Sociedad Civil de América Latina rechaza *software* espía de Hacking Team

El domingo 5 de julio, se expusieron públicamente 400GB de información de la empresa italiana Hacking Team, dedicada a la comercialización de software de espionaje para gobiernos. Los documentos incluyen facturas, correos electrónicos, datos fiscales y código fuente, entre otros archivos. Las revelaciones permiten entender los alcances a nivel global de Hacking Team, una compañía que fue catalogada en 2013 por Reporteros Sin Fronteras como uno de los "enemigos de Internet".

El software de espionaje comercializado por Hacking Team, conocido también como DaVinci o Galileo, es un programa que infecta los dispositivos de la persona atacada, permitiendo sustraer datos, mensajes, llamadas y correos. El atacante también obtiene acceso al micrófono, cámara y teclado para registrar imágenes, audio o cualquier otra actividad sin conocimiento de la persona afectada.

En la filtración se halló que seis países de América Latina son clientes de Hacking Team: Chile, Colombia, Ecuador, Honduras, México y Panamá. Dependencias como la Policía de Investigaciones de Chile (PDI), la Secretaría de Inteligencia de Ecuador (SENAIN) la Dirección de Inteligencia Policial de Colombia (DIPOL) o el Centro de Investigación y Seguridad Nacional de México (CISEN) han adquirido licencias de software de control remoto (RCS) a la empresa italiana. En el caso de México, se identificaron hasta 14 contratos individuales con la compañía, por parte del gobierno federal y los gobiernos estatales, algunos de ellos sin facultades legales para la intervención de comunicaciones privadas.

Las organizaciones de la sociedad civil de América Latina rechazamos la venta y adquisición de estos programas de vigilancia, que sin controles adecuados, ponen en riesgo los derechos humanos de la región, por los siguientes motivos:

1. El proceso de compra ha sido realizado con total opacidad. Exigimos que los Estados involucrados realicen esfuerzos para asegurar la transparencia de sus actividades de inteligencia, en particular relativos a la compra y tipo de utilización efectiva de tecnologías que permiten vigilancia informática, ante la posibilidad real de que este software esté siendo utilizado para espiar a activistas y disidentes sin causa justificada. En 2013, la firma Kaspersky ya demostró que DaVinci fue usado para el espionaje de activistas políticos en el Medio Oriente.

2. Debido a los bajos estándares de control legal en la adquisición y uso de las tecnologías de vigilancia en la región, se necesita una discusión abierta en los Congresos nacionales acerca de las leyes que rigen y regulan las actividades de vigilancia, sometidas al escrutinio público. Ante

la posibilidad técnica de que estas actividades pongan en riesgo derechos humanos, estas legislaciones deben reflejar los estándares más altos y sujetar las acciones de los organismos de inteligencia a la autorización previa de un organismo judicial imparcial e independiente.

3. Las labores de vigilancia de los gobiernos deben regirse bajo el principio de proporcionalidad, agotando todas las instancias legales posibles antes de violar la privacidad de un individuo. Se debe abogar por las medidas menos intrusivas y por la existencia de puntos de control estrictos. De lo contrario, no solo se violenta el derecho a la privacidad, sino que se atenta contra la libertad de expresión, el derecho a la información, la libertad de circulación y de asociación; así como el completo ejercicio de los derechos humanos.

La empresa Hacking Team y los gobiernos involucrados son responsables de dicho espionaje en la esfera internacional. Exigimos que las empresas tengan como prioridad el respeto de los derechos humanos y no los contratos de prestación de servicios con gobiernos opresores y abusivos. A los Estados, exigimos que respeten los derechos humanos de sus ciudadanos, cesen dichas prácticas ilegales de vigilancia y transparenten el objetivo de la compra de software, el presupuesto público gastado en cada caso y las garantías tanto legales como procedimentales para evitar la violación de derechos.

Artículo 19 (México y Centroamérica)
ACI-Participa (Honduras)
Contingente MX (México)
Derechos Digitales (América Latina)
Enjambre Digital (Mexico)
EFF (División America Latina)
RedPato2 (Colombia)
R3D Red en Defensa de los Derechos Digitales (México)
Fundación para la Libertad de Prensa (Colombia)
Fundación Karisma (Colombia)
Hiperderecho (Perú)