Nos escuchan

TODO AQUEL QUE UTILIZA UN MÓVIL PUEDE SER ESPIADO. LOS NUEVOS TELÉFONOS FACILITAN LA LABOR DE LOS INTERESADOS EN SEGUIR CONVERSACIONES AJENAS.

TEXTO **CARLOS TORRES** ILUSTRACIONES **ALBERTO VÁZQUEZ**

Nadie está a salvo. Las nuevas tecnologías han convertido el espionaje en un arma sencilla de usar. Ya no hace falta manejar los imponentes presupuestos de servicios secretos como el Mossad o la CIA. Los móviles de última generación han revolucionado el mundo del espionaje. Ahora, cualquiera puede husmear en la vida del prójimo, cualquiera puede estar siendo espiado.

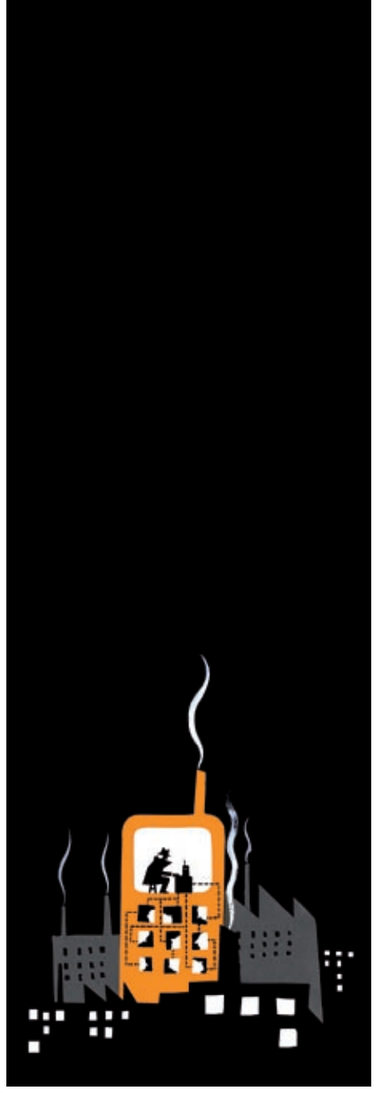
Espiar sale por 2.500 euros. Ese es el precio que cuesta regalar a alguien un Nokia N81 idéntico al habitual pero habilitado con el software necesario para escuchar las llamadas que el obsequiado realice o reciba. Además, el móvil espía hace las veces de micrófono ambiente, por lo que no solo pueden escucharse conversaciones telefónicas, sino también el entorno por el que se mueve la víctima, en todo momento y sin necesidad siquiera de que el teléfono esté encendido. El recurso, a simple vista sencillo, fue utilizado en 2002 por el FBI para investigar a la familia mafiosa los Genovese. Los federales activaron mediante control remoto los micrófonos de los móviles de varios miembros de este clan ligado al crimen organizado de Nueva York. Sin embargo, este dispositivo nació con otra función. "Nosotros lo vendemos como un móvil tutor para que los padres controlen qué compañías tiene su hijo o si está metido en problemas de drogas. Sin embargo, nos lo reclaman también empresarios que quieren controlar que no se esté sacando información de su empresa. También lo pide mucha gente para seguimientos de parejas infieles o empleados que se ausentan del trabajo o no cumplen con sus obligaciones", explica Antonio Durán, director de La Tienda del Espía (www.latiendadelespia.es), mientras manipula uno de estos móviles en la trastienda de una de sus sucursales en Madrid.

En este caso es más fácil conseguir que el espiado acepte un móvil a modo de regalo. "Los que compran el móvil se las arreglan para hacerlo llegar sin levantar sospechas a la persona que quieren escuchar. Se puede, por ejemplo, hacer que el trabajador lo utilice como móvil de empresa", cuenta Durán. Por motivos de seguridad, no todas las tiendas exhiben en sus catálogos fotografías de los modelos reales que modifican. "Así salvaguardamos mejor las características del producto", asegura el vendedor de dispositivos espías. Sin embargo, la mayoría de estos modelos son móviles de última generación y de grandes marcas para hacerlos más atractivos. Estos terminales se están sofisticando y algunos son capaces de valerse de la cámara que incorpora para grabar todo lo que ocurre cerca de él.

