Revelan red de escuchas telefónicas del FBI y se solicita a los lectores analizar los documentos

RYAN SINGEL :: 07/10/2007

Según muestran casi mil páginas de documentos confidenciales revelados recientemente en virtud de la Ley de Libertad de Información (Freedom of Information Act), y que la Fundación de la Frontera Electrónica (Electronic Frontier Foundation) le suministró a Wired News, el FBI ha construido silenciosamente un complejo sistema de vigilancia que comienza a funcionar con solo posicionar el cursor y hacer clic.

Según muestran casi mil páginas de documentos confidenciales revelados recientemente en virtud de la Ley de Libertad de Información (Freedom of Information Act), y que la Fundación de la Frontera Electrónica (Electronic Frontier Foundation) le suministró a Wired News, el FBI ha construido silenciosamente un complejo sistema de vigilancia que comienza a funcionar con solo posicionar el cursor y hacer clic. Dicho sistema interviene de manera inmediata casi cualquier dispositivo de comunicación. El sistema de vigilancia, conocido como DCSNet, sigla en inglés de Red de Sistemas de Recopilación Digital, conecta las salas de escuchas telefónicas del FBI con conmutadores controlados por operadores de cable de telefonía fija tradicionales, proveedores de telefonía por Internet y empresas de telefonía celular. La manera en que el sistema está entrelazado con la infraestructura nacional de telecomunicaciones es mucho más enrevesada de lo que sospechaban los observadores. Se trata de un "sistema de escuchas telefónicas abarcador que interviene teléfonos fijos, teléfonos celulares, sistemas de mensajes cortos (SMS, sigla en inglés) y sistemas 'pulse para hablar'", afirma Steven Bellovin, profesor de Ciencia de la Computación de la Universidad de Columbia y experto en vigilancia desde hace mucho tiempo. Esos son solamente los tres primeros párrafos del abarcador artículo sobre el sorprendente alcance de la arquitectura de vigilancia del FBI publicado hoy por Wired News. Matt Blaze, profesor de la Universidad de Pensilvania, conocido en parte por descifrar un hack para evadir los sistemas de escuchas telefónicas mediante la utilización de una característica del teléfono conocida como el Tono C, dedicó parte del tiempo de su apretado programa de viaje a ayudarme a comprender los documentos. Incluso, ya publicó un artículo propio acerca de estos, que fueron significativamente mutilados:

No obstante, la información que aparece en los documentos ofrece una visión singular, aunque fragmentada y críptica, del estado de la tecnología de vigilancia electrónica del FBI en general y, en particular, de las escuchas telefónicas practicadas en virtud de la Ley de Asistencia en Comunicaciones para los Cuerpos de Seguridad (CALEA, sigla en inglés).

Los documentos relativos al DCS, que tienen más de mil páginas, fueron publicados por la Fundación de la Frontera Electrónica. Solo pudieron salir a la luz gracias a los esfuerzos de Marcia Hofmann, quien demandó al FBI y logró que los revelaran. Todos los meses se publicarán más documentos sobre el DCS hasta que el FBI los haya revelado todos. Por su parte, el FBI respondió amablemente a mis preguntas acerca de los documentos y se ocupó de que yo no hiciera suposiciones infundadas ni me apoyara en información desactualizada. Randy Cadenhead, abogado de Cox Communications, también fue una pieza clave en la

confección del artículo. Entre las cosas que no quedaron en la versión final está el hecho de que Cox es la única gran empresa de telecomunicaciones que publica abiertamente sus planillas y tarifas para la realización de escuchas telefónicas. Esa documentación, que no revela ningún secreto nacional, debería estar en los sitios web de todas las compañías de telecomunicaciones, por una cuestión de transparencia. Desafortunadamente, ninguno de los grandes proveedores de telefonía inalámbrica respondieron —con la significativa excepción de AT&T— a las solicitudes de que hicieran comentarios sobre el asunto. Cadenhead también señaló que Cox Communications no participó en otros programas de escuchas telefónicas (entiéndase escuchas telefónicas realizadas sin orden judicial) que últimamente han hecho noticia; tampoco sabía nada acerca de ellos. En conclusión, todavía queda mucho por investigar sobre estos documentos y este asunto, y espero que los lectores de Wired News y THREAT LEVEL contribuyan. De hecho, ya Fat Cobra, un lector, señala que posiblemente las afirmaciones del FBI de que no ha habido penetraciones externas en el sistema de escuchas telefónicas no toman en cuenta el trabajo de Mossad, el servicio de inteligencia israelí. Actualizaré el artículo con los hallazgos de los lectores y con contribuciones de otros autores, como Steven Bellovin, profesor de la Universidad de Columbia, cuya valoración de los documentos hizo posible la realización de este trabajo. ----------

