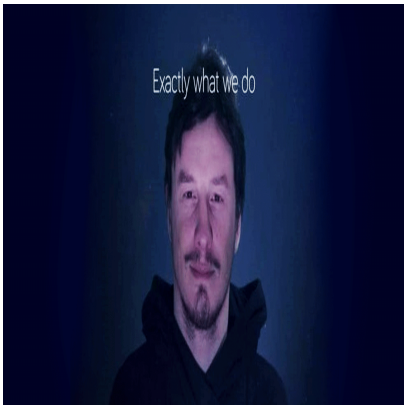


Hacking Team casi corona en Venezuela

Descripción

Se dice que a cada quien le llega el día de recibir una cucharada de su propia medicina. Para Hacking Team ese día fue el pasado domingo 5 de julio, cuando su cuenta de Twitter fue intervenida por ajenos para extraer y difundir 400GB con información privada de la compañía, incluyendo correos electrónicos, archivos con listas de clientes y código fuente.

Con esta filtración salieron a la luz los secretos detrás de la industria global del espionaje electrónico, que se ha ido extendiendo alrededor del mundo sin reglas deontológicas ni aparente control. Y aunque Venezuela no figura como cliente en los archivos, una serie de correos electrónicos compartidos entre Hacking Team y autoridades gubernamentales revelan el interés de entes del Estado venezolano en comprar el producto que comercializa la empresa italiana.

Hacking Team, con sede en Italia, vende a agencias nacionales de seguridad de todo el mundo un tipo de software conocido como Sistema de Control Remoto (RCS, por sus siglas en inglés) que permite *piratear* computadoras y teléfonos celulares. Al contratar el producto, el cliente podrá tener acceso a correos, registro de llamadas, mensajería de texto, micrófono, cámara, GPS y hasta grabar conversaciones telefónicas de cualquier dispositivo elegido como objetivo. El producto estelar en el portafolio de Hacking Team se llama Da Vinci, capaz de sortear barreras de encriptado, y especialmente concebido para la captura de teléfonos móviles inteligentes.

Ya para 2013, la organización de libertad de prensa Reporteros Sin Fronteras (RSF), desde su sede en París, Francia, había publicado un reporte en el que consideraba a la italiana Hacking Team un “enemigo corporativo de internet”, junto con otras cuatro empresas de tecnología: Gamma Group (Reino Unido), Trovicor (Alemania), Amesys (Francia) y Blue Coat Systems (Estados Unidos). El reporte criticaba la disposición de las compañías para convertirse en “mercenarios digitales” y vender sus productos a regímenes autoritarios.

Ese año, un estudio conjunto de la organización no gubernamental Electronic Frontier Foundation (San Francisco, California, Estados Unidos) y el Citizen Lab de la Universidad de Toronto (Ontario, Canadá), determinó que Venezuela había sido uno de los compradores del Packet Shaper de la empresa californiana Blue Coat. Los investigadores definen el producto como un sistema en la nube

que ofrece visibilidad externa de 600 aplicaciones para la web y control del “tráfico indeseable”.

Ahora, en la hoja de Excelque se filtró con la lista de clientes de Hacking Team apenas unos días atrás, aparecen los regímenes de Emiratos Árabes Unidos, Uzbekistán, Rusia, Bahrein, Kazajstán, Etiopía, Arabia Saudí y Azerbaiyán, entre otros con pésimo historial de derechos humanos.

Mientras a la luz quedaban expuestos serios indicios de que el Ecuador del presidente Rafael Correa, cercano aliado del régimen bolivariano en Caracas, contrató los servicios de Hacking Team para su Secretaría Nacional de Inteligencia (Senain), Venezuela no figura en la lista de clientes. Pero de que se dejó cortejar, no hay dudas: mantuvo conversaciones con la empresa e intermediarios para comprar el software de espionaje. Los correos electrónicos que explican con detalle las negociaciones fueron organizados y pueden ser consultados en Wikileaks.org.

Clientes de Hacking Team
Create your own infographics

Presentación a un general

El equipo de ventas de Hacking Team eligió una fecha poco propicia para visitar Caracas. Sus representantes pisan tierras venezolanas la mañana del miércoles 6 de marzo de 2013, menos de 24 horas después del anuncio de la muerte del presidente Hugo Chávez.

