hacerlo. Pero no os pude proporcionar una forma de conectarse a una VPN usando TOR para que la VPN no sepa quién eres.

Cuando se trata de TOR -> VPN, si no puedes confiar en tu VPN, lo cual raramente deberías hacer, mantener la identidad anónima desde nuestra VPN es una buena idea. Además, con cada vez más personas que usan TOR, con alrededor de 4000 nodos de salida TOR, muchas de las direcciones IP del nodo de salida se marcan como spammers en sitios web populares y así, se limita el uso “sólo” a usuarios TOR con buenas intenciones, para publicar en foros.

La forma en que se descubrió que se puede hacer TOR -> VPN es usando una máquina virtual, preferiblemente Virtual Box y ejecutando otra instancia de Windows, preferiblemente una que usa menos memoria que la versión actual. Deseamos ejecutar **TOR Expert** y **Tortilla** en su sistema operativo anfitrión. Configura tu Virtual Box para enrutar todo el tráfico de red a través de Tortilla (adaptador Bridge), que lo enruta a través de TOR.

Actualmente, Tortilla sólo es compatible con Windows, por lo que esta opción sólo está disponible para los usuarios de Windows en este momento.

Ahora que tenemos nuestra máquina virtual de Windows ejecutándose en TOR, podemos instalar una VPN de nuestra elección, preferiblemente una que use OpenVPN en nuestro sistema operativo anfitrión de Windows, y se conecte a ella. Verifica la dirección IP antes de la conexión y después,

deberíamos ver una dirección IP diferente. Si todo ha ido bien, ahora tenemos una máquina virtual ejecutando TOR -> VPN.

Si deseamos agregar otra capa, podemos descargar el paquete de navegador TOR en nuestra máquina virtual y ejecutar eso también, dándole TOR -> VPN -> TOR para otra capa de seguridad. Y, además tenemos la opción de usar este método para usar una VPN en el sistema operativo host, mediante **Tor Expert** con Tortilla, además de otra VPN en nuestro sistema operativo anfitrión y el navegador TOR, que nos proporcionará una estructura de capas de seguridad: **VPN -> TOR -> VPN-> TOR.**

No estoy abogando por ningún método en concreto, debéis tomar esa decisión por vuestra cuenta, sólo os brindo el conocimiento necesario para tomar una decisión informada que finalmente, os ayude a poder elegir el método con el que os sintáis más cómodos.

A veces, hacer TOR -> VPN es necesario motivados por los filtros de correo no deseado que mencionados anteriormente y otras veces teniendo TOR, ya que nuestro último nodo en Internet es necesario, como cuando se accede a la red ".onion".

Depende completamente de vosotros, sé que estamos tratando de evitar el uso de Windows debido a todos los exploits que existen, entre otras muchas razones, pero si no tenemos otra forma de permanecer anónimos desde nuestra VPN, es una buena idea, hasta que tengamos algo como Tortilla, que ese anonimato, sea compatible con las distribuciones de Linux.

13. Cookies de rastreo

Un artículo reciente explica cómo la **NSA usa cosas como Google Ads** y otras cookies de rastreo para identificar a los usuarios por encima de los términos de referencia, cuando hacerlo de otra manera no es posible.

Para aquellos que no sepan de lo que estamos hablando, dejadme preguntaros esto: **¿Alguna vez habéis notado que ciertos anuncios parecen seguiros de un sitio web a otro?** Tal vez, algo que buscasteis en Google o Yahoo, ¿ahora aparece en anuncios en otras páginas?

Esto fue diseñado originalmente para comercializar cosas en función de nuestras preferencias, instalando cookies de rastreo en el navegador. Afortunadamente, TOR borra todas nuestras cookies cada vez que reiniciamos el navegador sí lo hacemos con Tails, pero eso no significa que no seamos vulnerables dentro de la misma sesión de TOR. Lo que quiero

decir con esto es: digamos que fuisteis e hicisteis un poco de lucha por la "libertad", interactuando en un foro en algún lugar, y que luego, usando la misma sesión Tor, visitasteis otro sitio web con Google Ads en él.

Google puede usar estas cookies de seguimiento para conocer nuestro comportamiento de navegación. Nuestros términos de búsqueda, nuestros sitios preferidos, etc.

Algunas personas parecen ser tan estúpidas como para usar la misma dirección IP de TOR, y luego ir a comprobar su feed de noticias de Facebook, o su correo electrónico. Adivinad ¿quién se "acuesta" con las autoridades? Google, Yahoo, Facebook, MSN, y todos nuestros proveedores de correo electrónico también. Recordad, que cuando empecéis a dejar patrones, comenzarán a buscar similitudes que empiecen con sólo una sospecha.

Tal vez asociaron las publicaciones del foro de la lucha por la libertad con nosotros, porque entramos en nuestro correo electrónico, y comienzan a notar que siempre escribimos mal las mismas palabras, cometemos los mismos errores de gramática, los mismos términos de la jerga. Tal vez visitamos un sitio web perteneciente a alguien "local" con anuncios de Google en él.

No estamos del todo seguros de cómo pueden usar estas cookies de rastreo para identificarnos, pero el caso es, que lo guardan todo. Y si hacemos algo estúpido, como buscar un restaurante local en Google, o ver qué películas se reproducen en nuestra área local, con la misma dirección IP con la que hicimos antes, algo que no deberíamos haber hecho, entonces, Google podrá juntar 2 y 2.

Una vez que están en tu camino, “estamos jodidos”. ¡Así que no les demos nada para que puedan vincularnos con algo! Preguntémonos, ¿no podemos simplemente desactivar todas las cookies?

Sí, podríamos hacerlo, pero se requieren cookies para cosas como las sesiones de inicio. Sin cookies, no podríamos mantener un estado de inicio de sesión en ciertos sitios web, ya que utilizan esa ID de cookie para identificar la sesión en el servidor. Una vez más, definitivamente podemos desactivar las cookies, pero no podremos mantener un inicio de sesión en cualquier lugar.

14. Aprendiendo de los errores de los otros: LIBERTAS, DPR, SABU y LULZSEC

Finalmente, se confirmó, que Libertas (Gary Davis), uno de los 3 moderadores detenidos de **Silk Road**, fue sido liberado bajo fianza recientemente.

El motivo por el que menciono esto, es que debemos recordar a todos los usuarios los errores cometidos por Ross y los otros tres moderadores, para poder aprender de ellos. Debemos evitar este tipo de errores, **NUNCA proporcionéis absolutamente a nadie información personal y sensible online**.

Según la historia, Ross exigió a los moderadores que le dieran copias de sus identificaciones para convertirse en moderadores de Silk Road, y probablemente guardara un registro de estos en el ordenador. Estos registros pasaron a manos del FBI como resultado, arrestaron a 3 moderadores. Y ahora, según el artículo, también persiguen a los vendedores principales.

Utiliza siempre el cifrado PGP en todas tus comunicaciones, lo que lamentablemente en este caso no hubiera importado porque Ross terminó cediendo sus llaves privadas a las autoridades. Pero sigue siendo otro obstáculo en su camino para protegerte de que te quiten tu libertad.

Nunca proporciones información personal a nadie online sobre ti. Nunca pongas tu confianza en las manos de otra persona, porque al final del día, nadie irá a la cárcel por ti.

Este mismo escenario ocurrió con Sabu de LulzSec, que fue amenazado con 112 años de prisión, se volvió rápidamente contra sus amigos y trabajó con las autoridades para encerrarlos a todos para ayudar a reducir su sentencia. Sabu tiene 2 hijos y, obviamente, decidió que preferiría sobornar a sus amigos y tener la oportunidad de ser padre en lugar de pasar el resto de su vida encerrado en la cárcel. De nuevo, nadie irá a la cárcel por ti.

15. SABU se convirtió en hermano de Jeremy, informante del FBI

El día después de Navidad, **sup_g** tuvo otra conversación online sobre el truco de **Stratfor**, sobre unos 30,000 números de tarjetas de crédito que se

habían robado de la compañía. Su interlocutor, CW-1 participó con un poco de humor negro sobre lo que podría pasar en caso de que fuesen atrapados. Pero el ataque ya había sucedido. CW-1 era "Sabu", un Hacker de Anon / LulzSec que en la vida real era un desempleado de 28 años que vivía en viviendas públicas en la ciudad de Nueva York.

Su apartamento en el sexto piso había sido visitado por el FBI en junio de 2011, y Sabu había sido arrestado y "convertido". Durante meses, había sido un informante del FBI, observado las 24 horas por un agente, utilizando un portátil del gobierno que registraba todo lo que se hacía.

Es cuando se ve que Sabu está chateando con un usuario **sup_g** sobre los ataques que habían tenido lugar.

Sabu se dirigió a sup_g con un nuevo nombre, "anarchaos". Resultó que sup_g tenía por muchos nombres, incluyendo "anarchaos", "quemar", "yohoho", "PRISIONERO DE GUERRA", "tylerknowsthis" y "amenaza creíble":

> CW-1: si me asaltan los de “anarchaos” tu trabajo es causar “havok” en mi honor
> CW-1: <3
> CW-1: sup_g:
> @sup_g: será así

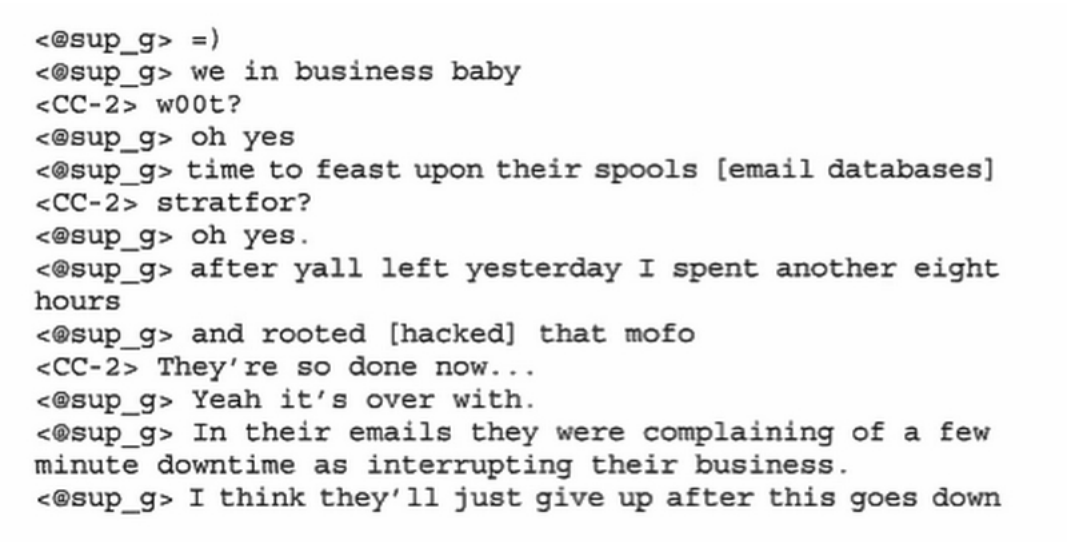
Normalmente, el intento de vincular diversos nombres, hubiese levantado las sospechas del hacker. Como le confió a Sabu, alguien más había intentado vincularle con los nombres "yohoho" y " grabar ", pero el hacker, nunca respondió... Pero este era Sabu, una especie de semidiós hacker en el mundo de **Anonymous**. Si no puedes confiar en él, ¿en quién puedes confiar? Sabu incluso había proporcionado un servidor para almacenar los datos robados de Statfor, por lo que no podría estar comprado.

Para identificar a sup_g, las autoridades primero recurrieron a los voluminosos registros de chat almacenados en el portatil de Sabu. Repasaron todos los comentarios que podrían ser plausiblemente vinculados a sup_g, o uno de sus alias. El objetivo era ver si el hacker se había descuidado en algún punto y había revelado cierta información personal.

El 29 de agosto de 2011 a las 8:37 a.m., "burn" dijo en un canal IRC que "algunos camaradas fueron arrestados en San Luis hace unas semanas ... para que funcionen las arenas bituminosas de midwestring". Los agentes del FBI en Chicago pudieron confirmar que un evento llamado Midwest Rising contó con la presencia del hermano gemelo del residente de Chicago, **Jeremy Hammond**. (Hammond tenía una historia de anarquismo y protestas violentas).

"Anarchaos" una vez indicó que había sido arrestado en 2004 por protestar en la Convención Nacional Republicana en la ciudad de Nueva York. Mucho más tarde, "yohoho" anotó que él no había estado en Nueva York "desde el RNC", uniendo los cabos a la misma persona.

El FBI fue a la policía de la ciudad de Nueva York y obtuvo una lista de cada persona detenida en la convención de 2004, supieron que Jeremy Hammond había sido detenido, aunque no había sido arrestado. Las piezas comenzaban a encajar.



```
<@sup_g> =)
<@sup_g> we in business baby
<CC-2> w00t?
<@sup_g> oh yes
<@sup_g> time to feast upon their spools [email databases]
<CC-2> stratfor?
<@sup_g> oh yes.
<@sup_g> after yall left yesterday I spent another eight
hours
<@sup_g> and rooted [hacked] that mofo
<CC-2> They're so done now...
<@sup_g> Yeah it's over with.
<@sup_g> In their emails they were complaining of a few
minute downtime as interrupting their business.
<@sup_g> I think they'll just give up after this goes down
```

"Sup_g" y "quemar" indicaron más tarde que habían pasado tiempo en prisión, con "quemaduras" que indicaban que había estado en una penitenciaría federal. Una búsqueda de los antecedentes penales de Hammond reveló que había sido arrestado en marzo de 2005 por el FBI de Chicago y se había declarado culpable de piratería informática en un "sitio web políticamente conservador y de robar su base de datos informática, incluida información de tarjetas de crédito".

Hammond fue sentenciado a dos años de prisión por dicha acción.

En otra conversación, "Anarchaos" le dijo a Sabu que una vez había pasado unas semanas en la cárcel de un condado por posesión de marihuana. También le pidió a Sabu que no le dijera a nadie, "porque podría comprometer su identidad", e indicó que estaba en libertad condicional.

Ambos coincidían con Hammond, que fue puesto en libertad condicional en noviembre de 2010 después de una violenta protesta contra los Juegos Olímpicos y la candidatura de Chicago. Cuando el FBI llevó a cabo un control

de antecedentes penales en Hammond, reveló dos arrestos por posesión de marihuana.

El FBI fue tan minucioso, que incluso dio seguimiento a un comentario de "POW" diciendo que "bucear en un basurero es bueno, soy una diosa **freegan**". El FBI fue a las autoridades de Chicago, que habían puesto a Hammond bajo vigilancia cuando lo estaban investigando en 2005. Como parte de esa vigilancia anterior, "los agentes vieron a Hammond ir a los contenedores de basura para conseguir comida".

Esta es la razón por la cual todos necesitamos ser “extra paranoicos” con cada cosa que decimos de nosotros online. He visto a personas hablar sobre el país en el que viven, algunos incluso hablan sobre en qué estado viven. Si crees que el FBI nunca juntará las piezas, es posible que estés tristemente equivocado, como descubrió Jeremy Hammond.

Monitorizar la red Wi-Fi reveló las direcciones de **Control de Acceso a Medios** (MAC) de cada dispositivo conectado a la red. La mayoría de las veces sólo había un PC Apple, y anteriormente, Hammond había dicho a Sabu que usaba un Macbook.

El 1 de marzo, los agentes obtuvieron una orden judicial que les permitía usar un dispositivo de "registro/trampa y rastreo" que podía revelar solo "información de direccionamiento" y no de contenidos. En otras palabras, si funcionaba, los agentes podían ver qué direcciones IP visitaba Hammond, pero no verían nada más.

Pronto se vio la dirección MAC de su Macbook conectándose a direcciones IP que se sabe que son parte de la red anónima de Tor.

Y aunque esto definitivamente sonaba como su hombre, la Oficina hizo todo lo posible para verificar su objetivo. La técnica principal era observar cuando Hammond salía de su casa, luego llamar a Sabu en Nueva York y preguntar si alguno de los supuestos alias de Hammond acababa de salir del IRC o del sistema de mensajería instantánea **Jabber** que utilizaban.

Si esto no os abre los ojos, para daros cuenta de algunos errores que muchos de vosotros podríais haber estado cometiendo online, entonces necesitáis reevaluar cómo actuáis online.

No lo hagáis, bajo ninguna circunstancia, nunca admitáis nada online a nadie. Nunca, en ninguna circunstancia, os atribuyáis el mérito de cualquier lucha por la libertad, o **hacktivismo** en el que hayáis participado online. Y por el amor de Dios, **¡NUNCA iniciéis sesión en un servidor, especialmente uno que guarde registros, con tu dirección IP real!**

16. ¿Dónde podrías dirigirte, si no tienes otra opción?

No soy ningún experto (ni en absoluto lo pretendo) en cómo evadir la extradición, ni cómo evadir al gobierno federal, la NSA, u otras superpotencias, ni seguramente en nada de nada, pero existen algunas recomendaciones que podrías considerar si decides que no tienes otra opción que no sea la ejecución.

Los siguientes países actualmente no tienen un tratado de extradición para los Estados Unidos: Afganistán, Argelia, Andorra, Angola, Armenia, Bahrein, Bangladesh, Bielorrusia, Bosnia y Herzegovina, Brunei, Burkina Faso, Birmania, Burundi, Camboya, Camerún, Cabo Verde, la República de África, Chad, China, Comoras, Congo (Kinshasa), Congo (Brazzaville), Djibouti, Guinea Ecuatorial, Eritrea, Etiopía, Gabón, Guinea, Guinea-Bissau, Indonesia, Costa de Marfil, Kazajstán, Kosovo, Kuwait, Laos, Líbano, Libia, Macedonia, Madagascar, Maldivas, Mali, Islas Marshall, Mauritania, Micronesia, Moldavia, Mongolia, Montenegro, Marruecos, Mozambique, Namibia, Nepal, Níger, Omán, Qatar, Rusia, Ruanda, Samoa, Santo Tomé y Príncipe, Arabia Saudita, Senegal, Serbia, Somalia, Sudán, Siria, Togo, Túnez, Uganda, Ucrania, Emiratos Árabes Unidos, Uzbekistán, Vanuatu, El Vaticano, Vietnam y Yemen.

Esto no significa que estos países no os extraditen, pero si vais a elegir un país al cual huir, sería recomendable elegir alguno de esa lista.

Un país notable en esta lista, y que es famoso por la extradición de uno de los propietarios de **Pirate Bay**, Gottfrid Svartholm a Suecia, es Camboya. Y aunque no existe tratado entre los dos países, extraditaron a Gottfrid, a petición del gobierno sueco.

Todos sabemos que **Edward Snowden** huyó a Rusia desde Hong Kong después de salir de los Estados Unidos desde Hawái, y ha permanecido allí desde entonces sin haber sido extraditado por el gobierno, se le concedió un asilo temporal.

No está claro si Snowden podrá quedarse más tiempo que sus concesiones temporales de asilo, pero a partir de ahora es más que buscado por el gobierno de los Estados Unidos, y Rusia se niega a entregarlo.

Otra persona involucrada en Pirate Bay, llamada **Fredrik Neij** huyó a Laos en Asia, tras ser declarada culpable de "ayudar a poner a disposición contenido de copyright", fue sentenciada a un año de prisión y se le ordenó pagar daños de 30 millones SEK (aproximadamente 2,740,900 €). Esto es, por supuesto, entre Laos y Suecia, pero Laos no ha extraditado a Fredrik, por lo que Laos puede sí ser una opción válida.

A menudo escuchamos a personas de los Estados Unidos afirmar que, si "la mierda se disparara", simplemente huirían a Canadá. Ni siquiera lo intentéis, ni siquiera cruzaríais la frontera.

Canadá es como el hermano pequeño de los Estados Unidos. Cuando Estados Unidos dice salta, Canadá dice "¿Cómo de alto?". Manteneos alejados de Canadá si estás leyendo esto desde los Estados Unidos.

Incluso un activista de marihuana llamado **Mark Emery**, que era ciudadano canadiense, vivía en Canadá, pero vendió semillas de marihuana por internet a personas en los EE.UU. fue extraditado para cumplir una condena de 5 años.

Según los otros vendedores de semillas en el área, aquellos que sólo vendían dentro de Canadá nunca habían sido arrestados, pero debido a que Emery lo vendió a los Estados Unidos, fue arrestado y extraditado.

Y por supuesto, también sabemos que Irlanda y Australia extraditaron a dos de los moderadores de Silk Road a los Estados Unidos.

Aunque no figura en la lista anterior, a una mujer, buscada en Estados Unidos por secuestro parental, llamada Chere Lyn Tomayko, se le concedió asilo en Costa Rica. Las autoridades de Costa Rica tomaron en cuenta las afirmaciones de Tomayko, de que sus acciones estaban justificadas por la violencia doméstica que ella sufría.

Assata Shakur fue acusada de asesinato, intento de asesinato, robo a mano armada, robo bancario y secuestro por parte de Estados Unidos y huyó a Cuba. Cuba en realidad tiene un tratado de extradición con Estados Unidos, pero las relaciones entre los dos países no han sido buenas desde la guerra fría entre los Estados Unidos y la Unión Soviética y por lo tanto las solicitudes no fueron respetadas, incluso para personas con cargos tan graves. Cuba puede ser una opción, pero nuevamente esto es sólo algo a considerar, ya que no soy ni pretendo ser, experto en esto de la ninguna manera.

