Se **venden** datos al peso

'HACKERS', APLICACIONES QUE 'CHUPAN' NUESTROS DATOS, VENTA DE PERFILES DE USUARIOS, ROBO DE INFORMACIÓN CONFIDENCIAL... CADA VEZ SOMOS MÁS VULNERABLES Y ALGUNAS EMPRESAS NO DUDAN EN CRUZAR LA LÍNEA ROJA PARA SABER MÁS DE NOSOTROS . ¿PODEMOS BORRAR NUESTRA HUELLA Y VOLVERNOS INVISIBLES?

POR AMAIA ARTETA

Era el último día antes de las vacaciones navideñas y Eva había quedado para comer con una amiga. Ambas se iban de viaje y querían contarse los planes, despedirse antes de terminar el año y desearse una buena entrada para el que estaba por llegar. De pronto, la conversación distendida a la que estaban entregadas se rompió por una llamada inesperada. Era del banco. Qué raro, pensó Eva, al tiempo que se levantaba en busca de un rincón menos ruidoso para hablar. "Hola Eva. Perdona que te moleste, soy Roberto Velarde, el director de la sucursal, ¿tienes un momento?", preguntó una voz con la que no estaba familiarizada. "Mira, solo quería saber si estás en Madrid", añadió. "Sí, de hecho estoy en un restaurante en la Castellana. ¿Por qué?", contestó inquieta. Roberto guardó un breve silencio antes de responder: "Es que hemos recibido la notificación de una compra en una tienda de fotografía en San Petersburgo por valor de 59.739 rublos, unos 1.500 euros al cambio. El pago es de ayer con la Visa y queríamos comprobar que era correcto", añadió.

Eva no daba crédito a lo que estaba oyendo. Se trataba de un golpe equivalente a ¡la mitad de su nómina mensual! "¿San Petersburgo? ¡Pero si nunca he estado en Rusia! ¿Cómo es posible? No entiendo nada", dijo al tiempo que comprobaba si la Visa seguía en su cartera. Allí estaba. "Bueno, eso significa que en algún momento alguien se ha apropiado de tus datos. Es algo que sucede con más frecuencia de la que desearíamos. Lo importante es que lo hemos detectado a tiempo", dijo Roberto tranquilizador. En el banco le explicaron que más que el importe de la operación fue la dirección de IP lo que les llamó la atención. "Rusia es una fuente habitual de fraudes de este tipo", dijeron. Y en la policía le contaron que lo más normal es que el robo de sus datos se hubiera producido en esos momentos en los que, por ejemplo, un camarero se lleva la Visa para pagar la cuenta en un restaurante, o en alguna compra por Internet.

El suyo no es, tristemente, un caso aislado. El robo de datos personales está a la orden del día. Un ejemplo llamativo ocurrió el pasado año, cuando los ciberdelincuentes accedieron de un solo golpe a los datos de 24,6 millones de cuentas de Sony Online Entertainment, proveedora de juegos para sistemas como la *PlayStation*, llevándose nombres, direcciones postales, emails, números de teléfono, fechas de nacimiento y hasta los datos bancarios de 10.700 clientes. Otro botón de muestra más: hace un mes, aparecieron en la Red 450.000 claves, de usuario y contraseña, de Yahoo! Voice, el servicio de voz por IP. Por no hablar de la conmoción que en España ha suscitado la recién destapada *Operación Pitusa*: unas 150 personas detenidas, hasta la fecha, entre funcionarios, detectives privados, *hackers*, policías, abogados y altos directivos que vendían sin escrúpulos listas con nombres y DNI, informes médicos o de la Seguridad Social y otra serie de datos confidenciales.

Nadie sabe a ciencia cierta cuánto dinero mueve este mercado negro de datos personales, aunque se estima que el 7% de todos los sistemas a escala mundial están controlados por *hackers*. "Hay todo un mundo paralelo creado para fabricar *malware*, herramientas de *hacking* e infección. Es una economía subyacente que va en aumento. Lo habitual es que los robos de información y ataques provengan de países del Este de Europa, pero el negocio de la compraventa se da en cualquier parte del mundo", señala María Ramírez de Trend Micro, un fabricante de seguridad *cloud*.