El software abarata las escuchas. En la primavera de 2007, la Guardia de Finanzas italiana puso en marcha en la ciudad de Vicenza la operación Spy Phones. La operación pretendía investigar las supuestas escuchas empresariales de un constructor a sus socios y a miembros de la competencia. El constructor, que se había opuesto a la OPA que el BBVA lanzó sobre el BNL de Italia, pidió a su secretaria que comprara un móvil para poder espiar conversaciones. La Guardia de Finanzas, que en un principio solo pretendía abrir diligencias sobre este caso, tiró del hilo y finalmente acabó investigando a más de 425 personas. Entre estas se encontraban los jóvenes inventores del software y las personas que lo vendían. El resto eran usuarios de este tipo de dispositivos. Francesco Polimeni, ingeniero italiano que vende este software a través de su tienda en Internet, spiare.com, asegura: "Nunca hemos tenido problemas con la policía, solo respetamos la ley. La ley dice que la venta del software es legal aunque esté prohibido instalarlo y utilizarlo. Nosotros hemos incluido la descripción del código penal en nuestra página para que los clientes sepan cuáles son los riesgos". A pesar de ello, aún hay quien se arriesga para conseguir escuchar determinadas conversaciones. "Hay muchos que se interesan en comprar el software, aunque algunos no pueden hacerlo porque no tienen el dinero suficiente o porque su móvil no es compatible. Por este tipo de productos se han interesado empresarios, políticos, policía, miembros de órganos del Gobierno y hasta hombres de la Iglesia", cuenta Polimeni desde Italia. Este software troyano debe ser introducido en el móvil de la víctima. Su precio, desde 859 euros, es más barato que comprar un móvil ya intervenido. "El uso de este software es, sin duda, una de las maneras más eficaces para mantener bajo vigilancia a una persona, en términos de coste, de privacidad y de rendimiento. Son teléfonos normales, al menos en apariencia, que ocultan en su interior un software instalado en secreto y que es invisible", asegura Polimeni.

Sin embargo, este sistema presenta más riesgos. Es el espía el que debe tener acceso al móvil del espiado para instalar el programa. Una vez realizada esta acción, el software será invisible para el usuario y todas las llamadas realizadas o recibidas por el móvil intervenido podrán ser escuchadas desde el teléfono asociado. Este tipo de programas sigue funcionando aunque el espiado lo detecte y cambie de tarjeta. Hay también otros sistemas más baratos que solo permiten la lectura de los mensajes de la bandeja de salida y entrada. Otros programas no necesitan siquiera tener un acceso físico al móvil en cuestión. Algunos troyanos enviados a través de SMS pueden conseguir modificar las características del móvil al que ataca hasta convertirlo en un flamante teléfono espía. Después, se puede descargar fácilmente al ordenador toda la información del teléfono, desde mensajes recibidos y enviados hasta la agenda telefónica del espiado. "Una vez convertido en móvil espía –asegura el ingeniero italiano–, el teléfono es una herramienta completa para la vigilancia en pequeños espacios y un localizador GPS, ya que mediante el satélite y la red del móvil es capaz de enviar SMS para desvelar su posición con un margen de error de unos pocos metros", cuenta.

