DESDE HACE AÑOS, ESTADOS Y EMPRESAS VIGILAN LOS MOVIMIENTOS DE LOS USUARIOS EN LA RED GLOBAL. LA MAGNITUD DEL CIBERESPIONAJE SUPERA TODO LO IMAGINADO. ESTAS ACTIVIDADES NO SON PRACTICADAS ÚNICAMENTE CON FINES DE SEGURIDAD O DEFENSA, SINO TAMBIÉN EN PERSECUCIÓN DE FINES COMERCIALES. ¿QUÉ SOLUCIÓN SE PUEDE ENCONTRAR A UN PROBLEMA QUE AFECTA TANTO LA PRIVACIDAD DE LAS PERSONAS COMO LA SOBERANÍA DE LOS ESTADOS?

UN MUNDO VIGILADO: LA (FALTA DE) PRIVACIDAD EN LA ERA DIGITAL

por MARTINIANO NEMIROVSCI.
Periodista, Agencia TELAM

talkphotography
Home
Forums
Resources
Trade
Gallery
Members
*****TALK PHOTOGRAPHY DAY 2014
Lifelock.com
AUTHOR
Kelack

Cualquiera que haya comprado en 2005 un disco de Celine Dion, de Santana o de Neil Diamond y lo haya escuchado en su computadora, pudo haber abierto la puerta de sus datos personales sin saberlo. A finales de ese año, el técnico Mark Russinovich reveló que la discográfica Sony BMG introdujo en millones de CDs un código malicioso que instalaba un *rootkit* (una herramienta que se aloja en la raíz de un sistema operativo y permite a terceros el acceso a comunicaciones, archivos o información sobre procesos de los equipos infectados) en las computadoras en las que se introducían los discos. La iniciativa, justificada en la lucha contra la "piratería", comenzó a hacer un ruido que fue aumentando poco a poco, a medida que se descubrían casos similares.

Pero recién en junio de 2013 esa disonancia alcanzó la magnitud de escándalo y pudo trascender los límites de los blogs especializados. La aparición en los principales medios de la prensa anglosajona de los documentos filtrados por el ex técnico de inteligencia Edward Snowden fue determinante para instalar un tema que concierne tanto a gobiernos como a empresas y personas de a pie. Estos documentos, que detallaron cientos de programas de espionaje masivo del gobierno estadounidense, desnudaron la profundidad de esa "vigilancia", los objetivos buscados y los métodos con los que la Agencia de Seguridad Nacional de ese país (NSA) recopila información en todo el mundo. Si bien Estados Unidos no es el único Estado ciberespía, sí es el de mayores recursos, desarrollo y organización, como fue quedando claro con el correr de los meses.

A través del desarrollo de soluciones de código abierto es posible evitar el uso del software comercial, que llega en su gran mayoría de Estados Unidos, con sus "puertas traseras" abiertas. Este mensaje cala profundo en varios especialistas de la región, quienes entienden que en la era digital, en la libertad de las comunicaciones se juega tanto la privacidad como buena parte de la soberanía.

El afán de vigilarlo todo

El 6 de junio de 2013 el diario inglés *The Guardian* publicó que en virtud de una orden judicial secreta el gobierno de los Estados Unidos escuchaba cada día todas las llamadas de los clientes de Verizon, una de las telefónicas más grandes de ese país, con la justificación de que se trataba de "una herramienta crítica" en el combate al terrorismo.

Fue la primera entrega de una saga de filtraciones que pondría en evidencia que, bajo la administración del presidente Barack Obama, todas las personas son objetivos de inteligencia, inclusive si no están sospechados de haber cometido algún delito.

Esto se hizo más patente al día siguiente, cuando se conoció la existencia de un programa llamado PRISM, a través del cual la NSA accede de forma directa a los servidores de nueve de las principales empresas globales de servicios de Internet –entre ellas Microsoft, Yahoo!, Google, Facebook, PalTalk, Apple y Skype– para recoger información personal de sus usuarios, sin necesidad de presentar órdenes judiciales.