“Rápida actualización, acabo de llegar al hotel. Es un poco loco aquí. Controles de seguridad en la propiedad del hotel, caminando por el lobby y entrando a los ascensores. El taxista dijo que no sería fácil moverse. Toda la ciudad está de luto. Se esperan manifestaciones y marchas. El funeral está pautado para el viernes. ¿En qué nos hemos metido?”, le escribe Alex Velasco, manager de cuentas de la empresa de hackers, a sus compañeros de trabajo en un *email* que lleva por asunto: *Caracas Chávez Caos*.

En ese momento Velasco había viajado a la capital venezolana con Alex Berroa y Richard Berroa de DTXT Corporation, una compañía estadounidense que provee aplicaciones de seguridad y servicios de suscripción de sistemas de tecnologías de la información. DTXT Corp era, junto con otros aliados locales cuyos nombres no se revelan en los documentos, el nexo entre los informáticos y los potenciales clientes del Estado venezolano.

Previo a su llegada a Caracas, DTXT corp envía un PDF donde especifica que "hay una instrucción presidencial" de recibirlos para mostrar la nueva solución de intercepción móvil, gracias al aumento de un 42% del uso de celulares en Venezuela en 2012. También nombran los organismos con quienes se reunirían para mostrar el demo: Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), División de Inteligencia Militar (DIM), Dirección General de Contrainteligencia Militar (DGCIM) y la Dirección de Comunicaciones de la Fuerza Armada Nacional Bolivariana (DICOFANB).

El equipo de Hacking Team, DTXT Corp y el aliado local se reúne finalmente el viernes 8 de marzo de 2013 con un general del Ejército venezolano. Allí, a pesar de los inconvenientes que han tenido, despliegan sus productos RCS y hacen una demostración en la que infectan en vivo un teléfono Android, por petición del general. Velasco, en su reporte, habla también de un "primer ministro" que no pudo llegar a la reunión debido a la "actual situación".

Como dato curioso, Velasco agrega que a unos 300 metros del edificio donde hacen la presentación ocurre un incendio que fue controlado. Velasco remata el correo con una frase casi jubilosa de cumplimiento del deber: *"Dead president, crazed loyalist and forest fires can't stop us from doing our job!"* ("¡Ni el presidente muerto, sus partidarios enloquecidos o los incendios forestales pueden detenernos de hacer nuestro trabajo!").

En uno de los correos electrónicos posteriores a la reunión que tuvo lugar en Caracas, Richard Berroa le explica a Marco Catino, ingeniero de aplicaciones de la empresa italiana, que los posibles clientes venezolanos han pedido una semana más para dar una respuesta porque necesitan reponerse de una serie de eventos desafortunados: ya no se refieren solo a la muerte del presidente Chávez, sino también a los decesos de la madre del presidente de la Asamblea Nacional y del padre del general con quien se encontraron en Caracas.

En efecto, Felicia Rondón de Cabello, madre del *número dos* del chavismo y presidente del parlamento, el ex teniente del Ejército Diosdado Cabello, falleció justo el domingo antes del deceso del comandante Chávez, que acaeció un martes.

También la prensa reportó que el 12 de marzo de 2013, poco más de una semana después de la muerte del líder revolucionario, falleció Juan José Barrientos Tarazona, padre del mayor general del Ejército Wilmer Barrientos, quien para ese entonces ejercía como jefe del Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana (Ceo-Fanb). El presidente encargado a la fecha –ratificado luego en las elecciones del 14 de abril–, Nicolás Maduro, le expresó públicas condolencias a través de su cuenta de Twitter: "Querido compañero, soldado de la patria, cuentas con toda nuestra solidaridad y todo nuestro amor… Tu padre vive y la lucha continúa".

https://youtube.com/watch?v=yPFocWw01xk

Este cruce puede llevar a pensar que el oficial militar de la reunión fue Barrientos, un activista bolivariano originario de la asonada del 4 de febrero de 1992, que Chávez –entonces, un teniente coronel de paracaidistas– lideró para intentar derrocar al presidente Carlos Andrés Pérez. Pero Barrientos, actual Embajador de Venezuela en Canadá, lo desmiente de manera enfática en conversación telefónica para este reportaje. "No conozco a la empresa (…) no me nombran en ninguna parte", dijo, a la vez que alegaba que la única reunión que ha sostenido "es con el país". Además el ex militar, ahora diplomático –y que en el gobierno de Nicolás Maduro ocupó las carteras ministeriales de Industrias y del Despacho de la Presidencia y Seguimiento de la Gestión del Gobierno– restó credibilidad a la filtración, por lo que no quiso hacer ningún otro comentario oficial.