EL ROBO DE DATOS Y LA SUPLANTACIÓN DE IDENTIDAD SON HOY AMENAZAS REALES

LOS 'HACKERS' CONTROLAN EL 7% DE LOS SISTEMAS QUE HAY EN EL MUNDO

Y, para colmo, todo resulta increíblemente más fácil en la era de Internet. "Cualquier persona que tenga una cuenta de email o un perfil en una red social puede ser objetivo de un ciberataque y puede encontrarse con que sus datos se venden en Internet al mejor postor. Su precio dependerá de si éstos se acompañan del PIN o de las claves de acceso", afirma Pilar Santamaría, directora de Ciberseguridad para el Sur de Europa de Cisco. Desde Trend Micro cifran entre uno y diez dólares lo que se paga por un número de tarjeta de crédito, en función del país de procedencia, y en unos 85 dólares, un paquete de 2.500 credenciales de cuentas de Gmail.

EXPOSICIÓN SIN FRONTERAS. Hoy una misma persona accede a su correo personal o consulta su muro de Facebook desde el ordenador del trabajo. Y puede manejar ficheros corporativos desde su *smartphone* cuando está en casa. Las fronteras se desdibujan y esto crea puertas de entrada traseras que aumentan las posibilidades de sufrir un ataque –los virus, *troyanos* y gusanos crecen un 300% al trimestre– o de perder datos por el camino. Y la amenaza de ser víctima de una suplantación de identidad o de recibir un ataque de *spam*, esos correos masivos falsificados, como anzuelo para ser estafados es más real de lo que imagina.

Aunque, tal vez, la mayor *amenaza* para la fuga de datos seamos nosotros mismos. ¿Lo había pen-

sado? El auge de las redes sociales ha provocado un fenómeno nuevo: las personas están dispuesta a revelar ingente información sobre sí mismas. Subimos fotos, colgamos tuits y *post* con nuestros pensamientos, anunciamos que vamos de vacaciones a tal sitio o que hemos estado cenando en tal otro, decimos de quién somos fans… Lo que antes contábamos a un puñado de amigos ahora lo proclamamos a los cuatro vientos.

Y cada clic que hacemos en Internet, dónde entramos, qué vemos, durante cuánto tiempo… todo deja un rastro cada vez más fácil de seguir. El periódico *The Wall Street Journal* llevó a cabo una investigación durante un año bajo el título *What they Know* –Lo que ellos saben (de ti)–, en la que identificó más de cien intermediarios, entre compañías de monitorización, *brokers* de datos y redes de anunciantes, compitiendo por saciar este creciente apetito por saberlo todo de nosotros. "El negocio que más crece en Internet es el de espiar a los consumidores", señala el rotativo. Y las técnicas son cada vez más "intrusivas y omnipresentes", añade. Si las famosas galletas –*cookies*– se utilizan para generar listas de páginas vistas desde un ordenador, los nuevos *beacons* o *web bugs* van más allá. "Son imágenes pixeladas que informan cuando un usuario visita una determinada web", explica Neha Chachra, una investigadora del departamento de Informáti- ►

ca e Ingeniería de la Universidad de California. Pueden rastrear lo que el usuario hace dentro de la web, qué teclea y por dónde mueve el ratón.

"Nunca antes la gente había sido observada, su comportamiento analizado y sus preferencias personales tenidas en cuenta tan al detalle como ahora. Desconocemos adónde nos conducirá esto, pero algunas consecuencias posibles de la compra y venta de los datos y las actividades de los usuarios pueden ser funestas y, en cierta medida están pasando ya. Ceder tus datos a terceros puede ser invasivo y perjudicial", advierte Michael Fertik, consejero delegado y cofundador de Reputation.com, una compañía creada para salvaguardar la reputación y privacidad online de las personas y empresas. ¿Quién le garantiza que las aseguradoras no utilicen esa información personal supuestamente privada, de sus hábitos y costumbres, para calcular el valor de la póliza sanitaria? Y ya sabe, cuanto más insanas sean sus costumbres, más cara será su póliza.

El *peaje* para darse de alta en una web, bajarse una aplicación o recibir promociones de nuestra empresa favorita es rellenar un sencillo formulario. En lugar de dinero, la nueva moneda de cambio son nuestros datos personales. Y darse de baja a veces es una tarea engorrosa. Recientemente la Red se incendió cuando un internauta avisó que desde Rastreator.com, la web comparativa de seguros, le había llegado un correo avisando de que, si en 30 días no denegaban el consentimiento, sus datos personales serían cedidos a terceros para realizar promociones, estudios de opinión, estadísticas y campañas o actividades de publicidad. "Cualquier día te dicen que tienes 30 días para no darles todo tu dinero. Y el que calla, otorga", rezaba un comentario. "Yo conseguí darme de baja de todas las guías blancas en las que aparecía. Solo tuve problemas con una, pero tras solicitar la tutela a la Agencia Española de Protección de Datos, me dieron de baja tan rápido como pudieron", recomendaba otro internauta.

Nuestra privacidad, ¿al descubierto?

