Asociación de Internautas

Subcontratando el Titanic

Imagino que, más o menos, todos ustedes habrán oído hablar del tema, aunque sólo sea de pasada. Una empresa de seguridad informática de nacionalidad italiana, que había comenzado ofreciendo servicios de auditoría, *pentesting* y esas cosas, pasó en los últimos años a comercializar lo que ellos llamaban "soluciones de seguridad ofensiva". En realidad, lo que estos fulanos tenían en el mercado era puro *malware*, programas diseñados y concebidos para obtener acceso ilegítimo a sistemas informáticos ajenos. Desde limitarse a husmear, a manejar a distancia el equipo completo. No en vano, su producto estrella era conocido como RCS (*Remote Control System*, no necesita traducción, ¿verdad?).

Artículo del Teniente Kaffee en el Diario.es.-

Pues bien, a estos señores les ha entrado alguien hasta la cocina, y ese alguien se ha llevado algo así como un terabyte de información, del que han filtrado más de cuatrocientos gigas a través de Internet, que cualquiera puede descargar, analizar y compartir sus hallazgos. Y claro, se ha liado parda.

No es este el lugar, ni yo la persona adecuada, para ponernos a hacer disquisiciones técnicas sobre la cuestión. Pero sí que hay algunas repercusiones jurídicas que me gustaría analizar.

Lo primero de todo, siento pinchar el globo y estropear el ?paren las rotativas?, pero que el CNI tuviera tratos comerciales con estos caballeros no es ningún escándalo. Ni nada ilegal. A menos, claro está, que a estas alturas de siglo, todavía alguien se escandalice de que los espías adquieran herramientas de espionaje. ¡Coño, que es su trabajo!

Pero no es sólo una cuestión de sentido común: como ya les expliqué hace más de un año, existe una ley que autoriza a hacer este tipo de cosas a nuestro servicio de inteligencia, y lleva más de una década en vigor.

Ahora bien, dejando de lado la cuestión de la habilitación legal, hay algo que me preocupa sobremanera: las herramientas de inteligencia son, por definición, material restringido, y debería de tenerse mucho cuidado antes de andar negociando con ciudadanos extranjeros sobre su adquisición. Estaría muchísimo más tranquilo si ese tipo de herramientas se desarrollasen en nuestro país, por gente sobre la que se pueda tener cierto grado de control.

Bueno, en realidad, me consta que ese tipo de herramientas sí se desarrollan en nuestro país. Así que me gustaría saber qué narices hacen nuestros espías de compras en Italia. ¿Es que tenían rebajas? La cosa no es para reírse, la verdad, sobre todo cuando uno lee que los fulanos estos habían dejado una ?puerta trasera? en sus propias herramientas de espionaje, lo que les ha permitido hacer cosas como desactivarlas a distancia, al conocer la filtración. O sea, mucho control de seguridad, mucho bunker secreto, mucha restricción de teléfonos móviles, y mucha gaita peliculera, pero nuestros Anacletos patrios dejan que un informático extranjero pueda trastear en sus ordenadores desde vete tú a saber dónde.

En fin, hasta aquí la cosa tiene un pase. Malo, pero lo tiene. Lo que no me cuadra es lo de los Cuerpos y Fuerzas de Seguridad del Estado. Porque, de entre los datos filtrados al público, hay cosas que indican que el Cuerpo Nacional de Policía pudo tener algún tipo de relación contractual con esta empresa. Y al parecer, existen emails que prueban lo propio con representantes de la Guardia Civil. Lo que es sumamente curioso porque, a pesar de los avances en la tramitación parlamentaria de la reforma de la Ley de Enjuiciamiento Criminal, el uso de tales herramientas no está autorizado por la legislación procesal española. Vamos, que no se pueden obtener válidamente pruebas a través de estos mecanismos.

