La Agencia Nacional de Seguridad y el escándalo del acceso a los celulares iPhone

La NSA y la erosión de la confianza mundial en Estados Unidos

> Todos los que están en la órbita de la NSA buscan una cobertura a raíz de las revelaciones sobre lo que podríamos llamar excesos de la agencia de espionaje.

Dan Farber, **News CNet** 31 de diciembre de 2013 9:43 AM PS [1]

Instalaciones de la NSA en Fort Meade, Md.
(Imagen proporcionada por la NSA)

Anteriormente la Agencia de Seguridad Nacional constaba de unos cuantos edificios grandes, fortificados, y un estacionamiento en Fort Meade, Maryland, donde magos de las matemáticas, de camisa blanca y tez pálida, trabajaban para descifrar claves de entidades extranjeras. Mientras la NSA lanzaba satélites espías y sus analistas estaban pegados a las pantallas de sus ordenadores, la CIA y el FBI concentraban toda la atención del público, desempeñando papeles protagónicos machistas en películas, programas de TV y libros. El nerd NSA era en sí mismo un sistema cifrado. NSA significaba "No hay tal Agencia".

Los libros de James Bamford la sacaron de las sombras y expusieron la agencia a la

1. http://news.cnet.com/8301-1009_3-57616388-83/the-nsa-and-the-erosion-of-trust/?part=rss&tag=feed&subj

luz, pero pocos prestaron mucha atención, hasta que ocurrieron las revelaciones de Edward Snowden, quien filtró documentos internos de la NSA. Ahora, la NSA se ha revelado como la verdadera estrella de la constelación de la inteligencia de Estados Unidos, capaz de infiltrarse secretamente en todo tipo de dispositivo electrónico, en Internet y en las comunicaciones globales.

Por ejemplo, según un informe de *Der Spiegel* y del investigador de seguridad Jacob Appelbaum, un programa de la NSA llamado DROPOUTJEEP abre a la agencia de espionaje la puerta trasera a cualquier iPhone. El spyware, caja de herramientas ANT de la NSA, realiza hazañas. Puede acceder a las listas de contactos y los correos de voz, usar datos de torres celulares para localizar un teléfono, interceptar mensajes de texto y activar el micrófono y la cámara del dispositivo.

El documento filtrado DROPOUTJEEP, fechado en 2008, clamaba una tasa de éxito del 100% en el acceso a los iPhones. Sin embargo, la hazaña requería del acceso físico al dispositivo. Es probable que en los últimos cinco años, la NSA haya encontrado la manera de instalar de forma remota el software espía, aunque Apple y otros traten de hacer sus teléfonos más seguros.

En un comunicado emitido el martes, el fabricante de iPhone dijo: "Apple nunca ha trabajado con la NSA para crear una puerta trasera para cualesquiera de nuestros productos, incluyendo el iPhone. Además, ignorábamos este supuesto programa de la NSA enfocado a nuestros productos".

La caja de herramientas de la NSA también incluye una falsa antena de telefonía móvil de 175,800 dólares que permite a la agencia captar subrepticiamente llamadas telefónicas y mensajes de texto. No es difícil imaginar que la NSA posee una tecnología similar para obtener acceso a cualquier marca de dispositivo conectado a las redes celulares de Internet.

Como informó *Der Spiegel* con base en documentos filtrados, internos de la NSA, la agencia es prácticamente omnisciente:

La NSA no sólo se centra en las hazañas de alta tecnología. La unidad de operaciones de acceso diseñadas a la medida (TAO, por sus siglas en inglés) trabaja con la CIA y el FBI para interceptar los envíos de hardware y llevarlos a un "taller secreto" para insertar spyware en los equipos. Según documentos internos de la NSA, *Der Spiegel* informó que la NSA obtuvo acceso a computadoras, discos duros, ruteadores y otros accesorios electrónicos de empresas como Cisco, Dell, Western Digital, Seagate, Maxtor, Samsung y Huawei.

Supongamos que la NSA quiere plantar spyware en los ordenadores portátiles destinados a una persona o empresa de la cual sabe que tiene alguna conexión con una organización terrorista o algunos otros delincuentes que estén en su radar.

¿Obtiene la NSA una orden judicial que autorice la operación o simplemente avisa al fabricante que atiende algunos asuntos gubernamentales de la mayor secrecía que implican a unas cuantas cajas de sus equipos electrónicos? ¿Saben los servicios de mensajería tales como FedEx, UPS y el Servicio Postal de EE.UU. que la NSA retendrá algunas cajas por unas horas? En cualquier caso, en la cadena de custodia alguien tiene que saber algo. Es improbable que los agentes encubiertos que trabajan con la NSA secuestren los camiones de reparto en tránsito.