Posicione el cursor, haga clic… y espíe: cómo funciona la red de escuchas telefónicas del FBI Según muestran casi mil páginas de documentos confidenciales revelados recientemente en virtud de la Ley de Libertad de Información, el FBI ha construido silenciosamente un complejo sistema de vigilancia que comienza a funcionar con solo posicionar el cursor y hacer clic. Dicho sistema interviene de manera inmediata casi cualquier dispositivo de comunicación. El sistema de vigilancia, conocido como DCSNet, sigla en inglés de Red de Sistemas de Recopilación Digital, conecta las salas de escuchas telefónicas del FBI con conmutadores controlados por operadores de cable de telefonía fija tradicionales, proveedores de telefonía por Internet y empresas de telefonía celular. La manera en que el sistema está entrelazado con la infraestructura nacional de telecomunicaciones es mucho más enrevesada de lo que sospechaban los observadores. Se trata de un “sistema de escuchas telefónicas abarcador que interviene teléfonos fijos, teléfonos celulares, sistemas de mensajes cortos (SMS, sigla en inglés) y sistemas ‘pulse para hablar’”, afirma Steven Bellovin, profesor de Ciencia de la Computación de la Universidad de Columbia y experto en vigilancia desde hace mucho tiempo. La DCSNet es un paquete de programas que recopila, filtra y almacena números telefónicos, llamadas telefónicas y mensajes de texto. El sistema conecta directamente los puestos de espionaje del FBI en todo el país a una red de comunicaciones privada de gran alcance. Muchos de los detalles sobre el sistema y sus prestaciones fueron eliminados de los documentos entregados a la Fundación de la Frontera Electrónica, pero estos sí revelan que la DCSNet tiene al menos tres componentes de recopilación, y que todos se ejecutan en computadoras que funcionan con el sistema operativo Windows. El cliente DCS-3000, que tiene un costo de 10 millones de dólares y que también se conoce como Anzuelo Rojo, maneja pen-registers y dispositivos para captar y rastrear. Con este tipo de vigilancia se recopila información de señalización —principalmente los números marcados desde un teléfono—, pero no el contenido de las llamadas. (Los pen-registers registran las llamadas que salen y los dispositivos para captar y rastrear, las que entran.) El DCS-6000, conocido como Tormenta Roja, capta y recopila el contenido de las llamadas telefónicas y los mensajes de texto en los

casos en que existan órdenes de intervención completa. Un tercer sistema, que es secreto y se conoce como DCS-5000, se utiliza para escuchar las conversaciones telefónicas de presuntos espías y terroristas.

Lo que puede hacer la DCSNet La combinación de estos sistemas de vigilancia les permite a los agentes del FBI escuchar las grabaciones incluso mientras se está captando el contenido de las llamadas (TiVo es un ejemplo), crear archivos matrices de escuchas telefónicas, enviar grabaciones digitales a traductores, rastrear la ubicación aproximada de los objetivos en tiempo real utilizando la información que proporcionan las antenas de telefonía celular y hasta transmitir las grabaciones de las llamadas hacia furgonetas de vigilancia móvil. Las salas de escuchas telefónicas del FBI que se encuentran en oficinas de dicho Buró y en locales secretos de todo el país están conectadas por medio de una red primaria privada y encriptada, que es independiente de Internet. La compañía Sprint la administra en nombre del Gobierno. La red le permite a un agente del FBI que se encuentre en Nueva York, por ejemplo, intervenir de manera remota un teléfono celular cuya estación se encuentre en Sacramento, California, y de manera inmediata, conocer la ubicación del teléfono y luego comenzar a recibir conversaciones, mensajes de texto y códigos de acceso a correos de voz en Nueva York. Con solo oprimir unas teclas, el agente puede enviar los registros a especialistas en lenguas para que los traduzcan. Los números marcados se envían automáticamente a analistas del FBI entrenados para interpretar patrones de llamadas telefónicas, y son transferidos todas las noches, por medio de dispositivos de almacenamiento externo, a la Base de Datos de Solicitudes Telefónicas del Buró, donde son objeto de un tipo de minería de datos conocido como análisis de enlaces. Según la información contenida en páginas sin fechar de los documentos revelados, las estaciones de trabajo del FBI en la DCSNet han aumentado con los años: existían 20 “plantas de control central” cuando se inició el programa; ya en 2005 había 57. Por el año 2002, las estaciones de trabajo se conectaban a más de 350 conmutadores. Según el FBI, actualmente la mayoría de los proveedores de telefonía tiene su propio concentrador central, conocido como “conmutador intermedio”, que está interconectado con todos los conmutadores individuales del proveedor. Los programas informáticos del FBI que pertenecen al DCS se enlazan a los conmutadores intermedios a través de Internet, probablemente utilizando una red privada virtual (VPN, sigla en inglés) encriptada. Algunos proveedores administran el conmutador intermedio ellos mismos, mientras que otros les pagan a compañías como VeriSign para que se ocupen en su lugar de todo el proceso de las escuchas. El alcance numérico de la vigilancia a través de la DCSNet no se ha revelado aún. Lo que sí sabemos es que, a medida que las compañías de telecomunicaciones se han tornado más abiertas a la realización de escuchas telefónicas, la cantidad de escuchas para la investigación de casos penales solamente ha ascendido de 1 150 en 1996 a 1 839 en 2006. El aumento fue del 60 por ciento. Según un informe publicado el año pasado, en 2005, el 92 por ciento de esas escuchas para la investigación de casos penales se realizaron en teléfonos celulares. Estas cifras incluyen tanto las escuchas ordenadas por los estados, como las ordenadas por el Gobierno, pero no las escuchas para la investigación de casos de terrorismo, las cuales aumentaron significativamente después de los sucesos del 11 de septiembre. Tampoco incluyen la recopilación que hace el DCS-3000 de los números telefónicos de los cuales se recibe llamadas o a los cuales se llama. Para realizar este tipo de vigilancia, que es mucho más frecuente que las escuchas propiamente dichas, los investigadores solo deben certificar que lo números telefónicos objetos de vigilancia son importantes para alguna investigación.