17. Protege tu cuenta de la monitorización del FBI

Algunas personas en el foro Skill Roads nunca se mostraban como online, incluso cuando claramente lo estaban, y otras veces aparecían online. Nos dimos cuenta de que había una manera de nunca mostrar tu estado como online.

¿Por qué querríamos hacer esto? Por las razones de las que hemos hablado anteriormente, no deseamos dar a las fuerzas del orden público la capacidad de ver cuando iniciamos sesión o cerramos la misma.

Es una mala práctica, podemos dejar un rastro, dejar un patrón, y si eres una persona de interés y pueden conocer la hora en la que "fichas" en el foro con el momento en que salgas de tu casa, o te vayas a dormir, das más razones para sospechar y más pruebas para usar en tu contra en los tribunales. **Considerad seriamente deshabilitar la opción de mostrar vuestro estado.**

18. Mentalidad de invencibilidad, tácticas de intimidación del gobierno

Algunas personas tienen una mentalidad de invencibilidad que nunca podrá vincularse con ellas, ni derivarse de sus comunicaciones online.

¿Adivinais qué? No tienen que usar tus comunicaciones online para descubrir quiénes somos. Todo lo que tiene que pasar es que hagamos algo estúpido y te convirtamos en una persona de su interés, supervisarán nuestras actividades online de la mejor manera posible. Recordad que sólo tenemos que “meter la pata” una vez.

Por ejemplo, tal vez lleguemos a ser una persona de su interés y el FBI obtenga una citación judicial para ver nuestra cuenta de Facebook, en la que estúpidamente alardeamos ante un amigo sobre una participación en “ciertas actividades”.

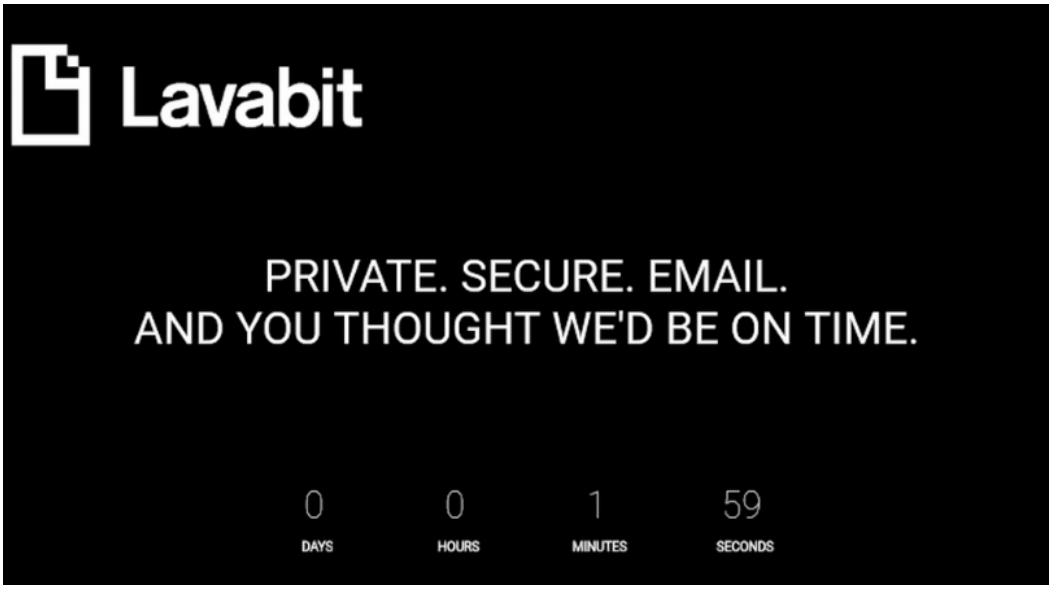
Esto es lo que le sucedió a uno de los miembros de **LulzSec,** que transfirió un archivo de datos que obtuvo a través de exploits de **inyección SQL** a un amigo suyo que usaba su propio Facebook con su verdadero nombre.

No habléis nunca de ninguna de vuestras “actividades” online en ninguna plataforma de redes sociales. Incluso si una empresa actualmente no tiene registros, una orden judicial podría usarse para obligar a una empresa a comenzar a recopilar registros de actividad.

Hush Mail se vio obligado a entregar 12 CDs de correos electrónicos de tres cuentas de Hushmail, obligado por una orden judicial, obtenida a través de un tratado de asistencia mutua entre los EE.UU. y Canadá.

Cuando se trata de ser amenazado por una orden judicial del gobierno federal, el 99.99% de todas las compañías cumplirán para evitar el enjuiciamiento, o ver su negocio cerrado.

Pero una compañía decidió hacer frente a este tipo de intimidación, llamada **LavaBit**, nadó río arriba como buen salmón, y no cedió los datos.



El servicio de correo electrónico utilizado por el informante Edward Snowden rechazó las solicitudes del FBI para evitar "mostrar su propio sistema".

El fundador de Lavabit, Ladar Levison, rechazó reiteradamente las demandas de las autoridades de entregar las claves de cifrado de su sistema, frustrando a los investigadores federales que intentaban rastrear las comunicaciones de Snowden.

Levison está ahora sujeto a una orden del gobierno, y ha apelado contra las órdenes de registro y las citaciones que exigen el acceso a su servicio. Cerró Lavabit en agosto de 2003 diciendo que no quería ser "cómplice en crímenes contra el pueblo estadounidense".

En julio de 2003, las autoridades obtuvieron una orden de búsqueda que exigía a Lavabit entregar las claves de cifrado y las claves SSL que protegían el sitio. Levison fue amenazado con desacato criminal, que podría haberlo llevado a la cárcel, si no cumplía. Tal medida habría dado al gobierno acceso a toda la información de los usuarios de Lavabit.

El tribunal ordenó que Levison fuese multado con $5,000 por día a partir del día 6 de agosto, hasta que entregase las copias electrónicas de las llaves.

Dos días más tarde, Levison entregó las llaves horas después de que cerrara la puerta de Lavabit.

¿Veis de lo que estoy hablando? El gobierno federal ordenó a este hombre que le entregara todas sus claves de cifrado y claves SSL, lo que comprometió la privacidad de 400,000 usuarios sólo para que pudieran obtener más datos sobre un hombre, Edward Snowden. Y usaron tácticas intimidatorias e intentaron llevar a la bancarrota al dueño de Lavabit, al multarlo con $5,000 por día hasta que le entregara las llaves. Levison no tuvo más remedio que entregar las llaves o perder todo.

Cualquiera que trate de enfrentarse al gobierno, especialmente en los Estados Unidos, recibirá una justicia rápida, órdenes judiciales y multas escandalosas a menos que cumplan y, además, con órdenes de mordaza para que no puedan contar a nadie la obra del gobierno.

19. ¿Cómo conectarse a la red TOR en la capa superior?

Podemos hacer una conexión **TOR -> TOR con Tails,** usando el programa llamado **Tortilla**, agregando así otra capa para que nuestros "adversarios" sufran buscándonos. Si esto vale la pena o no, depende completamente de vosotros, pero os comento esto, por si acaso pudiera ser algo que quisierais hacer.

Sin embargo, actualmente esto sólo funciona (hoy por hoy) para aquellos que usen Windows, porque fue diseñado para ser utilizado por usuarios de Windows. Tened en cuenta también, que esto ralentizará notablemente vuestra conexión, ya que está pasando por TOR dos veces.

La forma de hacerlo es muy simple en realidad. Primero debéis descargar **TOR Expert Bundle** desde la página de descargas de TOR Project, e instalarlo en el ordenador o, mejor aún, en una unidad USB.

Luego abrimos *tor.exe* y simplemente lo dejamos funcionar hasta que diga Bootstrapped 100% Listo. A continuación, ejecutamos el archivo *tortilla.exe*, asegurándonos de ejecutarlo con privilegios de administrador.

Además, si estamos ejecutando Windows Vista o posterior, es probable que obtengamos un error, indicándonos que este programa no tiene un certificado válido, porque en realidad está firmado con algo llamado "certificate" firmado por prueba. En este caso, deberemos permitir que los controladores firmados con prueba se ejecuten en el ordenador.

Para hacer esto, simplemente vamos al Menú de Inicio y escribimos en el cuadro de búsqueda "cmd". Cuando aparezca el comando, hacemos clic con el botón derecho y haz clic en ejecutar como Administrador, se abrirá un símbolo del sistema. Luego escriba el siguiente comando:

- Bcdedit.exe -set TESTSIGNING ON

Esto permitirá a Windows instalar los controladores firmados por prueba. Reiniciamos el ordenador y veremos que, en la esquina inferior derecha después de reiniciar el **Modo de Prueba de Windows**, ahora podemos ejecutar Tortilla. Lo que nos permitirá que nuestro PC se conecte a TOR.

Recordad tener tor.exe de TOR Expert Bundle abierto primero. Finalmente, abriremos Virtual Box o cualquier software de Máquina Virtual que estemos utilizando y haremos clic en Configuración, en la máquina virtual de Tails.

Haremos clic en la pestaña Red y eligiendo el menú desplegable donde dice Adjunto a: al adaptador bridge, y en el menú desplegable a continuación, denominado Nombre: Seleccionaremos el Adaptador de tortilla.

Ahora nuestra Máquina Virtual, en este caso Tails, siempre se conectará a internet a través de Tortilla, que a su vez se conectará a través de TOR. Y dado que Tails establece su propia conexión con TOR, conseguiremos ejecutar TOR por encima de TOR.

20. ¿Cómo verificar que tus archivos descargados son auténticos?

Como regla general, siempre debemos descargar los archivos de las páginas de inicio de sus respectivos desarrolladores.

La razón por la que esto es tan importante es, porque hay personas que alojan versiones modificadas de forma malintencionada de estos programas, y que alojarán sitios con apariencia legítima, para intentar que descarguen su versión, que puede instalar cosas como puertas traseras en nuestras máquinas, **keyloggers** y todo tipo de sorpresas desagradables.

A veces, los desarrolladores ofrecerán **mirrors** para sus proyectos, que son simplemente enlaces alternativos para descargar en caso de que el servidor principal sea demasiado lento o inactivo. A veces, estos espejos pueden verse comprometidos sin el conocimiento de los desarrolladores.

Tal vez no tengamos TOR o Tails en el portátil y estemos viajando fuera del país y el hotel en el que nos hospedamos tiene la página principal de TOR bloqueada. Hay momentos en que puede que necesitemos encontrar un mirror alternativo para descargar ciertas cosas.

Además, por supuesto, está el infame ataque de **Man in The Midle**, donde un atacante puede inyectar código malicioso en nuestro tráfico de red, y alterar el archivo que estemos descargando.

Los desarrolladores de TOR, incluso han informado de que algunos atacantes pueden tener la capacidad de engañar a nuestro navegador, para que pensemos que estamos visitando la página oficial de inicio de TOR, cuando en realidad no lo estamos haciendo.

Entonces, ¿qué hacemos al respecto? ¿Podemos verificar que el archivo que descargamos es el legítimo? La mejor herramienta para esto es **GnuPG**.

Podemos instalar este programa en una unidad USB, o en el ordenador real, el sistema operativo del ordenador real se conoce como host. Descargadlo, ejecutadlo, instaladlo, y os mostraremos cómo usar **GnuPG**.

Si permanecemos en la página de descarga de GnuPG veremos algo debajo del cuadro verde grande que se llama firma OpenPGP. Descargaremos eso en la misma carpeta que el archivo GnuPG, este es el archivo con el que se firmó la descarga. Básicamente la firma de alguien diciendo, hice este archivo. Y también necesitaremos la clave pública de PGP para verificar la firma.

Resumiendo, la firma se crea desde la clave privada de PGP, y se puede verificar con la clave pública de PGP. El archivo de firma se usa para verificar el programa en sí. Así que utilizaremos la clave pública de PGP para GnuPG también.

Si miramos en la misma página de descarga, debajo del título Instalación, veremos un enlace donde dice verificar la integridad del archivo.

En otras palabras, básicamente debemos promover que la clave pública de PGP que descargó está segura al firmar la clave pública de PGP con tu propia clave privada, pero en realidad no necesitamos hacer eso y por ello no lo veremos.

Tails nos explica que, si nos preocupa una clave pública PGP pueda estar comprometida, simplemente tenemos que descargar la clave de varias fuentes distintas, y compararlas, y si todas coinciden, es muy probable que estemos utilizando una clave legítima de PGP.

Ahora pasemos finalmente a TOR, porque este será un poco menos directo, pero una vez que lo hagamos, deberíamos ser capaces de averiguar cómo

verificar una app. Navega a la página de descarga de TOR y encuentra el paquete que deseas.

Para hacer las cosas un poco más simples, elegimos **Tor Browser Bundle**, debajo de la casilla de descarga veremos un enlace (sig) el cual nos mostrará la firma PGP:

```
-----BEGIN PGP SIGNATURE-----
iQIcBAABCgAGBQJa8XKtAAoJENFIP6bDwHE2er0P/REMPOIZmQE8GvSKUxLr8cMn
05p5AmEnOa/uZFYdWbXcSZpJXPneiBonRSocnMAiZoO67KUIwpd1w/QxJ4oLzR7S
uXFDpvG4uGaVU2fnnokvYfzx+4mUZZBCjLBV5FpaVfhM96Qo3UFUTpEbgsGM4HIz
xaOl/aCThfHS+UwdluoUst1sF6Ae1mIoVIqjM5qI6KpaBcQsE7LOaMBX6A08TyVN
51BczWFnZAd/dk9HB+DiK/x62EqYsC3Gl9Mjo7SjmXIny+CVAfd/L4EJhl2MT/Li
mDHeU2f9eFWbYa7i+nh5TZDqQGhAGGHtUty9dQpKvuWBv127RA09CtLqB3BCT2Ey
kx98rqV4AA17fwhVhDWSGPwSzZRQv5qJL8SrK/TDkOdifkGc2OlFVQ8hbrXKjL3q
TY+2BVBYooJSmKYbiHcxlXjds0ujuVzCE6XThP+Op9pcWlhasRhD0C7taNNBH+Ml
q99lfIWHto/y0xttgWhyhm8a/utysp7KZLaEQJXV1rKarA9jB1VMNqN05Xzb1FRK
ALFxOjQtoX1CKYetSJeb0+gHreVeCmb6L0FYl0c7BdvooqitU7Z+kBamaOJo7C/k
jHyejn2Sen0B2Ow8n46zdVFkLyGHPr2z0wa4uwqDpAYkjaQYQVSlNrJK/Oy5fEiK
+0YnruIUTTpxx72Egp+w
=mFrS
-----END PGP SIGNATURE-----
```

A continuación, necesitaremos la clave pública de PGP. Resulta que con tantos desarrolladores trabajando en TOR, hay varias claves públicas de PGP, y ciertos paquetes fueron firmados con claves diferentes a otros paquetes. Por ello, **necesitaremos encontrar la clave pública de PGP, que pertenece a nuestro paquete especifico de nuestro navegador TOR.**

Tenemos una lista de todas las claves de firma que utilizan en TOR, podemos usar estas ID de clave para obtener lo que queremos, simplemente haciendo clic derecho en el archivo de firma y haga clic en Verificar. Recibiremos una advertencia.

Mantened este número entero en mente para más adelante, se llama **huella digital**. Si comparamos los últimos 8 dígitos con la identificación de **clave de Erinn Clark (0x63FEE659)**, que se encuentra en la página anterior, y dado que es la persona que firma los paquetes del navegador Tor, veremos que coinciden. Pero queremos ser un poco más minuciosos, **nunca debemos conformarnos con la mediocridad**.

Id a la barra de tareas en Windows (si estamos en Windows) y encontrad el programa llamado **Kleopatra**, parece un círculo rojo con un pequeño cuadrado blanco. Haz clic derecho y ve a Abrir el Administrador de certificados. Vamos a importar las llaves completas usando este administrador.

También, debéis tener en cuenta que, si vamos a la pestaña que dice Otros Certificados, encontraremos las claves de Tails e Intevation (GnuPG) que utilizamos anteriormente almacenadas para el futuro cuando necesite descargar una nueva versión de esos programas y verificarlos de nuevo.

Vamos a seguir las instrucciones de la página de firmas de verificación en el sitio web de TOR Project.

Para importar claves, primero debemos agregar un directorio online donde se almacenen. Entonces, primero agreguemos el directorio online donde se almacenan las claves públicas de PGP según el sitio web de TOR. Hacemos clic en Configuración y luego en Configurar Kleopatra.

A continuación, hacemos clic en Nuevo y vamos a ingresar la siguiente URL que tomamos directamente desde la página anterior. *pool.sks-keyservers.net*, y dejemos todo lo demás como predeterminado, clic en Aceptar para finalizar.

Finalmente, hacemos clic en el botón que dice Certificados de búsqueda en el servidor y buscaremos la clave pública PGP de Errin Clark buscando su huella digital en la página web de TOR, verificando firmas, recuerde que ella es la promotora que firma el paquete del navegador Tor.

La huella digital que estamos introduciendo es **0x416F061063FEE659**, ¿os resulta familiar este número? Debería, es el número que obtuvimos la primera vez que intentamos verificar, pero sin la clave pública de PGP real, si recibes las advertencias que aparecen al hacer una búsqueda, simplemente hacemos clic en Aceptar y aparecerá la clave de Errin Clark, selecciónala y haz clic en Importar. Ahora deberíamos tener su clave en la lista de certificados importados.

Tened en cuenta que hay una advertencia, porque no se ha asignado un índice de confianza a esta persona. Esto significa que GnuPG verificó que la clave haya hecho esa firma, pero depende de vosotros decidir si esa clave realmente le pertenece al desarrollador. El mejor método sería conocer al desarrollador en persona e intercambiar las claves de huellas digital, pero eso no está al alcance de muchos creo yo, aunque nunca se sabe.

¡Parece que nuestro paquete TOR Browser es legítimo! Ahora que sabemos qué hacer cuando el archivo de clave pública de PGP no está alojado directamente en el sitio, no tenemos más excusas para no verificar nuestras descargas.

21. Verificar los mensajes firmados y firmar los mensajes propios

Como acabamos de terminar una sección sobre verificación de descargas con firmas y claves públicas, es bueno ver de forma rápida cómo verificar los mensajes utilizando las mismas dos cosas, firmas y claves públicas.

¿Por qué deberíamos preocuparnos por esto? ¿Cuál es el significado de firmar un mensaje? La razón es que, en caso de que alguien comprometa la cuenta del autor, debido, por ejemplo, a que tiene una contraseña débil o posiblemente un exploit en la codificación de un foro, entonces la persona no podría firmar los mensajes sin acceder a la clave privada del autor.

Así que veamos cómo podemos verificar este mensaje. Antes de nada, deberemos visitar la página de alguien que firme sus mensajes para coger la clave pública.

Entonces, a menos que la clave privada del autor fuera comprometida, sabemos que él mismo fue quien escribió ese mensaje. Es por esto, por lo que algunas personas deciden firmar sus mensajes. Es una manera de asegurarse de que su cuenta no se ha visto comprometida, verificando que

la persona que controla la cuenta, es la misma que tiene el control de la clave privada de PGP.

¿Quieres aprender a firmar un mensaje? Es muy fácil. Abre **gedit Text Editor** y escribe un mensaje. A continuación, selecciona el mensaje y cópialo en el portapapeles (haz clic con el botón derecho - Copiar) y luego haz clic en el icono del portapapeles, en la parte superior y selecciona Firmar/Encriptar portapapeles con claves públicas.

No elijas una clave de tu lista de claves públicas de PGP a menos que desees encriptar el mensaje. Si deseas cifrar el mensaje para enviarlo a la bandeja de entrada de alguien, o para que sólo una persona pueda verlo, selecciona su nombre y lo encriptas con tu clave pública de PGP. En este caso, sólo queremos firmar el mensaje sin encriptarlo, pero podríamos hacer ambas cosas al mismo tiempo si así lo deseamos.

Si miras hacia abajo cerca de la parte inferior, verás dónde dice Firmar mensaje como: haz clic ahí, y selecciona tu clave personal. Te pedirá tu frase de contraseña porque recuerda que está firmando el mensaje con tu clave privada.

Una vez que lo hagas correctamente, el mensaje firmado de PGP se copiará en tu portapapeles y podrás pegarlo en cualquier lugar.

¿Cuándo deberíamos firmar un mensaje? ¿Y cuándo no deberías firmar un mensaje? Gran pregunta, la mayoría de los usuarios probablemente no deberían firmar mensajes, a menos que tengan que hacerlo porque quieren tener la opción de una “negación plausible”.

Es más fácil negar la publicación de ciertas cosas, o ciertas comunicaciones que pudiésemos haber tenido con vendedores u otras personas, incluidas las fuerzas del orden público, si no firmamos nuestros mensajes, porque siempre podríamos argumentar que otra persona tuvo acceso a su cuenta.

Es más difícil hacer esto si firmamos el mensaje con nuestra clave privada de PGP.

Si estamos tratando con alguien que quiere verificar nuestra identidad y asegurarse de que nuestra firma actual coincida con la clave pública que tenían archivada desde hace 6 meses, tal vez podrían hacer que les envíes un mensaje firmado.

Sin embargo, todo lo que necesitan hacer es, enviarte un mensaje encriptado con tu clave pública de PGP, que tenían archivada, y si no podemos descifrarlo, ellos no son quienes dicen ser.

En la aplicación del mundo real, los desarrolladores pueden usar mensajes firmados de PGP en anuncios, o quizás nuevos lanzamientos de sus

programas, que proporcionen una URL de descarga, para que los usuarios puedan estar seguros de que el desarrollador es quien publica la URL, y no un atacante malintencionado que haya comprometido la cuenta del foro del desarrollador.