Algunos de los líderes de estas gigantes tecnológicas, como Mark Zuckerberg (fundador de Facebook) y Larry Page (cofundador de Google), negaron personalmente cualquier tipo de implicación con la agencia. Sin embargo, los documentos secretos señalaban que las empresas habían colaborado con la NSA y por ello los agentes podían recolectar de forma directa materiales como historiales de búsquedas, contenidos de correos electrónicos, transferencia de archivos y chats, entre otras cosas.

Estas "puertas traseras" en las empresas de Internet, así como los metadatos (los datos de los datos: aquella información referida a la identificación del número telefónico, la fecha, el tiempo de conversación o la localización de la llamada) provistos por las empresas telefónicas bien podrían haber sido fruto de una "colaboración" obligatoria, ya que las compañías pueden ser obligadas en función de órdenes del tribunal secreto FISA (el Tribunal de Vigilancia de Inteligencia Extranjera, creado por la Ley de Vigilancia de Inteligencia Extranjera).

La magnitud del ciberespionaje detallado en los documentos de Snowden superaba todo lo imaginado: desde mediados de 2012, la Agencia de Seguridad Nacional procesaba cada día más de 20 mil millones de comunicaciones provenientes de todo el mundo.

La metodología de la NSA para reunir una cantidad de comunicaciones tan grande también implica el acceso directo a muchos de los cables internacionales de fibra óptica que se utilizan para transmitir comunicaciones internacionales, incluidos los submarinos.

La agencia además desvía hacia sus servidores mensajes que atraviesan la infraestructura de red de los Estados Unidos –como lo hace buena parte de las comunicaciones mundiales– y coopera con servicios de inteligencia de otros países, que le ayudan en su recopilación.

En esta línea, la NSA cerró una serie de acuerdos con grandes empresas de telecomunicaciones estadounidenses para aprovechar el acceso que tienen a otras redes internacionales y así acceder a metadatos telefónicos extranjeros. Por ejemplo, un acuerdo alcanzado con la gigante telefónica AT&T estableció que, cuando esta firma un contrato para desarrollar o mantener los sistemas de compañías de otros países, la NSA mantiene la posibilidad de desviar las comunicaciones a sus servidores. Este procedimiento se realizó con operadoras de Brasil, Grecia, Francia, Alemania, Venezuela y Japón, entre otros países, en el marco de un programa secreto llamado "Blarney".

La recolección de datos privados también implicó al equipo de *crackers* –como se conoce a las personas que rompen sistemas de seguridad informática, mal llamados *hackers*– de la NSA. Los documentos dieron cuenta de la existencia del programa "Explotador de la red de computadoras" (CNE), mediante el cual la división de Operaciones de Acceso de Medida (TAO) de la agencia introduce *malware* en computadoras personales para vigilar a sus usuarios.

"Tomado en su totalidad, el archivo de Snowden conducía en última instancia a una conclusión simple: el gobierno de Estados Unidos había creado un sistema cuya finalidad era la completa eliminación de la privacidad electrónica en todo el mundo", escribió en su libro *Sin un lugar para esconderse* Glenn Greenwald, el periodista de *The Guardian* que entabló la relación con Snowden para publicar la información sobre el espionaje.

En su texto, Greenwald explicó que con unos 90 mil empleados, entre propios y tercerizados, la NSA es la mayor agencia de inteligencia del mundo, aunque casi toda su labor de espionaje la realiza mediante la alianza de los "Cinco Ojos". Este grupo llamado FVEY (por el inglés *"five eyes"*) nuclea a las agencias de los aliados más cercanos: Gran Bretaña, Canadá, Australia y Nueva Zelanda.

En una actitud corporativa, sus gobiernos están denunciados de priorizar el acceso a la información privada por parte de la NSA sobre el respeto a la privacidad de sus propios ciudadanos.

Personas comunes

Una investigación publicada en julio por el diario *The Washington Post* mostró que el 90 por ciento de los espiados por la NSA son usuarios comunes de Internet. Entre los cientos de miles de correos electrónicos y mensajes analizados, el matutino encontró muchas comunicaciones que los analistas de la NSA consideraban "inútiles", pero que igual se almacenaron, como historias de amor, encuentros sexuales, relatos de angustia económica, opiniones políticas y religiosas, enfermedades mentales y otros aspectos de la vida cotidiana. Los documentos también incluían cerca de 5.000 fotos, entre ellas imágenes de mujeres posando en ropa interior.