Intermediarios en Venezuela

Apenas un mes después de esa visita malhadada de Hacking Team a Venezuela, la empresa Importadora Ventech

, con oficinas en Madrid y Caracas, se puso en contacto con la compañía italiana para promocionar de nuevo el producto en el país.

En modo persuasivo, Ventech asegura en la comunicación que tiene varios “clientes pertenecientes a los organismos de seguridad de estado, inteligencia y contrainteligencia de Venezuela y otros países de Sudamérica”.

En un correo electrónico enviado el 13 de mayo de 2013, Franklin Colombo,<franklinc@ventech.com.es>, apoderado de la empresa en Madrid, le dice a Alex Velasco que las dos agencias gubernamentales donde tiene posibilidades de colocar el producto son la Dirección de Inteligencia Militar (DGCIM, sus siglas oficiales) y el Servicio Bolivariano de Inteligencia (Sebin).

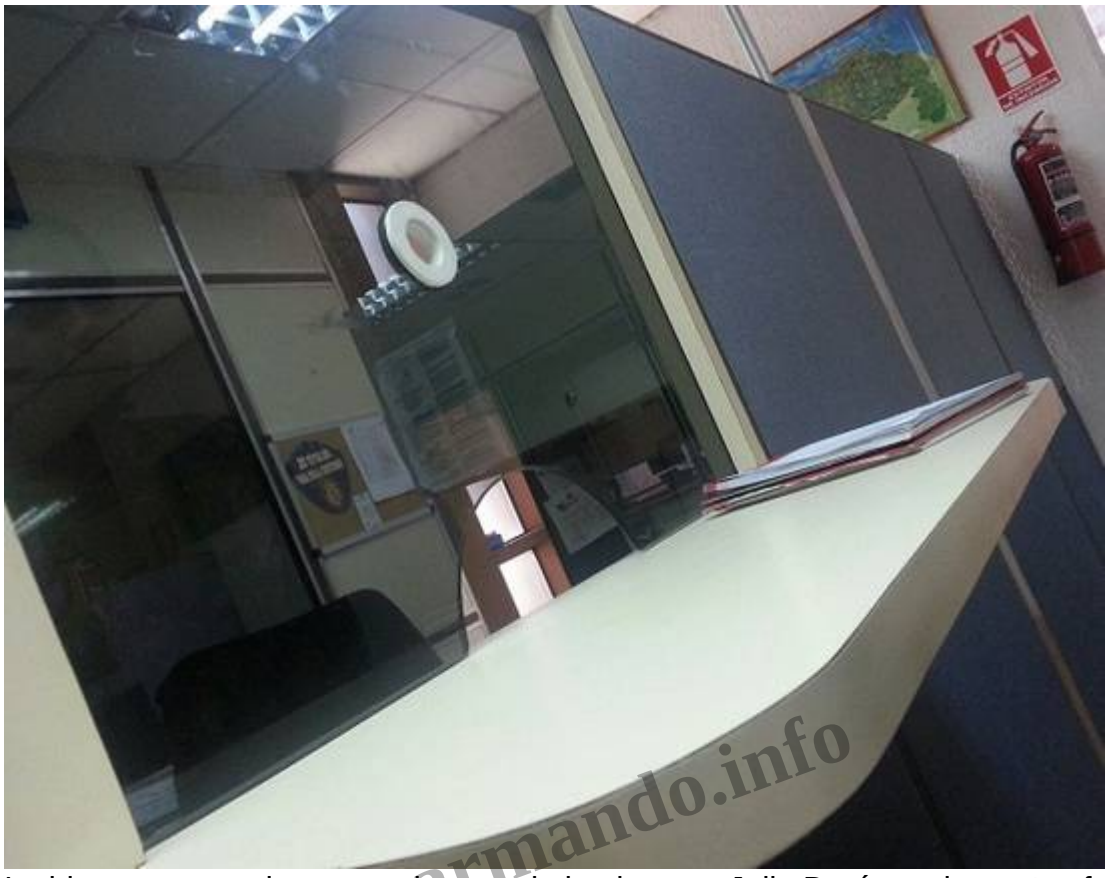
Nelson Colombo, presidente de Importadora Ventech en Venezuela, confirmó durante una entrevista que sí hubo contacto para ofrecer los productos a agentes del Estado venezolano. Sin embargo, ninguna negociación se concretó, según su testimonio.