Para un usuario promedio, no hay muchas veces en que debería estar firmando mensajes, pero es una opción válida, y muy aconsejable, ahora que ya sabéis cómo hacerlo.

22. Un ejemplo realmente malo de OpSec: Smarten Up

¡Rastréame si puedes!

Es increíble todo lo que se puede ver en **Netflix**. Esto no es algo realmente nuevo, ya se hizo en 2010, pero es bastante minucioso en su demostración de cómo desaparecer en la cultura moderna de EE.UU.

Debo añadir que parte de la tecnología que se presentó desde el otro lado es bastante alarmante.

Entonces, ¿por qué es esto tan revelador? ¿Por qué es tan malo que para estar preguntándonoslo? Netflix recopila metadatos de sus usuarios, al igual que cualquier otra corporación de big data. Si eres un usuario de Netflix, es probable que tengas un perfil que haga un seguimiento de cada película que hayas visto y lo que hayas calificado, y así sucesivamente.

¿Pero tal vez estaba usando una VPN para conectarte a Netflix? Estupendo… ¿Usas esa VPN para cualquier otra cosa? Para iniciar sesión en tu correo electrónico, navegando por la web, etc. Incluso si usaste una VPN, puede que quizás conserven los registros.

Estamos hablando de actividades poco seguras en ciberseguridad. Esto viene dado por un caso en el que un vendedor de droga, indicó en el foro de Skill Road, que anoche estuvo viendo una película de Netflix. Si a esto le sumamos que, en otro momento, también indicó en qué país vive, las drogas que importó a su país, y desde qué países lo había hecho.

Además, también habló sobre cocinar drogas, y comentó algo de estar en una zona fría de su país, cuando, no todas las partes de ese país en particular se enfrían. Esto sin duda alguna, servirá a las fuerzas del orden a reducir la lista de sospechosos que obtuvieron de Netflix.

¡Mantened SIEMPRE la boca cerrada sobre vuestra vida personal en las actividades online!

23. TOR Chat

Esto significa que, cosas como Gmail, Hotmail, Yahoo Mail, Mensajes de Skype, Mensajes Instantáneos/Privados de Facebook, Mensajes de texto, y otras formas de comunicación probablemente estén siendo monitorizadas hasta cierto punto, al menos registrando los metadatos.

Siempre debemos tratar todo como si aquellos que nos están monitorizando también pudieran leer el contenido del correo electrónico.

Hemos hablado sobre la comunicación con PGP, hemos hablado sobre el uso de TOR y los Hidden Services, y hemos hablado sobre las buenas prácticas de OpSec. Pero, ¿qué pasa si algunos de nosotros queremos poder enviar un mensaje instantáneo a otra persona? La buena noticia es que podemos hacerlo con algo llamado **Tor Chat.**

TorChat es un mensajero instantáneo anónimo y descentralizado que utiliza los servicios ocultos de Tor como red subyacente, en otras palabras, se comunica a través del protocolo de la red Tor ".onion".

Esto proporciona una encriptación de extremo a extremo. Ofrece mensajes de texto criptográficamente seguros, y transferencias de archivos, para negocios y comunicaciones confidenciales, entre dos personas.

La mejor noticia es que podemos usar TorChat en **Windows, Linux, Mac** y smartphones. Podemos obtener TorChat para el iPhone en la **Apple Store**, también podemos obtener TorChat en **Android Market**, así que incluso

podemos usarlo como un medio para enviar mensajes de texto a alguien más que también tenga TorChat.

En TorChat, cada usuario tiene una identificación alfanumérica única que consta de 16 caracteres. Esta identificación será creada aleatoriamente por Tor cuando el cliente se inicia por primera vez, básicamente es la dirección ".onion" de un servicio oculto. Los clientes de TorChat se comunican entre sí utilizando Tor para ponerse en contacto con el servicio oculto del otro.

Por ejemplo, la primera vez que abras TorChat, el ordenador podría generar d0dj309jfj94jfgf ".onion" y de aquí en adelante, d0dj309jfj94jfgf será tu ID de TorChat que darás a las personas que deseas enviar mensajes.

En este momento, hay personas que debaten si TorChat es completamente seguro, y yo diría que TorChat es tan seguro como Tor, sólo asegúrate de practicar las mismas buenas prácticas a las que estás acostumbrado. No proporciones nunca información personal, si estás enviando información confidencial, usa cifrado PGP.

La seguridad de Torchat es desconocida. No se ha sometido a una auditoría de seguridad adecuada, profesional o de otro tipo, que se sepa. Crea un servicio oculto en el ordenador que lo deja vulnerable a los ataques de *"desanonimación"* que se aplican a todos los servicios ocultos. También parece ser un protocolo muy básico que se parece a **netcat** sobre Tor.

No hay forma de rechazar una transferencia de archivos. Se Inicia automáticamente la transferencia y escribe el archivo en /tmp, que es un tmpfs montado en la RAM en Linux. En teoría, un atacante podría transferir /dev/urandom hasta que llene su RAM y bloquee el ordenador.

Esto sería ideal para inducir ataques de intersección. Aunque no estamos seguros si el kernel que está administrando el sistema, podría detener la transferencia cuando se quede sin RAM.

Otra cosa mala que tiene es, que una vez que alguien aprende tu ID de Torchat, no hay manera de evitar que sepan que estás online, incluso si los eliminas de tu lista de amigos.

La razón es porque tu instancia de Torchat es un servicio oculto que publica un descriptor de servicio oculto que cualquiera puede descargar. No hay forma de deshabilitarlo, por lo menos hasta donde yo sé (que tampoco es tanto).

Si deseamos cortar el contacto con alguien, deberemos obtener un nuevo ID de Torchat. Por lo tanto, debemos ser muy, muy conservadores sobre la distribución del ID Torchat.

Esto es algo que sólo deberíamos entregar (yo no lo haría) a contactos de la mayor confianza, pero como ya he dicho es algo que yo NO recomiendo y que, desde luego, yo NO haría.

24. Obtención, envío y recepción de Bitcoins de forma anónima

¿Cuál es la mejor manera de obtener BTCs? ¿Cómo puedo proteger mi identidad? Hemos hablado sobre una gran cantidad de formas de mantener nuestra seguridad, pero realmente no hemos hablado sobre cómo cambiar divisas. Lo primero que quiero decir es que no defendemos hacer cosas ilegales.

Esto es sólo para fines educativos y nuestras recomendaciones se realizan suponiendo que está intercambiando monedas de forma anónima como un medio para proteger la propia privacidad.

¿Has encontrado algo online que deseas comprar, y nos piden Bitcoins como forma de pago? ¿Cómo obtienes los Bitcoins y cómo los trasfieres? Vamos a explorar estas opciones hasta cierto punto, esperando que pueda tomar una decisión informada sobre qué método es mejor para cada situación.

Las opciones que tenemos para comprar Bitcoins son las siguientes:

1. **Registrarse en un intercambio online.** Webs populares son **MT Gox**, **BitStamp** y **Coinbase**. La desventaja de comprar Bitcoins en estos intercambios, es que necesitamos verificar nuestra identidad con ellos mediante el envío de documentos (Licencia de conducir o pasaporte y una factura de servicios públicos).

   Si podemos superar este primer obstáculo, debemos encontrar la manera de ingresar dinero en la cuenta. En general, los intercambios solo aceptan transferencias bancarias como forma de financiar nuestra cuenta, pero algunos de ellos ofrecen una forma de transferir dinero directamente desde nuestra cuenta bancaria.

   Obviamente, podemos ver que al hacerlo estamos exponiendo nuestra verdadera identidad a los intercambios de una forma u otra, y si no, al menos nuestra ubicación.

2. **LocalBitcoins**. LocalBitcoins nos ofrece una forma de encontrar una persona en nuestra área local, o si deseamos ir a otro país o provincia para encontrarnos con alguien más lejos, podemos elegir dónde

buscar personas en esa área que venden Bitcoins, ya sea online (transferencia bancaria o depósito en efectivo) o encuentros en efectivo y en persona.

Los comerciantes tienen listas de reputación, similares a una puntuación de comentarios en eBay, pudiendo encontrar un comerciante que tenga una buena reputación para comprar. Enviamos una solicitud comercial y una vez que el vendedor ha recibido el dinero, podemos liberar los Bitcoins de LocalBitcoins, enviándoselos a su billetera.

Algunas personas han expresado su preocupación de que la policía pueda actuar como compradores y vendedores en LocalBitCoins, pero no importa, siempre y cuando no deseemos comprar grandes cantidades. También podemos, si lo deseamos, comunicarnos con el comprador por correo electrónico, llegar desde el transporte público, usar sombrero y todo tipo de trucos de agente secreto para tratar de ocultar nuestra identidad. Usa una peluca si eres extremadamente súper paranoico.

3. **Usa un cajero automático de Bitcoin.** Hoy escasean los cajeros automáticos en el mundo. Afortunadamente, las compañías están lanzando estos cajeros automáticos de forma progresiva. Es probable que haya algún método para tratar de reducir el lavado de dinero haciendo que verifiques tu identificación, pero por lo que entiendo, actualmente solo lo hacen si estás vendiendo Bitcoins por dinero en efectivo usando el cajero automático, y no si los compras por dinero en efectivo.

   El funcionamiento de esto es, que eliges la cantidad de BTCs que deseas comprar y alimentas con efectivo el cajero automático. En ese momento puedes imprimir una billetera de papel generada o elegir una billetera propia para enviar las Bitcoins. Este método puede ser otra buena forma porque requiere tratar con otro ser humano fuera de la transacción.

   Algo de lo que debemos estar al tanto, son las cámaras de vigilancia, así que tal vez sería aconsejable usar capucha, sombrero, peluca, lentes de sol, etc. para disfrazarnos si estamos preocupados por nuestra identidad.

4. **Craigslist**. Lo creas o no, hay una cantidad decente de personas en Craigslist con la que puedes comprar bitcoins “face to face” con dinero en efectivo. Es posible que en tu área local no tengas una gran cantidad disponible, pero siempre puedes buscar en otras áreas metropolitanas cercanas y hacer una excursión diaria si lo deseas. Las

mismas consideraciones sobre la protección de nuestra identidad se aplicarian aquí. (Podemos encontrar de igual forma en sitios como Milanuncios, MercadoLibre, Ebay).

5. **Mina tus propios Bitcoins**. No voy a entrar en cómo extraer Bitcoins, o si deberías o no, pero si quieres obtener Bitcoins sin tratar con otras personas, esta es una de las formas en que puedes hacerlo. Ejecuta a tus mineros sobre Tor, mantente en el anonimato y tendrás algunos Bitcoins sin "contaminar".

Ahora que tenemos algunos Bitcoins, ¿cómo podemos traspasarlos a otra persona con la que queremos comprar algo o comerciar con él? Como probablemente ya sepa, cada transacción se registra en **BlockChain.info**. Podemos consultar las transacciones relacionadas con cada wallet, yendo a la siguiente dirección: http:// blockchain.info /address/**Dirección del wallet**.

Si tienes bitcoins en tu billetera, y se los envías a otra persona, aparecerán en Blockchain, indicando exactamente donde los enviaste. Por esto, un par de cosas a tener en cuenta:

1. Si has comprado con tus Bitcoins a alguien o algo ilícito, es posible que hayan guardado un registro de la billetera a la que se enviaron las monedas.

2. Si un agente del orden público o alguien que intente rastrearnos, podría ver dónde se envían los BTCs tras ser enviados a otra persona.

En este momento, el mejor método para tratar de perder el rastro, es usar algo que se llama mezclador o mixer. Es más, o menos como tirar tus Bitcoins en una pila gigante de monedas con otros usuarios y luego retirarlas en un momento posterior de la mezcladora. Si lanzaste 1 bitcoin y sacaste 1 bitcoin, piensa en todas las otras personas que hicieron exactamente lo mismo.

Posiblemente miles de personas retiren 1 Bitcoin del mismo montón de monedas. Ahora nos hemos vuelto mucho más difíciles de rastrear y ser vinculados con esos BTCs. Tal vez no retiremos 1 Bitcoin, tal vez solo retiremos 0.5 Bitcoins ahora mismo y dejemos los otros 0.5.

Bitcoin en el mezclador. Esto, hara mucho más difícil vincular dichos Bitcoins con nosotros. Un sitio web que hace esto se llama **Coinmixer**.

Coinmixer ha existido desde hace un tiempo y la mayoría de la gente parece estar contenta con el servicio que brindan. La forma en que trabajan es como mencioné anteriormente, y además de eso, el servicio cobra una comisión de 1% - 3% en cada depósito. Así que podemos poner 1.0 Bitcoins

y sacar 0.97 Bitcoins después de las tarifas y mexclarlo. También podmeos decidir cuándo deseamos retirarlo, ya sea en un mes, una semana, días, etc.

Este es un buen servicio para usar. Lo único que debemos tener en cuenta es que hay un rastro nuestro enviando monedas a Coinmixer, y algunas personas pueden sospechar o no de nuestras intenciones. Pero lo que hagamos con nuestras monedas después de Coinmixer será extremadamente difícil de rastrear, si no es casi imposible, debido a la gran cantidad de transacciones que se producen dentro y fuera de Coinmixer.

Cuando retiremos nuestras monedas de Coinmixer, asegúrate de enviarlas a una nueva billetera, y no a la misma billetera que utilizamos para depositarlas en Coinmixer. Otra opción que podemos tener al retirar las monedas de Coinmixer, es conseguir que Coinmixer retire las monedas directamente a la persona de la que deseamos comprar algo. Simplemente ten en cuenta las tarifas de transacción para asegurarnos de que nuestro vendedor deseado reciba la cantidad correcta de Bitcoins necesaria para la compra o el intercambio.

Blockchain.info proporciona otras dos opciones que podemos utilizar, crear una billetera e iniciándose sesión en ella y enviar monedas compartidas. Enviar monedas compartida es otra forma de mezclar monedas, la forma en la que funciona es que envía el dinero a un bote gigante y se empareja con otra persona que está enviando la misma cantidad.

Un ejemplo de esto es: Tenemos 4 personas. A, B y X, Y. La persona A está enviando 1 Bitcoin a la persona B, y la persona X está enviando 1 Bitcoin a la persona Y. El envío compartido (Send Shared) hará coincidir estas cantidades, y las mezclará para que la persona A envíe sus 1 Bitcoin a la persona Y y la persona X envíe su Bitcoin a la persona B. De esta manera estás rompiendo la cadena que vincula a la persona A con la persona B, porque no hay registro de que la persona A haya enviado algo a la persona B.

Esto es una muy buena opción para usar, y muchas personas lo prefieren. Por supuesto, hay muchas personas que usan Send Shared, por lo que la probabilidad de que nos rastreen, es prácticamente imposible.

La moneda compartida usa un método diferente llamado coinjoin. Shared coin aloja un servidor **coinjoin** que actúa como un punto de encuentro para que varias personas se unan en una sola transacción.

Tener varias personas en una transacción mejora la privacidad al hacer las transacciones más difíciles de analizar. La distinción importante entre los servicios de mezcla tradicionales es, que el servidor no puede confiscar, ni robar tus monedas.

Como podemos ver, múltiples entradas y salidas hacen que la determinación del emisor y receptor real sea mucho más difícil. Básicamente enviamos las monedas dentro y fuera de muchas carteras diferentes que están participando en la opción "moneda compartida" en ese momento, lanzando cientos o miles de transacciones en todas las carteras que participan por lo que es extremadamente difícil de seguir.

El inconveniente es que coinjoin nunca puede cortar por completo el vínculo entre la entrada y la dirección de destino, siempre habrá una conexión entre ellos, **es simplemente más difícil de analizar**.

El beneficio de Shared Coin es que, mientras se realiza este procesamiento, podemos presionar cancelar y recuperar nuestras monedas. Cuando enviamos nuestras monedas a un servicio de mezcla tradicional, un servicio de mezcla poco confiable, nos podrían robar las mismas.

Ahora que tenemos el conocimiento para tomar una decisión informada sobre cómo mezclar nuestras monedas en el camino hacia nuestro destino está más claro.

25. Clearnet vs Hidden Services: ¿Por qué debemos tener cuidado?

Como probablemente ya sepamos, un Hidden Service es un sitio web que utiliza una dirección ".onion", y un sitio clearnet usa internet regular. Debemos estar en TOR para acceder a la red de tor, mientras que se puede acceder a los sitios de clearnet desde cualquier navegador. ¿Por qué debes tener cuidado cuando visites los sitios de clearnet?

Cuando veamos un artículo, enlace o vídeo publicado en los foros de la DarkNet, debemos tener en cuenta que **sólo debemos ver esos vídeos a través de TOR**, o posiblemente como último recurso, usar una VPN, y aquí está el por qué.

Usemos YouTube, por ejemplo. YouTube es propiedad de Google, Google rastrea todo. YouTube realiza un seguimiento de qué direcciones IP buscan qué videos y almacenan toneladas de metadatos sobre sus usuarios.

Cuando se publica un enlace a un video de YouTube en los foros DarkNet, es probable que tengamos que usar nuestros navegadores habituales para mirarlo, porque el navegador Tor no es bueno para ver videos en flash. Pero el problema es que, si se escribió una publicación en un foro DarkNet el 10

de mayo de 2018 recomendando un vídeo, y este vídeo sólo tiene 500 visitas, tal vez este video haya estado en marcha durante unos meses, y no haya terminado siendo muy popular.

En los pocos días que se publicó este artículo, sólo 50 personas vieron el foro de la DarkNet donde esta ese vídeo. El número de visitas simplemente subió en un corto período de tiempo.

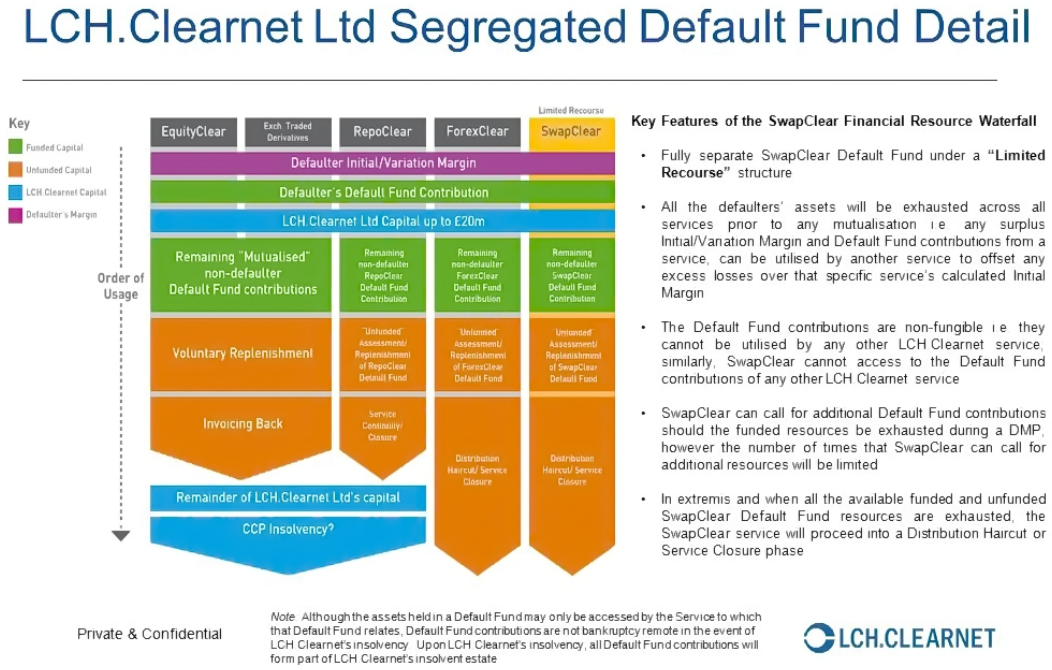
Es extremadamente fácil averiguar las personas que vieron ese vídeo de YouTube, especialmente porque no es un vídeo popular, y que vinieron de la DarkNet, y si cometimos el error de usar nuestra dirección IP real, nos habremos agregado a una lista de personas de "interés" automáticamente. Si lo hacemos varias veces con diferentes videos de YouTube, entonces comenzamos a generar un patrón y, antes de que nos demos cuenta, tendremos a las autoridades monitorizándonos.

Si usamos una VPN, esto se hace un poco más difícil, ya que no podrán vincularnos con el video. Pero una vez que vean una dirección VPN que aparece constantemente en los videos que se vinculan desde los foros DarkNet, las autoridades enviarán una orden judicial para supervisar las actividades de los usuarios de la VPN.

HideMyAss fue uno de los ejemplos más conocidos de VPN que recibieron la orden de entregar información sobre sus usuarios, y lo hicieron sin problemas.

Pues, lo mismo ocurre con todos los sitios clearnet. Nunca se sabe quién está monitorizando nuestra actividad. Cuando alguien publica un enlace de clearnet en los foros y las personas visitan ese enlace usando una dirección IP desprotegida, se puede comenzar a correlacionar patrones en nuestra contra.

Entonces, ¿qué puedes hacer para protegerte? Pregúntate primero, ¿realmente necesito ver ese video de YouTube? ¿Es algo importante que necesito ver? Si es así, podríamos considerar la opción de la que hablé anteriormente llamada **Tortilla**.



