Traducción de Cedric Sagne

¿COMO HACER UN BLOG **DE MANERA ANONIMA?**

Hice esta guia práctica poniendome en la piel de un funcionario cuya intención es sacar a la luz informaciones sobre un escándalo del cual es testigo, en un país dónde puede ser peligroso hacerlo. Estos consejos no se destinan a expertos en criptografía, más bien a personas que viven en países donde no se respeta la libertad de expresión y que temen por su seguridad y quieren proteger su vida privada. Un artículo de la EFF (Electronic Frontier Foundation), una organisación norteamericana de defensa de las ciberlibertades "How to blog safely" (http://www.eff.org/Privacy/Anonymity/blog-anonymously.php), da informaciones prácticas complementarias sobre este tema.

INDICE

Presentamos a Sarah
Primera etapa: los seudonimos
Segunda etapa: ordenadores públicos
Tercera etapa: los proxis
Cuarta etapa: ¡Ahora si que es confidencial!
Quinta etapa: el "onion routing", con Tor
Sexta etapa: MixMaster, Invisiblog y GPG
¿Que podemos decir? ¿Dónde está el límite?

PRESENTAMOS A SARAH

Sarah trabaja como contable en los servicios del Estado. Se da cuenta de que su jefe, un ministro, se apropria de fondos públicos. Quiere que esto salga a luz, pero teme perder su puesto. Si lo habla con el ministro, siempre que obtenga una entrevista, será despedida. Habla con un periodista que trabaja para un periódico local, pero le contesta que no puede trabajar sobre este asunto con las escasas informaciones que ella tiene, y que necesita documentos para demostrar lo que afirma.

Sarah decide montar un blog, para desvelar lo que pasa en el ministerio. Para protejerse, quiere asegurarse de que nadie pueda descubrir su identidad a partir de su blog. Debe crear un blog anónimo. Existen dos maneras de descubrir la identidad de un bloger. La primera, cuando él mismo revela su identidad en el contenido. Por ejemplo, si Sarah dice "Soy la asistenta contable del Ministro de Minas", será muy fácil deducir su identidad. La otra manera de descubrir su identidad es explotar las informaciones entregadas por los navegadores, o los programas de correo electrónico. Un ordenador (Lat.América: computadora) conectado a la red (internet) tiene o comparte una dirección IP: cuarto números entre 0 y 255, separados por puntos. Por ejemplo: 213.24.124.38. Cuando Sarah utiliza su navegador para poner un comentario en el blog del ministerio, la dirección IP aparece en su mensaje. Investigando, los informáticos del ministerio encontrarán la identidad de Sarah con esta dirección IP. Si Sarah se conecta desde su casa, con un PAI (Proveedor de Acceso Internet), éste podrá establecer el vínculo entre la dirección IP que utiliza y su número de telefono. En ciertos países el ministro necesitará la autorisación del juez para obtener estas informaciones. En otros, y particularmente en los países dónde los proveedores de acceso son propiedad del Estado, el gobierno podrá obtener estas informaciones facilmente y Sarah acabará en una situación desagradable.

Sarah tiene varias maneras de esconder su identidad en la red. El grado de protección depende de los esfuerzos que esté dispuesta a hacer para esconderse. Cualquiera que desee hacer un blog de manera anónima tienen que decidir hasta qué punto quieren ir para proteger su identidad. Veremos a continuación que algunos de los medios empleados para proteger la identidad de un internauta necesitan amplios conocimientos técnicos y mucho trabajo.

PRIMERA ETAPA: LOS SEUDONIMOS

Una manera sencilla para Sarah de esconder su identidad es utilizar una cuenta de correo electrónico así como herramientas de blog gratuitas, ubicados en el extranjero (utilizando una cuenta de pago para el correo electrónico o el blog no puede ser, ya que las transacciones desvelarán una carta de crédito, una cuenta corriente o una cuenta paypal, y la identidad del bloger).