El Departamento de Justicia informa la cantidad de pen registers que se someten a aprobación en el Congreso anualmente, pero esas cifras no se publican. Según las últimas estadísticas que se filtraron al Centro de Información de Privacidad Electrónica, los jueces firmaron 4 886 órdenes de pen registers en 1998, y prorrogaron otras 4 621.

La Ley de Asistencia en Comunicaciones para los Cuerpos de Seguridad cambia las disposiciones relativas a los conmutadores. La ley que permite el funcionamiento de la red de vigilancia del FBI tuvo su génesis durante el mandato de Clinton. En los años noventa, el Departamento de Justicia comenzó a quejarse al Congreso de que la tecnología digital, los teléfonos celulares y las prestaciones como la transferencia de llamadas les dificultarían a los investigadores continuar realizando escuchas telefónicas. El Congreso respondió con la aprobación en 1994 de la Ley de Asistencia en Comunicaciones para los Cuerpos de Seguridad, o CALEA (sigla en inglés), que exigía la existencia de puertas traseras en los conmutadores telefónicos de los Estados Unidos. La CALEA exige a las compañías de telecomunicaciones que instalen solo equipos de conmutación telefónica que cumplan con detallados estándares para la realización de escuchas. Antes de que existiera esta ley, el FBI obtenía una orden judicial para realizar una escucha y la presentaba a una compañía telefónica, que entonces creaba una conexión física al sistema telefónico. Con los nuevos conmutadores digitales que cumplen con la CALEA, ahora el FBI entra directamente a la red de la compañía de telecomunicaciones. Una vez que un proveedor recibe una orden judicial e interviene un teléfono, los datos de las comunicaciones de la persona sujeta a vigilancia se transmiten a las computadoras del FBI en tiempo real. La Fundación de la Frontera Electrónica solicitó documentos relativos al sistema en virtud de la Ley de Libertad de Información (FOIA, sigla en inglés) y demandó al Departamento de Justicia en octubre de 2006; ganó el caso. En mayo, un juez federal ordenó al FBI entregar documentos pertinentes a la Fundación todos los meses, hasta que haya satisfecho la solicitud hecha en virtud de la FOIA. “Se sabe tan poco hasta la fecha acerca de cómo funciona el DCS. Por eso es tan importante para los que solicitan información en virtud de la FOIA entablar demandas para conseguir lo que realmente quieren”, dice Marcia Hofmann, abogada de la Fundación. El agente especial Anthony DiClemente, jefe de la Sección de Adquisición de Datos e Intervenciones Telefónicas de la División de Tecnología Operativa del FBI, dijo que al principio, en 1997, el DCS se concibió como una solución temporal, pero, en virtud de la CALEA, se ha convertido en todo un paquete de programas de recopilación de datos. “La CALEA revoluciona el modo en que los cuerpos de seguridad obtienen información por medio de intervenciones telefónicas. Cuando no existía la CALEA, se utilizaba un sistema rudimentario que imitaba al Ma Bell”, dijo DiClemente a Wired News. Los grupos de privacidad y los expertos en seguridad se han quejado desde el principio de las disposiciones de la CALEA en materia de diseño, pero eso no impidió que los organismos federales rectores ampliaran recientemente el alcance de la ley para obligar a los proveedores de servicios de Internet de banda ancha y a algunas compañías de telefonía por Internet, como Vonage, a modernizar sus redes para que permitan la vigilancia del Gobierno.