Hay un caso infame de un asesino que llamó a la hermana de su víctima desde el teléfono celular de la víctima. Llamó desde **Times Square** en Nueva York y la insultó, y habló sobre cómo estaba torturando a su hermana, la policía rastreo el teléfono.Pero, debido a que Times Square es un lugar muy concurrido, incluso con todas las cámaras "buscándolo", no pudieron precisar exactamente qué persona estaba haciendo la llamada desde ese teléfono, y nunca atraparon al tipo.

Terminó abandonando el teléfono después de que, finalmente mató a su víctima. Se sabían que era un tipo caminando por Times Square con un teléfono celular, pero si alguna vez has estado en Times Square, sabes que hay millones de personas haciendo exactamente lo mismo, él simplemente se mezcló.

Es posible que deseemos utilizar una Wi-Fi pública en un área concurrida que tenga muchos usuarios durante todo el día para ver un vídeo y mantener nuestra dirección IP segura. Si no podemos mirar videos de forma segura sin identificarnos, entonces no los veáis. Es tan simple como esto. Sí, ya sé que es molesto que en Tor no funcione bien los videos flash, pero esto siempre es mejor que delatarnos.

Esta parte se escribe para recordar que, la vinculación de dos usuarios en Internet es mucho más fácil de lo que se cree. Una vez que comiencen a desarrollar patrones y a dejar huellas, el gobierno tiene un espacio de almacenamiento ilimitado disponible para realizar un seguimiento de todo lo que haces (no tiene limitaciones de SIEM).

¿Recordáis cómo capturaron a Sabu? Inició sesión en un IRC con su dirección IP real, **una vez**. Una sola vez, es todo lo que necesitan para derrotarte. **Siempre piensa antes de abrir un enlace, ¿qué información guardará este sitio web acerca sobre mí?**

26. Te están observando - Virus, malware, vulnerabilidades

Nuestro ordenador siempre será vulnerable a algún tipo de ataque por parte de aquellos que quieren hacernos daño de alguna forma. Si se trata de dañar tu privacidad, robar tu información, o llevarte a la cárcel, si has infringido la ley.

No debería sorprendernos que el gobierno de EE.UU. sea en realidad el mayor comprador de malware.

Según un nuevo informe, el gobierno de los Estados Unidos es, de hecho, el mayor comprador de malware del mundo gracias al cambio hacia la ciberseguridad "ofensiva" y nos está dejando a todos vulnerables en el proceso.

Para que el gobierno pueda explotar las vulnerabilidades descubiertas en el software principal, no puede revelar esas vulnerabilidades a los fabricantes o al público, para que no se solucione el problema.

“Mi trabajo consistía en tener 25 días-cero en una memoria USB, listas para funcionar”. Esto fue lo que dijo a Reuters un ex ejecutivo de un contratista de defensa. El contratista de defensa compraba las vulnerabilidades de los

Hackers independientes y las convertía en un exploit, para que el gobierno las utilizase como arma cibernética ofensiva.

Después de revisar las fuentes y artículos, algunos de estos contratistas de defensa expresaron su preocupación de que el gobierno esencialmente estaba financiando actividades delictivas. Están pagando hackers independientes, en algunos casos **blackhats** para encontrar **exploits de día cero** y comprar estos exploits por grandes sumas de dinero, más de 100.000 euros.

Si está usando un portátil con micrófono y cámara incorporada, es extremadamente vulnerable a un ataque como explica **John McAffee**, el hombre que inició McAfee Antivirus.

Exactamente dijo en una charla: **"Si necesito información sobre ti, te prometo que, dentro de tres días, puedo encender la cámara del ordenador de tu casa y ver lo que esté haciendo".**

Entonces, lo primero que debemos hacer es poner una pegatina opaca o una pegatina especial para tapar la webcam. Si estás en un escritorio y tienes una cámara web conectada, desenchúfela a menos que la estemos utilizando. No hay razón para darle a un atacante una ventana abierta a nuestro hogar.

El siguiente es su micrófono, nuevamente los equipos de escritorio generalmente no tienen micrófonos incorporados, pero la mayoría de las portátiles sí. Se puede activar un micrófono para escucharte hablando y por ello, necesita encontrar una forma de desactivarlo físicamente. La mejor forma, por supuesto, es eliminarlo físicamente. (En modo paranoia).

El **FBI** desarrolló un software de registro de teclas llamado **Magic Lantern**. Según los informes, Magic Lantern se puede instalar de forma remota, a través de un archivo adjunto de correo electrónico o mediante la explotación de vulnerabilidades comunes del sistema operativo, a diferencia de los Keyloggers anteriores utilizados por el FBI. Se han descrito de diversas maneras, como un virus y un Troyano. No se sabe cómo el programa podía almacenar o comunicar las pulsaciones de las teclas.

El FBI tenía la intención de desplegar Magic Lantern en forma de un archivo adjunto de correo electrónico. Cuando se abriese el archivo adjunto, se instala un Troyano en el ordenador del sospechoso.

El Troyano se activa cuando el sospechoso utiliza el cifrado PGP, que a menudo se utiliza para aumentar la seguridad de los mensajes de correo electrónico enviados. Cuando se activa, el troyano registrará la contraseña de PGP, que permitirá al FBI descifrar las comunicaciones del usuario.

Portavoces del FBI confirmaron la existencia del programa llamado Magic Lantern, pero negaron que se hubiera desplegado, y se negaron a comentar más.

Por supuesto, también tenemos smartphones que se pueden activar de forma remota. Los smartphones se pueden activar de forma remota, sin necesidad de acceso físico. Esta característica de "**error itinerante**" ha sido utilizada por las agencias de aplicación de la ley y los servicios de inteligencia para escuchar conversaciones cercanas.

Según algunas de las fuentes del artículo de la Wikipedia, el smartphone se puede activar para escucharte, incluso cuando está apagado. Sacar la batería probablemente lo inhabilitará, pero no hay garantías. Así que asegúrate de que el teléfono no esté en la misma habitación que tu si estamos hablando de algo delicado. En el documental **Snowden** se ve como él mismo, mete los teléfonos en un microondas.

Como siempre, sé “súper paranoico”. Enciende la ducha, y pon el teléfono en el baño si es necesario, o mejor aún, si vas a ir a algún lugar y no necesitas el teléfono, déjalo en casa. Como la mayoría de las personas nunca salen de su casa sin sus teléfonos, si alguien nos está observando, podría pensar que todavía estamos en su casa.

Al primer grupo de personas que fue a visitar a Snowden en Rusia se les dijo que no trajeran ningún portátil o teléfono con ellos por estas razones.

Sabemos que el gobierno está tratando activamente de obtener acceso remoto a tu ordenador, pueden escuchar tus teléfonos, ¿qué debemos hacer al respecto?

Debemos hacer todo lo posible para asegurarnos de que los ordenadores que usamos no estén expuestas a los elementos de riesgo. Siempre deshabilite JavaScript cuando visite cualquier sitio web a menos que el sitio web sea 100% fiable.

Comienza a eliminar gradualmente el uso de Microsoft Windows y MAC OSX porque estos sistemas operativos de código cerrado no están abiertos al escrutinio y auditan la forma en que se encuentran las distribuciones de código abierto de Linux. Hay más usuarios de Windows y, por lo tanto, más exploits disponibles para Windows.

Ejecuta tu sistema operativo en una máquina virtual, incluso si tu sistema operativo anfitrión es Linux (recuerde que Virtual Box puede funcionar en Linux) ayudará a reducir la retención de cualquier malware que pueda detectar cuando estamos en Internet. No vayas a ningún sitio potencialmente dañino en tu libertad.

No abras ningún correo electrónico de ninguna persona en la que no confíes al 100%. Formatea regularmente tus discos duros para mantenerlos limpios de cualquier virus oculto.

Si no estás seguro de si algo es seguro o no, pruébalo en un ordenador que sólo esté diseñado para pruebas, y en otro que no esté conectado a Internet.

Si puedes reiniciar tu sector de arranque de tu disco duro de vez en cuando, sería una buena idea también, ya que existen virus maestros del sector de arranque, que reiniciarían un virus antes de que el ordenador arranque en el sistema operativo.

Controla tu BIOS, la **BIOS** es lo primero que se ejecuta al encender tu ordenador, si tienes un virus en tu BIOS, no hay un antivirus que pueda eliminarlo, necesitarías flashear tu BIOS e instalar un nuevo firmware. Asegúrese de que el firmware sea 100% confiable ya que el firmware infectado es la forma más común de obtener un virus BIOS.

27. Monitoriza con una antena

En la red hay montones de vídeos que muestran cómo usar una antena, sentado en una camioneta, fuera de nuestro hogar (ejemplo arquetípico de película policiaca) para realizar todo tipo de “escuchas más o menos ocultas”.

De hecho, muchas personas especulan con que los nuevos medidores inteligentes, instalados en muchos hogares, ya cuentan con esta tecnología para determinar electrónicamente todo lo que estás haciendo en tu hogar. Los teclados con cable e inalámbricos emiten ondas electromagnéticas, ya que contienen componentes electrónicos.

Esta radiación electromagnética podría revelar información sensible, como las pulsaciones de teclas, como se muestra en el video. Cada onda electromagnética es exclusiva del dispositivo que las usa, lo que da a una persona que le espía la capacidad de diferenciar entre el ordenador en comparación con el lavavajillas.

De acuerdo con personas que han hecho estas pruebas, se puede extender el alcance hasta 20 metros, utilizando tecnología relativamente barata en el caso de los teclados cableados, para teclados y ratones inalámbricos es mucho más fácil.

Lo que nos lleva a otra área de interés, las transmisiones inalámbricas. Cosas como los teclados inalámbricos y los ratones inalámbricos, son también vulnerables a las "escuchas".

Si no usamos una encriptación lo suficientemente fuerte como para enviar datos al receptor, cualquiera puede estar escuchando las teclas presionadas y la actividad del mouse. Probablemente, algo en lo que la mayoría de la gente nunca pensaría.

Microsoft ha actualizado el cifrado débil que se encuentra en los teclados inalámbricos de mercado masivo de hoy con un nuevo diseño que usa **AES de 128 bits** para asegurar la comunicación desde y hacia el PC.

Hasta ahora, el cifrado del teclado ha sido débil, con claves elegidas de una pequeña paleta de posibilidades. Un grupo de Hackers afirmó en 2009 que había desarrollado una herramienta específica para capturar las pulsaciones de teclado de Microsoft en un rango de hasta 10 metros.

¿Estás usando tecnología inalámbrica? Puede ser el momento de actualizar tu equipo. 10 metros es poco, pero recuerda que la tecnología utilizada por el gobierno podría potencialmente ir más allá, y con toda seguridad irá muchísimo más lejos.

Luego, hay otras cosas que la gente olvida, como los monitores inalámbricos que transmiten tu pantalla a un receptor que puede recogerlo (todos hemos visto cómo podemos duplicar la pantalla de nuestro smartphone en la TV de forma inalámbrica).

Pensad en las viejas antenas que la gente solía tener en la parte superior de sus casas, y cómo desde lejos podían capturar las señales de las estaciones de televisión, si tenías una de esas apuntándote desde una camioneta al otro lado de la calle, no hay duda de que podrían estar escuchando a escondidas tus actividades íntimas.

Un investigador pudo usar una señal inalámbrica enviada por un medidor inteligente hasta a 300 metros de distancia, para averiguar de qué casa provenía y cuál era el consumo de energía actual en texto sin formato. Luego, pudo usar esta información para determinar cuándo las personas estaban y no estaban en el hogar debido al aumento promedio del consumo ya que los medidores emiten pulsos cada 30 segundos.

Los datos enviados eran en texto plano, y llevaban el número de identificación del medidor y su lectura. El nombre del propietario de la casa o la dirección no están incluidos, pero cualquier persona suficientemente motivada podría averiguar rápidamente la fuente.

La identificación del medidor estaba impresa en la parte frontal del mismo, por lo que teóricamente podríamos leer el ID, desactivarla, e intentar capturar paquetes.

En sus pruebas, **Xu** descubrió que podía sacar paquetes del aire de los medidores meta entre una vez cada dos.

Tan solo 10 minutos. Eso es suficientemente rápido como para poder calcular el consumo de energía promedio de una casa y notar que comienza a deducirse cuando alguien está en casa.

Cosas como temporizadores, valdría la pena invertir para que siempre parezca que alguien está en casa hasta que los investigadores de seguridad comiencen a buscar formas de evitar la puerta abierta que estamos dando a cualquiera que quiera encontrar datos sobre nosotros.

¿Qué podemos hacer con este tipo de escuchas? No mucho, a menos que quieras comenzar a convertirte en un tipo de persona con sombrero de hojalata. Sin embargo, hay algunas cosas divertidas que puedes hacer si quieres volverte loco.

Y-Shield - Pintura protectora de alta frecuencia YShield. Pintura de base acuosa fácil de aplicar para paredes, techos, puertas y otras superficies interiores o exteriores. Muy efectivo para bloquear señales de teléfonos, señales de CB, TV, AM, FM, radiación de radiofrecuencia y microondas. ¡Probado altamente efectivo hasta 18 GHz!

También hay muchas otras cosas como cortinas, prendas de vestir, telas, etc. que interrumpen la transmisión de señales. Depende completamente de nosotros lo que deseamos hacer, solo damos las opciones y la educación para que podamos tomar una decisión educada sobre cómo de lejos deseamos ir para proteger nuestra privacidad.

28. Cookies y JavaScript, más cookies de Flash y otros seguimientos del navegador

Tu navegador puede revelar una cantidad alarmante de información sobre ti. Sorprendentemente, o no demasiado sorprendente, cuando visitamos un sitio web hay una cantidad enorme de datos de identificación que se envían al sitio web con el que se nos estamos comunicando.

29. Cookies

Las cookies son piezas de información que un sitio web puede enviar a tu navegador. Si tu navegador los "acepta", serán enviadas de regreso al sitio cada vez que el navegador acepte una página, imagen o script del mismo. Una cookie establecida por la página/sitio que está visitando es una cookie de "segunda parte".

Una cookie establecida por otro sitio que sólo proporciona una imagen o secuencia de comandos (un anunciante, por ejemplo), se denomina cookie de "terceros".

Las cookies son los mecanismos más comunes utilizados para registrar el hecho de que un visitante en particular ha ingresado a una cuenta de un sitio, y para rastrear el estado de una transacción de varios pasos, como una reserva o carrito de compras. Como resultado, no es posible bloquear todas las cookies sin perder la capacidad de iniciar sesión en muchos sitios y realizar transacciones en otros.

Las cookies también se usan para otros fines que afectan menos a los intereses de los usuarios, como registrar el uso de un sitio durante un largo período de tiempo o incluso rastrear y correlacionar sus visitas a muchos sitios separados, a través de cookies asociadas a anuncios publicitarios, por ejemplo.

Con los navegadores recientes, la configuración de cookies que ofrece a los usuarios la compensación más pragmática entre la funcionalidad dependiente de cookies y la privacidad es permitir que las cookies permanezcan hasta que el usuario cierre el navegador, también conocido como "cookies de sesión". Tails lo hace automáticamente con Iceweasel.

Además de las cookies habituales que los navegadores web envían y reciben, y que los usuarios han comenzado a conocer y administrar para su privacidad, las empresas han seguido implementando nuevas "características" que se comportan como cookies pero que no se gestionan de la misma manera.

Adobe ha creado "Objetos almacenados locales" (también conocidos como "Flash Cookies") como parte de sus complementos de Flash, Mozilla ha incorporado una función llamada "almacenamiento DOM" en las versiones recientes de Firefox. Los sitios web pueden usar cualquiera o ambos, además de las cookies para rastrear a los visitantes. Se recomienda que los usuarios tomen medidas para evitar esto.

Administrar la privacidad de almacenamiento DOM de Mozilla/Firefox. Si usas un navegador Mozilla, puedes desactivar las pseudo cookies de DOM escribiendo: **about: config** en la barra de URL.

Esto abrirá una extensa llena de opciones de configuraciones internar del navegador. Escribe "almacenamiento" en el cuadro de filtro y presione regresar. Deberíamos ver una opción llamada **dom.storage.enabled**. Cámbialo a "falso" haciendo clic con el botón derecho y seleccionando Alternar.

30. Administrar la privacidad de Adobe Flash

Adobe enumera consejos sobre cómo deshabilitar las cookies Flash en tu sitio web. Hay algunos problemas con las opciones que ofrece Adobe (por ejemplo, no existe la opción "solo sesión"), por lo que probablemente sea mejor configurar globalmente el espacio del Objeto Almacenado Local en 0 y solo cambiarlo para los sitios que deseamos tener un seguimiento.

En la versión de Linux del complemento Flash de Adobe, no parece haber una manera de establecer el límite en 0 para todos los sitios y, por lo tanto, su uso debe limitarse o evitarse. Afortunadamente, **Tails no tiene flash instalado**, pero en caso de que no estemos utilizando Tails, debemos tenerlo en cuenta.

Si necesitas ver un vídeo online, busque una manera de descargar el video al ordenador y verlo posteriormente. Esto saca al navegador del proceso de procesar un video y elimina esas cookies Flash que nos ayudan a identificarnos.

31. JavaScript

JavaScript es probablemente el gran padre de todas las vulnerabilidades en la navegación por Internet. La mayoría de los exploits, malware, virus y otras formas de toma de control de los ordenadores suceden debido a la ejecución de código JavaScript en el navegador. JavaScript tiene muchos usos.

Algunas veces se usa simplemente para hacer que las páginas web se vean más llamativas al hacer que respondan a medida que el ratón se mueve o cambie continuamente.

En otros casos, JavaScript agrega significativamente a la funcionalidad de una página, lo que le permite responder a las interacciones del usuario sin la necesidad de hacer clic en un botón "enviar" y esperar a que el servidor web envíe una nueva página de respuesta.

JavaScript también contribuye a muchos problemas de seguridad y privacidad en la web. Si una parte maliciosa puede encontrar una forma de tener tu JavaScript, incluido en una página, pueden usarlo para todo tipo de maldad, hacer que los enlaces cambien a medida que el usuario hace clic en ellos, enviar nombres de usuario y contraseñas a lugares equivocados, informar de gran cantidad de datos sobre el navegador de los usuarios a un sitio.

JavaScript suele formar parte de esquemas para rastrear personas en la Web o, lo que es peor, para instalar malware en las computadoras de las personas. Lo mejor es deshabilitar JavaScript (about:config en la barra de URL buscar JavaScript y Alternarlo en deshabilitado) a menos que confiemos plenamente en el sitio o usemos el complemento del navegador **NoScripts** que viene con Tails y está disponible en Firefox para bloquear al menos selectivamente scripts maliciosos y deshabilitar JavaScript directamente.

Supuestamente, NoScript no bloquea todo el JavaScript, incluso cuando está habilitado y no hay sitios en la lista blanca. Hay un complemento de Firefox (que también funciona en el navegador Tor) llamado **toggle_js** que nos permite alternar el parámetro about: config JavaScript.enable a través de un icono de la barra de herramientas para que no tengamos que estar entrando en about: config. Bastante útil la verdad.

JavaScript también puede revelar una cantidad alarmante de información sobre nosotros. Incluso si estamos utilizando TOR o una VPN, incluidos los complementos del navegador, nuestra zona horaria, qué fuentes hemos instalado (flash también lo hace), y por supuesto, la mayoría de los navegadores envíe tu agente, lo que significa que le estamos diciendo al sitio web qué navegador estamos utilizando y, en algunos casos, tu sistema operativo.

Es posible que algunos de estos detalles no sean muy importantes, pero recopilados en su totalidad, puede facilitar la identificación de quién está online al generar casi una huella digital con nuestra configuración específica relacionada con nuestro navegador. Cuando saltas de un sitio a otro con tu huella dactilar, nos pueden extraer correlaciones y patrones de esta

información y, finalmente, vincularlo con nosotros si no somos extremadamente cuidadosos.

Afortunadamente, **Tails** y **Whonix** anulan la mayoría de esta información de identificación, por lo que siempre que usemos Tails con JavaScript deshabilitado, o al menos con NoScripts (Flash se desactiva automáticamente), podemos reducir la cantidad de información que compartimos. Decir, que no siempre es posible navegar con Tails, por lo que estas son cosas que debemos tener en cuenta cuando navegamos con navegadores regulares en nuestro sistema operativo nativo con nuestro navegador.

32. Algunas recomendaciones de ciberseguridad

Aquí hay algunas recomendaciones que podemos pasar a un usuario promedio:

1. Nunca dejéis desatendido el ordenador que utilizáis. Esto es algo que puede parecer obvio, pero si tienes hijos, o un cónyuge o un hermano que no entiende lo que haces en el ordenador, deciden usar tu cuenta, iniciar sesión en tu correo electrónico, Facebook o hacer cosas que podrían comprometer nuestra ubicación mientras estaba en el ordenador, y podría potencialmente causarnos problemas.

Tal vez nos estemos conectando a través de múltiples capas como esta TOR -> VPN (1) -> TOR -> VPN (2), por lo que son 4 capas y VPN (2) es la dirección IP que todos ven. Si nuestro hijo o cónyuge abre su correo electrónico con esa dirección IP y luego cierra la misma sin nuestro conocimiento. Esa VPN ahora está vinculada a nosotros. Y recordamos, es probable que las compañías den información sobre sus clientes para evitar multas, cierres y enjuiciamiento.

2. No digáis a vuestros familiares lo que estáis haciendo, sólo dales instrucciones para que no toquen el ordenador. Nunca debéis contarle a nadie lo que estáis haciendo en el ordenador, porque si alguna vez se presentara un agente de la ley, interrogaría a tu familia y amigos.