“Nosotros conocimos de sus productos en una feria, nos interesó el software y lo presentamos a nuestros clientes. Pero ellos no quisieron venir a Venezuela y eso quedó así. No tenemos ninguna relación con Hacking Team. Ventech es una empresa limpia, con todo al día, que no se ha visto involucrada en problemas”, explicó Colombo.

Según el Registro Nacional de Contratistas (RNC), la Importadora Ventech, tiene por objeto “la compra, venta, arrendamiento, gravamen y en general de todo acto inherente a la comercialización, importación, exportación de equipos, partes y piezas de la industria en general”. Entre sus clientes destaca la telefónica estatal Cantv.

Por lo que se ve en los correos filtrados, el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz (MRIJP) también había mostrado interés en el software de espionaje. A mediados del 2013, revelan los documentos, el manager de cuentas de Hacking Team, Mostapha Maanna y el venezolano Julio Durán <duran.julio@gmail.com, jduran@mij.gob.ve>, se conocieron en la conferencia ISS World Europe en Praga, República Checa. Desde ese día, mantuvieron conversaciones para promocionar RCS en Venezuela.

Julio Ernesto Durán Malaver, al momento del intercambio de correos, ejercía como Director Encargado de la Comisión Ministerial de Proyectos Especiales del MRIJP y Director General de la Oficina de Tecnologías de Información de la misma entidad. Para entonces, el titular de la cartera del Interior era el ex general del Ejército Miguel Rodríguez Torres, también compañero de Chávez en la aventura golpista de febrero de 1992, que en el Gobierno del comandante barinés ocupó por mucho tiempo la jefatura de la policía política (Dirección de Servicios de Inteligencia y Prevención, Disip) y llevó adelante la transformación de ese cuerpo en el actual Sebin.



La bisagra venezolana con el grupo de hackers es Julio Durán, quien antes fungía como funcionario público y ahora está al frente de la empresa Telecorp, en cuya oficina dijeron que se encuentra de viaje. Foto: Katherine Pennacchio.

Durán lideró en ese despacho uno de los proyectos bandera de la gestión de Rodríguez Torres: el Sistema Integral de Monitoreo y Asistencia (Sima), una tecnología de origen chino –su proveedor era el *holding* estatal China National Electronics Import and ExportsCorporation– que combina vigilancia por video y comunicación satelital para controlar alteraciones del orden público, con la que se iban a instalar 30.000 cámaras de vigilancia en todo el país. Durante su implementación por fases, que empezó por el municipio Sucre (este de Caracas) del estado de Miranda, tuvieron lugar diversos actos de inauguración transmitidos por los medios oficiales. En algunos de ellos, donde llegó a participar el Jefe de Estado, Nicolás Maduro, Durán sirvió de vocero.

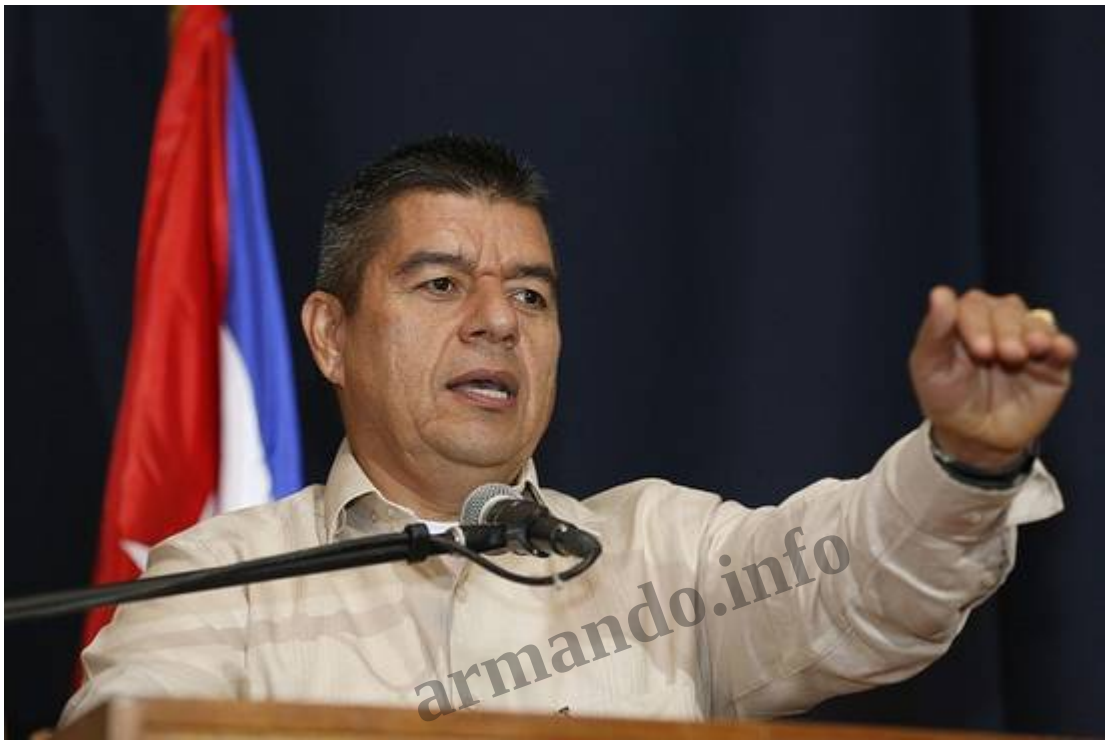
Durán solicitó al equipo de Hacking Team que tuviera lista una versión en español del acuerdo de confidencialidad (NDA, por sus siglas en inglés) para firmar en cualquier momento, y hablaron de reunirse en Berlín, Alemania, para una presentación del *demo*.

