Publicado en New York el 02/07/2013

First National Innovation Brokers Presenta: Monedas Digitales y Protección de la Privacidad

"Cualquier analista, en cualquier momento puede hacer blanco a cualquier persona. Cualquier selector, en cualquier lugar... Yo, sentado en mi escritorio, sin duda tenía las facultades para intervenir el teléfono de cualquiera, de usted o de su contador, a un juez federal, inclusive del Presidente... " Edward Snowden

Es posible que haya escuchado hablar de Edward Snowden, el alumno desertor con 29 años de edad de un colegio comunitario y contratista de la Agencia Nacional de Seguridad que desertó a China a través de Hong Kong y dijo que él tenía la capacidad tecnológica y la frazada de autoridad legal para espiar a cualquiera.

La historia fue rota por Glenn Greenwald en la Guardia y está enviando ondas de choque a través de medios diplomáticos y medios de comunicación. Esto viene de la mano del escándalo de las citaciones de registros telefónicos de The Associated Press, el escándalo del partido IRS-tea, los escándalos de piratería telefónica de los Rupert Murdoch y el policía informante encubierto de la Toma Wall Street, así como otras revelaciones incitadoras.

"Con esta capacidad, la gran mayoría de las comunicaciones humanas son ingeridas de forma automática y sin orientación. Si yo quiero ver sus e-mails o el teléfono de su esposa, todo lo que tengo que hacer es interceptar. Puedo obtener tus correos electrónicos, contraseñas, registros telefónicos, tarjetas de crédito ", dijo Snowden.

Sus confesiones no deben ser entendidas en el vacío. Hay un sinnúmero de videos de Youtube de bajo nivel, pero enormemente poderosos de funcionarios gubernamentales estadounidenses metiendo los dedos enguantados en las áreas genitales de los viajeros, causando angustia permanente y vergüenza. La discriminación racial y religiosa, así como la evaluación de perfiles de inteligencia contraria de los niños blancos y de las abuelas que suelen refutar es el sello distintivo del Departamento de Seguridad Nacional del comportamiento Aeroportuario, que ahora se encuentra en las estaciones de tren, estaciones de autobuses y carreteras también. Durante más de dos siglos, este pesado puño de hierro no figuraba en cualquier lugar en la república americana. Ahora, los departamentos de policía de todo el país "emiten citaciones administrativas", es decir, sin una orden de registro firmada por un juez, para aprovechar de forma rutinaria tesoros de datos de clientes de las

compañías de telefonía móvil, lo que les permite rastrear el paradero de millones de suscriptores. Aviones son adquiridos para espiar a los estadounidenses desde lo alto, mientras que el especialista en derecho constitucional y presidente del Premio Nobel de la Paz utiliza los aviones no tripulados de la Fuerza Aérea para matar a miles en el extranjero, incluidas las mujeres y los niños e incluidos los estadounidenses, sin molestarse en interponer cargos criminales en la corte, y mucho menos condenarlos de cualquier delito. A menudo, los nombres de los objetivos son desconocidos. El asesinato se basa en apariencias llamadas firmas: discurso supuestamente interceptado, incluyendo correos electrónicos y a quienes estén asociados con los objetivos. Son remotos los perfiles de alta tecnología y es en este contexto que las revelaciones de Snowden necesitan ser digeridas. La afirmación de que sólo los chicos malos tienen que preocuparse de PRISM es muy ingenua. Algo tan inocente como marcar un número mal que podría traer un escrutinio injustificado. Una persona con un interés personal podría dejar caer una moneda de diez centavos sobre usted y arruinar su vida.

Los servicios de inteligencia y los militares tienen un enfoque profiláctico. Esto significa que cada vez están más convencidos de que con programas como PRISM, pueden identificar probables criminales y terroristas antes de un crimen o de que un acto terrorista haya ocurrido.

A pesar de sus siglas y jerga técnica, el programa espía PRISM se basa en una premisa simple: Secretamente grabar toda la información acerca de todo el mundo, en todas partes, en todo momento, y luego archivarlo para siempre. Dado que todo ser humano tiene el potencial de convertirse en un sospechoso criminal o terrorista en el futuro, un expediente sobre esa persona va a estar disponible, incluyendo con quién esa persona se haya asociado en el pasado. El expediente se centra en cuatro áreas: las transacciones financieras, registros telefónicos, registros de Internet y los registros de viajes. Este diario de byts hace posible arruinar a cualquiera sin ningún pretexto a voluntad. Se crea una inimaginable ventaja del estado para aterrorizar a los individuos y grupos de individuos. Todo abuso se justifica en virtud de la "Guerra contra el Terror."

¿Qué hacer?

Una revisión exhaustiva está fuera del alcance de este artículo, pero con unos pocos pero inteligentes cambios de hábitos puede recorrer un largo camino protegiéndose de la orden judicial menor, la recolección ilegal, inconstitucional e invasiva de la privacidad de su información genuina. Para empezar, me centraré en los pagos cifrados y sistema de comunicación llamado Swiftcoin, del comunicado de prensa reciente:

“Los usuarios de Internet que ejecutan el programa Swiftcoin les colocan un desafío a los intrusos. Este programa gratuito no requiere identificación o pago para ser descargado. Una vez instalado, permite a los usuarios decidir entre utilizar o no los servidores de correo electrónico comunes gestionados por grandes empresas que están obligadas, bajo la reserva del sumario, a proveer el

acceso por la puerta trasera al invasor, dándole alcance a los intereses públicos y privados. Swiftcoin, como cuentas bancarias suizas numeradas, no identifica a los usuarios por su nombre. A diferencia de las cuentas bancarias, el número del usuario cambia cada vez que él / ella presiona el botón Enviar. El programa Swiftcoin se puede mover fuera de la computadora del usuario en un dispositivo de almacenamiento y ser abierta de nuevo en el equipo que se desee. Los usuarios Swiftcoin no pueden ser rastreados por nombre, por dirección IP o por dispositivo. “

Este programa es llamado el cifrado profundo porque la comunicación cifrada literalmente, incluyendo sus "metadatos", no es identificable a menos que el usuario elija hacer pública su Identificación de la cartera. Cada mensaje enviado sale de una nueva "localización" o la misma ubicación si el usuario lo desea. Lo mismo ocurre con el destinatario. Todos los mensajes o pagos son único y se pueden emplear los metadatos desechables. Además, el dispositivo de usuario en sí mismo puede ser sustituido voluntariamente. Una cartera Swiftcoin se puede mover a un pen drive y luego subirse a un dispositivo diferente. Todo esto hace que sea mucho más difícil de espiar y registrar la actividad de un usuario debido a que la correlación entre una identificación Swiftcoin y una persona en particular es tenue. Swiftcoin no depende enteramente de cifrado que, al final del día, puede ser violado por los criptógrafos. La manera en que Swiftcoin está diseñado para ser utilizado no se presta para el seguimiento de cualquier persona con el paso del tiempo.

Por desgracia, la página Swiftcoin www.firstnationalbnak.com no está disponible para ciudadanos estadounidenses. Sin embargo, el telegrama Swiftcoin queda a libre disposición de todos, independientemente de su nacionalidad. Cada nuevo usuario puede recibir diez Swiftcoins libres, (bueno para 10 000 telegramas; cada "telegrama" Swiftcoin cuesta 0.001 Swiftcoin) que se devuelve al remitente en un correo de vuelta del destinatario, por un costo neto de cero para enviar y recibir un telegrama. No se requiere dinero o compra de Swiftcoin para descargar el programa y utilizar la función de telegrama.

Datos de contacto:
First National Innovation Brokers

Nota de prensa publicada en: New York