Pero el registro de imágenes ajenas no es potestad exclusiva de la NSA. Su socio más cercano, el británico Cuartel General de Comunicaciones Gubernamentales (GCHQ), puso en práctica un programa llamado "Nervio Óptico", que le permitió durante seis meses de 2008 acceder a las *webcams* de 1,8 millones de usuarios de Yahoo!

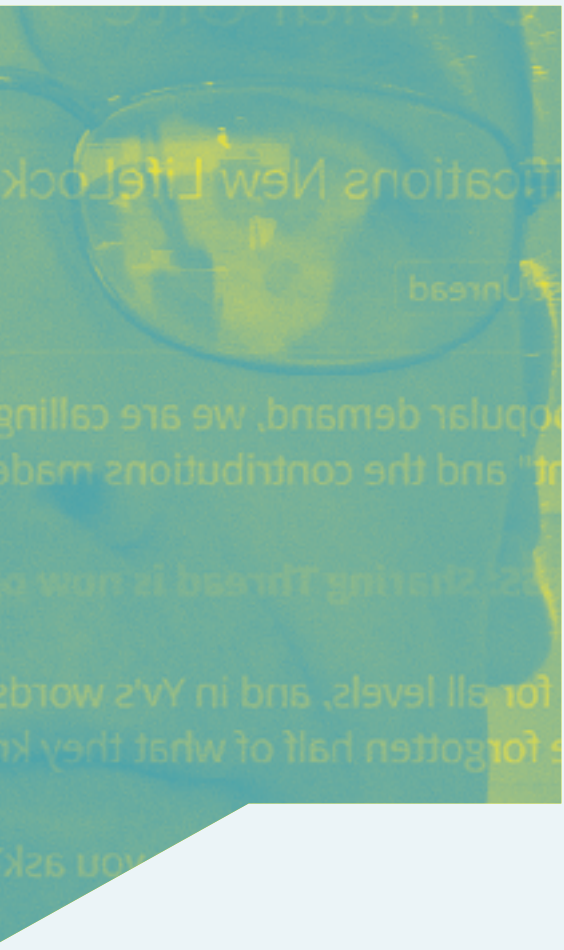
Según documentos filtrados, entre el 3% y el 11% del contenido recolectado por el GCHQ consistía en imágenes de desnudez. El sistema capturaba una imagen cada cinco minutos con el supuesto objetivo de realizar tareas de reconocimiento facial para monitorear la actividad de "potenciales objetivos".

Un software utilizado con el mismo fin por la NSA es el "Tundra Freeze", un desarrollo con el que la agencia extrae cada día millones de fotos de los correos y mensajes que intercepta, los analiza, reconoce los rostros e incluso determina dónde fueron tomadas las fotografías, según una investigación publicada en junio por *The New York Times*.

Esta pareja de agencias unió fuerzas para la implementación del *malware* (código malicioso) "Implants" con el que, además de acceder a las *webcams*, la NSA y el GCHQ pudieron controlar el micrófono de las computadoras infectadas y grabar las conversaciones. En algunos casos este código se esparció con técnicas propias de ciberdelincuentes: se enviaron mails con links que contenían el *malware*. En otros, directamente se camuflaron

Una responsabilidad significativa les cabe a empresas gigantes cuyas acciones involucran potencialmente a cientos de millones de personas. Sus motivaciones no están fundadas en razones de "seguridad nacional", sino en la persecución de fines comerciales o de otro tipo.

