ADC / Asociación por los Derechos Civiles

La ADC alerta: software de interceptación y vulneración a los derechos humanos

Agosto de 2015

Recientes noticias relativas a la presencia de virus espías en los celulares del fallecido Fiscal Nisman y del periodista Jorge Lanata, que se producen escasos días después de la revelación de las filtraciones de la empresa Hacking Team y sus contactos con autoridades de la Argentina, pone una vez más la alerta en los sistemas de vigilancia de las comunicaciones y la necesidad de adecuar estos sistemas a estándares internacionales de Derechos Humanos, tal y como lo puso de manifiesto la Relatoría para la Libertad de Expresión de la Corte Interamericana de Derechos Humanos (CIDH)[1].

El momento resulta crítico pues estas noticias se ubican en un contexto de proceso electoral presidencial y legislativo y, paralelamente, de transición del Sistema de Inteligencia desde la desacreditada ex SIDE a la actual conformación de la AFI y la Nueva Doctrina de Inteligencia Nacional de reciente reglamentación.

Destacamos que utilizamos este tipo de información (correos privados filtrados) pues es información que se ha hecho pública y que permite conocer cómo funciona un sector del Estado injustificadamente opaco. Si hubiera información pública disponible no sería necesario referir a este tipo de filtraciones, pero como el sector se caracteriza por su secretismo lo que el mundo ha logrado conocer sobre el funcionamiento de los servicios de inteligencia y los mecanismos de vigilancia lo ha logrado a través de este tipo de filtraciones de material en principio secreto o privado.

I. La declaración de la Relatoría Especial para la Libertad de Expresión

El pasado martes 21 de julio de 2015 la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) publicó un comunicado de prensa expresando su preocupación por las recientes filtraciones de la empresa Hacking Team y su incidencia sobre los gobiernos de la región en relación

[1] Área de Privacidad de la ADC. Agradecemos la colaboración de Leandro Ucciferri en la producción de este informe.

a la implementación de programas de vigilancia masiva de comunicaciones electrónicas.

La Relatoría estableció que la compra e implementación de software de vigilancia puede generar un serio perjuicio a los derechos a la intimidad y a la libertad de pensamiento y expresión e instó a las autoridades a investigar, ofrecer una explicación clara sobre los hechos sucedidos y aplicar las sanciones correspondientes. En esta Declaración la Relatoría hizo un llamado a los Estados para que revisen sus legislaciones pertinentes y modifiquen sus prácticas de vigilancia con el fin de adecuarlas a los principios internacionales sobre Derechos Humanos, según los cuales el uso de sistemas de vigilancia debe estar establecido en la ley en forma clara y precisa para casos excepcionales y selectivos y limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos.

La ley debe consagrar un objetivo legítimo; establecer los límites, naturaleza, alcance y duración de las medidas de vigilancia, así como también las razones para ordenarlas; determinar cuáles son las autoridades competentes para su autorización, ejecución y supervisión y brindar los mecanismos legales para su impugnación. Todas las decisiones para realizar tareas de vigilancia deben ser autorizadas por autoridades judiciales independientes respetando siempre los principios del debido proceso.

Finalmente la Relatoría resaltó que tanto la transparencia como el acceso a la información sobre los programas de vigilancia utilizados por los Estados son elementos esenciales de una sociedad democrática Asimismo llamó la atención sobre cualquier intento por silenciar a periodistas y medios de comunicación que denuncien estas actividades quienes bajo ningún motivo pueden ser sometidos a sanciones ulteriores por divulgar esta información considerada de interés público.

II. ¿Qué es Hacking Team?

En el año 2001 dos programadores italianos desarrollaron el software conocido como Ettercap, una herramienta gratuita y de código abierto que permite realizar ataques de tipo man-in-the-middle a través de los cuales pueden interceptarse contraseñas, realizarse escuchas y manipularse computadoras de manera remota. La herramienta rápidamente se convirtió en la elección de analistas de seguridad informática para probar la infraestructura de su red y comenzó a ganar popularidad. Años más tarde y, gracias a la efectividad de Ettercap, los autores del mismo recibieron una llamada de la policía de Milán ya que estaban interesados en contratarlos para que desarrollaran un controlador para Windows que les permitiera escuchar las llamadas de Skype de un objetivo determinado.

Así fue como Alberto Ornaghi y Marco Valleri, junto a Valeriano Bedeschi y David Vincenzetti, fundaron luego Hacking Team en el año 2003, empresa que fue creciendo hasta ser uno de los principales proveedores de software de vigilancia del mundo con clientes en más de una docena de países en múltiples continentes.