Control sobre al privacidad de algunas conocidas webs. Puntuación: máxima, 100 puntos; mínima, 0 puntos.

LAS QUE MÁS NOS PROTEGEN...

Twiter.com	100
Wikipedia.com	100
Orbitz.com	98
Delicious.com	95
Blogger.com	95

■Y LAS QUE MENOS

Thepiratebay.com	22
PCworld.com	37
Mercurynews.com	38
Footlocker.com	39
Hotels.com	43

FUENTE: PRIVACY CHOICE

REBASAR LOS LÍMITES. Toda esta exhibición en la Red, unida a las posibilidades que brindan las nuevas tecnologías, ha suscitado un acalorado debate: ¿nuestros datos son tan privados como pensamos? "Está en nuestra mano decidir si compartimos dicha información o no. Las empresas trabajan dentro de los marcos legales aunque, a veces, también en los huecos existentes para conseguir información de valor para su negocio", señala José Curto, analista de IDC. A este experto le gusta comparar la protección de datos con la Fórmula1 y con compañías como Redbull, que analizan los huecos de la legislación mecánica para diseñar coches con ventajas competitivas. El problema es que, en este caso, no está en juego ganar una carrera sino un derecho fundamental. Y lo cierto es que las empresas, en su afán por rentabilizar ese valioso activo cruzan con demasiada asiduidad la línea roja.

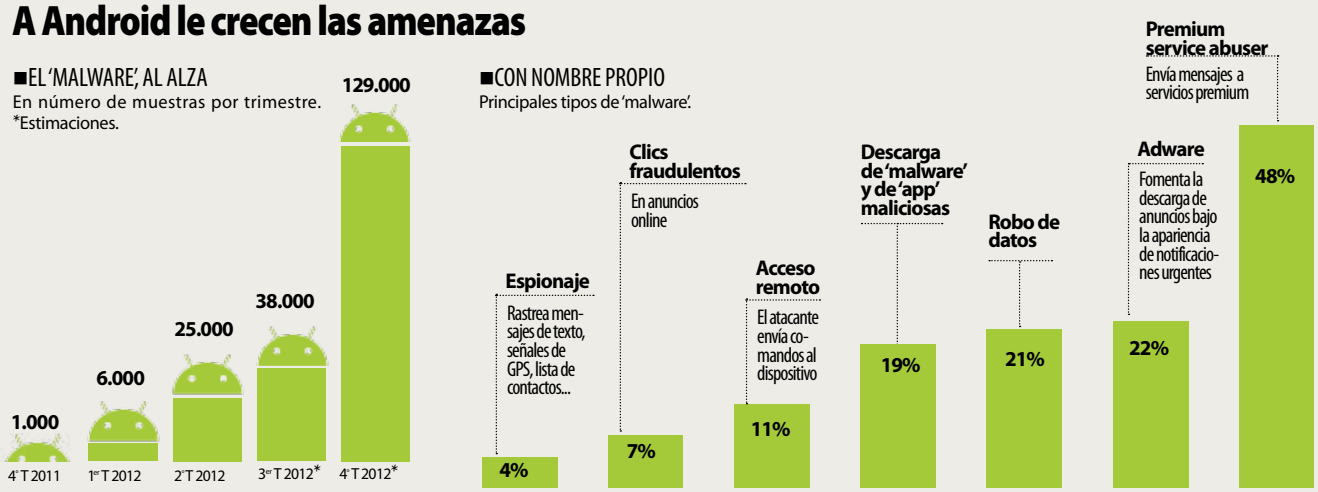
MUCHOS USUARIOS TIENEN QUE PELEARSE PARA DARSE DE BAJA DE BASES DE DATOS

Así, el pasado mayo la Comisión Federal de Comercio de Estados Unidos –FTC en sus siglas en inglés–, dio un severo tirón de orejas a MySpace por "haber engañado" a sus treinta millones de usuarios. Cada usuario de esta comunidad recibe un identificador llamado *friend ID* –por ejemplo, myspace.com/589685795–, que viene a ser como una ficha con datos personales: edad, sexo, lugar de residencia, aficiones, fotos y listas de amigos, el nombre de guerra o *nickname* e, incluso, el real, con apellidos incluidos. La FTC ha acusado a la red social de "violar" las leyes federales por permitir que anunciantes no afiliados accediesen a los *friend ID*. "Éstos podían fácilmente combinar los datos personales con otros adicionales facilitados por las propias *cookies* del anuncio que rastrean el historial de navegación del usuario", señala la FTC.