Que esa es otra, claro. Porque lo que prevén las futuras reformas son sistemas de inspección a distancia. Es decir, mirar pero no tocar. Al fin y al cabo, si hay que llevar esas evidencias ante un juez, resulta indispensable que estén intactas, que nadie haya hecho nada con los datos del sospechoso, más allá de recolectarlos. Y la posibilidad de controlar y auditar todo esto, poder demostrar en juicio que la evidencia no ha sido manipulada, es clave. En otras palabras, si el creador del software no puede acreditar suficientemente que no hace nada más que eso, el Estado no debería ni siquiera plantearse su uso.

Sin embargo, todo indica que Hacking Team no puede alardear de tales características. Sus ?soluciones de seguridad? usan esquemas idénticos a los del crimen organizado en Internet, y permiten manipular los datos del usuario inspeccionado. Vamos, que se parecen más a un troyano bancario tipo ZeuS, de los que se usan para vaciar cuentas corrientes en fraudes de ?phishing?, que a lo que tiene en mente el legislador para obtener pruebas de forma remota. El colmo del despropósito resulta que dicho software permita ?plantar? en el ordenador del objetivo falsas evidencias de tenencia de pornografía infantil. Inaceptable desde cualquier punto de vista. Por no decir delictivo.

Además, está la cuestión de la legitimidad de cara a la ciudadanía. No se puede investigar el delito de cualquier manera y a cualquier precio. Hay que tener infinito cuidado a la hora de diseñar un sistema legal en el que, adaptándose a los nuevos tiempos, se dote a la Justicia de herramientas tecnológicas aptas para combatir el crimen en entornos digitales. Cuando se persigue a un delincuente del que no se tienen datos para identificarle, sino tan sólo un punto de contacto a través de Internet, la posibilidad de usar software como el que contempla el proyecto de reforma de la Ley de Enjuiciamiento Criminal es sumamente valiosa. Pero hay que tener exquisito cuidado en el respeto a los derechos fundamentales. De lo que está surgiendo a la luz, resulta evidente que las aplicaciones informáticas comercializadas por los italianos no cumplen esos estándares ni de broma. Y alguien en la Administración española debería dar explicaciones al respecto.

Un viejo dicho popular, de esos que ahora aparecen en publicaciones de Facebook y cadenas de mensajes por Whatsapp, dice que el Titanic fue construido y pilotado por profesionales, mientras que el Arca de Noé lo fue por aficionados, y ya sabemos todos cómo acabó cada uno. Dejando aparte el dato de que el hundimiento del transatlántico fue un hecho históricamente documentado, mientras que lo del barco de madera lleno de animales es ficción religiosa, lo cierto es que la frase tiene su miga. En pocos campos se puede ver tan claramente como en este, y para muestra un botón: Hacking Team recurrió a un hacker ruso para comprar agujeros de seguridad que poder explotar con sus programas. No presentó un curriculum, ni tenía referencias de grandes empresas de seguridad informática, sólo un correo electrónico y una cierta reputación en los foros donde se discuten y presentan vulnerabilidades informáticas.

Aquí tenemos una gran parte del problema. Estados y empresas pueden invertir millones de euros en diseñar complejos sistemas de protección digital, en formar y reclutar ingenieros y expertos en seguridad de primer nivel. Pero en las catacumbas de Internet sigue habiendo gente anónima, con un conocimiento obsesivo de las máquinas a las que dedican sus desvelos, capaces de encontrar un error entre millones de líneas de código. Y eso resulta ser suficiente para ponerlo todo patas arriba.

Así que atraer y utilizar ese talento puede resultar sumamente tentador. El problema es que no se trata del tipo de gente que se presenta a una oposición, o que tenga el menor interés en correr cien metros, hacer diez flexiones o hacer prácticas de tiro. Así que resulta difícil encontrarlos entre los representantes de la Ley, aunque alguno hay.

Como decía la maldición china, nos esperan tiempos interesantes.

La actualización de la LECrim a las necesidades de la sociedad de la información. **El agente encubierto.**
