El terreno expansivo de los ciberataques

Por Fátima Cárdenas
Ilustración: Camilo Pazmiño

Empresas de seguridad web, entre ellas MacAfee, Kaspersky y GMS, han catalogado a 2013 como el año de los ciberataques. En este período podrían cumplirse promesas como aquella de incursionar a gran escala en las entrañas del sistema bancario estadounidense. América Latina se apunta como un terreno fértil para este tipo de delitos que atacarán en 25% más a los usuarios de móviles, con respecto a 2012.

En octubre de 2012, vorVzakone, un *hacker* de origen ruso manifestó públicamente que planificaba intervenir el sistema bancario de EEUU para 2013. La operación, según lo mencionó, se denominaría Proyecto Blitzkrieg. Frente a estas declaraciones la empresa McAfee Labs señaló que la amenaza de vorVzakone no debe caer en saco roto y más bien tiene que ser considerada como creíble. ¿Bajo qué mecanismo operarán los *hackers*? La entidad señala que no se tratará de un ataque masivo, sino que más bien se apuntará a cuentas en diversos bancos de inversión y cooperativas de crédito para así burlar los controles de seguridad, en cuya mejora los bancos alrededor del mundo invierten alrededor de $ 1.000 millones al año.

En febrero pasado, China blandió sus espadas y le hizo saber a EEUU que la ciberguerra estaba declarada. Lejos de esconder su identidad, los *hackers* orientales dieron la cara, un asunto que —a la vista de los expertos— tiene que ver con su cultura y con la intención manifiesta de dar a conocer su poder. El *New York Times* fue uno de los más recientes blancos de los ataques de los ciberexpertos chinos, por lo cual dicho diario pidió a la consultora Mandiant un informe que revela —entre otros muchos detalles— que China, por carecer de leyes de propiedad intelectual, es un potencial atacante, pero no el único. De hecho hay voces que apuntan a EEUU como el país que más ataques de *malware* realiza, seguido del gigante asiático. Así

El *hacktivismo* se refiere al uso de herramientas tecnológicas para causar impactos que llamen la atención sobre alguna causa política, ambiental o idealista. En un entorno político cada vez más polarizado, es de esperarse este tipo de ataques tanto de defensores como de detractores de las políticas que el país esté llevando a cabo.

lo señala el informe de Symantec y McAfee de 2012.

El autor del libro *Inside Cyber Warfare*, **Jeffrey Carr**, prefiere guardar cautela y se suma a una postura que, aunque reconoce a China como un potencial *hacker*, no lo señala de frente, ya que, según él, acusaciones de este tipo podrían generar el riesgo de una escalada por parte del Ejército Popular de ese país.

Dispositivos móviles: entre los más vulnerables

De acuerdo con estimaciones de la empresa de seguridad informática GMS, los virus para móviles aumentarán en 25%, con respecto a 2012. En su último informe de tendencias, la entidad señala que los ataques se registrarán mayoritariamente en usuarios de la plataforma Android, que es la de mayor crecimiento y acceso. Además, menciona que para quienes emplean iOS, que es un sistema operativo más restringido mediante el cual toda aplicación debe pasar por el filtro de Apple, los peligros disminuyen.

Las amenazas para estos usuarios tienen nombre y apellido: *Men in the Middle* y *Men in the Browser* serían las formas de ataque más empleadas para violentar la seguridad de este segmento. En el primer caso, el atacante se interpone en la comunicación entre el usuario y el sitio al que quiere conectarse. Al insertarse en esta comunicación, puede acceder a toda la información que se transfiere de uno a otro lado, con lo cual el *hacker* accede a los movimientos del internauta. Por otro lado, en *Men in the Browser*, el atacante va mucho más allá, aquí se integra al navegador (Explorer, Firefox, etc.) y, no solamente puede ver lo que el operador de una *tablet* o una *laptop* está transmitiendo, sino que puede modificar los datos enviados desde el origen. Este tipo de ofensiva es muy utilizada para realizar fraude financiero y bancario.

En este campo, el desarrollo de las redes sociales ha cambiado la percepción de la privacidad y la confianza en línea. En su informe, GMS menciona que mientras los consumidores entienden que una parte importante de sus datos personales han sido entregados a los servicios en línea, la pregunta que cabe es si los consumidores confían en estos. La interrogante cobra fuerza una vez que sitios web tan populares como Dropbox y LinkedIn registraron una fuga de contraseñas.

Frente a este panorama, los expertos recomiendan desechar la idea de que los virus no afectan a quienes emplean teléfonos celulares o dispositivos móviles, ya que eso puede poner al internauta en la cuerda floja sin previo aviso. De ahí que las recomendaciones apuntan a contar con una herramienta *antimalware* que permita controlar la seguridad de la información en el dispositivo móvil.

Industrias y Gobiernos: los blancos clásicos

Los casos de campañas de *hackers* orientadas a violentar la seguridad bancaria y varios mercados estadounidenses, entre ellos, el editorial, no son temas aislados, ya que el *hacktivismo* mantendrá su actividad este año a partir de la creación de virus o *malwares* con miras a lo que los entendidos definen como una suerte de guerra electrónica, que obligará a las industrias y Gobiernos a protegerse frente a posibles sabotajes, terrorismo o labores de espionaje.

Y pese a que las potencias económicas como la estadounidense han sido hasta ahora las que más han sufrido de estos males, América Latina será un epicentro que en este año se presenta como uno de los más codiciados en temas de vulnerabilidad informática. Países como Brasil y México se apuntan como los blancos predilectos de este tipo de delitos. Los pronósticos de los expertos de Kaspersky develan un incremento del desarrollo de ciberprogramas con fines de ciberespionaje y cibersabotaje. Estos ataques afectarían no solo a instituciones gubernamentales, sino también a negocios e instalaciones de infraestructura críticas.

El Ecuador preferido para los jubilados

La Asociación de Corredores de Bienes Raíces de Pichincha organizó una conferencia magistral, dictada por el consultor y conferencista internacional **Carlos ThurdeKoos**, en la que se abordó el tema Ecuador: país preferido para inversión de bienes raíces de retirados americanos y canadienses.

ThurdeKoos, quien es actualmente representante y enlace de la National Association of Realtors de EEUU (NAR) para Argentina y Ecuador, abordó durante la conferencia temas como el desarrollo del sector inmobiliario en el país, la inversión extranjera y el desarrollo de zonas de descanso en el Ecuador.

La globalización, dijo, alcanzó a los bienes raíces. Grandes compañías con sede en EEUU han buscado concretar negocios inmobiliarios de envergadura en el Ecuador, pues el país todavía es considerado superior a otros de la región como destino para personas de la tercera edad. El *boom* inmobiliario para este segmento apunta principalmente a las ciudades de Cuenca en la Sierra y Bahía de Caráquez en la Costa.

Los corredores americanos operan bajo la modalidad de asociación con instituciones locales para desarrollar negocios —*online* básicamente—. Hoy promocionan paquetes de vivienda para jubilados de EEUU y Canadá, a manera de referencia, a través de estas asociaciones estratégicas se han vendido al menos dos proyectos en Bahía que abarcan un interesante número de cuatro mil viviendas, donde vivirán exclusivamente jubilados americanos y canadienses.

Quienes están involucrados en este tipo de negocios inmobiliarios consideran que es 'época de cosechar', pues las oportunidades son de doble vía, tanto para quienes buscan invertir en el Ecuador como para los que desean ir a hacer negocios en EEUU bajo la modalidad de asociaciones.