Infectar usuarios para vigilarlos y controlarlos

¿La mejor defensa es el ataque?

Autor: Abog. Marcelo Temperini

Abogado (UNL). Doctorando CONICET con especialización en Delitos Informáticos. Co-director de la Red Elderechoinformatico.com. Analista de Seguridad y Director de AsegurarTe – Consultora en Seguridad de la Información. Contacto: temperinimarcelo@gmail.com

Versión: 1.0 (20130609)

Hace pocos días, el diario El País de España, publicó una noticia que afirmaba que "La polícia podrá usar troyanos para investigar ordenadores y tabletas". La nota se basa sobre el borrador de anteproyecto de Código Procesal Penal del Ministerio de Justicia, el cual permitiría a los jueces que autoricen a la policía la instalación de troyanos en las computadoras de los investigados para obtener la información que contienen o a la que se puede acceder a través de ellos. El texto (no está aprobado aún) prevé el acceso remoto de equipos informáticos para delitos con penas máximas superiores a tres años, para el cibercrimen y para el terrorismo y el crimen organizado siempre que el juez justifique la proporcionalidad de la intervención. Hasta el momento, solo Alemania ha aprobado una regulación similar, aunque solo para casos de terrorismo, ante la invasión de la intimidad que supone.

La noticia no deja de sorprender, incluso habiendo tenido conocimiento de otras intenciones similares, pero nunca con tanta pretensión de legitimidad. Es decir, en el mundo de las investigaciones sobre delitos informáticos, uno puede llegar a conocer casos donde la urgencia y la necesidad pueden llegar a "flexibilizar" ciertos procedimientos legales (por ejemplo, para obtener datos sobre determinada dirección IP). Ejemplos que probablemente respondan a que nuestros sistema jurídico aún no cuenta con medidas o canales más rápidos de colaboración para casos de delitos informáticos, donde la información puede desvanecerse en cuestión de minutos.

Ahora, la pretensión de legitimidad a la utilización de malware para obtener información que permita llegar a los delincuentes, parece exceder el límite. Un límite jurídico, no técnico por supuesto. Un límite que viene a poner a prueba (como tantas situaciones de este mundo digital) al derecho. La balanza de la justicia, parece definir claramente dos bienes jurídicos encontrados: por un lado, un derecho tan fundamental como la intimidad, consagrado constitucionalmente (Argentina). En el otro extremo, fundamentos basados en la seguridad pública. Esta discusión, tuvo en parte lugar en Argentina en el Fallo Halabi, donde se afirmó que:

> *Que, en sentido coincidente, la Corte Interamericana de Derechos Humanos tiene dicho que el poder del Estado para garantizar la seguridad y mantener el orden público no es ilimitado, sino que "su actuación está condicionada por el respeto de los derechos*

fundamentales de los individuos que se encuentren bajo su jurisdicción y a la observación de los procedimientos conforme a Derecho (...) con estricta sujeción a los procedimientos objetivamente definidos en la misma" (Corte Interamericana de Derechos Humanos. Serie C, n° 100, caso "Bulacio v. Argentina", sentencia del 18 de septiembre de 2003, ptos. 124 y 125; ver Fallos: 330:3801).

Acerca de estas situaciones este Tribunal ha subrayado que sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos: 306:1892; 316:703, entre otros). Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (confr. art. 236, segunda parte, del Código Procesal Penal de la Nación, según el texto establecido por la ley 25.760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el artículo 18 de la ley 19.798 que establece que *"la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente"*.

Digo en parte, porque justamente en el Caso Halabi, se cuestionaba que la Ley establecía una especie de marco general, y que como bien señala el párrafo final citado, toda intervención a las comunicaciones (como sucede hace decenas de años con las telefónicas) debe ser ordenada por juez competente, previo justificación de su necesidad. Nuevamente, digo que es útil en parte, porque todo esto existe en la propuesta española (la motivación necesaria, la autorización judicial, etc.). Es decir, la utilidad del fallo, radica más en la claridad que tuvo la CSJN al afirmar que **si bien el Estado debe garantizar la seguridad y orden público, sus acciones están condicionadas al respeto por los derechos fundamentales de los individuos**. Algo que en esta propuesta no parece suceder.

Saliendo del ámbito estrictamente jurídico, es interesante analizar la propuesta desde la real utilidad para las investigaciones. En un artículo del Laboratorio de ESET España, acertadamente se refieren a algunos de estos aspectos. Puntualmente me interesa destacar el hecho que en la mayoría de los casos, los delincuentes informáticos no cometen los ilícitos desde sus propias computadoras o redes. No vamos a descubrir nada nuevo diciendo que los cibercriminales utilizan una importante variedad de opciones que existen para precisamente evitar ser atrapados, ello quiere decir, que la IP que obtenemos como generadora del ataque, bien puede ser de la Isla de Man o Russia, y el delincuente estar en el cuarto de al lado, con máquinas virtuales, *proxies* y pizza.

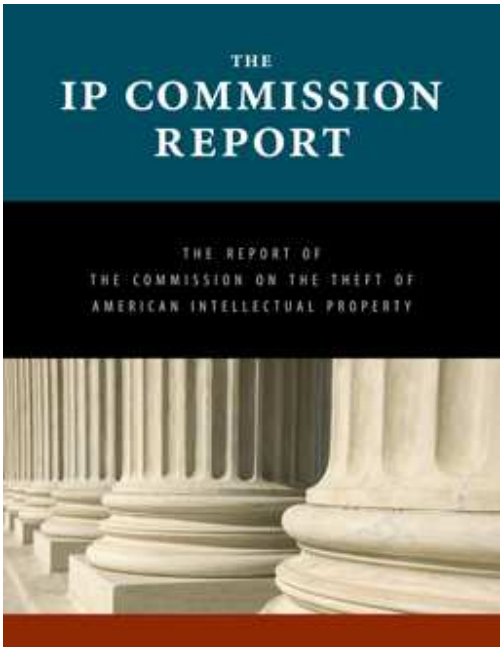
Entonces, para que nos sirve la posibilidad de insertar un troyano en una máquina que probablemente sea de un pobre muchacho que no tiene idea de lo que está pasando en su

computadora. O una familia cualquiera que tiene su computadora en el living. ¿Van a tomar control y revisar toda la computadora de un inocente?, que quizás ni sabe lo que es un troyano o un correo de phishing.