   Si honestamente no lo saben, no pueden ser acusados por un tribunal, por lo que es mejor mantenerlos en la oscuridad. O tal vez la policía podría asustarlos para que cuenten todos sus secretos porque le dicen a tu familia que, si no confiesan, tú y ellos irán a la cárcel, posiblemente

por un tiempo prolongado. Simplemente ingresa en el ordenador con contraseña y nunca lo dejes desatendido con la pantalla desbloqueada.

3. Si usáis varias capas para conectarnos, aseguraros de verificar regularmente que todas ellas estén intactas. Las VPN pueden caerse algunas veces sin previo aviso y, aunque nunca debéis configurar vuestro sistema de modo que, si una capa cae, lo pierdes todo, solo tened en cuenta vuestra forma de navegar hasta que levantéis la siguiente capa.

   Esta es una de las cosas que me gustan de Tortilla, si mi capa TOR no funciona, no la omite y pasa a la siguiente capa, simplemente deja de funcionar. Cuando las VPN caen, el ordenador evita la VPN descartada y pasa a la siguiente capa, que en algunos casos podría ser la dirección IP real. Os recomiendo encarecidamente Tortilla.

4. No uséis la misma contraseña para múltiples foros, mercados, correos electrónicos, etc. Esperad que uno o más de los sitios web en los que estás registrado almacene nuestra contraseña en texto plano. Esto significa que, si alguien encuentra un exploit y vuelque la base de datos, pueda encontrar nuestra contraseña.

   Si usamos la misma contraseña para otros sitios, y mismo nombre de usuario, nuestra lista completa de cuentas se verá comprometida. Siempre usad contraseñas diferentes y mantenedlas fuertes. No permitáis que nada sobre su contraseña identifique cómo eliges la misma, y mucho menos, identifique nada personal sobre vosotros.

33. Ataques de arranque frío, extracción de RAM no conectada

¿Sabías que incluso si nuestro sistema está encriptado en un disco completo, nuestros datos aún se pueden extraer utilizando algo llamado **ataque de arranque en frío**?

Lo primero de lo que tenemos que hablar es de **RAM**, que significa **memoria de acceso aleatorio**. Todo lo que necesitamos saber sobre la memoria RAM es, que la memoria RAM es el lugar en una computadora donde se guardan el sistema operativo, los programas de aplicación y los datos en uso actual para que el procesador del ordenador los pueda acceder rápidamente.

La memoria RAM es mucho más rápida de leer y escribir que otros tipos de almacenamiento en una computadora, disco duro, disquete y CD-ROM. Sin embargo, los datos en RAM permanecen allí solo mientras el ordenador esté funcionando. Cuando apagas el ordenador, la RAM pierde sus datos.

Cuando enciendes el ordenador de nuevo, tu sistema operativo y otros archivos se cargan nuevamente en la RAM, generalmente desde tu disco duro. La memoria RAM se puede comparar con la memoria a corto plazo de una persona y el disco duro con la memoria a largo plazo. La memoria a corto plazo se centra en el trabajo en cuestión. Si la memoria a corto plazo se llena, su cerebro a veces puede actualizarla de hechos almacenados en la memoria a largo plazo.

Un ordenador también funciona de esta manera. Si la RAM se llena, el procesador necesita ir continuamente al disco duro para superponer los datos antiguos en la RAM con datos nuevos, ralentizando la operación del ordenador. A diferencia del disco duro, que puede estar completamente lleno de datos, la RAM nunca se queda sin memoria.

Los datos se pueden extraer de la RAM usando varias herramientas. Cuando tienes un documento de texto abierto y estás trabajando en él, estamos trabajando desde la RAM. Lo que significa que, si estamos trabajando en un documento confidencial, ese documento se almacena temporalmente en la memoria RAM y es vulnerable a ser extraído mientras el ordenador esté encendido.

Cuando se almacena la memoria RAM, se almacena sin ningún tipo de encriptación, lo que hace que sea muy fácil de robar y un gran riesgo de seguridad.

Apagar un ordenador a través de su ciclo de apagado normal generalmente pasa por un proceso de limpieza de la RAM. Sin embargo, si la computadora pierde energía abruptamente, como en un corte de energía, el ordenador no pasa por su ciclo de apagado normal y parte de la información permanece en los chips RAM desde unos segundos hasta unos minutos. Esta es una de las formas en que los ataques de arranque en frío pueden funcionar.

Presentamos rápidamente un tipo de RAM que te ayudará a comprender mejor el resto de este concepto. **DRAM** significa memoria de acceso aleatorio dinámica. DRAM es el tipo más común de memoria de acceso aleatorio (RAM) para ordenadores personales y estaciones de trabajo. DRAM es dinámica, y a diferencia de la RAM estática (SRAM), necesita tener sus celdas de almacenamiento actualizadas, o recibir una nueva carga electrónica cada pocos milisegundos.

DRAM está diseñado para perder su memoria rápidamente después de perder potencia eléctrica. Luego hay subsecciones de DRAM llamadas **DDR**. Esta es una forma de hacer que la memoria esté disponible más rápidamente, pero no es realmente importante comprenderla por completo.

La mayoría de los ordenadores, que circulan hoy en día, tienen DDR3, y los más modernos y potentes usan DDR4, en ellas a menos que sean ordenadores viejos, esto incluye ordenadores portátiles. DRAM se conoce como un tipo de memoria volátil, es la memoria del ordenador que requiere energía para mantener la información almacenada. Conserva el contenido mientras está encendido, pero cuando se interrumpe la energía, los datos almacenados se pierden rápidamente. Pero, ¿Cómo de rápido se pierden?

En 2008, un grupo de investigadores quería ver la practicidad de extraer datos no encriptados de la memoria RAM en el ordenador. Argumentaron que las DRAM usadas en la mayoría de los ordenadores modernas retienen su contenido por segundos o minutos después de que se pierde la energía, incluso a temperaturas de funcionamiento o si se retiran de una placa base.

Al usar una herramienta de análisis, pudieron buscar los archivos clave (como las llaves PGP) almacenados en la RAM que podrían usarse para descifrar volúmenes encriptados (unidades) en el ordenador. Con éxito pudieron descifrar volúmenes utilizando **BitLocker**, **FileVault**, **dm-crypt** y **TrueCrypt**.

Contrariamente a lo que se suele suponer, las DRAM utilizadas en la mayoría de los ordenadores modernos retienen su contenido por segundos o minutos después de que se pierde la energía, incluso a temperaturas de funcionamiento e incluso si se retiran de una placa base.

Aunque las DRAM se vuelven menos confiables cuando no se actualizan, no se borran de inmediato, y su contenido persiste lo suficiente para la adquisición maliciosa (o forense) de imágenes de la memoria de sistema completamente utilizables.

Se demostró que este fenómeno limita la capacidad de un sistema operativo para proteger el material de claves criptográficas de un atacante con acceso físico. Se montaron reinicios en frío para simular ataques en los sistemas de encriptación de discos populares (BitLocker, FileVault, dm-crypt y TrueCrypt) sin usar dispositivos o materiales especiales.

Experimentalmente, se caracterizó el alcance y la predictibilidad de la remanencia de la memoria y se informó que los tiempos de remanencia se pueden aumentar drásticamente con técnicas simples.

Ofrecieron nuevos algoritmos para encontrar claves criptográficas en imágenes de memoria y corrigieron errores causados por la disminución de bits. Aunque se discutió varias estrategias para mitigar parcialmente estos riesgos, no se conoce ningún remedio simple que los elimine.

Fue algo muy preocupante para la mayoría de la gente, y muchas personas se volvieron locas cuando se lanzó el documento de investigación en 2008 porque incluso las herramientas de encriptación difíciles como TrueCrypt podrían volverse inútiles con un ataque de este estilo.

Tras un análisis posterior del documento, señalar que utilizaron SDRAM, DDR y DDR2, y no DDR3 porque no estaba disponible en ese momento. Esto provocó que TrueCrypt lanzara la siguiente declaración en su sitio web: “Datos no encriptados en RAM”.

Es importante tener en cuenta que TrueCrypt es un software de cifrado de disco que encripta sólo discos, no la memoria RAM.

Tened en cuenta que la mayoría de los programas no borran el área de memoria (búferes) en la que almacenan archivos no encriptados (porciones de) que se cargan desde un volumen TrueCrypt.

Esto significa que después de salir de dicho programa, los datos no cifrados con los que se trabajó pueden permanecer en la memoria (RAM) hasta que el ordenador se apague (y, según algunos investigadores, incluso durante un tiempo después de que se apague la alimentación).

También hay que tener en cuenta que, si abrimos un archivo almacenado en un volumen TrueCrypt, por ejemplo, en un editor de texto y luego forzamos el desmontaje en el volumen TrueCrypt, el archivo permanecerá desencriptado en el área de memoria (RAM) utilizada por (asignado a) el editor de texto. Esto también se aplica al desmontaje automático forzado.

Intrínsecamente, las claves maestras no cifradas también deben almacenarse en la memoria RAM. Cuando se desmonta un volumen TrueCrypt no perteneciente al sistema, TrueCrypt borra las claves maestras (almacenadas en la RAM).

Cuando el ordenador se reinicie limpiamente (o se apague limpiamente), todos los volúmenes TrueCrypt que no pertenecen al sistema, se desmontan automáticamente y, por lo tanto, todas las claves maestras almacenadas en la memoria RAM se borran mediante el controlador TrueCrypt (excepto las claves maestras para particiones/unidades del sistema).

Sin embargo, cuando la fuente de alimentación se interrumpe abruptamente, cuando la computadora se reinicia, no se reinicia limpiamente, o cuando el sistema falla, TrueCrypt deja de funcionar de

forma natural y, por lo tanto, no puede borrar ninguna clave ni ningún otro dato confidencial.

Además, como Microsoft no proporciona ninguna API adecuada para manejar la hibernación y el apagado, las claves maestras utilizadas para el cifrado del sistema no se pueden borrar de manera confiable (y no se borran) de la memoria RAM cuando el ordenador hiberna, se apaga o se reinicia.

Para resumir, TrueCrypt no puede y no garantiza que la memoria RAM no contenga datos confidenciales (por ejemplo, contraseñas, claves maestras o datos descifrados). Por lo tanto, después de cada sesión en la que trabaja con un volumen TrueCrypt o en el que se ejecuta un sistema operativo encriptado, debe apagar (o, si el archivo de hibernación está encriptado, hibernar) la computadora y luego dejarla apagada por lo menos varios minutos (cuanto más, mejor) antes de volver a encenderlo. Esto es algo necesario para borrar la RAM.

Supuestamente, durante 1,5-35 segundos bajo temperaturas normales de funcionamiento (26-44 ° C) y hasta varias horas cuando los módulos de memoria se enfrían (cuando el ordenador está funcionando) a temperaturas muy bajas (por ejemplo, -50 ° C). Se alega que los nuevos tipos de módulos de memoria exhiben un tiempo de desintegración mucho más corto (por ejemplo, 1,5-2,5 segundos) que los tipos anteriores (a partir de 2008).

Antes de poder borrar una clave de la RAM, se debe desmontar el volumen TrueCrypt correspondiente. Para volúmenes que no son del sistema, esto no causa ningún problema.

Sin embargo, dado que Microsoft actualmente no proporciona ninguna API adecuada para manejar la fase final del proceso de apagado del sistema, los archivos de paginación ubicados en volúmenes del sistema cifrados que se desmontan durante el proceso de apagado del sistema pueden contener páginas de memoria intercambiadas válidas (incluidas partes de Archivos del sistema de Windows).

Esto podría causar errores de "pantallazo azul". Por lo tanto, para evitar errores de 'pantallazo azul', TrueCrypt no desmonta los volúmenes del sistema cifrado y, en consecuencia, no puede borrar las claves maestras de los volúmenes del sistema cuando el sistema se apaga o se reinicia.

Algunos puntos clave para extraer de este comunicado, son, que el apagado correcto del ordenador reduce, si no completamente, este riesgo, excepto en el caso de los discos del sistema encriptados. Lo que se entiende por esto es, por ejemplo, si nuestro sistema operativo principal es Windows y se ha cifrado esa unidad, esta es su unidad del sistema y la clave maestra para esa unidad no se borra al apagar o reiniciar.

La solución es simplemente no almacenar nada sensible en el volumen de su sistema. Ya sea que utilicemos una unidad particionada o una memoria USB cifrada, solo asegúrate de que la unidad principal en la que se inicia no contenga datos confidenciales.

Y si no tienes otra opción, necesitas cifrar por separado los datos dentro del volumen del sistema con una frase de contraseña diferente y una clave privada para que, incluso si entran en el volumen de nuestro sistema, no puedan acceder a los demás datos cifrados que deseamos proteger.

Puedes utilizar estas mismas técnicas para buscar los archivos de clave privada de PGP en la memoria RAM, por lo que esta es una amenaza muy real en el caso de que si el ordenador todavía está encendido si vienen a buscarlo, pueden usar estas técnicas para recuperar datos del ordenador.

Sin embargo, existe un debate sobre si este tipo de ataque puede persistir incluso ahora en 2018 con nuevos tipos de RAM.

Si intentamos este ataque hoy en día y para probar el mismo. Llenemos la memoria con alrededor de 1000 marcadores de sombras, solo para asegurarnos que hay suficiente.

Ahora cortamos la luz del ordenador. Ostensiblemente, los marcadores podrían ser reconocibles en la memoria RAM después de unos minutos, pero estábamos impacientes, así que solo se esperó 10 segundos para la primera prueba. Arrancamos, con la instalación mínima de Linux.

Cargamos el módulo kernel: insmod/rmem.ko. Ejecutamos nuestro "cazador". **Nada.**

Eso está bien, sin embargo. Debería haber al menos alguna corrupción de datos. El tamaño del marcador predeterminado es de 128 bytes, así que establezcamos la **distancia hamming** en 128, lo que significa que un bit de cada byte puede voltearse. Estadísticamente, eso equivale a una tasa de corrupción del 25%, ya que un bit dañado tiene un 50% de posibilidades de permanecer igual. **Nada.**

Al parecer, en 10 segundos, la memoria estaba completamente corrupta. Probemos un intervalo más corto: 2 segundos. Mismos resultados: No queda nada de nuestra "clave de cifrado".

En la prueba se afirmaba estar usando DDR3, que se sabe que mantiene la memoria por un tiempo mucho más corto que DDR2. Un nuevo trabajo de investigación publicado en septiembre de 2013 intentó reproducir los hallazgos de la investigación de 2008 pero usando computadoras con DDR1, DDR2 y DDR3 y sus hallazgos fueron interesantes.

A pesar de que una máquina utilice cifrado de disco completo, los ataques de arranque en frío pueden recuperar datos no encriptados de la RAM. Los ataques de arranque en frío se basan en el efecto de remanencia de la memoria RAM, que dice que los contenidos de la memoria no desaparecen inmediatamente después de cortar la corriente, sino que se desvanecen gradualmente con el tiempo.

Este efecto se puede aprovechar reiniciando una máquina en ejecución, o trasplantando sus chips RAM en una máquina de análisis que lea lo que queda en la memoria. En teoría, este tipo de ataque se conoce desde la década de 1990. Sin embargo, solo en 2008, **Halderman et al**. han demostrado que los ataques de arranque en frío se pueden implementar bien en escenarios prácticos. En el trabajo en cuestión, investigaron la viabilidad de los ataques de arranque en frío.

Se verificaron las afirmaciones de Halderman et al, independientemente de forma sistemática. Para DDR1 y DDR2, proporcionaron los resultados de nuestras mediciones experimentales que en gran parte concuerdan con los resultados originales. Sin embargo, también se señaló que no se pudo reproducir los ataques de arranque en frío contra los modernos chips DDR3. El conjunto de las pruebas comprende 17 sistemas y configuraciones de sistema, de las cuales 5 están basadas en DDR3.

¿Qué deberías hacer? Número uno, apaga siempre el ordenador cuando no estés cerca del o colócalo en modo de hibernación, de lo contrario, tus documentos confidenciales podrían permanecer en la memoria RAM. Simplemente bloquear la pantalla no te servirá de nada.

Asegúrate de que el ordenador está usando un tipo de RAM DDR3, si es posible. Nunca almacenes información sensible en un volumen cifrado del sistema, ya que este ataque puede usarse para entrar en el volumen y cualquier elemento no cifrado puede recuperarse.

Si estamos usando un portátil, extrae la batería para que se apague de inmediato. Si tienes tiempo, apaga el ordenador, de lo contrario, apágalo inmediatamente para que no se ejecute nada. Cuanto más tiempo puedas perder, mejor, son preciosos segundos en los que no pueden recuperar ningún dato. Así que apaga inmediatamente las cosas si no tienes tiempo suficiente para hacer un apagado correcto.

Considera poner un candado en la carcasa del ordenador, y si quieres ir un paso más allá, atorníllalo al suelo. De esta forma, la cantidad de tiempo que tardarían en ingresar a el ordenador desperdiciaría valiosos minutos y es más que probable que inutilice cualquier memoria recuperable.

Algunas personas, incluso han sugerido que sueldes la memoria RAM en la placa base para que no puedan sacarla. Esto puede ayudar a ralentizar las

cosas, pero recuerda que enfriar la memoria puede conservar las cosas por bastante tiempo (sobre todo en el caso de memorias antiguas DDR1 y DDR2).

Con DDR3, deberíamos estar listos y creo que, con esta comprensión, los fabricantes probablemente comenzarán a buscar formas de cifrar la RAM, pero hasta ese momento debemos ser consciente de esto como un medio posible para robar nuestros datos confidenciales. Como hemos dicho, prepararse por si acaso.

34. La fuerza de la criptografía y el anonimato cuando se utiliza correctamente

Esta parte pretende servir como un ejemplo de cómo y cuándo la criptografía y el anonimato se utilizan correctamente, puede evadir casi a cualquiera, incluidos a la policía.

A estas alturas, es probable que todos hayan escuchado que alguien ha bloqueado o cifrado nuestro acceso al ordenador y el atacante nos ha obligado a pagar para su rescate (**WannaCry**,**CryptoLocker**) Dell SecureWorks estimó que CryptoLocker afectó a 250,000 víctimas, y que el pago promedio fue de 300 € cada una. Millones en Bitcoin han sido rastreados.

CryptoLocker es un troyano ransomware dirigido a ordenadores con Microsoft Windows y que apareció por primera vez en septiembre de 2013. Un ataque de CryptoLocker puede provenir de diversas fuentes, uno de ellas está disfrazada como un archivo adjunto de correo electrónico legítimo (método cada vez más común).

Un archivo ZIP adjunto a un mensaje de correo electrónico contiene un archivo ejecutable con el nombre del archivo y el icono disfrazado como un archivo PDF, aprovechando el comportamiento predeterminado de Windows de ocultar la extensión de los nombres de archivo para disfrazar la extensión real .EXE.

Cuando se activa, el malware encripta ciertos tipos de archivos almacenados en unidades de red locales y montadas utilizando la criptografía de clave pública RSA para generar un par de claves RSA de 2048 bits, con la clave privada almacenada solo en los servidores de control del malware.

Posteriormente, el malware muestra un mensaje que ofrece descifrar los datos si uno paga (a través de Bitcoin o un cupón prepago) si se realiza antes de una fecha límite establecida, amenazando con eliminar la clave privada si se cumplen los plazos.

Si se cumplen los plazos, el malware ofrece descifrar datos a través de un servicio online proporcionado por los operadores del malware, a un precio significativamente más alto en Bitcoin.

En noviembre de 2013, los operadores de CryptoLocker lanzaron un servicio online que afirmaba permitir a los usuarios descifrar sus archivos sin el programa CryptoLocker, y comprar la clave de descifrado, una vez que expiraba el plazo.

El proceso implicaba cargar un archivo cifrado en el sitio, como muestra, y esperar a que el servicio encontrara una coincidencia, que el sitio afirmaba que ocurría dentro de las 24 horas siguientes.

Una vez que se encuentra una coincidencia, el usuario puede pagar la clave online, si la fecha límite de 72 horas ha pasado, el costo aumenta a 10 Bitcoin.

Una de las razones por las que os cuento esto es que CryptoLocker usa encriptación RSA 2.048, y si recordáis en las publicaciones de PGP anteriormente, lo recomendable es usar 4096. Aunque incluso con encriptación de 2.048 bits, nadie ha derrotado exitosamente a CryptoLocker (hasta donde yo sé), este es el poder de una encriptación implementada correctamente.

Utilizando los métodos adecuados de anonimato, esta persona o grupo han logrado adquirir, según una investigación realizada por ZDNet, alrededor de 41.928 BTC.

En la investigación de este artículo, ZDnet trazó cuatro direcciones de bitcoin publicadas (y reubicadas) en foros por varias víctimas de CryptoLocker, mostrando un movimiento de 41.928 BTC entre el 15 de octubre y el 18 de diciembre.

Como se puede ver, la encriptación y el anonimato correctamente ejecutados, permitieron que este grupo de personas adquiriera el equivalente de Bitcoin de casi $ 42 millones de aquel entonces en solo 4 meses.

No estoy recomendando que hagáis esto, simplemente estoy dando un ejemplo perfecto de lo poderosa es la combinación de estos dos factores muy importantes en la protección de cualquier persona online cuando se usa correctamente.

35. Direcciones de correo electrónico PGP/GPG

Mucha gente usa direcciones de correo electrónico reales. Me gustaría recordar a todos, que cuando le das a alguien tu clave pgp/gpg, **pueden ver la dirección de correo electrónico que asociaste a esa clave**.