como falsos servidores de Facebook y utilizaron a la red social para infectar los equipos de los usuarios de la plataforma.
El tamaño del archivo y el detalle de los documentos filtrados por Snowden permitieron conocer con cierta profundidad las características del ciberespionaje de las principales agencias de inteligencia. Pero la violación de la privacidad de las personas no es exclusividad de estas. En este sentido, una responsabilidad significativa les cabe a empresas gigantes cuyas acciones involucran potencialmente a cientos de millones de personas. Sus motivaciones no están fundadas en razones de "seguridad nacional", sino en la persecución de fines comerciales o de otro tipo.
En julio pasado, el científico forense Jonathan Zdziarski demostró que iOS, el sistema operativo de los iPhones de Apple, tiene "una serie de servicios sin documentar de alto valor", que no están referenciados en ningún software de la empresa, y "sospechosas omisiones de diseño que hacen más fácil la recolección" de datos por parte de terceros. El forense explicó que estas "puertas traseras introducidas por el fabricante" permiten extraer información de forma remota, sin que el dueño del teléfono se entere. Este tipo de datos pueden ser aprovechados tanto por Apple como por socios comerciales, interesados en, por ejemplo, las características de consumo de los usuarios de iPhone, sus intereses o sus búsquedas web.



Por su parte, tras eludir una demanda colectiva millonaria por violación de la privacidad, en abril Google reconoció explícitamente que lee todos los correos que entran y salen de Gmail, su servicio de correo electrónico utilizado en todo el mundo por más de 425 millones de personas. Según explicó en la actualización de sus "Condiciones de servicio", un software escanea los contenidos de los correos que están en tránsito, así como los que están almacenados en los servidores –además de revisar el historial de búsquedas–, con el objetivo de crear anuncios publicitarios personalizados.
Cuatro meses después, el gigante de Internet dejó en claro que puede violar la privacidad con otros objetivos, arrogándose el papel simultáneo de policía y juez. Esto quedó demostrado con la detención del ciudadano estadounidense John Henry Skillern después de que Google encontrara que en su cuenta de Gmail tenía fotos de pornografía infantil. La empresa escaneó los correos de Skillern, detectó fotos de una niña con contenido sexual y avisó a una ONG, que a su vez llamó a la policía.
Lo mismo hizo Microsoft una semana más tarde. Sin que nadie se lo solicitara, revisó la cuenta de "One Drive" (su servicio de almacenamiento en la nube) de Tyler James Hoffman, un estadounidense de 20 años, en donde supuestamente encontró imágenes de pedofilia. El circuito siguió el mismo camino: la firma fundada por Bill Gates dio aviso al mismo "Centro nacional para los niños perdidos y explotados", que a su vez avisó a la policía. Con una orden de arresto fundada en el aviso de Microsoft, Hoffman fue detenido.
La introducción de "puertas traseras" en su propios productos así como las tareas de escaneo y vigilancia de estas empresas son indicadores de que la violación de la privacidad y el ciberespionaje a escala masiva no son necesariamente actividades practicadas con fines de seguridad o defensa. Y en este punto, las empresas coinciden con algunos Estados.
De hecho, además de la vigilancia arbitraria ejercida sobre poblaciones enteras –como sucedió con el registro y grabación de todas las llamadas telefónicas en Afganistán o el almacenamiento durante un mes de todas las comunicaciones móviles que se realizan desde y hacia Bahamas–, los documentos de Snowden demostraron que la NSA se implicó por igual en el espionaje económico y diplomático.

El tamaño del archivo y el detalle de los documentos filtrados por Snowden permitieron conocer con cierta profundidad las características del ciberespionaje de las principales agencias de inteligencia. Pero la violación de la privacidad de las personas no es exclusividad de estas.

Relaciones conflictivas

Ejemplos de ello fueron los sonados casos de ciberespionaje a unos 35 altos dirigentes políticos de distintos países, entre ellos el Papa, la mandataria alemana Angela Merkel, el presidente mexicano Enrique Peña Nieto y la jefa de Estado brasileña Dilma Rousseff (a quien le pincharon el correo electrónico y el celular privado).

La agencia también espió información sensible de la petrolera brasileña Petrobras y ayudó al Centro de Comunicaciones y Seguridad de Canadá a espiar al Ministerio de Minas y Energía de Brasil, área en la que las empresas de ese país norteamericano tienen especial interés.

Estas revelaciones generaron roces y potenciaron desconfianzas en las relaciones internacionales. Desde la Comisión Europea exigieron explicaciones y levantaron la voz, aunque las acciones parecen haber quedado ahí. Dilma Rousseff suspendió su primera visita de Estado a Washington y, durante su discurso ante la Asamblea General de la ONU, acusó a los Estados Unidos de una "grave violación de los derechos humanos y civiles y una falta de respeto por la soberanía nacional".