El principal software que comercializa Hacking Team es una suite de herramientas denominada Remote Control System (RCS), también conocida como Da Vinci o Galileo. La misma se configura y personaliza de acuerdo a los requerimientos particulares de cada cliente y el tipo de espionaje que éste llevará cabo. Una vez infectado el dispositivo del objetivo, a través de RCS es posible recolectar emails, conversaciones de WhatsApp, chats de Skype, SMS, historial de llamadas y contactos; grabar las pulsaciones del teclado; acceder al disco duro, las llaves de seguridad cifradas y el audio e imagen de la webcam; registrar el historial de búsqueda; utilizar el micrófono del teléfono de un objetivo para captar sonidos de ambiente y conversaciones; activar el teléfono o la computadora de manera remota e interceptar el GPS del teléfono para realizar seguimientos del objetivo.

El domingo 5 de julio fue publicado, a través de la cuenta oficial de Twitter de Hacking Team, una serie de mensajes que ponían de manifiesto que la empresa había sido hackeada y más de 400 GB de información habían sido liberados para que cualquier persona los pudiese bajar a través de BitTorrent. Por el momento se sospecha que el responsable habría sido la misma persona o grupo de personas que estuvo detrás del hackeo a Gamma International, otra empresa del mismo rubro de Hacking Team. A través de este suceso, se pudo acceder a millones de emails, grabaciones de audio, código fuente de diversos software, listas de clientes, información fiscal, contratos y documentos financieros.

Hacking Team siempre negó públicamente que trabajara junto a países con regímenes autoritarios, gobiernos corruptos, represores de derechos y libertades civiles. Pero a través de las filtraciones se pudo conocer quiénes habrían sido, y seguirían siendo, clientes de la empresa y cuáles serían las inversiones que realiza cada gobierno. Desde Estados Unidos, con la Drug Enforcement Administration (DEA) y la Federal Bureau of Investigation (FBI) y España con la Policía Federal y el Centro Nacional de Inteligencia (CNI), hasta Egipto, Sudán, Rusia, Omán, Emiratos Árabes Unidos y Kazajistán, por nombrar algunos.

En Latinoamérica la presencia de Hacking Team impactó principalmente en México que encabezaría la lista de clientes de la empresa con una suma de casi 6 millones de euros invertidos en la compra de software para espionaje. De la región también se sumarían Chile, Colombia, Ecuador, Honduras y Panamá, aunque con inversiones menores.

III. Presencia en Argentina

A pesar que Argentina no se encontraba en los listados de clientes de Hacking Team ni se encontraron contratos de transacciones realizadas, los emails filtrados daban cuenta de conversaciones que habrían tenido lugar entre representantes de la empresa italiana y empresas nacionales interesadas en adquirir sus productos para el uso de distintas entidades estatales argentinas.

De los correos filtrados surge el siguiente relato.

En marzo del 2012 tres integrantes de Hacking Team, organizaron una visita a Buenos Aires con el fin de realizar una demostración de la herramienta Remote Control System (RCS) a varias entidades estatales argentinas. Las reuniones se habrían desarrollado entre el 19 y el 23 de marzo en el Hotel Hilton de Puerto Madero y habrían contado con la presencia de miembros del Ministerio de Seguridad de la Nación (Dirección Nacional de Inteligencia Criminal), del Ministerio Público Fiscal (Unidad de Investigaciones Complejas) y del Ministerio de Justicia y Seguridad de la Provincia de Buenos Aires.

A los pocos días de la visita, en el email con su reporte sobre las reuniones, uno de los representantes de Hacking Team contó que el Jefe de Prefectura, ausente en las reuniones, habría solicitado una charla privada sin especificar los motivos. A su vez, aclaró que para que las operaciones se pudieran completar con éxito, se debería sobornar a los diferentes jefes de cada departamento por cada producto (software) que trajera al país.

En julio del 2014 un intermediario de la empresa Nullcode Team dedicada al reporte de vulnerabilidades, audición de código, búsqueda de bugs y servicios de seguridad, se habría puesto en contacto con Hacking Team con el fin de conocer los costos de la herramienta RCS Hacking Team contestó que la política interna de la empresa únicamente les permitía brindar sus productos a agencias de seguridad y entidades gubernamentales, pero que podrían trabajar en conjunto sobre posibles negocios en Argentina mientras estuvieran relacionados con el gobierno. Los emails no mencionan que se haya concretado ninguna operación, tan solo la firma de un NDA (acuerdo de confidencialidad) entre Nullcode Team y Hacking Team para seguir con la negociación.

