**De cómo LaRepública ha sido atacada con la asesoría de Hacking Team**

*Publicado el Viernes 10 de julio de 2015 en*[*POLÍTICA*](http://www.larepublica.ec/blog/seccion/politica/)

****Foto: Hacking Team

El portal **LaRepública** ha sido atacado con la **instalación de software malicioso** con la**asesoría de la empresa italiana Hacking Team**, de acuerdo a mails difundidos por **Wikileaks**esta semana después que el 8 de julio dicha compañía [**fuera hackeada**](http://www.larepublica.ec/blog/politica/2015/07/07/compania-de-espionaje-hacking-team-es-atacada-por-hackers/), su tecnología sustraída y miles de sus mensajes expuestos al público.

Publicidad

El ataque fue confirmado por la propia Hacking Team en un [**comunicado**](http://hackingteam.com/index.php/about-us) en el que advirtieron  que “terroristas, extorsionistas y otros” podrían utilizarla sin control por parte de ellos, lo cual consideran que es una “situación extremadamente peligrosa”.

Entre los miles de correos electrónicos subidos a la plataforma de Wikileaks algunos de ellos revelan una aparente **relación contractual del Gobierno ecuatoriano con Hacking Team**. Hasta el momento, el Secretario de Inteligencia, Rommy Vallejo no ha emitido ningún pronunciamiento, si bien el Canciller Ricardo Patiño y el Ministro del Interior, José Serrano, han dicho desconocer sobre el tema.

**Por lo menos cuatros mensajes electrónicos enviados a las personas mencionadas en los mails revelados por Wikileaks no han sido contestados.**

De acuerdo a la investigación realizada por un equipo de La República EC, el 20 de noviembre de 2014 una persona que firmaba como **elmarcopoloh**, y que escribía mediante un correo de Yahoo, solicitó**soporte técnico a Hacking Team para realizar dos tipos de ataques en contra de LaRepública**.

Primero se planificó un ataque que utilizaría como gancho la noticia de nuestro sitio web del 20 de noviembre de 2014 titulada ‘[**Masivas protestas sindicales de Ecuador contra reforma laboral del Gobierno**](http://www.larepublica.ec/blog/politica/2014/11/20/masivas-protestas-sindicales-ecuador-reforma-laboral-gobierno/)‘ para instalar de manera silenciosa software malicioso en equipos de personas que no hemos logrado determinar. Solicitudes similares se hicieron en esos mismos días en contra de El Universo y el diario Hoy.

Una serie de correos relacionados al ticket JHN-213-29703 de la plataforma de soporte técnico de Hacking Team, entre las cuentas elmarcopoloh@yahoo.com y support@hackingteam.com relatan cómo sucedió.

Según la [**documentación**](https://wikileaks.org/hackingteam/emails/emailid/624185) encontrada con fecha 10 de noviembre de 2014, quien escribe desde la cuenta de correo elmarcopoloh@yahoo.com es una persona que se hace llamar Luis Solís, que dice trabajar en la SIN y que también usa la dirección de correo electrónico luis.solis@sin.gob.ec. En esa documentación, un colaborador de Hacking Team confirma que la SIN y la SENAIN son la misma institución y que era indistinto utilizar los dominios de correo electrónico [**sin.gob.ec**](http://sin.gob.ec/) y [**senain.gob.ec**](http://senain.gob.ec/)

**La persona que dice llamarse Luis Solís, utilizando la cuenta con domino yahoo.es, solicita la ayuda a Hacking Team para realizar un “ataque de día cero” (0-day)**, el cual tiene como objetivo aprovecharse de la vulnerabilidad de un sistema para la ejecución de un código malicioso, sin que el usuario lo note y así poder **tener control sobre algún dispositivo para que este realice alguna acción en el futuro** lo que podría incluir espionaje, control del equipo de manera remota, entre otros.