Nuevas tecnologías Entretanto, según DiClemente, son interminables los esfuerzos que hace el FBI para mantenerse al día con la actual explosión de las comunicaciones. De acuerdo con los documentos revelados, los ingenieros del FBI especializados en escuchas telefónicas sostienen una ardua lucha contra la red de telefonía entre pares Skype, que no ofrece una

ubicación central que permita realizar escuchas telefónicas, así como contra innovaciones como la suplantación del número identificador de una llamada telefónica y el carácter portátil de los números telefónicos. No obstante, al parecer la DCSNet ha logrado mantenerse al día con al menos algunas nuevas tecnologías, tales como los sistemas "pulse para hablar" de los teléfonos celulares y la mayoría de los medios de la telefonía por Internet que utilizan el protocolo VOIP. "Vale decir que realmente podemos manejar los sistemas 'pulse para hablar'", dice DiClemente. "Todos los proveedores están cumpliendo cabalmente con sus responsabilidades en virtud de la CALEA". Matt Blaze, investigador de asuntos de seguridad de la Universidad de Pensilvania, quien en 2002 ayudó a evaluar el sistema de vigilancia de Internet denominado Carnivore, desarrollado por el FBI y actualmente en desuso, se sorprendió al ver que la DCSNet parece estar equipada para lidiar con tan modernas herramientas de las comunicaciones. Durante años el FBI se ha quejado de no poder intervenir estos servicios. No obstante, la documentación editada a conveniencia suscitó muchas interrogantes en Blaze. Particularmente dijo que no estaba claro el papel que debían jugar los proveedores al instalar un micrófono de escucha y la manera en que se asegura ese proceso. "La verdadera interrogante radica en la arquitectura de conmutación de las redes de telefonía celular ¿Cuál es el papel del proveedor en ese caso?", dijo Blaze. Randy Cadenhead, asesor de privacidad de Cox Communications, compañía que ofrece servicios de telefonía por Internet y acceso a Internet, dice que el FBI no tiene acceso independiente a los conmutadores de su compañía. "Nunca nada se conecta o desconecta hasta que yo lo ordeno, siempre y cuando tengamos una orden judicial en nuestras manos", dice Cadenhead. "Nosotros dirigimos el proceso de intervención desde mi escritorio, y las rastreamos cuando se inician. Damos orientaciones a las personas pertinentes de nuestra rama para interconectarnos y para establecer comunicación verbal con representantes técnicos del FBI". Los mayores proveedores de teléfonos celulares de la nación, cuyos clientes son objeto de la mayoría de las escuchas telefónicas, fueron los que menos colaboraron. AT&T rehusó gentilmente hacer comentarios, mientras Sprint, T-Mobile y Verizon sencillamente ignoraron nuestras solicitudes de que comentaran. El agente DiClemente, sin embargo, apoyó la versión de Cadenhead. "Los proveedores tienen todo el control. Esto se ajusta a lo establecido por la CALEA. Los proveedores tienen equipos de abogados que leen la orden; han establecido procedimientos para examinar in situ las ordenes judiciales y también verifican la información y confirman si el objetivo es uno de sus abonados", dijo DiClemente.

Costo Pese a su fácil utilización, se ha demostrado que la nueva tecnología es más costosa que un sistema tradicional de escucha telefónica. Según el inspector general del Departamento de Justicia, el Gobierno paga como promedio 2 200 dólares a las empresas de telecomunicaciones por realizar escuchas telefónicas conformes a la CALEA durante 30 días; una intervención tradicional, en cambio, cuesta solamente 250 dólares. En 2006, una orden federal de escuchas telefónicas costó unos 67 mil dólares a los contribuyentes, según se conoció por el más reciente informe sobre escuchas telefónicas de la Corte de los Estados Unidos. Más aún, en virtud de la CALEA, el Gobierno tuvo que pagar para que se hicieran adaptaciones a los conmutadores telefónicos fabricados antes de 1995 para hacer posible la realización de escuchas telefónicas. El FBI ha invertido casi 500 millones de dólares en este empeño, no obstante, muchos conmutadores tradicionales de cable metálico aún son incompatibles. También resulta costoso procesar todas las llamadas telefónicas captadas por la DCSNet. En la última etapa del proceso de recopilación de datos, las conversaciones