Ese mismo mes un intermediario de la empresa TAMCE, que trabajaría junto a organismos gubernamentales brindando tecnología para investigación y seguridad ciudadana, se habría puesto en contacto con Hacking Team con el fin de discutir oportunidades de negocio en México y Latinoamérica. Un año después, en marzo del 2015, este mismo intermediario de TAMCE se habría puesto nuevamente en contacto con Hacking Team preguntando esta vez si la empresa estaría interesada en trabajar con el nuevo servicio de inteligencia de Argentina (Agencia Federal de Inteligencia, ex SIDE) ya que ellos -en referencia a TAMCE- eran proveedores oficiales y la agencia estaría buscando soluciones IT.

La conversación sigue con con otro representante de Hacking Team, quien comparó el producto de Hacking Team (es decir, la herramienta RCS), con Pegasus de la firma israelí NSO Group. Este representante aclaró en los emails que Hacking Team estaría trabajando a la vez con otro socio en Argentina, en referencia a la firma Global Interactive Group S.R.L.

El intermediario de TAMCE les comunicó que el 23 de junio de 2015 se habría reunido con el director de la Agencia Federal de Inteligencia para (AFI) una demostración del producto de Hacking Team ya que aún no habría cerrado la negociación con NSO Group y, por lo tanto, seguirían buscando soluciones. Hacking Team habría

contestado que “le parece muy bien que estén a tiempo con AFI y que estén buscando una solución ofensiva de intercepción”.

El 21 de abril de 2015 un intermediario de la empresa Global Interactive Group S.R.L, que se enfoca a la consultoría estratégica y tecnológica junto a organismos gubernamentales e instituciones públicas y privadas, se habría comunicado con Hacking Team solicitando un NDA (acuerdo de confidencialidad) e información de sus productos poniendo de resalto que tenía un excelente mercado para sus herramientas en Argentina con llegada directa a varias entidades estatales: Ejército, Gendarmería, Prefectura, Policía Federal, Policía provinciales y AFI.

En mayo de 2015 Hacking Team y Global Interactive Group S.R.L. habrían firmado un NDA (acuerdo de confidencialidad), y y Global Interactive Group S.R.L. estaría organizando demostraciones del software en el mes de agosto de 2015.

IV. Reflexiones

Si bien las circunstancias referidas en el relato anterior son todavía materia de comprobación, este tipo de información es la única que hasta ahora ha permitido conocer sobre el funcionamiento de este sector.

Las prácticas de vigilancia mantenidas durante años en nuestro país dan cuenta de la opacidad, distorsión e irregularidades que han caracterizado a nuestros organismos de inteligencia tal y como lo puso de manifiesto la ADC en el informe publicado el pasado mes de enero.

No está demás entonces recordar, dado el contexto mencionado, los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (ver aquí), de los cuales ADC es signataria junto con más de 400 organizaciones y expertos a nivel mundial.

En este documento se establece que para determinar si el Estado puede llevar a cabo vigilancia de comunicaciones que interfiera con información protegida (que es aquella que incluye, refleja, surge de o se refiere a las comunicaciones de una persona y que no está fácilmente accesible o disponible para el público en general) el mecanismo de vigilancia debe ser compatible con los principios de Legalidad, Objetivo Legítimo, Necesidad, Idoneidad, Proporcionalidad, Autoridad Judicial Competente, Debido Proceso, Notificación del Usuario, Transparencia, Supervisión Pública, Integridad de las Comunicaciones y Sistemas, Garantías para la Cooperación Internacional y Garantías contra el Acceso Ilegítimo y Derecho a Recurso Efectivo.

La Nueva Doctrina de Inteligencia Nacional contiene aspectos, al menos en su origen, alineados con algunos de estos principios y así lo pusimos de manifiesto en nuestro análisis preliminar (ver aquí) pero queda todavía un largo camino por recorrer.

Los eventos y noticias mencionadas, que aparecen como pequeñas puntas del iceberg de un sistema hasta ahora inquietante, muestran el enorme desafío que tenemos por

delante, no sólo los organismos de sociedad civil, sino también los legisladores, los funcionarios públicos y judiciales, las empresas de telecomunicaciones y de tecnología y la sociedad toda. En este camino los estándares de derechos humanos deben ser nuestra guía.