Sarah puede crear una falsa identidad, un seudonimo, que utilizará para estas cuentas. Cuando el ministerio encuentre su blog, descubrirá que pertenece a "A.N.O.Nimo" cuya dirección es anonyme.blogger@hotmail.com

Algunos proveedores de cuentas mail gratuitas:
Hotmail
Yahoo
Hushmail: cuentas gratuitas con encriptación
Algunas herramientas de blog:
Blogsome: herramienta de blog de Worldpress

Blogger
SEO Blog
Esta estrategia tiene un problema: cuando Sarah crea una cuenta mail o un blog, el proveedor de acceso registra su dirección IP. Si esta dirección esta asociada con el domicilio o el trabajo de Sarah, y si la empresa que gestiona el servicio de correo electrónico tiene la obligación de facilitar esta información, el ministerio podrá descubrir a Sarah. No es fácil obligar a los proveedores de servicios Web a entregar este tipo de información. Por ejemplo, para que Hotmail reconozca que Sarah tiene un contrato con ellos, el ministerio tendrá que obtener un mandato del juez, en colaboración con la agencia estadounidense de aplicación de leyes.
Pero Sarah no quiere correr el riesgo de que su gobierno consiga convencer a su proveedor de correo electronico de que desvele su identidad.

SEGUNDA ETAPA: LOS ORDENADORES PUBLICOS
Sarah puede también pensar en utilizar ordenadores públicos, es decir utilizados por muchas personas, para gestionar su blog. En vez de crear su blog o su cuenta de correo electónico desde casa o desde el trabajo, puede hacerlo a partir de una biblioteca o de un café de Internet. Cuando el ministerio averigüe la dirección IP utilizada para escribir los mensajes en el blog, descubrirá que se hizó desde un cibercafé, donde los ordenadores los utilizan muchas personas. Esta estrategia tiene desventajas. Si el cibercafé o el laboratorio de informática de la universidad tiene un registro de la identidad y de las horas de uso, entonces la identidad de Sarah está en peligro.Igualmente, deberá abstenerse de poner mensajes en mitad de la noche, cuando esté sola en el laboratorio de informática, ya que el empleado podrá acordarse de ella. Le será necesario cambiar de café de Internet a menudo, ya que si el ministerio se percata de que todos los mensajes proceden del “Café La Esquina”, es posible que envíen a alguien para averiguar quién coloca estos mensajes.

TERCERA ETAPA: LOS PROXIS ANONIMOS
Sarah no quiere tener que ir al “Café La Esquina” cada vez que quiere poner su blog al día. Con un vecino, efectúa un sistema que le permite acceder a Internet desde su propio ordenador, utilizando un proxi anónimo. Ahora, cuando utiliza su correo electrónico o su blog, la dirección que aparece es la del proxi, y ya no la de su ordenador. El ministerio tendrá más dificultades para encontrarla. Primero, obtiene una lista de proxis del internet con las palabras “servidor proxi” en Google. Por ejemplo, desde la lista en publicproxer.com, optando por proxis de categoría “High anonymity”. Apunta la dirección del proxi así como el puerto (ver el artículo “Como pasar la censura” para el uso de proxis). Entonces en las “preferencias” de su navegador, en “General”, “Red” o “Seguridad”, encontrará una opción que le permita entrar en la dirección y el puerto del proxi para el acceso a Internet (en el Firefox que utilizo, ésto se encuentra en “Preferencias”, “General”, “Parametros de conexión”).
Mete la dirección IP del proxi y el puerto en las secciones “proxy http” y “proxi SSL”, y los confirma. Después de cerrar el navegador, ahora navega por Internet con este proxi anónimo. La conexión es un poco más lenta. Esto se debe a que cada página que ve en pantalla tiene que pasar por un desvío. En vez de conectarse directamente a Hotmail.com, primero conecta con el proxi, y es el proxi el que conecta con Hotmail. Cuando Hotmail envía datos, los recibe el proxi, y el proxi los envía a Sarah. También es posible que encuentre algunos problemas con ciertos sitio Web, en particular con los que exijen identificarse. Pero al menos su dirección IP ya no la registra su herramienta de blog.
Algo divertido con los proxis: en noreply.org (un sitio de reenvío muy popular). El sitio le da la bienvenida con su dirección de IP “Buenas pool-151-203-182-212.wma.east.verizon.net 151.203.182.212”.
Ahora, conectése en anomyser.com, un servicio Web que le permite aceder a (ciertas) páginas Web desde un proxi anónimo. En el campo arriba y a la derecha de la página principal de anomyser, entre en esta dirección: http://www.noreply.org
(o haga clic aquí http://anon.free.anomyzer.com/http://www.noreply.org). Ahora puede ver que noreply.com piensa que viene de vortex.anomyzer.com (Anomyzer es un buen método para poner a prueba los proxis sin cambiar los parametros del navegador, pero no funcciona con los servicios Web más elaborados, como los correos electrónicos o los servidores de blog.
Por fin, configure su navegador utilizando un proxi anónimo con las instrucciones dadas anteriormente, y entre en noreply.com para encontrar si sabe de dónde viene.
Desafortunadamente los proxis no son perfectos. De hecho, muchos países bloquean el aceso a los proxis más populares, para prohibir a los internautas el aceso a páginas prohibidas. Los internautas deben cambiar de proxi cuando acaban bloqueados por las autoridades. Estos cambios de configuraci’on pueden ser una pérdida de tiempo.
Si Sarah es la única persona en su país que utiliza un proxi determinado, puede aparecer otro problema. Si el blog solamente contiene datos relativos a un solo servidor proxi, si el ministerio tiene aceso a los datos de todos los proveedores de aceso a Internet del país, podría acabar descubriendo que el ordenador de Sarah es el único que se ha conectado con este proxi. No pueden demostrar que Sarah utilizó el proxi para conectarse al blog, pero sí averiguar que es la única que utilizar este proxi y deducir que es ella la que pone el blog al día.
Por lo tanto, Sarah tiene que utilizar proxis muy concurridos en la zona donde vive, y cambiar a menudo.

