Filtración en Italia compromete a jefes de inteligencia

Por Raphael Satter
Associated Press, 16 julio 2015

LONDRES (AP) — Una espectacular filtración de información de una firma italiana de vigilancia sacó a la luz los detalles de ciberataques lanzados por gobiernos de todo el mundo y compromete a los jefes de inteligencia de gobiernos que van desde Ecuador y México hasta Corea del Sur. Un jefe de inteligencia ha renunciado y se ha levantado el telón sobre el espionaje en la era del iPhone.

Más de un millón de emails difundidos en el internet tras la filtración del 5 de julio revelan que la empresa Hacking Team vendió su software de espionaje al FBI y a la inteligencia rusa. Colaboró con gobiernos autoritarios en el Medio Oriente e hizo publicidad entre departamentos de policía de los suburbios estadounidenses. Incluso trató de vender sus productos al Vaticano, al tiempo que elaboraba una app bíblica para infectar las computadoras de la gente devota.

México es uno de los usuarios más activos de la tecnología, de acuerdo con la lista filtrada de los clientes. En Ecuador, se ha producido un escándalo al aflorar pruebas de que la Secretaría Nacional de Inteligencia utiliza el programa.

El caso "es un mini-Snowden", dijo el investigador de seguridad israelí Tal Be'ery, al comparar el impacto de la filtración con la difusión de documentos ultrasecretos de la NSA estadounidense por el excontratista de inteligencia Edward Snowden.

Be'ery, como muchos otros, sospecha que las agencias de seguridad del mundo se dedican a la ciberpiratería, pero lo notable, dijo, es "la ubicuidad: la usan en todos los continentes, tanto las democracias como las dictaduras".

Ante la difusión de facturas del servicio de inteligencia sudanés y de un fabricante de armas ruso, varios críticos, incluido un parlamentario europeo, han preguntado si la compañía violó sanciones internacionales. Una lista de clientes que incluye a Uzbekistán, Egipto y Azerbaiyán hace temer a grupos como Privacy International que el software espía es utilizado para amordazar a los disidentes.

Adicionalmente, mensajes del tipo "nos encanta su producto" enviados por alguaciles, policías y fiscales de todo Estados Unidos indican que las fuerzas de la ley y el orden quieren ensayar el programa.

El software de Hacking Team fue utilizado por 97 agencias de espionaje o investigación de 35 países, dijo el jefe de inteligencia surcoreano Lee Byoung Ho, al dar explicaciones al Parlamento el martes cuando salió a la luz que su agencia era uno de los clientes de la empresa con sede en Milán.

Hacking Team no respondió de inmediato a los pedidos de declaraciones, pero la compañía niega que haya violado sanciones o cometido delito alguno.

En declaraciones al diario italiano La Stampa el fin de semana, el gerente David Vincenzetti dijo que el programa se usa para combatir el terror y "descubrir a los lobos solitarios".

"Nosotros somos los buenos", aseguró.

Como revelan los mensajes, el programa de Hacking Team, llamado Remote Control System (sistema de control remoto), llega a los blancos por medio de enlaces maliciosos, documentos "envenenados" y pornografía. Se crean programas con trampas cazabobos adaptados a blancos de todo tipo; parece que Hacking Team está elaborando apps llamadas "Quran" (Corán) y "DailyBible" (BibliaDiaria).

Los emails revelan que la agencia de espionaje de Kazajistán trató de obtener el chateo del teléfono Samsung de un blanco y el ministerio del Interior saudí usó un auricular infectado como una señal de rastreo. También revelan cómo la autoridad anticorrupción de Mongolia trató de robar la contraseña para Facebook de una persona al registrar su tecleo y cómo la policía checa transformó el micrófono de un BlackBerry en un artefacto de escuchas. Vincenzetti dijo a La Stampa que el programa espía incluso podía fotografiar automáticamente a una persona cuando efectuaba una llamada telefónica.

Legisladores en Italia y República Checa han interrogado a jefes policiales y de inteligencia sobre el uso del programa. El jefe del servicio de inteligencia chipriota, Andreas Pentaras, renunció al revelarse que utilizaba el programa.

Rara vez se sabe quiénes son los blancos del espionaje, pero en uno de los emails filtrados, fechado el 15 de diciembre de 2014, Vincenzetti insinúa que a veces tiene una idea bastante exacta de quién se trata.

"A veces me llama, digamos, el subjefe de la policía italiana y me dice, '¡Felicitaciones, señor Vincenzetti!' Le digo, 'Gracias, señor, ¿podría decirme a qué se refiere?' '¡Me refiero a lo que usted leerá mañana en los titulares de los periódicos!', dice entre risas y corta la llamada. Al día siguiente leo que han arrestado por fin a un capo de la mafia, que el misterio aparentemente impenetrable de un asesinato brutal ha sido resuelto y el asesino arrestado, etcétera".

Vincenzetti insinuó que se le ocultaba al resto del mundo los ciberataques de los gobiernos.

Las autoridades "nunca revelan cómo lo hicieron porque quieren proteger nuestra tecnología y protegernos", dijo.

Para investigadores como Be'ery, la filtración les ha permitido comprender como nunca antes cómo hackean los gobiernos. Para los defensores de los derechos humanos, confirma sus temores sobre la vigilancia estatal. Adicionalmente, para

las víctimas del programa del Hacking Team —como el conocido bloguero emiratí Ahmed Mansoor— ha sido una buena oportunidad para regocijarse con el mal ajeno.

"Ahora comprenden qué se siente cuando alguien se entromete en tu vida privada", dijo.

___

Los periodistas de The Associated Press Menelaos Hadjicostis en Nicosia, Chipre; Karel Janicek en Praga, República Checa; y Gonzalo Solano en Quito, Ecuador, contribuyeron para este despacho.