Cómo saber si tu móvil está pinchado y cómo asegurarte de que no te espían con él

OTROMADRID.ORG :: 13/08/2009

La forma de evitar el espionaje mediante *roving bug* es dejar el móvil fuera de la sala en la que mantengas una reunión en la que se intercambie información delicada

Después de la denuncia de la oposición por escuchas ilegales, denuncia que ya está en los tribunales y que viene tristemente precedida de sonados casos de usos ilícitos de los servicios de inteligencia del Estado desde 1983 hasta la actualidad, en algunos medios políticos y sociales empieza a cundir la alarma ante la posibilidad de que cualquier llamada pueda ser "pinchada" e incluso filtrada a ciertos medios. A continuación me gustaría contestar a dos preguntas muy concretas sobre este tema: ¿existe un peligro real de que nuestras llamadas sean interceptadas? ¿Podemos hacer algo para detectarlo y para evitarlo?

¿Eres susceptible de ser espiado?

Empecemos por la primera pregunta. Para evitar caer en actitudes paranoicas, debemos tener en cuenta que la mayoría de la población carece de interés para los servicios de inteligencia. O dicho sea de forma más clara, que a los servicios de inteligencia les trae sin cuidado lo que comenta por teléfono la amplia mayoría de la población. Además, por supuesto, de los delincuentes, hemos de tener en cuenta que las personas cuyas llamadas podrían ser intervenidas son aquéllas que manejan información sensible o se sitúan en ámbitos incómodos para el poder: periodistas de medios críticos, políticos de la oposición, personas significadas de colectivos sociales, jueces desafectos al poder…

Así pues, si quieres tener una idea aproximada de si el Estado -o cualquier otro que tenga medios para hacerlo- está interceptando tus llamadas, has de responder en primer lugar a una pregunta: ¿tratas por teléfono asuntos que sean de interés para el poder o para grupos o medios capaces de intervenir tus llamadas? Si la respuesta es negativa -lo será en la mayoría de los casos-, puedes dejar de leer aquí este artículo.

Cómo saber si tu móvil está intervenido

Si la respuesta es un "sí", pasamos a la segunda pregunta, con la que ya entramos en consideraciones técnicas. Ante todo, has de tener claro que hoy los móviles ya casi no se "pinchan".

Es cierto que pueden ser intervenidos mediante la alteración de su tarjeta SIM, introduciéndoles sistemas de escucha o instalando en ellos software especialmente destinado a interceptar llamadas, como el FlexiSpy, que se vende con el reclamo de ser un método práctico para inutilizar o monitorizar tu móvil si te lo roban. También existen los "móviles espías", que se venden con el pretexto de controlar las llamadas de los hijos.

Sin embargo, hoy en día el método de intervención de llamadas más frecuente en los

móviles es el rastreo de la señal y es imposible detectarlo. Además, ese método de espionaje precisa de medios más o menos asequibles e incluso existe software para romper el cifrado A5/1 que usan las comunicaciones GSM de los móviles actuales. Para que nos hagamos una idea de los sencillos medios que se requieren para interceptar llamadas de esta forma, hace dos años un periodista británico fue condenado a prisión por interceptar 600 sms de personas del entorno de la familia real de ese país.

Para hacer frente a esa amenaza contra la privacidad de nuestras comunicaciones existen en el mercado varias soluciones, como el software de encriptación para móviles e incluso los móviles encriptados, pero lo que he visto en ambos terrenos hasta la fecha excede con mucho el precio de los móviles sin encriptar más caros del mercado, con lo que queda fuera del alcance de los bolsillos de la mayoría de los usuarios.

Tu móvil, un micrófono que puede ser activado a distancia Existe otro aspecto a tratar sobre el espionaje a los móviles y que mucha gente desconoce. Se trata de la técnica que se conoce como *roving bug*o escucha itinerante. Sobre la misma existencia de esta técnica de espionaje se ha especulado mucho durante años. Creo recordar que la primera noticia que tuve de ella, más en concreto de su utilización en España, fue en 2005 o 2006. Las especulaciones terminaron cuando en diciembre de 2006 un juez de EEUU reconoció que el FBI había activado remotamente los micrófonos de los móviles de una banda de mafiosos.

En eso consiste el *roving bug*: en activar el micrófono de un móvil de forma remota, aunque esté apagado, para utilizarlo como método de escucha.

Se ha discutido mucho sobre los requisitos que ha de reunir un móvil para poder ser activado de esta forma. Según algunos hace falta la instalación en él de un software que lo permita, bien físicamente o recibiendo un sms que lo contenga (es decir, con el *modus operandi*que siguen muchos virus informáticos). Sin embargo, hay muchos móviles que se activan si está programada una alarma a determinada hora. Ese mismo sistema de activación tal vez pueda usarse para convertirlos en micrófonos sin que su dueño se entere.

Cómo detectar y evitar que te espíen con el micro de tu móvil

De momento, existen tres formas de saber si un móvil está siendo usado como un *roving bug*, pues la activación remota del micrófono no se traduce en símbolo alguno en la pantalla del aparato. El primero es vigilar el consumo de energía: si el móvil consume batería más rápido de lo normal en reposo, es posible que el micrófono haya sido activado a distancia. También se puede notar ese uso en el calentamiento del móvil entre llamadas, al estar procesando más información de lo habitual en estado de reposo. Otro indicio es escuchar en el altavoz de una radio, de un televisor o de un ordenador la típica interferencia que provocan los móviles al recibir una llamada o un sms. Si un móvil en reposo produce continuamente esa interferencia tal vez esté remitiendo datos -los que recoge su micrófono- de forma furtiva.

La forma de evitar el espionaje mediante roving bug es dejar el móvil fuera de la sala en la que mantengas una reunión en la que se intercambie información delicada, o bien directamente sacarle la batería al móvil mientras dure esa reunión, pues el micrófono de tu móvil precisa de la energía de la batería para funcionar.

Por supuesto, estas instrucciones no pretenden ser un tratado técnico sino aportar soluciones que sean fáciles de entender para cualquier usuario. Si deseas corregir alguna parte de esta información o aportar algún dato más, puedes hacerlo en los comentarios de esta entrada (gracias por anticipado).

Artículos relacionados:
- Remotely Eavesdropping on Cell Phone Microphones, por Bruce Schneier
- 'This goes no further…', por Brian Wheeler en BBC News Online Magazine
- Roving Bug: espiado por el móvil, por Kriptópolis
- Telescreens and Roving Bugs, por Politricks
- ¿Tienes el teléfono móvil pinchado?, por Yoigo
- FlexiSpy
- ¿Cómo espiar el uso de un móvil?, por Constanza Villanueva

Ver También:
http://www.outono.net/elentir/?p=13370