CUARTA ETAPA: ¡AHORA SI ES CONFIDENCIAL!

Sarah tiene dudas sobre lo que ocurrirá si los servidores de proxi que utiliza están en peligro. Si el ministerio consigue convencer al operador de un proxi mediante la ley, o corrompiendole, para que conserve el registro de todos los usuarios y de las páginas que visitan. Cuenta con que el administrador del proxi la protegerá pero ¡ni siquiera sabe quién es!

(De hecho, el administrador del proxi podría ni saber que ella pasa por su intermedio para conectarse a Internet, por haber dejado el proxi abierto por accidente).

Afortunadamente, Sarah tiene un amigo que vive en Cánada (un país dónde censurar Internet no es práctica corriente) que podría quizás estar de acuerdo en ayudarla a conservar su blog y seguir siendo anónima. Sarah le llama y le pide que instale "Circumventor " (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) en su ordenador. Circumventor es un software que permite convertir a un ordenador en un proxi, para que pueda ser utilizado como tal por otros internautas.

Jim, el amigo de Sarah, baja Circumventor en peacefire.org y lo instala en Windows. No es facil instalarlo. Tendrá que instalar primero Pearl, y luego OpenSA para poder instalar Circumventor. Luego tiene que dejar su ordenador encendido constantemente para permitir que Sarah lo utilice como proxi sin tener que pedirle que se conecte cada vez que quiera conectarse a Internet. Lo hace, llama a Sarah con su móvil y le entrega una URL que ella puede utilizar para navegar en Internet, o conectarse a su blog desde su propia casa o desde un café internet sin tener que cambiar nada en su configuración. Aunque Sarah se lo agradezca mucho a Jim, esta solución tiene un problema importante. El ordenador de Jim, que utiliza Windows, arranca bastante a menudo. Cada vez, su proveedor de aceso le da una nueva dirección IP, y cada vez, Sarah no puede utilizar su proxi sin conocer la nueva dirección. Cada vez, Jim puede contactar a Sarah para dársela, pero cuesta dinero y es incómodo. Sarah teme además que si utiliza la misma dirección IP demasiado a menudo, su proveedor de aceso ceda a la presión de su gobierno y la acabe prohíbiendo.

