

Violar la privacidad digital: el sueño que Hacking Team cumplió en América Latina (Video)

Por: Gisela Pérez de Acha. Aristegui Noticias. 22/04/2016

El uso de programas de espionaje como Galileo o Da Vinci es contrario a los estándares legales de cada país y viola los derechos a la privacidad, a la libertad de expresión y al debido proceso, concluye el informe “Hacking Team Malware para la Vigilancia en AL”, de acuerdo al informe de Derechos Digitales.

Acceso ilimitado a la vida digital de los ciudadanos: el sueño de los gobiernos de América Latina que cumplió Hacking Team, la empresa italiana que vende un software capaz de entrar y robar todo tipo de información de celulares, computadoras y tabletas.

El informe “Hacking Team: malware de espionaje en América Latina”, publicado por Derechos Digitales en conjunto con Aristegui Noticias, aporta un análisis legal en cada uno de los 13 países de la región que compraron -o intentaron comprar- el programa que accede a contraseñas, contactos, mensajes y correos electrónicos; llamadas telefónicas; que además controla micrófono y webcams; tiene acceso a nuestras redes sociales; puede saber dónde estamos en todo momento y registra cada una de las teclas apretadas, clics del mouse y sitios de internet visitados.

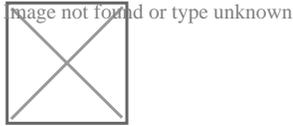
La principal conclusión del documento es que el uso de esta tecnología es contraria a los estándares legales de cada país y viola los derechos a la privacidad, a la libertad de expresión y al debido proceso.

Una buena parte de los países de América Latina tiene pasados dictatoriales, y democracias presentes cuestionadas por su autoritarismo. Por lo mismo, es especialmente preocupante que las autoridades cuenten con herramientas de este tipo.

Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá compraron licencias

para el uso de Galileo o DaVinci, los nombres comerciales del programa Remote Control System (RCS), que es capaz de invadir cualquier dispositivo electrónico.

Argentina, Guatemala, Paraguay, Perú, Uruguay y Venezuela contactaron a la empresa y negociaron precios, pero las ventas no fueron concretadas.



Mapa basado en la obra “Hacking Team en América Latina: El negocio de espiar a las personas”
CC:BY Constanza Figueroa y Vladimir Garay
Diseño: Gustavo Varguez / Aristegui Noticias

El *Acuerdo de Wassenaar* impide que Hacking Team venda el *software* de espionaje directamente a los gobiernos, por lo mismo todas las compras y negociaciones se hicieron través de empresas intermediarias. Las más recurrentes en América Latina son Robotec en Colombia, Ecuador y Panamá; y la israelí NICE Systems, en Colombia, Honduras y Guatemala.

El representante de NICE Sytems es **Ori Zoller**, un ex militar israelí dedicado a la venta de armas AK-47 que eventualmente terminaron en manos de grupos paramilitares de Colombia, según The Intercept.

Las negociaciones se realizaron en secreto, hasta que el 5 de julio de 2015 se expusieron públicamente 400GB de información de la empresa, incluyendo correos electrónicos, facturas, documentación interna y parte del código de Hacking Team.

sitio

Image not found or type unknown

La filtración reveló que varios gobiernos compran el programa con el objetivo de **combatir a la delincuencia**, pero en algunos casos se utilizó con fines políticos o bajo un marco legal que no garantiza el beneficio público.

En Ecuador se utilizó tecnología de Hacking Team para vigilar a Carlos Figueroa, opositor del gobierno de **Rafael Correa**. **En México**, un país que vive una seria crisis de derechos humanos, ocho de las diez autoridades que compraron el *software* no están facultadas para ejercer actividades de vigilancia.

México es el cliente más importante de Hacking Team en el mundo, pagando una suma de 5 millones 808 mil 875 euros. El organismo de inteligencia, Centro de Investigación y Seguridad Nacional (CISEN), pidió 2 mil 74 órdenes judiciales para

poder utilizarlo; hasta la fecha, no hay forma de saber si su uso está justificado.

En Puebla el *software* se utilizó para espiar a periodistas, opositores políticos y estudiantes de la Universidad Iberoamericana.

En Panamá, el ex presidente **Ricardo Martinelli** estuvo personalmente al tanto de las negociaciones con Hacking Team. En Chile, en cambio, la Policía de Investigaciones dijo en un comunicado que la vigilancia se hacía con fines estrictamente legales y bajo orden judicial. Sin embargo, las órdenes judiciales en este caso no son suficientes para garantizar el uso legítimo del *software* de espionaje.

La información de Hacking Team permitió saber que la Administración para el Control de Drogas de Estados Unidos (DEA, por sus siglas en inglés) **intercepta todas las comunicaciones de los ciudadanos colombianos**. Así mismo, se sospecha del uso de herramientas de este tipo contra Vicky Dávila, periodista que investiga una red de prostitución masculina al interior de la policía.

En términos legales, este tipo de *software* no está regulado explícitamente en ningún país, y ahí está el problema de legalidad. En México y Colombia existen disposiciones más amplias al respecto, pero con lenguaje vago e impreciso. La ausencia de regulación deja al arbitrio de las autoridades, muchas veces corruptas, el uso, aplicación y objetivos del programa de espionaje de Hacking Team.

El requerimiento de una orden judicial para interceptar comunicaciones está en todos los países analizados, pero no es una herramienta suficiente de control, porque el *software* de Hacking Team es mucho más invasivo que una interceptación y accede a otro tipo de documentos que no son comunicaciones. Por lo mismo, se viola el derecho al debido proceso.

En todos los países analizados existen sanciones penales contra quien invada o intervenga los sistemas informáticos o las comunicaciones privadas de una persona fuera de la legalidad de una investigación, pero hasta ahora sólo Panamá ha abierto procesos al respecto.

El problema del espionaje indebido va mucho más allá de Hacking Team, implica a un mercado global que **abusa la tecnología de vigilancia** en manos de gobiernos alrededor del mundo.

Debe existir mayor transparencia en el uso y adquisición de estas herramientas, una discusión abierta sobre los estándares que deben regir esta tecnología y además sanciones penales en los casos **que lo ameriten**.

Fuente: <http://aristeguinoticias.com/1804/mexico/violar-la-privacidad-digital-el-sueno-que-hacking-team-cumplio-en-america-latina/>

Fotografía: aristeguinoticias

Fecha de creación

2016/04/22