Gobierno sondeó compra de más equipos de espionaje

En mayo de 2014, un año después de haber confirmado la compra de El Guardián para espiar llamadas, correos electrónicos y redes sociales, jerarcas del gobierno de José Mujica continuaban haciendo consultas por otros equipos de espionaje, más poderosos y polémicos aun, y recibieron a los representantes de una controversial firma italiana que ofreció su producto estrella.

El software permite obtener no solo información, sino seguir los pasos del sospechoso.

Por GONZALO TERRA - 10 julio 2015

Por separado, el 9 de mayo del año pasado los empresarios fueron recibidos por el entonces coordinador de Inteligencia del Estado, Ramón Bonilla, y por el actual director nacional de Policía, Julio Guarteche. Según el reporte realizado ese mismo día por los empresarios, ambos jerarcas quedaron muy bien impresionados por la demostración de sus productos. Guarteche lo elogió y en el caso de la reunión con Bonilla, los "socios" hicieron incluso un compromiso de interceder ante el entonces presidente José Mujica para convencerlo de las ventajas de adquirir el nuevo programa de vigilancia.

Galileo.

Las reuniones salieron a luz esta semana como consecuencia de la filtración por parte de Wikileaks de miles de correos y documentos que pusieron en el ojo de la tormenta a la empresa que ofreció el programa de espionaje por sus polémicos negocios en todo el mundo.

El jueves 8 de mayo de 2014 llegaron a Uruguay y se hospedaron en el hotel Four Points, Alex Velazco y Sergio Solis, ejecutivos de la firma italiana dedicada al espionaje electrónico Hacking Team.

Por la tarde recibieron la llamada de Pablino Martínez, Gerente de Proyectos Especiales de la empresa de seguridad paraguaya Radar, quien se había hospedado en el hotel Days Inn. Se reunieron, prepararon la presentación para el gobierno uruguayo y luego cenaron juntos.

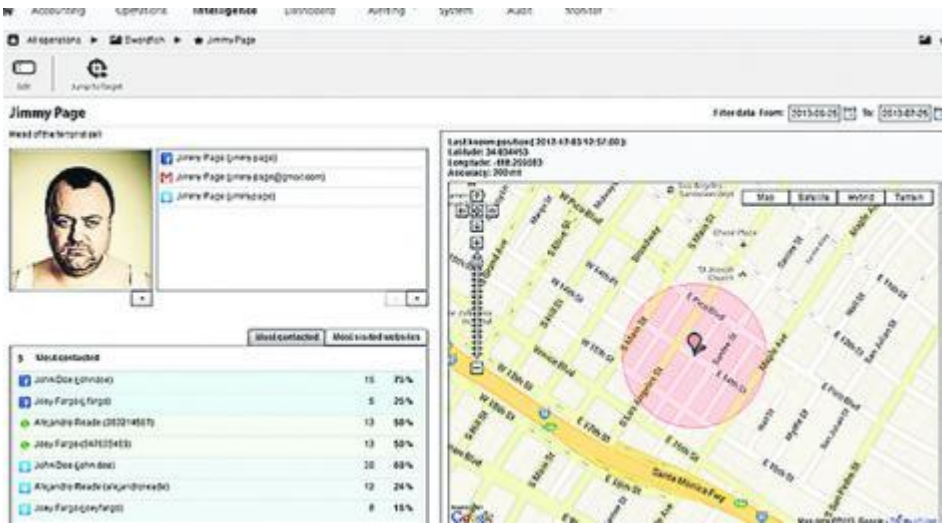
A las nueve de la mañana del día siguiente se reunieron con Guarteche, un asesor, dos oficiales de Inteligencia y otro de Narcóticos. Por la tarde mantuvieron otra reunión, esta vez con Bonilla, el capitán de navío Jorge Menini y el coronel González. Ayer, El País se comunicó con Pablino Martínez pero, tras mostrar sorpresa por la llamada, dijo que no podía dar información sobre ambas reuniones.

Entre los correos de Hacking Team filtrados por Wikileaks se encuentra uno perteneciente a Sergio Solis que reporta el resultado de las dos reuniones en Uruguay.

Debe tenerse en cuenta que el gobierno ya había adquirido hacía un año y en secreto El Guardián, un avanzado sistema de espionaje brasileño que potencia la capacidad del Estado uruguayo para interceptar llamadas, correos electrónicos y redes sociales, además de sistematizar la información recolectada y ofrecer otras funciones.

Solis cuenta que en la reunión con Guarteche hizo la presentación del Remote Control System (RCS), producto estrella de Hacking Team y también conocido como Da Vinci o Galileo.

Se trata de un programa que, de forma totalmente invisible, 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 su objetivo. También puede grabar conversaciones en Skype. Hacking Team se jacta de vender un sistema de espionaje "ofensivo".



Galileo: una imagen de la presentación del programa.