No se supone que uses **cualquier** tipo de servicio de correo electrónico de clearnet como: gmail, yahoo, hotmail, etc. Si quieres usar una dirección de correo electrónico válida, entonces necesitas usar un proveedor de correo electrónico que soporte Tor y el anonimato. Por ejemplo, uso **Safe-Mail**. Puedes acceder a este servicio de correo electrónico desde Tor, lo que te permite permanecer en el anonimato.

36. Bajo ninguna circunstancia asocies una dirección en claro con tu clave PGP/GPG

Definición de **DOX**: Información personal sobre personas en Internet, que a menudo incluyen nombre real, alias conocidos, direcciones, número de teléfono, SSN, número de tarjeta de crédito, etc.

37. Otro correo electrónico de estafa, cuidado

Una cosa que debes tener en cuenta es que cualquier tipo de anuncio legal y honesto, se firma de PGP. Compruebe siempre si hay una firma de PGP, y si no la hay, solicita amablemente al administrador o moderador

de los sitios que vuelva a enviar el mensaje con una firma. Protégete al verificar el nombre y asegúrate de que cualquier usuario tenga una cierta reputación ¡Cuidado!

38. Una introducción a MD5 Plus y SHA-1

Las personas que se mantienen anónimas online, utilizan, "**The Grugq**".

Cabe señalar que Grugq estuvo en algún momento en la nómina del gobierno de Estados Unidos por encontrar y vender exploits de zero day. Si recordamos la publicación anterior sobre cómo el gobierno federal de EE.UU. es el comprador más importante de malware en el mundo, bueno, pues Grugq fue uno de esos que vendió malware al gobierno.

Pero, cuando se dio a conocer al público, el gobierno ya no quería comprar malware porque les gusta mantener su propio anonimato al comprar estos exploits. Grugq nos cuenta la historia mediante su biografía: The Grugq es un profesional de la seguridad de la información que ha trabajado como forense digital, realizando ingeniería inversa binaria, rootkits, voz sobre IP, telecomunicaciones y seguridad financiera. Por último, pero no menos importante, también ha hablado en varias conferencias de seguridad.

Desarrolló **Hash** (hacker shell), una herramienta que permite a las personas evadir la detección al penetrar en un sistema. Ha lanzado un software de ataque VoIP.

¿Por qué estamos hablando de Grugq? ¿A quién le importa? Bueno, él tiene la mejor información sobre mantenerse anónimo y mantener la privacidad online y es alguien con quien todos deberíamos estar familiarizados.

Escribe publicaciones de blog y ha realizado presentaciones de vídeo en conferencias de seguridad y hackers, y su presentación más famosa. La presentación dura aproximadamente 1 hora y es esencial para todos los que desean mantener su anonimato online.

Si descargáramos el video, podríamos comprobar:

SHA1: 1a9e6c67a527b42a05111e1b18c7a037744bb51e
MD5: b6de41da8d1fca2fabf725f79d2a90df

Una vez que hayamos descargado el archivo, podemos comprobar algo llamado suma de comprobación del archivo. La suma de verificación es donde el contenido de todo el archivo se conecta a un algoritmo matemático y genera una cadena específica. Podemos ver las dos cadenas de arriba. Esto es algo que de lo que debemos tener el hábito de hacer cuando sea posible.

Si recordamos cuándo hablamos sobre archivos de firma y PGP, este es otro método para verificar las descargas, pero no tan bueno como los archivos de firma. Sin embargo, siempre que se proporcione debemos realizarlo para verificar nuestras descargas cuando la combinación de archivo de firma + PGP no esté disponible.

Una vez que hayamos descargado el archivo en Tails, lo primero que debes hacer es mover el archivo que hemos descargado a la carpeta tmp.

Para hacerlo, busca en la parte superior y haga clic en Lugares -> Equipo -> Sistema de archivos -> tmp. Aquí es donde se mueven el archivo descargado, y para facilitar las cosas, renombramos el archivo grugq.zip.

A continuación, vamos a abrir una ventana de terminal (como un mensaje de DOS) haciendo clic en el ícono de rectángulo negro en el área central superior izquierda de Tails. Una vez que hayamos abierto nuestra ventana de terminal, vamos a realizar algunos comandos de Linux.

cd /tmp: Esto cambiará el directorio actual que está operando dentro del terminal a nuestra carpeta tmp y nos permitirá acceder más fácilmente a los archivos en esa carpeta.

sha1sum grugq.zip: Esto realizará una suma de comprobación SHA1 en el archivo que acabamos de descargar, podemos ver por qué queríamos cambiar el nombre del archivo. Debería darnos el mismo resultado que la suma de SHA1 enumerada anteriormente.

md5sum grugq.zip: Esto realizará una suma de comprobación MD5 en el archivo que acabamos de descargar, y es otra forma de verificar el archivo. SHA1 es mejor porque es más difícil producir el mismo resultado dos veces con diferentes contenidos de archivo usando SHA1 versus **MD5** pero, no obstante, usa ambos siempre que sea posible y siempre verifica tus archivos descargados.

De acuerdo, suponiendo que nuestro video descargado pasase la prueba de suma de comprobación, podemos estar seguro de que el archivo de video que descargamos no ha sido alterado o se ha inyectado ningún código malicioso. Cuando se cambia un solo carácter en el código fuente de un archivo determinado, la salida de suma de comprobación será completamente diferente. La diferencia siempre es bastante grande, y es por eso que realizamos sumas de verificación como forma importante de verificar nuestras descargas.

39. Cosas obvias cuando estas usando TOR

En esta parte hablaremos sobre un error del que todos podemos aprender, cuando un estudiante de Harvard envió por correo electrónico con una amenaza de bomba a la escuela mientras usaba Tor para evitar un examen final...

El estudiante "tomó medidas para disfrazar su identidad" mediante el uso de Tor, un software que permite a los usuarios navegar en la web de forma anónima, y **Guerrilla Mail**, un servicio que permite a los usuarios crear direcciones de correo electrónico gratuitas y temporales.

A pesar del objetivo de anonimato de Eldo Kim, de 20 años, sus intentos de enmascarar su identidad llevaron a las autoridades a la puerta de su casa. ¿Significa eso que Tor falló? En lo más mínimo.

Si bien el estudiante de Harvard sí utilizó Tor, fueron sus otras medidas de seguridad descuidadas las que llevaron a su arresto. La demanda dice que la universidad "pudo determinar que, en las horas previas a la recepción de los mensajes de correo electrónico. Eldo Kim accedió a Tor utilizando la red inalámbrica de Harvard.

Lo que Kim no se dio cuenta es que Tor, que enmascara la actividad online, no oculta el hecho de que se está usando el software. Al analizar los encabezados de los correos electrónicos enviados a través de la cuenta de Guerrilla Mail, las autoridades pudieron determinar que el remitente anónimo estaba conectado a la red TOR.

Usando esa conclusión, intentaron descubrir qué estudiantes habían estado utilizando Tor en la red inalámbrica de Harvard en el momento de las amenazas. Antes de lanzar TOR, Kim tuvo que iniciar sesión en el sistema inalámbrico de la escuela, lo que requiere que los usuarios se autentiquen con un nombre de usuario y contraseña.

Al revisar los registros de red y buscar usuarios que se conectaran a las direcciones IP conocidas públicamente como parte de la red TOR, la universidad pudo correlar entre los usuarios que usaban TOR y su conexión inalámbrica en el momento en que las amenazas de bomba fueron recibidas.

No nos queda mucho más que añadir, aparte de que, si planeas hacer hacktivismo o simplemente usar DarkNet, asegúrate de que puedes hacerlo cuando el uso de TOR no levante sospechas. En el caso de este estudiante, era probable que fuera el único estudiante de Harvard que usaba TOR en el momento en que se envió este correo electrónico, y cuando las autoridades llegaron a su dormitorio.

Probablemente nunca lo hubieran atrapado, pero recuerde que cuando usas TOR, otros pueden ser conscientes de que lo estás usando. Una mejor idea para él habría sido conectarse a otro ordenador remotamente y tener ese ordenador conectado a la red para enviar el correo electrónico.

De esta forma, nunca podrían haber visto el ordenador conectada a TOR. No me preocuparía de utilizar TOR regularmente desde su casa, porque hay

cientos de miles de usuarios de TOR, pero de nuevo, es algo a tener en cuenta.

40. ¿Estás usando safe-mail.net?

Si eres un usuario de la DarkNet, probablemente hayas visto a muchos usuarios abogar por el uso de un servicio llamado **Safe-Mail.net**. Esta compañía se describe a sí misma como "el sistema de comunicación más seguro y fácil de usar", y muchos usuarios de la DeepWeb la han adoptado. Pero hay algunas cosas que debemos tener en cuenta.

Los usuarios conocidos del servicio web de Safe-mail incluyen operadores, vendedores y clientes de muchos sitios del mercado de la DarkNet.

Cuando me comuniqué con Safe-mail para comentar, Amiram Ofir, presidente y CEO de Safe-mail, respondió en un correo electrónico que la compañía y sus empleados "ciertamente no están al tanto de ninguna actividad criminal" y agregó que la compañía sigue las órdenes emitidas en Israel por un tribunal israelí.

Cualquier otra agencia de aplicación de la ley debe ponerse en contacto con las autoridades israelíes. Vale la pena señalar, sin embargo, que Israel firmó un Tratado de Asistencia Legal Mutua (MLAT) con los EE.UU. en 1998, y que se utilizó una solicitud MLAT para obtener una imagen del servidor web Silk Road, según la querella penal del 27 de septiembre de 2013.

Ofir comentó que las comunicaciones entre los usuarios y el servicio web están protegidas por SSL, y que la información almacenada en el servidor está encriptada con claves específicas del usuario. Cuando se le preguntó si Safe-mail había recibido órdenes judiciales emitidas por un tribunal israelí en nombre de una agencia de aplicación de la ley no israelí, como el FBI, Ofir respondió con un breve "Sí".

Es probable que Safe-mail les den todo lo que necesitan para leer los correos electrónicos. Por lo tanto, debemos recordar que no se debe confiar en este servicio de correo electrónico. Ningún servicio de correo electrónico irá a la cárcel por ti. Y si enviamos algo sensible por correo electrónico utilizando texto sin formato, es probable que lo lea alguien que no sea el destinatario.

Esta es la razón por la cual cosas como el fuerte cifrado PGP son esenciales para cualquier tipo de comunicación sensible. Con esto, se debe tener en cuenta que Safe-Mail no es más seguro que Gmail cuando se trata de

proteger nuestra privacidad con nuestro servicio de correo electrónico centralizado. Nunca confíes tu privacidad en ninguna compañía, siempre encripta todo.

41. Otro ejemplo de cómo la criptografía robusta SÍ puede proteger a cualquiera

Sí, leísteis el título correctamente. Usando los mismos tipos de técnicas que hemos visto, podemos y debemos permanecer en el anonimato sin importar lo que estemos haciendo.

Los pedófilos y los pornógrafos infantiles son algunas de las personas más buscadas y despreciadas del planeta. Son cazados por agencias federales castigados muy seriamente (Menos castigados de lo que yo los castigaría). Entonces, el motivo de este parte del post es demostrar que cualquiera puede permanecer libre y en el anonimato si utiliza la ciberseguridad y la OpSec de forma adecuada.

En ciberseguridad, si vuestra plataforma de comunicaciones segura (supuestamente), no está siendo utilizada por terroristas o pedófilos, probablemente es que no estemos usando las herramientas adecuadas en cuanto a ciberseguridad nos referimos.

Quiero hablarte sobre un grupo de pornógrafos infantiles que operaron durante varios años online, llamado **YardBird**. Durante un período de 15 meses, hubo alrededor de 400,000 imágenes y 11,000 videos cargados en un servidor central administrado por el grupo y compartido por los miembros.

La razón por la que sabemos eso, es porque, durante esos 15 meses, el FBI realizó una operación encubierta para infiltrarse en el grupo con la esperanza de detener a los miembros. Capturaron con éxito a 1 de cada 3 miembros del grupo. Un usuario de los que sigue libre hasta la fecha, es el líder del grupo, que también usaba el nombre online YardBird.

Cómo es posible que después de tantos esfuerzos por parte de la Oficina Federal de Investigaciones (FBI), la Policía Federal Australiana (AFP) y el Servicio de Policía de Queensland australiano, que las personas de alto rango en las listas de personas buscadas ¿pudieran evadir la captura? Utilizaron criptografía fuerte y reglas de ciberseguridad apropiadas. Ahora hablemos sobre la historia del intento de aprehensión de este grupo.

De acuerdo con el FBI. Hubo aproximadamente 60 miembros que se identificaron de manera general, y de los 60, aproximadamente 20 se identificaron positivamente en este grupo.

Hubo numerosos desafíos presentados durante la operación. El grupo utilizó un nivel de organización y sofisticación sin precedentes. Tuvieron una prueba cronometrada para posibles nuevos miembros. Tuvieron que usar tecnología de cifrado y anonimizadores basados en internet, servicios de reenvío.

También dañaron intencionalmente sus propios archivos de pornografía infantil y solo los nuevos miembros sabían cómo reconfigurar esos archivos para poder leer las imágenes o el video.

Además, tenían la extraña habilidad de monitorizar las noticias mundiales relacionadas con los esfuerzos de aplicación de la ley en materia de pornografía infantil a fin de educarse mejor para evitar la detección de la aplicación de la ley.

Como dije antes, el presunto líder de este anillo usó el nombre online "Yardbird". Yardbird volvió a aparecer en **Usenet** en 2009 y 2010 en la fecha correspondiente al primer y segundo aniversarios de los arrestos en 2008. Su intención era mostrar que todavía era libre y responder a las preguntas de los usuarios.

Una de las cosas más importantes que declaró Yardbird fue que todos los integrantes del grupo que usaban TOR y los **remailers** permanecían libres, mientras que los que dependían de servicios como Privacy.li fueron arrestados y condenados. Privacy.li fue un servicio VPN offshore que prometía el anonimato. Reclaman de su sitio web lo siguiente.

Yardbird comentó que varios miembros del grupo, incluido su segundo al mando Christopher Stubbings (Helen) y Gary Lakey (Berenjena), eran usuarios de Privacy.li, de hecho, afirmaron que lo usaban para todo. (Actualmente Helen cumple una condena de 25 años en el Reino Unido, mientras que Berenjena está cumpliendo cadena perpetua en una prisión de Arizona).

Berenjena, literalmente, se hizo notar por su constante promoción de la Privacidad. Se jactaba continuamente de que no podía ser atrapado porque Privacy.li no mantenía registros, y se encontraban fuera de la jurisdicción de los EE.UU.

Si bien hubo cierto grado de privacidad, no hubo ningún anonimato en absoluto, por lo que realmente no fue una sorpresa que los clientes de Privacy.li estuvieran entre los arrestados.

Al final del día, ningún proveedor de servicios irá a la cárcel por ti. Una simple orden judicial puede hacer que incluso los proveedores de VPN más duros se deshagan de los usuarios, porque preferirían traicionar a un usuario de 20 €/mes antes de ser multados, cerrados y posiblemente encarcelados por interferir con una investigación federal.

¿Qué otros errores se hicieron para conducir al arresto de algunos miembros de este grupo? La policía australiana arrestó a un hombre por cargos de pornografía infantil totalmente ajenos, y presumiblemente como parte de un acuerdo con el fiscal, reveló la existencia de "el grupo" y entregó un par de claves pública / privada de PGP y una contraseña.

Al haber adquirido del informante el par de llaves públicas / privadas del grupo actual de PGP, y su frase de contraseña, la policía podía asumir la identidad de este miembro del grupo y, además, leer todo el tráfico encriptado publicado por los miembros del grupo.

Una vez que el grupo fue vulnerable, la policía pudo aprovechar algunos factores:

1. Tenían la computadora del informante, con todo su correo electrónico, claves PGP. Esto proporcionó una historia, lo que hizo más fácil continuar la interpretación.
2. En el momento en que el grupo fue penetrado, el grupo había estado operando durante aproximadamente 5 años. En este momento, el grupo se había convertido en una comunidad: la gente estaba familiarizada el uno con el otro, a menudo bajando las defensas, lo que hacía que a veces revelaran fragmentos de información personal. Esto se da especialmente cuando uno piensa que sus mensajes son seguros, y más allá de la capacidad de la policía para interceptar, dirían cosas que nunca dirían públicamente.

Por lo tanto, es importante tener en cuenta en este momento que no importa qué tan cómodo te sientas con alguien, siempre hay una posibilidad de que puedan comprometerte. De hecho, el grupo tenía un conjunto de reglas, a todos los miembros se les dijo que obedecieran, y si se descubría que algún miembro violaba las siguientes reglas, serían expulsados:

- Nunca revelar la verdadera identidad a otro miembro del grupo
- Nunca se comunique con otro miembro del grupo fuera del canal de Usenet
- La membresía grupal se mantiene estrictamente dentro de los límites de Internet
- Ningún miembro puede identificar positivamente a otro

- Los miembros no revelan información de identificación personal
- El grupo de noticias de comunicaciones primarias se migra regularmente
- Si un miembro infringe una regla de seguridad, por ejemplo, no encripta un mensaje, será expulsado
- En cada migración de grupo de noticias, crear un nuevo par de claves PGP, desvincularse de los mensajes anteriores
- Cada miembro se creará un nuevo sobrenombre

Los que fueron atrapados, fueron los que no siguieron las reglas al confiar demasiado en sus "amigos" online. Vimos esto en el arresto de Sabu cuando ayudó al FBI a arrestar a sus "amigos" en **LulzSec**.

Si a alguien se le ofreciera un trato para reducir la cantidad de tiempo que pasa en prisión a la mitad, es muy probable que lo aceptara a costa tuya. A continuación, se muestra un ejemplo de un alegato versus tratar de luchar contra los cargos en este caso concreto.

Siete de los sujetos estadounidenses se declararon culpables antes del juicio a una acusación de 40 cargos y recibieron sentencias federales que iban de 13 a 30 años en prisión. Los siete acusados restantes optaron por un juicio conjunto y simultáneo. Los siete fueron condenados por un jurado y posteriormente sentenciados a cadena perpetua.

13-30 años frente a cadena perpetua, pueden tentar incluso a algunos de los criminales más duros, y si crees que tu "amigo" online que nunca has conocido en persona va a mantener la boca cerrada para mantenerte fuera de la cárcel, sería gran sorpresa. Como pueden ver, el grupo era prácticamente un libro abierto para la policía. Fueron comprometidos completamente.

Sin embargo, a pesar de eso, la mayoría del grupo todavía permanece en libertad, y no fueron identificados ni arrestados. Esto se debe a las herramientas de privacidad (pgp, tor, **nymservers**, remailers) que se emplearon. Incluso siendo todo lo demás un libro abierto, aquellos que usan estas herramientas aún logran evadir la captura. Pero todavía puede estar diciendo: Ok, entiendo PGP, lo entiendo, pero ¿qué diablos es un servidor de ny y un remailer?

En pocas palabras, un **remailer anónimo** es un servidor que recibe mensajes (en este caso un correo electrónico) con instrucciones integradas sobre dónde enviarlos a continuación, y que los reenvía sin revelar de dónde provienen originalmente.

Un servidor de nymserver también conocido como remailer pseudónimo asigna a sus usuarios un nombre de usuario, y mantiene una base de datos

de instrucciones sobre cómo devolver mensajes al usuario real. Estas instrucciones generalmente involucran la red de remailer anónimo, protegiendo así la verdadera identidad del usuario.

Algunas de las ventajas de usar estos servicios son proteger al destinatario de un adversario y también proteger al remitente del mensaje. Algunos de estos servicios usan lo que se llama un buzón común, en el que todos los mensajes se almacenan en un buzón central sin encabezados "A y desde".

Depende de los usuarios que usan el servicio intentar usar sus claves PGP para tratar de descifrar todos los mensajes almacenados en el cuadro de mensaje central y ver si pueden descifrar alguno de ellos. Si pueden, este mensaje está destinado para ellos.

De esta manera se descarta de nuevo, el emisor y el receptor. Este sistema de remailers, también puede formar una cadena, en la que el mensaje se recupera de múltiples repetidores antes de llegar a su destinatario previsto para ampliar la brecha entre el emisor y el receptor.

Otra opción efectiva que ofrecen algunos servicios es la posibilidad de retrasar el envío del mensaje al siguiente servidor de la cadena o al propio destinatario. Si nos encuentra que estamos enviando tráfico cifrado PGP a través de algún tipo de análisis a las 5:00 PM, y otra persona que está siendo monitorizada lo recibe a las 5:01 PM, es más fácil correlacionar que este mensaje pudo venir de nosotros a la otra persona.

Dejando de lado mis sentimientos personales sobre los pedófilos, trajimos este caso, como un ejemplo por varias razones:

1. La pornografía infantil es un delito grave en prácticamente todas las jurisdicciones y países. Como demuestra este ejemplo, la policía trabajará en conjunto, incluso a través de fronteras nacionales, para investigar estos crímenes. Ellos están dispuestos invertir un tiempo considerable, mano de obra y dinero en la búsqueda de estos sospechosos. Los únicos otros crímenes que generalmente merecen este tipo de enfoque son el tráfico de drogas / armas o el terrorismo.

   El nivel de esfuerzo gastado en la búsqueda de este grupo se puede ver en que, incluso el subdirector ejecutivo del FBI J. Stephen Tidwell estuvo involucrado.