y los números telefónicos se transfieren al Sistema de Vigilancia Electrónica y Administración de Datos del FBI, una base de datos Oracle SQL que durante los últimos tres años ha experimentado un crecimiento de un 62 por ciento en el volumen de escuchas telefónicas y más de un 3 mil por ciento de crecimiento en archivos digitales como los correos electrónicos. En lo que va de 2007, el FBI ha gastado 39 millones de dólares en el sistema, que indexa y analiza datos para agentes, traductores y analistas de información de inteligencia.

Fallas en la seguridad Sin embargo, para los expertos en asuntos de seguridad la mayor preocupación en cuanto a la DCSNet no es el costo, sino la posibilidad de que el sistema de escuchas telefónicas mediante la presión de botones abra nuevas brechas en la seguridad de la red de telecomunicaciones. En 2005, más de 100 funcionarios del gobierno en Grecia supieron que sus teléfonos celulares habían sido intervenidos, luego de que un pirata informático desconocido se aprovechara de una prestación similar a las establecidas por la CALEA en la red de telefonía móvil de Vodafone. El intruso utilizó el software de control de escuchas telefónicas de los conmutadores para enviar copias de las llamadas y los mensajes de texto de los funcionarios a otros teléfonos, a la vez que impedía que el software de auditoría detectara las intervenciones. DiClemente, del FBI, dice que hasta donde sabe nunca la DCSNet había sido objeto de una infracción similar. “No he sabido de ningún acuerdo interno o externo”, dice DiClemente. Dice que la seguridad del sistema es más que adecuada, en parte porque para las intervenciones telefónicas aún “se requiere la ayuda de un proveedor”. El FBI también utiliza medidas de seguridad física para controlar el acceso a las estaciones de trabajo de la DCSNet y ha creado cortafuegos, entre otras medidas, para mantenerlas lo “suficientemente aisladas”, según DiClemente. Sin embargo, los documentos muestran que una auditoría interna realizada en 2003 puso al descubierto numerosas vulnerabilidades en la seguridad de la DCSNet, muchas de las cuales reflejan los problemas que años antes se detectaron en el programa Carnivore del FBI. En especial, las máquinas DCS-3000 carecían de un mecanismo adecuado para la entrada al sistema, su administración de contraseñas era insuficiente, no tenían programas antivirus, permitían un número ilimitado de contraseñas incorrectas sin bloquear la máquina y utilizaban sesiones compartidas en lugar de cuentas individuales. Para utilizar este sistema también era necesario que las cuentas de los usuarios del DCS-3000 tuvieran privilegios administrativos en Windows, lo que permitiría que un pirata informático con acceso a la máquina obtuviera un control total del sistema. Bellovin, el profesor de la Universidad de Columbia, dice que estos errores son terribles y que demuestran que el FBI no se da cuenta de los riesgos que se corren con el personal interno. “Las debilidades identificadas no constituyen precisamente el problema subyacente, sino la actitud que adopta el FBI hacia la seguridad”, dice. Para el FBI “la amenaza viene de afuera, no de adentro” y piensa que “en la medida en que existan amenazas internas, se pueden controlar por medio del proceso, más que por medio de la tecnología”, añade. Bellovin dice que cualquier sistema de escuchas telefónicas enfrenta un gran número de riesgos, tales como el hecho de que aquellos que son objeto de vigilancia descubran que su teléfono ha sido intervenido, o que alguien ajeno a la entidad o algún miembro corrupto de esta realice escuchas sin autorización. Además, los cambios en la arquitectura de los conmutadores telefónicos y de Internet dirigidos a facilitar la vigilancia pueden abrir nuevas brechas en la seguridad y la privacidad. “Desde el momento en que algo se puede intervenir, existe un riesgo. Con esto no quiero decir que no se realicen escuchas telefónicas, pero cuando se comienza a diseñar un sistema para que sea

intervenido, se comienza a crear una nueva debilidad. Una escucha telefónica es, por definición, una debilidad desde el ángulo de un tercero. La pregunta entonces sería: ¿puedes controlarlo?”.

Publicado en Rebelión.org

---

https://www.lahaine.org/est_espanol.php/revelan_red_de_escuchas_telefonicas_del9