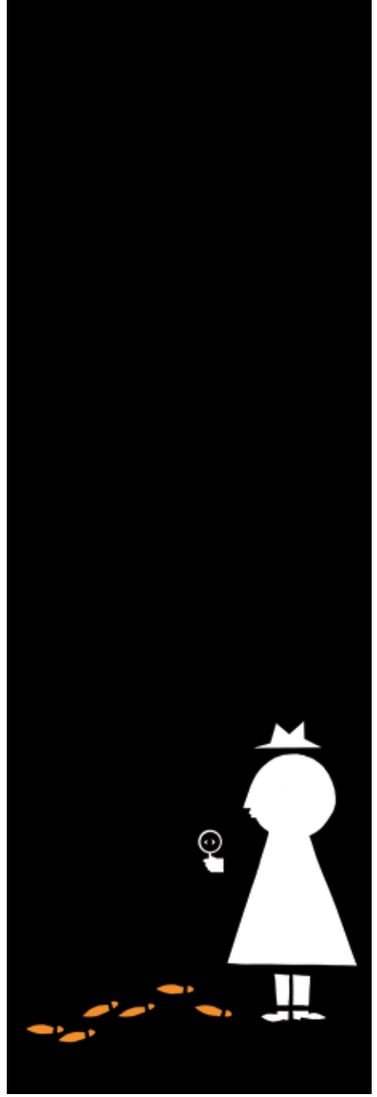
Codificar para estar seguros. En el transcurso de la investigación de la Operación Malaya, los cuerpos de seguridad trataron de intervenir todas las llamadas de Juan Antonio Roca, supuesto cerebro de la trama marbellí. Sin embargo, cuando este hablaba con su gente de confianza, las potentes máquinas de intervención telefónica de las que dispone la policía solo pudieron recoger un ruido extraño. Roca se había gastado 72.000 euros en la compra de ocho móviles especiales que utilizaban un sistema de codificación llamado secrafonía que garantiza un nivel de seguridad similar al que se utiliza en las conversaciones entre altos mandos militares. "Si todos los interlocutores utilizan aparatos con esta tecnología, sus conversaciones no podrán ser descifradas en años. Este dispositivo no solo evita que te escuchen, sino también que llegue al móvil software troyano", cuenta Antonio Durán. En su tienda, pueden encontrarse por 2.250 euros terminales de móvil a prueba de pinchazos. La secrafonía es también el sistema que utilizan los altos mandatarios para comunicarse entre ellos. Por ejemplo, cuando George Bush y José María Aznar eran presidentes de sus respectivos países instalaron una línea que permitía la comunicación sin escuchas entre la Casa Blanca y el palacio de la Moncloa. Después, con la victoria electoral de Zapatero y la reelección de Bush la línea cayó en desuso. Sin embargo, tras la llegada de Obama al poder, ambos mandatarios han retomado la utilización de la línea que coloca sus conversaciones al margen de oídos ajenos. Algunos mandatarios le cogieron el gusto, como el ex canciller alemán Gerhard Schröeder, que todavía utiliza móviles con esta tecnología a prueba de escuchas.



George Bush y Aznar instalaron una línea protegida por secrafonía para encriptar las conversaciones entre la Casa Blanca y la Moncloa

Las empresas también se blindan. El pánico al espionaje ha motivado también el blindaje tecnológico de muchas empresas ante la nueva amenaza de que cualquiera pueda convertirse en un espía a sueldo para la competencia. En 2003, Hyundai instaló en su centro de investigación de Namyang, próximo a la capital coreana de Seul, controles de rayos X para evitar la entrada de teléfonos con cámara, además de utili-

zar un sistema de rastreo de visitantes para conocer en todo momento donde se encontraban éstos dentro de sus dependencias. La compañía fabricante de vehículos también prohibió a directivos y altos ejecutivos el uso en sus oficinas centrales de móviles sofisticados e instaló potentes inhibidores que evitaran llamadas salientes o entrantes en las reuniones más importantes. La paranoia también se adueñó de los boxes de la Fórmula 1. Sobre todo a raíz de los últimos escándalos de fuga de información como el que salpicó al equipo McLaren hace dos años. El clásico espionaje entre escuderías dio un vuelco con la aparición de los nuevos móviles. Ahora, los controles de seguridad son más exhaustivos y las marcas han convertido en fortalezas sus sedes de fabricación. Más curioso es aún el caso de Samsung Electronics, uno de los mayores fabricantes de móviles. Esta empresa prohibió el uso de terminales de última generación en todas las plantas de su fábrica por considerar que las cámaras podían acrecentar el riesgo de espionaje industrial. No es un caso excepcional. "Muchas empresas españolas han prohibido la entrada de móviles y varias han comprado inhibidores para evitar que se produzcan llamadas. Por lo general, las empresas que invierten en este tipo de seguridad son las que investigan sobre nuevas patentes, como las farmacéuticas, o aquéllas que se juegan la campaña en la que van a lanzar un modelo nuevo", cuenta Francisco Marcos, detective privado y director de la agencia internacional de investigación Método 3. A veces, todas las precauciones son pocas. La compañía Microsoft sospecha que el robo de un móvil durante



un congreso de nuevas tecnologías celebrado el pasado febrero en Barcelona puede ser parte de una trama de espionaje industrial. El teléfono, que tenía instalado el último prototipo de sistema operativo para móviles fabricado por Microsoft, Windows Mobile 6.5, estaba siendo utilizado por un alto ejecutivo australiano hasta su desaparición.