Supongamos el caso que la conexión pertenezca al delincuente, un *newbie* que estuvo jugando donde no debía. El hecho que la policía tenga los conocimientos para hacerlo caer en alguna trampa para infectarlo, o bien que el propio delincuente tenga algún tipo de vulnerabilidad para ser explotada, parece ser una probabilidad que deja abierta la puerta a que el mismo caso podría ser investigado con técnicas más sencillas y menos intrusivas

La posibilidad de legitimar este tipo de acciones, es sin dudas un paso complejo y que avanza sobre la tradicional "pinchada de comunicaciones". Recordemos que en los casos autorizados por la ley, y con orden judicial, es posible que personal autorizado intervenga una comunicación. Aquí no estamos hablando de una comunicación, aquí estamos hablando de tomar el control de un equipo entero, completo, con toda la información almacenada, sus acciones y además, de yapa, sus comunicaciones. Se me viene a la mente que esto vendría a ser una especie de "allanamiento virtual", revisando todo lo que está en tu casa para encontrar algo que te incrimine... ¡y sin que lo sepa el dueño de casa!

Una descabellada propuesta con tintes de manotazos de ahogado en la lucha contra la ciberdelincuencia. Al menos aquí en Argentina tenemos cientos de aspectos (políticos, jurídicos, procesales y prácticos) para mejorar si es que realmente estamos interesados en atrapar a los ciberdelincuentes.



Similar propuesta fue presentada en EE.UU., más precisamente en la IP Commision Report, de la Comission on the Theft of American Intellectual Property, una entidad que tiene por finalidad documentar y analizar el problema del robo de propiedad intelectual en EEUU y China, y además, proponer nuevas respuestas políticas al tema.

Casi al final del informe, se analiza una de las recomendaciones tituladas: *"Reconcile necessary changes in the law with a changing technical environment"* que a simple vista parecería inofensivo. En el desarrollo de esta propuesta, se puede leer que *"Si bien no está permitido por la ley de EE.UU., cada vez hay más llamadas para crear un ambiente más permisivo para la defensa activa de la red, que permita a las empresas no sólo estabilizar la situación, sino adoptar nuevas medidas, incluida la recuperación de forma activa la información*

robada, alterar las redes del intruso, o incluso la destrucción de la información dentro de esa red. Otras medidas van más allá, incluyendo fotografiar el hacker usando su propio sistema de cámara, la implantación de programas maliciosos en la red del hacker, o incluso inutilizar o destruir físicamente el propio ordenador o la red de los hackers" (traducción propia).

La propuesta es fundada, afirmándose que *"casi todas las ventajas están en el lado del hacker, y que la situación actual no es sostenible, dado que la tecnología y la velocidad de internet juega a favor de los chicos malos"*. Justifican además la propuesta diciendo que *"tomar medidas de seguridad continúa siendo cada vez más caros y cada vez menos efectiva, siendo poco probable que cambie el cálculo costo-beneficio de los piratas dirigidos lejos de atacar a las redes corporativas"* y que estos contraataques *"harían elevar el costo de sus acciones a los ladrones de propiedad intelectual, lo que puede disuadir a la realización de estas acciones en primer lugar".*

La idea creo que está bastante clara, pero por si quedan dudas al respecto, lo que se está proponiendo es la **legitimación del contraataque informático**. Parece que las empresas interpretan que la idea sería algo así como una especie de legítima defensa frente a aquellos que atacan sus contenidos protegidos por propiedad intelectual en los EE.UU. La Comisión comienza el análisis diciendo que cada vez *"hay más llamadas",* lo que podría ser nuevamente traducido a que hay cada vez más presión por parte del sector de los gigantes afectados por la piratería, por intentar de cualquier manera conservar su negocio.

Afortunadamente, la Comisión consideró que no están dadas las condiciones para avanzar con este tipo de propuestas, porque aún no existen los fundamentos jurídicos suficientes para avanzar sobre la recomendación de semejante medida, además de considerar los eventuales (y muy posibles) daños colaterales que se darían en este tipo de guerra electrónica entre las empresas y los atacantes.

Además, consideró que para este tipo de propuestas, hace falta la realización de deliberaciones y debates sobre si las empresas y los individuos deben estar legalmente habilitados para llevar a cabo operaciones de disuasión basadas en la amenaza contra la intrusión en la red, algo que sin duda, será un tema que traerá amplios e interesantes debates en la red.

La Comisión concluye que **no está dispuesta a apoyar esta recomendación debido a las grandes cuestiones de daños colaterales causados por los ataques informáticos, los peligros del abuso que podrían surgir de estas "autorizaciones" para hackear a los hackers, además de las diferentes medidas no-destructivas que podrían analizarse antes.**

El informe en todo caso, cierra con una frase interesante para redondear el artículo: **hace falta más trabajo e investigación antes de seguir adelante**. Personalmente diría que mucho más, trabajo e investigación, incluso para darse cuenta que algunas propuestas, distan de ser razonables.