Las empresas con las que *Der Spiegel* estableció contacto alegaron que no tenían conocimiento de ninguna puerta trasera para la NSA en sus equipos. Si se hubieran enterado de tales intervenciones, es probable que el gobierno les hubiera prohibido reconocerlo.

En un comunicado, la NSA dijo:. "Las Operaciones de Acceso diseñadas a la medida (TAO) constituyen un activo nacional único de primera línea que permite a la NSA defender a la nación y a sus aliados. No discutiremos acusaciones concretas sobre la misión de TAO, pero su trabajo se centra en explotar la red informática en apoyo de la recolección de la inteligencia extranjera".

Es vergonzoso. Funcionarios de gobierno electos para los comités de inteligencia no entienden realmente lo suficiente sobre la destreza técnica y las operaciones de la NSA para controlarlas. Tampoco lo hace el tribunal de la FISA, que faculta a la agencia para llevar a cabo actividades de vigilancia. Las compañías tecnológicas están sujetas a cooperar con la NSA como lo exigen la ley, el patriotismo o el miedo. No quieren ser vistas como indignas de confianza por parte de sus clientes ni como impedimentos para prevenir un ataque terrorista.

La prominente empresa de seguridad RSA presuntamente recibió diez millones de la NSA para implementar puertas traseras en sus fichas de cifrado. La compañía niega haber contratado o participado en ningún proyecto cuya intención fuera debilitar sus productos, pero la comunidad de equipos de seguridad permanece escéptica.

> Estos agentes de la NSA, que se especializan en puertas secretas traseras, son capaces de mantener un ojo en todos los niveles de nuestra vida digital, desde centros de cómputo hasta computadoras individuales y desde computadoras portátiles hasta teléfonos móviles. Para casi todas las cerraduras, ANT parece tener una clave en su caja de herramientas, No importa los muros que las empresas erijan, los especialistas de la NSA parecen haberlos superado de antemano.

Los CEOs de las empresas tecnológicas se reúnen con el presidente Obama 17 de diciembre 2013.
(Imagen proporcionada por la Casa Blanca).

No es exactamente un encubrimiento, pero todos los que están en la órbita de la NSA buscan una cobertura a raíz de las revelaciones sobre lo que podríamos llamar excesos de la agencia de espionaje. Los CEOs de las empresas tecnológicas que se reunieron con el presidente Obama pidieron reformas a la NSA y más transparencia sobre las solicitudes de información del gobierno acerca el usuario. El Informe Final del Grupo de Revisión de Inteligencia y Tecnologías de Comunicación comisionado por la Casa Blanca emitió 46 recomendaciones y piden mayor supervisión judicial y transparencia.

El espionaje ha ocurrido desde los comienzos de la civilización. La tecnología lo ha facilitado y lo ha extendido. En el mundo conectado, todos están al alcance de las miradas indiscretas. Cada país lo practica, y muchas empresas recurren a alguna forma de ingenio para obtener información de inteligencia sobre sus competidores. Poner freno a algunos aspectos de las prácticas de la NSA no hará mucho para aliviar la erosión de la confianza. Tampoco se le pedirá a la NSA que altere cualquier práctica que ponga al gobierno de EE.UU. en una posición menos ventajosa frente a sus supuestos enemigos.

Como experto en seguridad Bruce Schneier lo ve: las empresas de tecnología no serán capaces de escapar de los tentáculos de la NSA.

Descarga de productos electrónicos de los camiones de FedEx y UPS.
(Foto: Josh Lowensohn/CNET)

Tal es, al menos, la impresión que da un vistazo a través del documento de 50 páginas. La lista se lee como catálogo de ventas por correo, de los cuales otros empleados de la NSA pueden servirse para ordenar tecnologías de la división ANT para obctener los datos de sus objetivos. El catálogo incluso enumera los precios de estas herramientas de ruptura y penetración electrónica, cuyos costos van desde los gratuitos hasta los que valen 250,000 dólares.

> Aunque no sepamos qué empresas ha puesto en peligro la NSA —o por qué medios—, el hecho de saber que podrían haber comprometido a cualquiera de ellas es suficiente para hacernos desconfiar de todas. Esto dificultará a las grandes empresas como Google y Microsoft conseguir que recuperen la confianza que perdieron. Aun si tienen éxito en limitar la vigilancia gubernamental. Aun si triunfan en mejorar su propia seguridad interna. Lo mejor que estarán en aptitud de decir será: "Nos hemos asegurado ante la NSA, excepción hecha de aquello que, o bien desconocemos o es de lo que no podemos hablar".