QUINTA ETAPA: EL "ONION ROUTING", CON EL SOFTWARE TOR

Jim le sugiere a Sarah probar Tor, un software reciente para conservar su anonimato en Internet. El "onion routing" funciona de la misma manera que los servidores proxi, es decir que Sarah se conecta a Internet pasando por otro ordenador como intermediario, pero va más lejos. Cada conexión a un grupo de "onion routing" utiliza entre 2 y 20 ordenadores. Es muy difícil en estas condiciones saber cuál es el ordenador que inició la petición. El gobierno tendrá muchas más dificultades para encontrar a Sarah, ya que además las transmisiones están cifradas. Además de esto, cada ordenador en esta cadena solamente conoce a sus vecinos inmediatos. En otras palabras, el servidor B sabe que el servidor A le envió una petición para una página web, y se la transmite al servidor C. Pero la petición está cifrada. El servidor B no sabe cuál es la página que le pide, y tampoco cuál es el servidor que acederá a la página. Dado lo complejo de está tecnología, a Sarah le sorprende lo fácil que fue instalarla (http://tor.eff.org/cvs/tor/doc/tor-docwin32.html). Luego, baja e instala Privoxy, un proxi que funciona con Tor y que quita la publicidad de las páginas web que Sarah visita. Tras instalarlo y después de arrancar su ordenador, Sarah visita noreply.com y descubre que está "cubierta" por Tor. Noreply.com piensa que se conecta desde la universidad de Harvard. Lo intenta de nuevo, y noreply piensa que está en Alemania. Deduce que Tor cambia su identidad con cada petición, lo cual le ayuda a proteger su anonimato.

Ocurren algunas cosas raras. Cuando visita Google con Tor, ¡cambia de idioma todo el tiempo! Una búsquedad en inglés, otra en japonés, luego alemán, danés, y holandés. Sarah aprovecha la oportunidad para aprender nuevos idiomas, pero algunas consecuencias le molestan un poco más. A Sarah le gustaría contribuir al diccionario colaborativo Wikipedia, pero se da cuenta de que éste bloquea sus intentos de edición de artículos cuando pasa por Tor. Tor parece tener los mismos problemas que los proxis que Sarah utilizó. Navegar en Internet es más lento en comparación con quien no usa proxi. Acaba utilizando Tor unicamente cuando acede a páginas cuyo contenido es delicado, o para crear entradas en su blog. Tiene otra desventaja, no puede instalarlo en un ordenador público y solamente puede utilizarlo desde su casa. Lo que más le molesta a Sarah es que Tor a veces deja de funcionar. De hecho, el proveedor de aceso de Sarah bloquea ciertos servidores de enlace que Tor utiliza y cuando Tor intenta utilizar alguno de ellos, Sarah tiene que esperar mucho tiempo y a veces no consigue nunca la página que pidió.

SEXTA ETAPA: MIXMASTER, INVISIBLOG Y GPG

Sarah se pregunta si existe una solución para tener un blog sin utilizar un servidor proxi. Tras pasar algo de tiempo con un técnico a quien conoce, empieza a explorar una opción nueva: Invisiblog. en un grupo de australianos anónimos, llamados "vigilant.tv", que gestionan este web, destinado a los paranoicos. No puedes llegar a Invisiblog mediante el Web, como haces con la mayor parte de las demás herramientas de blog. Lo haces con un correo electrónico de formato específico, cuya firma cifrada la crea un sistema de remailer: Mixmaster

Sarah tuvo dificultades para entender esta frase. Acaba instalando el GPG, una versión GNU de Pretty Good Privacy, un sistema de criptado con clave pública. En dos palabras, el criptado con clave pública es una técnica que permite enviar mensajes estando seguro de que será la única en poder leerlos, sin que tenga que compartir una clave secreta contigo (lo cual le permitiría leer los mensajes que recibe de otras personas). El criptado con clave pública permite "firmar" documentos utilizando una firma numérica casi irreproducible. Crea un par de claves que Sarah podrá utilizar para colocar mensajes en el blog, firmándolos con su "clave privada". Invisiblog utilizará la "clave pública" de Sarah para asegurarse que el mensaje viene de ella, antes de colocarlo en su blog. (para más