El espía casi siempre juega en casa. "El espía puede ser cualquier empleado dentro de la empresa. Casi siempre suelen ser personas con graves problemas de dinero o con grandes deudas. Además, muchas veces son ellos mismos los que van a la competencia y ofrecen sus servicios y su información", asegura Francisco Marco. Ahora, los móviles han convertido a casi cualquier empleado en susceptible de volverse un espía. "En España, aunque todavía no está tan generalizado como en otros países, se rumorea que el espionaje a través de teléfonos móviles se utilizó, por ejemplo, en la OPA lanzada sobre Gas Natural", asegura el detective Francisco Marco. Este tipo de movimientos empresariales es uno de los escenarios donde con más celo se salvaguarda la información. Para evitar fugas o la aparición de espías las empresas con intereses económicos en juego contratan agencias de investigación privadas. Estas ponen en marcha un control exhaustivo en la empresa: "Se monitoriza en todo momento que no haya dispositivos con micrófonos, se hacen barridos periódicos para evitar escuchas, se comprueba que los ordenadores no hayan recibido ningún ataque o que los teléfonos no estén intervenidos… Se trata en el fondo de hacer un buen contraespionaje, sobre todo para evitar filtraciones cuando va a haber una OPA o fusión entre empresas", describe Marco.

Los empleados son los más pinchados. Sin embargo, los móviles como herramientas de espionaje se utilizan en mayor proporción en el ámbito de seguimiento a empleados sospechosos. Si se tienen dudas de un determinado trabajador, las empresas invierten en su seguimiento o en el control de sus llamadas. Alemania se ha visto salpicada por grandes casos de espionaje como los del Deustche Bank, que admitió haber espiado a sus propios directivos y a periodistas ajenos a la empresa, o el Deustche Bahn, compañía de ferrocarriles que intervino los e-mails de sus trabajadores. Pero quizá el más sonado sea el de la operadora de telefonía móvil Deustche Telekom, que tuvo que confesar haber espiado desde 2005 a varios de sus empleados. La mayor servidora de telecomunicaciones europea puso en práctica tácticas de espionaje para descubrir quién estaba filtrando noticias a la prensa. Para ello comenzó a controlar las llamadas de varios de los empleados de sus departamentos y de varios periodistas de los diarios que publicaban las noticias filtradas. Cuando es el propio servidor de la conexión móvil el que se convierte en espía, las posibilidades de éxito se multiplican. Sin embargo, para empresas más modestas o para particulares, existen otro tipo de herramientas más baratas. "Tenemos localizadores que pueden instalarse en un coche de la empresa o en cualquier otro lugar para asegurarse de que el empleado no lleva la información o un determinado objeto al lugar equivocado", explica Antonio Durán, director de La Tienda del Espía

Evita que te escuchen

* Vigila al detalle las facturas de móvil. Si tu teléfono envía un sms a un número desconocido después de cada llamada, tu terminal podría estar infectada con un software espía.
* Evita abrir mensajes de texto extraños. Podrían contener un troyano para controlar el móvil.
* Si cada vez que se acaba una llamada el móvil trata de conectarse a Internet o se activa el buzón de voz podría ser que el software espía esté tratando de enviar información.
* Si cuando hablas con alguien tu interlocutor escucha un pitido intermitente, tu teléfono podría estar intervenido.
* Si la batería se gasta más rápido de lo habitual y el móvil se calienta mucho, podríamos tener un software espía trabajando en nuestro móvil.
* Evita dejar el móvil al alcance de quien se sospecha que podría instalarnos este software.