   Normalmente, uno no esperaría que el personal del FBI de la dirección participase, esto muestra el nivel de importancia que se le otorga a esta particular investigación (Un año después, el mismo Yardbird, expresó el asombro de que el FBI considera a su grupo como una prioridad).

2. Este caso es el único que conozco, donde los sospechosos utilizaban herramientas sofisticadas como PGP, Tor, remailers anónimos y nymservers.
3. Este caso subraya la efectividad de estas herramientas incluso contra oponentes poderosos y bien financiados como el FBI, Europol e Interpol. Aquellos que fueron atrapados utilizaron inapropiados herramientas y técnicas ineficaces para protegerse.
4. Entiendo completamente el disgusto de la mayoría de la gente por los tipos de crímenes/criminales discutidos aquí. Dicho esto, es importante recordar que uno simplemente no puede diseñar un sistema que proporcione protección para una clase de personas, pero se la niegue a otras. No se puede ni se debe, por ejemplo, implementar un sistema que proporcione privacidad/anonimato para los disidentes políticos, o los denunciantes, y se lo niega a los pedófilos, **o todos** están a salvo, **o nadie.**

Resumiendo, hemos visto que incluso los delincuentes más perseguidos pueden evadir la captura cuando usan criptografía robusta y sistemas de **ciberseguridad** de forma apropiada. El líder del Ring User de uno de los anillos de pornografía infantil más investigados todavía permanece prófugo hoy en día porque siguieron las reglas.

42. Escondiéndote de tu ISP - Puentes y transporte

Esta parte del post va a hablar sobre algo que se ha discutido comúnmente ¿Cómo puedo ocultar mi uso de tor de mi **ISP**?

La gente está más preocupada por ocultar su uso de TOR a su ISP, que por esconderlo en una VPN. Parece haber un debate de ida y vuelta sobre si usar una VPN nos protegerá o no. Si la VPN puede ser convencida o no para registrar nuestra conexión, etc.

He comentado anteriormente cómo los anillos de pedófilos, LulzSec y YardBird han demostrado que históricamente se sabe que quienes confían en las VPN para protegerse, terminan en la cárcel. Incluso nuestro amigo The Grugq indica que TOR -> VPN está bien, pero los que usan VPN -> TOR, van a la cárcel.

Anteriormente hablamos sobre VPN -> TOR y TOR -> VPN, y tratamos de mantenernos neutrales. Pero recuerda, al final del día, nadie va a ir a la

cárcel por ti. Si simplemente quieres ocultar el hecho de que estás utilizando a tu ISP, entonces tenemos otras opciones aparte de una VPN. Tenemos Bridges y varios transportes conectables diferentes. ¿Qué son los bridges y cómo podemos usarlos en Tails?

43. ¿Qué son los Bridges? y, ¿cuándo usarlos?

Al utilizar TOR con Tails en su configuración predeterminada, cualquier persona pueda observar el tráfico de nuestra conexión a Internet (por ejemplo, tu proveedor de servicios de Internet y tal vez el gobierno y las agencias encargadas de hacer cumplir la ley) pueden saber que estamos utilizando TOR.

Esto puede ser un problema si se encuentra en un país donde se aplica lo siguiente:

1. El uso de TOR está bloqueado por la censura: dado que todas las conexiones a Internet están obligadas a pasar por TOR, esto haría que Tails sea inútil para todo, excepto para trabajar sin conexión en documentos, etc.

2. Usar Tor es peligroso o se considera sospechoso: en este caso, iniciar Tails en su configuración predeterminada puede ocasionarte serios problemas.

Los **Bridges TOR**, también llamados relés de puente Tor, son puntos de entrada alternativos a la red Tor que no están todos públicamente enumerados. El uso de un puente hace que sea más difícil, pero no imposible, que nuestro proveedor de servicios de Internet sepa que estamos utilizando TOR.

Lo primero que vamos a hacer es obtener **algunos puentes TOR**. Debemos obtener los mismo antes de configurar Tails para usar puentes, porque una vez que Tails esté en modo bridge, no podremos conectarnos a tor sin puentes de trabajo.

Deberías obtener una lista de puentes como se ve aquí. Estos son puentes reales extraídos de la página de puentes TOR.

> 5.20.130.121:9001 63dd98cd106a95f707efe538e98e7a6f92d28f94
> 106.186.19.58:443 649027f9ea9a8e115787425430460386e14e0ffa

69.125.172.116:443
43c3a8e5594d8e62799e96dc137d695ae4bd24b2

Estos puentes están disponibles públicamente en el sitio web de Tor Project, por lo que pueden ser o no la mejor opción para usar, pero son un buen comienzo. Otra opción es enviar un correo electrónico a **bridges@bridges.torproject.org** con un mensaje en el cuerpo que diga "**get bridges**" sin las comillas. Solo funcionará si se envía desde una cuenta de Gmail o Yahoo.

Si deseáis usar esto, configurad la cuenta de correo electrónico usando TOR y recibiréis una lista de alrededor de 3 puentes poco después. Guardadlos en algún lugar donde los podáis usar la próxima vez que iniciéis Tails.

Ya tenemos nuestros puentes. ¿Cómo usamos puentes en Tails? Esta, es una opción que debemos activar cuando iniciamos Tails. Para activar el modo bridge, agregaremos la opción de inicio del puente al menú de inicio. El menú de inicio es la primera pantalla que aparece cuando se inicia Tails. Es la pantalla negra que dice Boot Tails y le da dos opciones. 1-Live, 2- Live (Fail Safe).

Cuando os encontréis en esta pantalla, presione Tab y aparecerá una lista de opciones de inicio en forma de texto en la parte inferior de la pantalla. Para agregar una nueva opción de inicio, agregad un espacio y luego escribid "bridge" sin las comillas y presionad Entrar.

Ya hemos activado el modo puente. Una vez que Tails se iniciad por completo, recibiréis una advertencia de que hemos entrado en el modo bridge y no eliminaremos la dirección IP predeterminada, que es 127.0.0.1.

Este es un consejo que seguiremos, así que simplemente haced clic en Aceptar y aparecerá la ventana de configuración para TOR. En este punto, necesitamos agregar nuestros puentes. Cogemos los tres puentes que obtuvimos e ingresamos la dirección IP y el puerto. Si fuéramos a usar el ejemplo anterior, esto es a lo que ingresaríamos:

5.20.130.121:9001
106.186.19.5:443
69.125.172.116:443

Para cada puente que agreguemos, escribidlo en el cuadro de texto disponible donde dice "Agregar un puente" y luego haced clic en el botón verde + para agregar ese puente. Tendremos que agregar un puente cada vez. Una vez que hayamos terminado de agregar los bridges, podemos hacer clic en Aceptar.

En este punto, nuestro ícono de cebolla amarilla en la esquina superior derecha se volverá verde poco después, y se conectará a la red TOR mediante Bridge. Y dado que es menos probable que tu ISP conozca estos puentes, es menos probable que sepan que estamos usando TOR cuando usamos Bridge.

Sin embargo, es posible que deseemos buscar esos puentes antes de usarlos. Tal vez queramos saber dónde están ubicados, quizás queramos ver quién está alojando el bridge. Podemos hacerlo buscando un servicio de búsqueda de IP online, haciendo una búsqueda y escribiendo la dirección IP. Las tres IPs listadas arriba están ubicadas en las siguientes ubicaciones:

5.20.130.121 - País: Lituania
106.186.19.58:443 - País: Japón
69.125.172.116:443 - País: Nueva Jersey, Estados Unidos

Y con eso, podemos decidir qué puente sería una mejor opción para nuestro uso. Sin embargo, sugiero que vayas y obtener nuevos puentes y que no utilices los que he enumerado anteriormente por razones obvias, ya que ahora están vinculados a los usuarios del blog.

Debo señalar que la forma en que los bridges ocultan el hecho de que estamos usando TOR desde nuestro ISP, es que nos estamos conectado a una dirección IP que probablemente nuestro ISP desconoce si está afiliada a nodos de entrada TOR.

Si bien los bridges son una buena idea, pueden no ser suficientes. Según **Jacob Applebaum**, (un desarrollador de Tor), el tráfico bridge sigue siendo vulnerable a algo llamado DPI (**inspección profunda de paquetes**) para identificar los flujos de tráfico de Internet por protocolo, en otras palabras, pueden averiguar que estamos usando TOR mediante el análisis del tráfico.

Mientras TOR utiliza relés puente para evitar un censor que bloquea por dirección IP, el censor puede usar DPI para reconocer y filtrar los flujos de tráfico, incluso cuando se conectan a direcciones IP inesperadas.

Es menos probable que nuestro ISP lo haga, pero es bastante más probable que lo haga la NSA, u otros gobiernos opresores como China e Irán.

Últimamente, los censores han encontrado formas de bloquear TOR incluso cuando los clientes están utilizando puentes. Por lo general, lo hacen instalando cuadros en los ISP que miran el tráfico de la red y detectan TOR; cuando se detecta TOR, bloquean el flujo de tráfico.

Para eludir esa censura tan sofisticada, TOR introdujo **Pluggable Transports** o **puentes ofuscados**. Estos puentes usan complementos

especiales llamados transportes conectables que ofuscan el flujo de tráfico de TOR, lo que dificulta su detección.

Los **Pluggable Transports** son una tecnología más nueva, que está siendo implementada por TOR para disfrazar el hecho de que estamos usando TOR por nuestro ISP y otros censores. Como se mencionó anteriormente, intenta transformar nuestro tráfico en un tráfico de aspecto inocente que con suerte no se distinguiría del tráfico normal de navegación web.

Actualmente, los Pluggable Transports más populares son puentes ofuscados. La ofuscación, por definición, es la ocultación del significado pretendido en la comunicación, haciendo que la comunicación sea confusa, intencionalmente ambigua y más difícil de interpretar.

Los puentes ofuscados en realidad transforman el tráfico para que parezcan paquetes de datos aleatorios. Los puentes ofuscados actualmente tienen 2 protocolos.

1. **Obfs2** (The Twobfuscator).

Para los no expertos, básicamente obfs2 usa un protocolo que disfraza el tráfico para que parezca información aleatoria, mientras que TOR tiene una estructura más distinta.

Sin embargo, debe observarse en el caso de obfs2 que, si un atacante esnifa el "saludo inicial" entre el ordenador y el puente ofuscado, podría obtener la clave de encriptación utilizada para disfrazar nuestro tráfico y usarlo para descifrar el tráfico disfrazado que revelaría el verdadero tráfico.

No podrían descifrar tu tráfico, pero podrían ver que estás usando TOR. Es probable que esto no sea algo que nuestro ISP haría, pero puede ser algo que la aplicación de la ley o la NSA haría. Si solo estamos preocupado por nuestro ISP, obfs2 probablemente valdría.

2. **Obfs3** (The Threebfuscator).

Obfs3 usa un protocolo muy similar para disfrazar nuestro tráfico como obfs2, sin embargo, utiliza un método más avanzado de **handshake** inicial llamado intercambio de claves **Diffie Hellman**.

Sin embargo, encontraron algunas vulnerabilidades en el protocolo y tuvieron que ir un paso más allá y personalizar el intercambio de claves de Diffie Hellman para que sea un método aún más sólido para establecer ese Handshake inicial. Usar obfs3 sería la mejor opción para "disfrazar" el tráfico si tu adversario es la NSA o las fuerzas del orden público.

¿Cómo obtenemos esos puentes ofuscados? No son tan fáciles de obtener, pero se pueden obtener a través del correo electrónico anterior. Sin embargo, debemos solicitar esos puentes específicamente para obtenerlos.

Debemos usar una cuenta de Gmail o Yahoo y enviar un correo electrónico a **bridges@bridges.torproject.org** e ingresar en el cuerpo del correo electrónico "**transport obfs2**" sin las comillas, y para obfs3, simplemente ingrese "**transporte obfs3**". Ten en cuenta que solo podemos enviar una solicitud a Tor por correo electrónico, cada 3 horas. Cuál debemos usar, es nuestra elección. Introdúcelos de en este formato para que Tails sepa qué protocolo usar:

obfs3 83.212.101.2:42782
obfs2 70.182.182.109:54542

TOR también proporciona algunos puentes ofuscados en su página de inicio que también podemos usar, y los enumeraremos a continuación. Si enviamos una solicitud a TOR y obtenemos una respuesta que contiene bridges sin obfs2 u obsf3 al principio de las líneas, estos son puentes normales, no ofuscados, y es probable que estemos fuera de los puentes ofuscados, teniendo que intentarlo nuevamente otro día.

Si obtenemos una respuesta con bridges que no tienen obfs2 o 3 al comienzo de cada línea, ten en cuenta que estos son puentes normales, a diferencia de los que se muestran a continuación:

obfs3 83.212.101.2:42782
obfs3 83.212.101.2:443
obfs3 169.229.59.74:31493
obfs3 169.229.59.75:46328
obfs3 209.141.36.236:45496
obfs3 208.79.90.242:35658
obfs3 109.105.109.163:38980
obfs3 109.105.109.163:47779
obfs2 83.212.100.216:47870
obfs2 83.212.96.182:46602
obfs2 70.182.182.109:54542
obfs2 128.31.0.34:1051
obfs2 83.212.101.2:45235

Tengo la sensación de que algunos de vosotros os sentiréis inclinados a salir y obtener algunos puentes de obfs3 de inmediato, porque creen que son la mejor opción para mantenerse anónimos. Y ahora tienen el potencial de ser lo que esperan en ese sentido, a excepción de un gran defecto. El número de puentes obfs3 es limitado.

Por lo tanto, mientras obfs3 es la opción más segura (ya tenemos obfs4), **su número limitado de puentes disponibles** nos uniría a un grupo pequeño que no nos brindaría mucho anonimato. En este momento, se necesita una mayor cantidad de bridges, y esto es un factor que debemos tener en cuenta cuando utilizamos bridges ofuscados.

Una de las soluciones a este problema de escasez es ejecutar nuestro propio puente ofuscado. Si estamos interesado hacerlo, debemos, comprar algunos VPS y configurarlos como obxs obfs3 o obfs4.

Una de las mejores opciones para hacerlo es de esta manera poder configurarlo para que sea un puente oculto privado y, por lo tanto, no lo daremos a conocer al público. Luego podemos conectarnos a nuestro propio puente privado obfs3/4. Pero nuevamente, asegúrate de confiar en ordenador que estamos utilizando, de lo contrario, no es más seguro que una VPN.

Otra posible solución a la falta de puentes ofuscados puede ser otra opción de Pluggable Transports, algo llamado **proxy flash**. Cuando pensamos en un proxy flash, piensas en las características de un flash, de vida rápida y corta.

Este protocolo fue desarrollado por un desarrollador de TOR que asistió a la Universidad de Stanford, y la idea es que las direcciones IP utilizadas cambien más rápido de lo que una agencia censuradora puede detectarlas, rastrearlas y bloquearlas.

Este método es similar al uso de puentes normales, ya que oculta el hecho de que nos estamos conectando a direcciones IP que se sabe que están relacionadas con TOR, incluso cuando las direcciones IP del puente enumeradas por TOR son descubiertas por nuestro ISP o la policía.

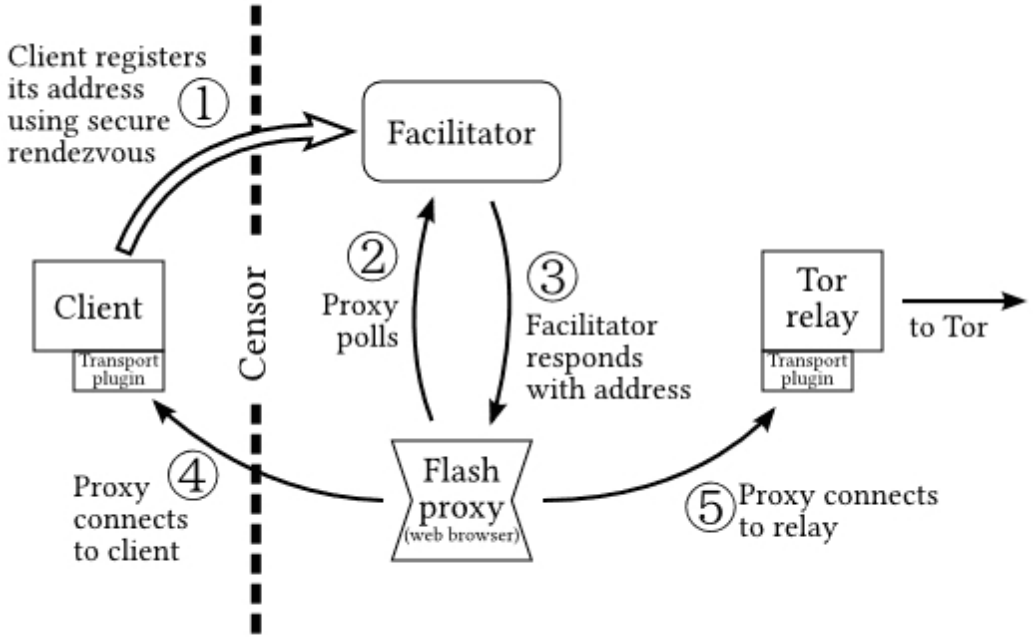
Sin embargo, esto no oculta el hecho de que estemos usando el programa si alguien está analizando nuestro tráfico usando DPI (inspección profunda de paquetes).

El principal beneficio de esta opción es que los proxies son administrados por muchas personas en todo el mundo. Se ejecutan cuando los usuarios de Internet aleatorios visitan una página web con un complemento específico que convierte su navegador en un proxy siempre que estén en esa página.

Básicamente estamos usando la conexión de otra persona a través de su navegador para conectarnos a un TOR. Solo estamos utilizando 1 conexión activa en cada momento, pero tenemos alrededor de 5 conexiones establecidas con diferentes proxies en caso de que nuestra conexión activa se caiga, entonces podemos comenzar a usar otro proxy en su lugar.

Además del cliente y el relé TOR, ofrecemos tres nuevas piezas. El cliente TOR se pone en contacto con el facilitador para anunciar que necesita una conexión (proxy). El facilitador es responsable de realizar un seguimiento de los clientes y los apoderados, y asignarlos a los demás.

El proxy flash sondea al facilitador para los registros de los clientes, luego comienza una conexión con el cliente al recibir una petición. Los complementos de transporte en el cliente, retransmiten la conexión entre **WebSockets** y TCP simple.



Una sesión de muestra puede ser así:

1. El cliente inicia Tor y el programa de complemento de transporte del cliente (flashproxy-client), envía un registro al facilitador mediante una cita segura. El complemento de transporte del cliente comienza a escuchar una conexión remota.
2. Un proxy flash entra online y sondea al facilitador.
3. El facilitador devuelve un registro de cliente, informando al proxy flash dónde se conecta.
4. El proxy realiza una conexión saliente con el cliente, que es recibida por el complemento de transporte del cliente.

5. El proxy realiza una conexión de salida al plugin de transporte en el relé TOR y comienza a enviar y recibir datos entre el cliente y el relevo.

En otras palabras, terminas yendo desde el ordenador, al proxy, luego al proxy y al Tor retransmisor.

La razón por la que esto es necesario es porque el cliente no puede comunicarse directamente con el relevo. (Quizás el censor haya enumerado todos los relevos y los haya bloqueado por la dirección IP).

En el diagrama de arriba, hay dos flechas que cruzan el límite del censor, esto es por lo que pensamos que están justificados.

La conexión inicial del cliente con el facilitador (el registro del cliente) es una comunicación de solo escritura de ancho de banda muy bajo que idealmente puede ocurrir solo una vez durante una sesión. Un protocolo de encuentro cuidadoso, lento y especializado puede proporcionar esta comunicación inicial.

La conexión del proxy flash al cliente proviene de una dirección IP que el censor nunca había visto antes. Si estamos bloqueado en unos minutos, está bien, hay otros proxies alineados y esperando para proporcionar el servicio.

Sé que esto podría ser un poco complicado, pero realmente no es necesario que comprendas cómo funciona para beneficiarnos de él. También podríamos estar preguntando sobre alguien que simplemente bloquea su capacidad al conectarse con el facilitador (el proveedor de los "poderes").

Pero, la forma en que realmente se conecta con el facilitador es de una manera muy especial que ha diseñado Tor, y esto está integrado en el plugin de transporte del proxy flash.

La forma en que el cliente se registra con el facilitador es un paso de encuentro especial que no se comunica directamente con el facilitador, diseñado para ser encubierto y muy difícil de bloquear.

La forma en que esto funciona en la práctica es que el complemento de transporte del cliente de proxy flash realiza una conexión TLS (HTTPS) a Gmail y envía un correo electrónico cifrado desde una dirección anónima (**nobody@localhost**) a una dirección especial de registro del facilitador.

El facilitador revisa este buzón periódicamente, descifra los mensajes e inserta los registros que contienen. El resultado es que cualquier persona que pueda enviar correos electrónicos a una dirección de Gmail puede hacer una cita, incluso si el facilitador está bloqueado.

Dos preguntas que te deberías estar haciendo:

1. ¿Puedo confiar en los proxies y/o facilitadores?
2. ¿Cómo uso esto?

Bueno, el facilitador es elegido y actualmente solo lo dirige TOR, por lo que puedes tomarlo al pie de la letra. En lo que respecta a los proxies, los proxies en sí mismos pueden o no ser confiables, y este es el riesgo que corremos cada vez que usamos TOR. Los puentes que utilizas pueden verse comprometidos, tus nodos de entrada, tus nodos de salida, cada salto posible en el camino a internet puede verse comprometido en cualquier momento.