Luego de su paso por la administración pública, Julio Durán figura como director de Telecorp, C.A, una empresa venezolana de servicio de internet satelital que, según reza su página web, se especializa en “soluciones de Acceso a Internet, Datos y Voip de Alta Velocidad”.

Además dirige, junto a Mariange Durán Malaver, la compañía Sistemas Simulnet, C.A que tiene como objeto “todo lo relacionado con la consultoría en el área de telecomunicaciones e informática (...) exportación e importación de equipos y componentes”, tal como aparece en su ficha del Registro

Nacional de Contratistas.

Se solicitó una entrevista a Durán en las oficinas de Telecorp, C.A, ubicadas en la Torre Unión de El Rosal (municipio Chacao, este de Caracas), pero no fue posible concretarla, pues el ejecutivo se encontraba de viaje.



El mayor general del Ejército Wilmer Barrientos, hoy embajador de Venezuela en Canadá y para ese momento jefe del Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana, se desligó del caso y restó credibilidad a la filtración.

Triangulación colombiana

La última vez que se nombra Venezuela en los correos electrónicos de la filtración fue en febrero de 2015. Entonces Eduardo Pardo <e.pardo@hackingteam.com> le dice a Alex Velasco <a.velasco@hackingteam.com> que conoció a un sujeto en el puesto de Robotec durante la feria Expodefensa 2014 en Bogotá, Colombia, quien a su vez podía ponerlos en contacto con agencias del Estado bolivariano.

Se habla del ministerio de Defensa, de grupos antisecuestros, y de la empresa petrolera estatal PDVSA, que estaría interesada en comprar una “herramienta de seguridad para luchar contra la corrupción dentro de la compañía”.

Ya en comunicaciones anteriores, el Director de Defensa y Seguridad Nacional de Robotec Corporation, Hugo Fernando Ardila Miranda, aparecía diciendo que tres agencias venezolanas le habían consultado sobre el producto: Comando Nacional Antiextorsión (Conas), la Dirección de Inteligencia Militar (DGCIM) y el Ministerio del Poder Popular para la Defensa (MPPD).

Robotec Corporation, empresa colombiana dedicada al desarrollo, suministro, instalación y

mantenimiento de tecnologías especializadas, explica en un comunicado público que la única relación que tenía con Hacking Team era como agente de distribución de sus productos en la región.

“No operamos, ni investigamos, ni tampoco tenemos acceso a las bases de datos ni a los equipos, solamente vendemos la tecnología”, se lee en la página web de la corporación.

En un escueto correo electrónico que envió a ***Armando.info***, la empresa –en persona de Hugo Ardila– se limita a aclarar “que no hemos vendido nada a su país”.

Todo indica que Venezuela no compró las soluciones RCS de Hacking Team. No aparece en la lista de clientes. Sin embargo, manifestó la clara intención de comprar el software para filtrarse entre los dispositivos de cualquier ciudadano, incluyendo entre sus potenciales objetivos de quienes conforman la principal empresa del país. El Gobierno de Maduro tiene apetito por husmear las comunicaciones electrónicas. Cabe preguntar: ¿habrá quién lo haya satisfecho?

Fecha de creación
2015/07/18