Por su parte, en el marco de la Unasur, el canciller ecuatoriano Ricardo Patiño anunció a finales de 2013 que los países de la región exploran de manera conjunta la creación de un sistema de comunicaciones propio para evitar "seguir siendo objeto y presa del espionaje ilegal que los organismos de espionaje norteamericano han desarrollado contra nosotros". Según explicó, el planeamiento e implementación de esta tarea recayó sobre el Consejo de Defensa de la Unasur, integrado por los ministros de Defensa de la región.

Sin embargo, la principal rispidez parece haber sido la desatada con China. Como coletazo de la actividad de la NSA así como de agentes chinos, en los últimos meses fue creciendo un intercambio de acusaciones entre ambas potencias que amenaza con derivar en consecuencias geopolíticas y económicas.

En mayo, el fiscal general estadounidense Eric Holder anunció el inicio de un proceso criminal contra cinco oficiales del Ejército Popular de Liberación acusados de ingresar en las computadoras de varias empresas estadounidenses y un sindicato, para robar secretos comerciales. La respuesta china llegó pronto, con la suspensión del grupo de diálogo bilateral sobre seguridad informática y un informe gubernamental en el que tildó de "inescrupuloso" el accionar de las agencias de inteligencia norteamericanas.

En el escrito acusó a Estados Unidos de operaciones de ciberespionaje que fueron "mucho más allá de la justificación legal del 'antiterrorismo'" y le atribuyó intrusiones en la fábrica de teléfonos Huawei, los ministerios de Comercio, de Asunto Exteriores y algunas universidades.

A partir de allí, Beijing tomó medidas en pos de su "seguridad informática" contra empresas norteamericanas: entre otras acciones, prohibió el uso del sistema operativo Windows 8 en las computadoras gubernamentales, pidió a los bancos que dejen de usar servidores fabricados por IBM y le exigió a Apple que almacene los datos de los ciudadanos chinos en servidores en ese país. Además, el ejército del país asiático anunció recientemente un programa para fortalecer el desarrollo de software nacional para cimentar su ciberseguridad.

Anónimos y encriptados

Desde que estalló el escándalo del ciberespionaje masivo, algunas soluciones propuestas para escapar de la aparentemente inevitable mirada ajena pasan por garantizar el anonimato a la hora de navegar por la Web. Un caso testigo de este aspecto es el de la red TOR, un sistema de uso libre y gratuito que sirve para no dejar huellas en Internet. Funciona con una red de servidores proxy que se ubican en medio de una computadora y el sitio web al que el usuario se conecta. Así, el sistema elige un proxy en particular, de forma aleatoria, y "enmascara" la dirección de IP del internauta, con lo que resulta difícil de rastrear.

El uso de TOR, que según un reciente análisis del investigador Virgil Griffith se duplica cada 14 meses, preocupa a más de un gobierno. A fines de julio, Rusia –de donde provienen la mayoría de los "capos" ciberdelincuentes del mundo, según la Europol– lanzó un peculiar concurso: ofreció 110 mil dólares a la primera persona que sea capaz de "des-anonimizar" esta red, con el fin de identificar a sus usuarios y "proteger la seguridad nacional". Quizá con un objetivo similar, en agosto el gobierno estadounidense asumió haber financiado a investigadores de la universidad Carnegie Mellon para atacar esta red.

La otra solución propuesta pasa por encriptar las comunicaciones. Uno de los principales impulsores de esta vía, además del propio Snowden, es el periodista y activista australiano Julian Assange, quien urgió a fines de septiembre a transitar este camino desde el software libre. A través del desarrollo de soluciones de código abierto es posible evitar el uso del software comercial, que llega en su gran mayoría de Estados Unidos, con sus "puertas traseras" abiertas. Este mensaje cala profundo en varios especialistas de la región, quienes entienden que en la era digital, en la libertad de las comunicaciones se juega tanto la privacidad como buena parte de la soberanía.