Durante muchos años las tarjetas SIM, ese pequeño dispositivo electrónico que sirve de lazo entre el usuario y el operador de telefonía móvil que todos nosotros tenemos insertados en nuestros móviles (ya sean inteligentes o no) e incluso tabletas, fueron considerados como totalmente seguros, invulnerables según operadores y los responsables de fabricar estas pequeñas tarjetas. Hoy, un reconocido investigador de seguridad alemán, llamado Karsten Nohl, ha dado la primicia y algunos detalles a Forbes de cómo ha logrado hackear tarjetas SIM, aprovechándose incluso de protocolos de seguridad que tienen varias décadas de haber sido ideados, y exponiendo así a millones de teléfonos y dispositivos ante esta vulnerabilidad.

Nohl asegura que le ha tomado tres años el lograr dar con la manera de hackear tarjetas SIM, y que no todas las tarjetas son afectadas, pero si alrededor de un 13% de las que hay en el mundo, lo que de igual manera supone muchos millones de terminales expuestos ante esta vulnerabilidad.

El fallo descubierto por Nohl y su equipo permitiría a criminales o espías (por ejemplo) vigilar de esta manera al usuario, al mejor estilo de la NSA y PRISM, pudiendo copiar por completo el contenido de la tarjeta SIM, grabar llamadas, redirigir las llamadas, enviar mensajes de texto desde la tarjeta SIM vulnerada e incluso, dependiendo del país, efectuar fraudes de pago (en África, por ejemplo, los pagos utilizando la tarjeta SIM son muy comunes).

La vulnerabilidad que haría posible el hackear tarjetas SIM estaría relacionada con dos factores. Primeramente, que muchas de estas tarjetas en el mundo aún utilizan un protocolo de cifrado y seguridad llamado DES (estándar de cifrado digital, por sus siglas en inglés), el cual fue creado por IBM en la década de 1970, y que hasta ahora no había sido vulnerado. Sin embargo, operadores como AT&T aseguran que sus tarjetas no son vulnerables dado que utilizan un nuevo protocolo llamado 3DS, que nació como evolución del creado por IBM.

El segundo factor al que estaría ligada esta vulnerabilidad tiene que ver con el lenguaje de programación *Java Card*, con el que han sido programadas unas seis mil millones de tarjetas SIM. Según el investigador Nohl, enviando un mensaje de texto binario (que el usuario ni siquiera podrá ver) se podría hackear esta tarjeta. El analista lo compara con la programación

sobre aire, mejor conocida como OTA.

Los detalles de este descubrimiento son muy técnicos y realmente el analista de seguridad no los ha explicado al detalle, aunque si se ha puesto en contacto con la asociación GSMA (de operadores móviles y compañías relacionadas a este mundo) para ofrecer la información correspondiente. Kohl dará todos los detalles de su descubrimiento durante la conferencia Black Hat 2013 de hackers y analistas de seguridad, que se llevará a cabo a finales del mes de julio.

Finalmente el analista alemán asegura que actualmente no hay manera de que esta información esté en manos malintencionadas, pero al conocerse que ya es posible vulnerar tarjetas SIM, calcula que en aproximadamente seis meses ya podrían haber hackers que descubran el fallo de seguridad, por lo que los operadores y la GSMA deben trabajar rápido.

Fuente: alt1040.com