Las escuchas se castigan con cárcel. En el año 2006, Andy Coulson, director del diario británico *News of the World,* tuvo que dimitir tras el grave escándalo que salpicó a su periódico. Clive Goodman, su especialista en la Casa Real, había contratado los servicios de Glenn Mulcaire, un detective privado, para pinchar el teléfono móvil del Príncipe de Gales. Goodman, que fue condenado a cuatro meses por poner en práctica sus dudosos métodos informativos, había publicado jugosas exclusivas del Príncipe Carlos. Pero en la Casa Real británica empezaron a sospechar. Goodman había informado de temas que solo se habían hablado en privado, como por ejemplo la lesión de rodilla del príncipe Guillermo. Poco después se descubrió que el periodista había accedido a esa información a través de las conversaciones entre padre e hijo. Cuando la policía siguió investigando al detective del que se había valido Goodman, descubrió que en su casa tenía listas de más de mil móviles controlados. La tela de araña de Mulcaire había alcanzado, entre otros, a George Michael, al alcalde de Londres, a Alex Ferguson, el entrenador del Manchester United, a la actriz Gwyneth Paltrow o a la modelo Elle Macpherson. Este tipo de escuchas pudieron hacerse mediante dos métodos. El más eficaz es utilizar "la máquina pura y dura que intercepta todas las llamadas telefónicas de un móvil. Sin embargo, su precio –ronda los 600.000 euros– hace que en España no haya ninguna en manos de particulares. Solo existen las que tienen las fuerzas de seguridad o el CNI", asegura Francisco Marco. Por su parte, Mulcaire no había utilizado este sistema. Los agentes de Scotland Yard descubrieron que el detective había conseguido atacar el buzón de correo del móvil del Príncipe Carlos. Si el buzón estaba codificado o necesitaba alguna clave, era Goodman quien llamaba al servicio de atención al cliente haciéndose pasar por el dueño del móvil para conseguir la información necesaria. En el transcurso del juicio reconoció haber llamado cerca de 500 veces. Finalmente, a Rupert Murdoch, magnate de la comunicación y dueño del periódico, la jugada de su periodista le costó un millón de libras en indemnizaciones por los daños causados. En España, la dureza con la que la Ley se emplea contra el espionaje hace que muchas empresas o particulares se lo piensen antes de llevar a cabo algún tipo de escuchas. El detective Francisco Marco asegura: "En este país hubo mucho espionaje industrial en la década de los 80 y los 90. Ahora, las escuchas telefónicas se penan con de uno a cuatro años de cárcel y ya no hay tantos empresarios dispuestos a arriesgarse con estos métodos".

Empresas como Samsung prohíben a sus empleados utilizar móviles de última generación en sus plantas por el riesgo de espionaje industrial

Contra los espías solo vale prevenir. Aunque resulta el más seguro, la secrafonía no es el único método eficaz de contraespionaje. "También se pueden comprar sistemas que detectan si hay algún teléfono pinchado o si se ha incorporado algún tipo de seguimiento por satélite a nuestro coche, maletín o demás", asegura Antonio Durán. Estos aparatos descubren si el micrófono del móvil está emitiendo información o si el móvil ha sido intervenido. "Los modernos sistemas de comunicación –apunta el italiano Polimeni– dan variadas posibilidades de intercambio de información. Sin embargo, estos dispositivo importantes pueden llegar a ser un peligroso instrumento para recoger información de forma ilegal. Para evitarlo yo recomiendo la utilización de una caja GSM, un dispositivo diseñado para detectar y avisar sobre cualquier tipo de software espía que tuviese el móvil. Además, también sirve para eliminar las interferencias de alrededor o evitar las ondas de radio que pretendan intervenir la llamada". A pesar de todo, el mejor camino es estar siempre alerta ante cualquier sospecha. "En España no somos de tomar medidas, somos más bien un país represivo que solo actúa cuando ya se ha producido el espionaje", opina Marco, que aconseja la previsión como mejor arma contra el espionaje. Sin embargo, nadie está a salvo. Los móviles han cambiado el espionaje. Antes todos podíamos ser espiados, ahora también todos podemos ser espías.