Afortunadamente, incluso si el proxy está en peligro y registrando nuestro tráfico, solo podremos ver tráfico encriptado. Y como mencioné anteriormente, cualquiera que visite una página web con un complemento específico se convertirá en un proxy flash siempre que se encuentre en ese sitio.

Esto significa que algunas personas serán un proxy flash sin su conocimiento, y otras serán representantes instantáneas porque quieren serlo. La idea detrás de esto es tener múltiples usuarios, decenas de miles, si no cientos de miles de servidores proxy flash disponibles en todo momento para aumentar la cantidad de direccionamiento IP posibles entre las que rotaría para mantener a nuestro ISP y posiblemente la NSA entretenidos.

¿Usamos esto? En realidad, actualmente no es compatible con Tails. Pero se puede usar con **TOR Pluggable Transports** y TOR Browser Bundle fuera de Tails.

Básicamente se trata de habilitar el reenvío de puertos sobre el puerto 9000, agregando "**bridge flashproxy 0.0.1.0:1**" sin las comillas, a nuestro torrc, y dejar todo lo demás a menos que necesitemos usar un puerto diferente, lo cual es poco probable. Es posible que debamos hacer una excepción en nuestro firewall para el complemento flashproxy si nos lo pide.

Siempre y cuando estemos utilizando el paquete Tor Browgable Transports Tor Browser, debería ser bastante fácil hacer funcionar esta característica.

Intenta configurar puentes normales, luego intenta hacer los puentes ofuscados, y una vez que los obtengas, entonces, considera hacer los proxies flash para practicar. Hazte algunas preguntas, ¿solo quiero ocultar el hecho de que estoy usando TOR desde mi ISP? ¿O me estoy escondiendo de alguien mucho más grande que eso?

Considera si es plausible que ejecute un proxy privado ofuscado, o incluso un puente privado. Ya tienes suficiente información para tomar una decisión informada.

Actualmente, hay otros transportes conectables actualmente en desarrollo, pero aún no están implementados. Os contamos algunos proyectos:

- **ScrambleSuit** es un Pluggable Transports que protege contra los ataques de sondeo de seguimiento y también es capaz de cambiar su huella digital de red (distribución de la longitud del paquete, tiempos entre llegadas, etc.). Es parte del marco Obfsproxy.
  Estado: no desplegado
- **StegoTorus** es una bifurcación de Obfsproxy que la extiende a TOR a través de conexiones múltiples para evitar firmas de tamaño de paquete. Incorpora los flujos de tráfico en trazas que se parezcan a html, JavaScript o pdf.Mantenido por Zack Weinberg.
  Estado: no desplegado
- **SkypeMorph** transforma los flujos de tráfico de TOR para que se vean como si fuera un vídeo de Skype.
  Estado: no desplegado
- **Dust** proporciona un protocolo resistente a DPI basado en paquetes (en lugar de en conexiones).
  Estado: no desplegado
- El Cifrado de **Transformación de Formato** (**FTE**) transforma el tráfico TOR en formatos arbitrarios usando las descripciones de idioma.
  Estado: no desplegado

44. Capacidades de la NSA

En un video de 1 hora uno de los desarrolladores de TOR, **Jacob Applebaum** habla sobre las capacidades legitimadas y confirmadas de la NSA de los documentos filtrados de la FOIA que muestran cuán técnicamente capaz es la NSA.

En cualquier lugar, desde simples puertas traseras, volando un avión no tripulado sobre la parte superior de nuestra casa para esnifar paquetes, moldear inyectando chips de puerta trasera en la carcasa del ordenador, y transferir energía a nuestra casa. Nada de esto es teoría de la conspiración,

todo está confirmado con los documentos que se muestran en su presentación.

45. ¿Por qué siempre debemos respaldar las transmisiones?

Esto es una historia embarazosa de algo que ha sucedió en los últimos días, y fue una lección bien aprendida, ya que algunas de las cosas que he perdido no serán recuperables. - Jolly Roger.

¿Tienes un wallet de Bitcoin guardados en una unidad flash? ¿Qué pasaría si perdiésemos nuestra memoria USB? ¿Tenemos respaldo? ¿Qué pasaría si tus archivos se corrompieran, y no pudiéramos recuperarlos? ¿podríamos vivir con eso? ¿Tienes ciertas cosas que nos causarían un gran problema si las perdiésemos? Entonces, es mejor que comiences a hacer copias de seguridad de tus discos con regularidad, mejor aún, **¡hazlo todos los días!**

Soy del tipo de personas que generalmente realiza copias de seguridad de sus archivos con regularidad, pero desafortunadamente a la gran cantidad de eventos extraños que ocurren online últimamente con **Utopía** derribado, foros de BMR siendo confiscados y demás, no había respaldado mis archivos en aproximadamente 2 semanas. Tenía todos mis archivos más recientes, incluyendo algunos nuevos monederos de Bitcoin con saldos en ellos en mi unidad portátil principal y, además, esta unidad estaba encriptada.

Entonces, sin previo aviso, de repente recibí un error de que el sistema de archivos estaba dañado y mi disco no se podía leer. No importa, si tienes una unidad no cifrada, simplemente puedes ejecutar un programa de recuperación de datos como **testdisk**. Instálalo cuanto antes: **sudo apt-get install testdisk.**

Al utilizar este programa, es probable que podamos recuperar la mayoría de nuestros archivos porque ignora los encabezados del sistema de archivos y otros tipos de organización de archivos necesarios para identificar la forma en que se almacenan los mismos.

El problema en mi caso, fue que todos mis archivos fueron encriptados. Esto significa que, para descifrar los archivos, necesitaba un archivo de clave que se almacena en la unidad para desbloquear los mismos. Si este archivo de clave se daña, incluso si tenemos la contraseña para los archivos, no los recuperaremos.

La clave es exclusiva de esa instancia particular cuando se cifró la unidad. Lo que significa que incluso si tratamos de volver a crear el archivo de clave con la misma contraseña, el resultado sería un archivo de clave diferente. Esto significa esencialmente que mis datos son irrecuperables, porque mi archivo de claves estaba corrupto de alguna manera.

La tecnología es delicada, los datos se almacenan en forma de frecuencias magnéticas y no hay garantía de que los archivos no se corrompan un día sin razón aparente.

Inundación, huracanes, sobre-voltaje, incendio, daños por humedad, pisar accidentalmente el disco, un miembro de la familia (generalmente un niño) lo rompe, lo pierde, derrama agua sobre él, sobre calentamiento, etc.

Todo esto podría ocasionar que tus datos o unidades se dañen y pierdan todos sus datos. Es por eso que **necesita un mínimo de 2 copias de seguridad**. No 1, sino 2. Y ten una de tus copias de seguridad almacenadas preferiblemente fuera de tu hogar. Si trabajas, almacénelo en el trabajo o en tu coche, o en algún lugar al que puedas acceder regularmente, y trata de hacer una copia de seguridad de tus datos con la mayor frecuencia posible.

Si tu casa se quema y mantenemos todas las copias de seguridad en casa, perdemos todo. Si conservaste una copia en el trabajo, puedes recuperarlo. Cuantas más copias de seguridad, mejor, siempre que estén cifradas. Cada vez que creemos un nuevo wallet y transfiramos Bitcoin a ella, haz una copia de seguridad.

Cada vez que configures una nueva cuenta o un nuevo correo electrónico con una contraseña única (debería ser cada vez una), haz una copia de seguridad. Haz copia de seguridad de todo.

Por suerte para mí, mi wallet principal era recuperable con la mayoría de mis monedas, pero perdí algunas monedas, que nunca puede recuperar, confía en mí, lo intenté de verdad. Obtener unidades USB adicionales o tarjetas SD es muy barato, por lo que debemos gastarnos unos euros extra para tener copias de seguridad múltiples, podrían terminar perdiendo datos que costarían mucho más de lo que hubiese costado tener algunas unidades adicionales por ahí como copias de seguridad.

46. Hablemos de seguridad

A raíz del exploit **Freedom Hosting**, creo que deberíamos reevaluar nuestro modelo de amenaza y actualizar nuestra seguridad para protegernos mejor de las amenazas reales a las que nos enfrentamos.

Por esto escribo sobre estos temas, para iniciar una larga conversación, pero de ninguna forma es algo integral, trato de enfocarme en la seguridad técnica. Quizás otros puedan abordar el envío y la seguridad financiera.

Agradezco desde aquí sus futuros comentarios y me gustaría que estas ideas puedan ser criticadas de manera constructiva, pero por supuesto, también ampliadas y actualizadas.

Mientras se desarrollaba este post, decidimos dar un paso atrás y hacernos una pregunta básica: ¿cuáles son nuestros objetivos? Me he propuesto dos objetivos básicos que queremos lograr con nuestra seguridad técnica:

1. Evita ser identificado.
2. Minimiza el daño cuando somos identificados.

Podemos pensar en estos puntos como nuestros *"principios de seguridad"*. Si tienes una pregunta de seguridad técnica, puedes llegar a una respuesta haciéndote estas preguntas:

1. ¿El uso de esta tecnología aumenta o disminuye las posibilidades de que me identifiquen?
2. ¿El uso de esta tecnología aumenta o disminuye el daño (p. Ej., La evidencia que se puede usar en mi contra) cuando me identifican?

Obviamente, deberemos comprender la tecnología subyacente para responder estas preguntas.

El resto de esta guía explica las amplias características tecnológicas que disminuyen las posibilidades de que seamos identificados y que minimizan el daño cuando somos identificados.

Hacia el final, enumero tecnologías específicas y las evalúo basadas en estas características.

En primer lugar, permítanme enumerar las amplias características que se me han ocurrido, y luego las explicaré.

1. Simplicidad
2. Confiabilidad
3. Ejecución mínima del código que no es de confianza
4. Aislamiento

5. Cifrado

Hasta cierto punto, nos hemos estado enfocando en cosas equivocadas. Principalmente, me han preocupado los ataques a la capa de red o los "ataques a la red TOR", pero ahora me parece claro que es mucho más probable que los ataques de la capa de aplicación nos identifiquen.

Las aplicaciones que ejecutamos sobre TOR representan una superficie de ataque mucho más grande que TOR. Podemos minimizar nuestras posibilidades de ser identificados asegurando las aplicaciones que ejecutamos sobre TOR.

47. Simplicidad en ciberseguridad

A menos que no usemos ordenador, podemos minimizar las amenazas contra nosotros simplificando las herramientas tecnológicas que usamos. Es menos probable que una base de código más pequeña tenga errores, incluidas vulnerabilidades. Es menos probable que una aplicación más simple se comporte de formas inesperadas y no deseada.

Como ejemplo, cuando el Proyecto TOR evaluó las huellas dejadas por el paquete del navegador, encontraron 4 rastros en **Debian Squeeze**, que usa el entorno de escritorio Gnome 2, y 25 huellas en Windows 7. Está claro que Windows 7 es más complejo, y se comporta de formas más inesperadas que Gnome 2.

Sólo a través de su complejidad, Windows 7 aumenta su superficie de ataque y lo expone a más amenazas potenciales. (Aunque hay otras formas en que Windows 7 también lo hace más vulnerable).

Las huellas que quedan en Gnome 2 son más fáciles de prevenir que las huellas dejadas en Windows 7, por lo que al menos con respecto a esta amenaza específica, Gnome 2 es deseable en Windows 7.

Entonces, al evaluar una nueva herramienta tecnológica por simplicidad, debemos hacernos estas preguntas:

- ¿Es más o menos complejo que la herramienta que estoy usando actualmente?
- ¿Realizo más o menos funciones (innecesarias) que la herramienta que estoy usando actualmente?

48. Confiabilidad en ciberseguridad

Deberíamos favorecer las tecnologías que son construidas por profesionales o personas con muchos años de experiencia en lugar de newbs. Un claro ejemplo de esto es **CryptoCat**, que fue desarrollado por un programador aficionado bien intencionado, y ha sufrido severas críticas debido a las muchas vulnerabilidades que se han descubierto.

Deberíamos favorecer las tecnologías que son de código abierto, tienen una gran base de usuarios y un largo historial de uso, ya que se revisarán más a fondo.

Al evaluar una nueva herramienta tecnológica para la confiabilidad, hazte estas preguntas:

- ¿Quién escribió o construyó esta herramienta?
- ¿Cuánta experiencia tiene?
- ¿Es de código abierto y cómo de grande es la comunidad de usuarios, revisores y colaboradores?

49. La ejecución mínima del código que no es de confianza

Las dos primeras características suponen que el código es de confianza, pero tenemos posibles problemas no deseados. Esta característica supone que, como parte de nuestras actividades de rutina, es posible que tengamos que ejecutar un código arbitrario que no sea de confianza.

Este es un código que no podemos evaluar de antemano. El principal lugar donde esto sucede es en el navegador, a través de complementos y scripts.

Deberíamos evitar por completo ejecutar código que no sea de confianza, si es posible. Hazte estas preguntas:

- ¿Son las características que proporciona absolutamente necesarias?
- ¿Hay alternativas que brinden estas características sin requerir a complementos o scripts?

50. Aislamiento en ciberseguridad

El aislamiento es la separación de componentes tecnológicos con barreras. Minimiza el daño ocasionado por los exploits, por lo que, si se explota un componente, otros componentes seguirán protegidos. Puede ser nuestra última línea de defensa contra los exploits de la capa de aplicación.

Los dos tipos de aislamiento son, físicos (o basados en hardware) y virtuales (o basados en software). El aislamiento físico es más seguro que el aislamiento virtual, porque las barreras basadas en software pueden ser explotadas por códigos maliciosos. Preferimos el aislamiento físico sobre el aislamiento virtual.

Al evaluar las herramientas de aislamiento virtual, hazte las mismas preguntas sobre la simplicidad y la confiabilidad en ciberseguridad. ¿Esta tecnología de virtualización realiza funciones innecesarias (como proporcionar un portapapeles compartido)? ¿Cuánto tiempo ha estado en desarrollo y cuán exhaustivamente se ha revisado? ¿Cuántos exploits se han encontrado?

51. Cifrado en ciberseguridad

La encriptación es una de las dos defensas que tenemos para minimizar el daño cuando somos identificados. Cuanta más encriptación usemos, mejor estará. **En un mundo ideal, todos sus medios de almacenamiento estarían encriptados**, junto con cada correo electrónico y mensaje que enviemos.

La razón de esto es porque, cuando algunos correos electrónicos se cifran, pero otros no, un atacante puede identificar fácilmente los correos electrónicos interesantes.

Podemos aprender con quién se comunica con las partes interesantes, porque esas serán a las que se enviarán correos electrónicos encriptados (esto se conoce como fuga de metadatos). Los mensajes interesantes se pierden con el ruido cuando todo está encriptado.

Lo mismo ocurre con el cifrado de medios de almacenamiento. Si almacenamos un archivo encriptado en un disco duro no encriptado, un adversario puede determinar trivialmente que todo lo bueno está en ese pequeño archivo o en los cifrados.

Pero cuando utilizamos el cifrado de disco completo, tenemos una negación más plausible de si la unidad contiene datos que serían interesantes para ese adversario, porque hay más razones para encriptar un disco duro completo que un solo archivo.

Además, un adversario que elude tu encriptación tendría que eliminar más datos para encontrar las cosas que le interesan.

El uso del cifrado implica un coste que la gran mayoría de la gente no puede soportar, por lo que, como mínimo, la información confidencial debe estar encriptada.

La otra defensa contra el daño es la eliminación segura de datos, pero eso lleva tiempo que podemos no tener. El cifrado es un borrado de datos seguro preventivo. Es más fácil destruir datos cifrados, ya que solo tenemos que destruir la clave de cifrado para evitar que un adversario acceda a los datos.

Finalmente, hablaremos sobre una función no técnica relacionada.

52. Comportamiento “seguro” en ciberseguridad

En algunos casos, la tecnología que utilizamos es sólo tan segura como nuestro comportamiento. La encriptación es inútil si nuestra contraseña es "**password**". TOR es inútil si le dices a alguien tu nombre. Puede sorprenderte lo poco que un adversario necesita saber sobre nosotros para identificarnos.

Algunas reglas básicas a seguir:

1. No le digas a nadie tu nombre.
2. No describas tu apariencia, ni la apariencia de ninguna posesión importante.
3. No describas a tu familia y amigos.
4. No le digas a nadie tu ubicación, más allá de un área geográfica amplia.
5. No le digas a las personas dónde viajarás con anticipación.
6. No revele los horarios y lugares específicos donde vives o visitaste en el pasado.
7. No discutas arrestos específicos, detenciones, altas, etc.
8. No hables de tu escuela, trabajo, servicio militar ni de ninguna organización con membresía oficial.
9. No hables de visitas al hospital.

En general, no hables de nada que nos vincule con un registro oficial de nuestra identidad.

53. Configuración “segura” en ciberseguridad

Debemos comenzar señalando que las características descritas anteriormente no son todas igual de importantes. El aislamiento físico es probablemente el más útil y puede protegernos incluso cuando ejecutamos código complejo y no confiable.

En cada una de las configuraciones a continuación, suponemos que tenemos un navegador completamente actualizado con scripts y complementos desactivados.

El término **"ocultación de sesión"** significa que alguien que mira nuestra conexión a Internet no sabe que está usando TOR. Esto es especialmente importante para los vendedores "no legales". Podemos usar bridges, pero he incluido VPN extra-jurisdiccionales como una capa adicional de seguridad.

Con esto en mente, aquí hay una lista descendente de configuraciones seguras para los usuarios de DarkNet, y como tal, trasladable a la ClearNet.

Aquí tenéis una sugerencia de configuración muy segura:

1. Un enrutador con una VPN + una caja central anónima con TOR + un ordenador que ejecute **Qubes OS**.

Ventajas: Aislamiento físico de TOR con las aplicaciones, aislamiento virtual de las aplicaciones entre sí, cifrado según sea necesario, ocultamiento de la membresía contra los observadores locales con VPN.

Desventajas: Qubes OS tiene una pequeña base de usuarios y no está bien probado o evolucionado.

2. **Anon middle box** (o enrutador con TOR) + Qubes OS.

Ventajas: Aislamiento físico de Tor de las aplicaciones, aislamiento virtual de las aplicaciones entre sí, cifrado según sea necesario.

Desventajas: Qubes OS tiene una pequeña base de usuarios y no está bien probado, no hay ocultación de sesión

3. Enrutador VPN + anon middle box + sistema operativo Linux.

Ventajas: Aislamiento físico de TOR con las aplicaciones, cifrado de disco completo, base de código bien probada si es una distribución importante como Ubuntu o Debian.

Desventajas: Ningún aislamiento virtual de aplicaciones entre sí.

4. Anon middle box (o enrutador con TOR) + SO Linux.

Ventajas: Aislamiento físico de TOR con las aplicaciones, cifrado de disco completo, base de código bien probada.

Desventajas: Sin aislamiento virtual de las aplicaciones entre sí, sin ocultación de la sesión.

5. Qubes OS sólo.

Ventajas: aislamiento virtual de TOR con las aplicaciones, aislamiento virtual de las aplicaciones entre sí, cifrado según sea necesario, ocultamiento de la sesión.

Desventajas: Sin aislamiento físico, no bien probado.

6. **Whonix** en un host de Linux.

Ventajas: Aislamiento virtual de TOR de las aplicaciones, cifrado de disco completo, ocultación de la sesión, se puede ejecutar una VPN en el host.

Desventajas: Sin aislamiento físico, sin aislamiento virtual de las aplicaciones entre sí.

7. **Cross**.

Ventajas: Cifrado y no deja rastro, los exploits a nivel de sistema se borran después del reinicio, relativamente bien probado.

Desventajas: Sin aislamiento físico, sin aislamiento virtual, sin ocultación de la sesión, sin guardas, persisten, pero podemos establecer bridges manualmente.

8. Whonix en otro host, como Windows o Mac.

Ventajas: Aislamiento virtual, encriptación (posible), ocultamiento de sesión (posible).

Desventajas: Sin aislamiento físico, sin aislamiento virtual de aplicaciones entre sí. Las Máquinas Virtuales están expuestas al mismo malware de Windows o similar.

9. Sistema operativo Linux.

Ventajas: Cifrado de disco completo (posible), ocultación de sesión (posible).

Desventajas: Sin aislamiento físico, sin aislamiento virtual.

10. Sistema operativo Windows.

Ventajas: cifrado de disco completo (posible), ocultación de sesión (posible).

Desventajas: ¡sin aislamiento físico, sin aislamiento virtual, el mayor objetivo de malware y exploits!

Suponiendo que hay un acuerdo general sobre el orden de esta lista, nuestro objetivo es configurar nuestros sistemas y configuraciones personales para estar lo más arriba posible en la lista.

"La seguridad al 100% no existe. Toda transacción realizada en internet, sea del tipo que sea, absolutamente toda, siempre deja un rastro en la red, y ningún sistema es seguro.

Así pues, de lo que se trata, es de dificultar al máximo el seguimiento de ese rastro, y de impedir que nuestro sistema pueda ser comprometido "en un tiempo asequible" para los ciberdelincuentes.

El tiempo es fundamental en esto, y lo que hoy no se puede atacar con éxito, mañana sí será vulnerable, y el rastro que hoy no se ve, mañana será totalmente claro y visible hasta para un corto de vista.

Espero haberos mostrado un amplio y, ojalá que interesante, conjunto de procedimientos y buenas prácticas de ciberseguridad, dignos de ser tenidos en cuenta por todos vosotros."

Fran Brizzolis