Solis cuenta en su reporte que presentó las bondades del RCS y "presionó" con ejemplos y preguntas. Siempre de acuerdo a su relato ante sus superiores, afirma en un correo electrónico enviado desde Uruguay ese mismo día a las 22.20 horas que "el director (Guarteche) estaba realmente satisfecho y de a ratos miraba al tipo de las drogas por su interés, hasta que no pudo más y elogió en voz alta el sistema". Cuenta que luego Guarteche tuvo que irse pero los otros cuatro policías se quedaron e hicieron preguntas. "A ellos les gustó", afirma.

En el caso de la reunión con Bonilla, Solis cuenta que usó dispositivos infestados y "los clientes quedaron realmente satisfechos".

Dice que puso ejemplos de posibles objetivos sobre los cuales utilizar el sistema, pero sin hacer foco en algo específico porque, a diferencia de otros países, en Uruguay no existen casos como las Farc, Sendero Luminoso o el EPP en Paraguay.

"Después de la reunión, que el cliente disfrutó, nuestros socios me dijeron que van a presionar a la mano derecha del presidente (entonces Mujica), un hombre de las Fuerzas Armadas que tiene mucha influencia sobre el presidente como su asistente". No obstante, Solis no identifica a nadie por su nombre.

Finalmente señala sobre ambas reuniones que están esperando las elecciones y, además, "manejan presupuestos por cinco años, lo que no está lejos de definirse aunque no sabemos si se decidirán por algo o no".

La filtración de Wikileaks dejó en evidencia que Hacking Team es proveedora de su sistema de espionaje para gobiernos de países como Ecuador, Chile, España o Sudán, lo que ha generado una fuerte polémica en todos ellos.

"En Hacking Team pensamos que combatir el crimen debe ser una tarea fácil: proporcionamos tecnología ofensiva para el mundo entero, eficaz y de simple utilización", dice el lema de la compañía, ahora víctima de sus propios inventos.

Espía cualquier tipo de dispositivo y no deja ningún rastro.

Nacimiento. Hacking Team se creó en 2003 y sus fundadores son hackers italianos. La empresa afirma que está "exclusivamente" centrada en la seguridad "ofensiva". "Equipo técnico Hacking Team consta de innumerables profesionales de alto perfil, con años de experiencia en el campo de la seguridad y la piratería. Muchos de los desarrolladores de RCS (Galileo) son bien conocidos en el mundo subterráneo de la seguridad", sostiene la presentación que se hace en cada país.

Galileo. El programa estrella de Hacking Team consiste en un software de seguridad que se oculta en el interior de los dispositivos de destino (computadoras o celulares) y permite el monitoreo de datos activos y control de procesos. "Datos sensibles a menudo se intercambian utilizando canales encriptados, o no intercambiando en absoluto; a veces se intercambia utilizando redes fuera del alcance de su agencia. El uso de RCS (Galileo) permite recopilar dicha información. Una vez instalado en el dispositivo de destino, le permite evadir la encriptación y recopilar la información de la actividad de su objetivo sin límite físico. El agente es diseñado para evadir antivirus y anti rootkits. La trasmisión de los datos recogidos en los dispositivos se realiza con un sistema cifrado de algoritmos de encriptación de grado militar", sostiene el detalle del producto.

Capacidad. El programa permite recopilar todo tipo de datos y traducirlos automáticamente a cualquier idioma. Puede acceder a los dispositivos del objetivo y de todos aquellos que tengan algún tipo de intercambio con él. También, a través de Google Map, puede reconstruir todos sus movimientos. Permite al usuario etiquetar e incluir notas para cada pieza de evidencia para mejorar el valor de los datos recogidos. El programa se puede desinstalar de forma remota con un simple clic. Una vez eliminado, el programa y todos sus datos se borrarán permanentemente del dispositivo. Es posible configurar el programa para que limpie de forma segura todos los archivos del dispositivo, con el fin de ser resistente a cualquier análisis forense.

Seis países de la región tienen esa tecnología

La difusión de los correos de la empresa Hacking Team puso en evidencia que varios gobiernos tienen contratos secretos por poderosos servicios de vigilancia, entre ellos algunos de la región como Ecuador o Chile.

10 julio 2015

Organizaciones sociales vinculadas a la protección de datos personales, entre ellas DATA de Uruguay, hicieron conocer su voz de alerta.

"El domingo 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", sostiene el comunicado.

En la filtración se halló que seis países de América Latina son clientes de Hac-king Team: Chile, Colombia, Ecuador, Honduras, México y Panamá. Dependencias como la Policía de Investigaciones de Chile, la Secretaría de Inteligencia de Ecuador, la Dirección de Inteligencia Policial de Colombia o el Centro de Investigación y Seguridad Nacional de México 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 estaduales, algunos de ellos sin facultades legales para la intervención de comunicaciones privadas.

Las organizaciones declararon que rechazan la venta y adquisición de estos programas de vigilancia, que sin controles adecuados, ponen en riesgo los derechos humanos de la región.

"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", sostiene.

Argumenta además que 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.