**El método consistiría en realizar un “exploit”**, proporcionando al blanco del ataque con un archivo o liga a una dirección web, y que al darle clic, lo llevaría a un sitio web que ejecutaría una serie de instrucciones rápidamente, y luego redireccionarlo a la noticia de nuestro diario. De esta manera el usuario no sospecharía nada, ya que terminaría leyendo la noticia que le compartieron, pero sin saber que antes, por unos segundos, “pasó” por otro sitio que instaló el programa malicioso.

En menos de 6 minutos de la solicitud, el caso es asignado y **la persona que dice llamarse Solís recibe la liga de la dirección web que se encargaría de realizar la infección**. La gente de Hacking Team le advierte que no la publique en redes sociales ya que sería descubierta rápidamente y que lo más efectivo sería crear un correo con formato HTML, que tenga un hipervínculo que lleve al usuario a visitar el sitio web infectado sin ver la dirección a la que apuntaba. El formato HTML  permite desplegar fotos y texto con hipervínuclos; Microsoft Outlook, Gmail, Hotmail, entre otros, soportan recibir correos HTML. Le adjuntan un ejemplo de un correo en dicho formato.

Además, comentan que en caso de no ser posible hacer un envío de ese tipo de correos, que también podían enviarlo enmascarando la dirección maliciosa con algún servicio tipo tinyurl.com, goo.gl, de esos que hoy hay muchos. Lo podían entonces pasar por el chat de Skype, o alguna otra plataforma. Le advierten que el exploit estaría limitado por un período de tiempo limitado.

También se encontró otro ticket de soporte, el LOX-522-92715 , que incluía archivos comprimidos con nombres: ‘2014-11-21-RESUMEN-REVOLUCIÓN-DEL-TRABAJO.rar’ y ‘RESUMEN MARCHA DE TRABAJO.rar’. Se explica que dentro esos archivos .rar, extensión conocida para archivos comprimidos, venían archivos infectados. Dado que la infección se daría apenas se ejecute el archivo dentro del .rar, le recomienda al cliente de Hacking Team no abrirlo en los equipos dentro del laboratorio/oficina.

El técnico le pide que revise si empieza a recibir información del equipo objetivo del ataque y al igual que en el otro ticket de soporte se le pide que tampoco lo publique en redes sociales ni en sitios web públicos; avisándole además de la limitante de la duración del “exploit”.

No logramos determinar si ambos tickets de soporte estaban relacionados y hemos decidido no incluir los hipervínculos a esos casos para evitar que por error nuestros lectores descarguen el software malicioso.

Hemos escrito a la cuenta luis.solis@sin.gob.ec preguntando acerca de la veracidad de esta información publicada y obtuvimos un correo de respuesta que hacía referencia al error 5.0.0 que está relacionado a la inexistencia de una cuenta de correo. Otros [**correos**](https://wikileaks.org/hackingteam/emails/emailid/1062678) revisados en Wikileaks muestran una supuesta conversación de junio de este año, enfocada en organizar una conferencia entre Hugo Ardilla, de la empresa [**Robotec**](http://robotec.com/), con número telefónico registrado en Colombia, con Luis Solís y Paúl López, personas que a las que se identifica como miembros de la SIN del Ecuador.

En otro correo, del 15 de agosto de 2014, quien dice llamarse Solís, envía un correo a Hacking Team, y copiando a la dirección de correo de José Vaca, perteneciente a la SIN para al parecer concretar una videoconferencia con “la persona encargada de la administración de este tipo de proyectos” vía Skype.

Hemos escrito a las cuentas de correo electrónico relacionadas y también al portal de la Secretaría para cuestionar sobre la veracidad de la información, pero **hasta el momento de esta publicación no hemos obtenido respuesta**.

Toda esta información ha sido encontrada en Wikileaks, portal creado por **Julian Assange**, quien actualmente reside en la embajada del Ecuador en Londres.

LaRepública ha sido [**víctima de ataques DDoS**](http://www.larepublica.ec/blog/sociedad/2015/06/25/aumentan-ataques-ciberneticos-a-sitios-web/), que la han sacado de circulación, por lo menos diez veces en lo que va de este año, cada vez que ha transmitido, vía streaming, protestas en contra del gobierno del Presidente **Rafael Correa**.

****

Captura de pantalla de email de Hacking Team.