información sobre el criptado de correos electrónicos, ver el capítulo “Como proteger la confidencialidad de vuestros correos electrónicos”).
Sarah instala MixMaster, un sistema de mensajería que permite encubrir el origen de un correo electrónico. MixMster utiliza una cadena de remailers anónimos, es decir programas que destruyen todas las informaciones que permiten identificar un correo electrónico, antes de enviarlo a su destinatario con total seguridad. Utilizando una cadena entre 2 y 20 de ellos, es muy difícil encontrar el origen de un mensaje, incluso si uno o más están al descubierto, u obtener informaciones sobre el remitente. Sarah tiene que “construir” MixMaster compilando el código fuente, un proyecto para el cual necesita el ayuda de técnicos a quién conoce. Envía un primer mensaje MixMaster a Invisiblog con su clave pública. Invisiblog la utiliza para crear un buevo blog llamado “invisiblog.com/ac4589d7001ac238”; esta serie de números son los últimos 16 bytes de su clave GPG. A partir de este momento, los mensajes que envíe a Invisiblog contendrán un texto firmado con su clave pública, y serán enviados mediante MixMaster. No es tan rápido como un blog normal. Debido a que MixMaster reenvía los correos electrónicos, puede tardar entre dos horas y dos días hasta que su mensaje llegue al servidor. Es importante que no visite el blog demasiado a menudo, ya que si el blog recuerda su dirección IP podría delatar que es ella la autora del blog. Ahora bien puede estar tranquila ya que Invisiblog no tiene ni idea de quién puede ser. El mayor problema con Invisiblog es que resulta demasiado difícil de instalar para la mayor parte de la gente, y no saben como utilizar claves públicas y privadas. La mayor parte de las herramientas de encriptado fáciles de usar, como Ciphire, han sido creadas para ayudar a los que menos sabemos de técnica, pero incluso esas acaban siendo difíciles de utilizar. Así que muy pocas personas, incluso las que más lo necesitamos, utilizamos el encifrado.
Hay que decir que MixMaster es un desafío para la mayor parte de la gente. Los que utilizan Windows solamente pueden utilizar una versión en DOS. Lo intenté, pero o bien no funciona o mi correo sigue siendo enviado entre los remailers. Si alguien desea utilizarlo en Linux o Mac tiene que compilar el programa él mismo, una tarea delicada incluso para un experto. Invisiblog sería muchísimo más útil si fuese posible aceptar los mensajes de los remailers disponibles en Internet, tipo riot.eu.org. De momento, no es muy práctico para que lo use la gente que más lo necesita. El criptado plantea otro problema en los países en que el gobierno tiene una política represiva. Si el gobierno confisca el ordenador de Sarah y encuentra en él su clave privada, tendrá pruebas de que ella es el autor del blog. Y en países donde el criptado no se utiliza de manera frecuente, el mero hecho de enviar mensajes con MixMaster puede ser suficiente para que las autoridades empiecen a controlar lo que Sarah hace cuando se conecta a Internet.

¿QUÉ DECIR? ¿CUÁL ES EL LIMITE?

Sarah eligió aprender las bases de criptado y de Mixmaster. ¿Es la solución que más le conviene? ¿O será suficiente el anonimato de las etapas 1 a 5? Hay varias respuestas. Cuando eliges ser anónimo, tienes que tener en cuenta las condiciones del país en que estás, tus propios conocimientos técnicos y tu nivel de paranoia. Si tienes motivos para pensar que lo que haces podría ponerte en peligro, y eres capaz de instalar Tor, ¡adelante!
Ultimo consejo, no te olvides de firmar con un seudonímo.

ETHAN ZUCKERMAN
Ethan Zuckerman es un estudiante investigador en el Berkman Center for Internet and Society de la escuela de derecho de Harvard. Su investigación trata de las relaciones entre el periodismo ciudadano y los medios de comunicación convencionales, en particular en los países en vía de desarrollo. Es fundador y antiguo director de Geekcorps, una organisación sin fines lucrativos que trabaja sobre las tecnologías educativas en los países en desarrollo.
También es uno de los fundadores de la empresa de alojamiento Tripod.