Éste es el último abuso de una larga lista de casos. Ahí están las controversias desatadas en torno a las prácticas de Google o la amonestación que este mismo organismo dio a Facebook el pasado noviembre por incumplir su política de privacidad al permitir el acceso a fotos y vídeos de cuentas que habían sido desactivadas o, incluso, borradas, compartir información personal con anunciantes o permitir que sus aplicaciones accedan a casi todos los datos personales, más de los que necesitarían saber para funcionar. "La innovación no tiene que venir a costa de la privacidad del consumidor", ha dicho Jon Leibowitz, presidente de la FTC.

Pero, seamos sinceros, ¿quién es capaz de leerse la política de privacidad de cualquier empresa? En Reputation.com hicieron una encuesta y el 86% contestó que nunca lo había hecho. Y si lo han intentando alguna vez, les habrá tocado enfrentarse a tres o cuatro folios ininteligibles. Y,

A Android le crecen las amenazas



FUENTE: TREND MICRO

El mercado negro de los datos

Valor estimado.

De **1a 10$** por cada número de tajetas de crédito.
De **25 a 35$** por una cartera de datos bancarios.
15$ por 1.000 credenciales de cuenta de Facebook.
75$ por 2.200 credenciales de Twtiter.
8$ por 1.000 credenciales de Yahoo! y Hotmail.
85$ por 2.500 credenciales de Gmail.

FUENTE: TREND MICRO

al final, casi seguro que ha acabado ¡perdido!

"La solución es que las escriban como si todos tuviéramos menos de catorce años y que se especifique de manera clara quiénes son esos terceros con los que comparten nuestros datos", explica el abogado Ignacio Suárez, experto en nuevas tecnologías, derecho de Internet y protección de datos. En Estados Unidos, el regulador no solo ha exigido a MySpace y Facebook, por ejemplo, unas políticas de privacidad más comprensibles, sino que les obliga a someterse a evaluaciones periódicas e independientes durante los próximos 20 años.

Pero llegado el caso, ¿sería posible borrar nuestro rastro, hacernos invisibles? "Es casi virtualmente imposible conocer toda nuestra huella digital, así que más lo es borrarla por completo", advierte Jim Brock, consejero delegado de PrivacyChoice, una compañía evalúa la transparencia y responsabilidad en la recogida y uso de datos en webs y en aplicaciones.

A esta batalla se lanzó el austríaco Max Schrems, de 24 años, decidido a conocer todo lo que Facebook sabía de él. Al final, recopiló 1.222 páginas en un CD, con datos personales. La sorpresa vino cuando, entre la montaña acumulada durante sus tres años de actividad, le alarmó que aparecieran conversaciones que había borrado, pero que la red social siguió conservando en sus archivos digitales. Fue el detonante para iniciar un pulso con este gigante de Internet ante el organismo irlandés para la protección de datos –el país acoge la sede en Europa– que al final dio razón a este estudiante.

EL DERECHO AL OLVIDO EXIGIRÁ A LAS EMPRESAS BORRAR LOS DATOS DEL USUARIO QUE LO PIDA

La preocupación es de tal alcance que las autoridades a ambos lados del Atlántico están pensando en cómo mejorar la protección de los consumidores. En Estado Unidos, donde no existe una legislación de protección de datos específica como en Europa, la Casa Blanca ha propuesto crear una ley sobre el derecho a la privacidad. Y aunque la mayoría de las empresas ofrece a los usuarios la posibilidad de denegar el acceso a terceros de sus datos –eso sí, esta opción no viene por defecto, sino que hay seleccionarla en la casilla de turno–, la FTC trabaja en una propuesta bautizada como *Do not track*, que "exige a las webs no rastrear a los usuarios que tengan la correspondiente propiedad en sus navegadores", explica Neha Chachra.

Por su parte, Europa trabaja para armonizar con un único reglamento la protección de datos en todo el territorio. Una de las novedades incluidas es reconocer expresamente el derecho al olvido. Bajo el *leitmotiv mis datos son míos*, si la propuesta sale adelante, las redes sociales y cualquier empresa que almacene datos personales estará obligada por ley a borrarlos de inmediato y por completo si su titular lo solicita. "Ahora, el problema es que se inicia un procedimiento que puede durar horas, días, años o, simplemente, se acabe denegando ese derecho si la persona es pública. Si se aprueba esta propuesta sería una buena noticia para garantizar un derecho nacido al calor de las nuevas tecnologías y las plataformas digitales no podrán seguir alegando tener su sede fuera de Europa para no retirar un contenido", asegura el abogado Suárez. "Y la petición de consentimiento expreso para usar *cookies* hará que la gente sea más consciente del valor de este intercambio de información", añade Jim Brock.

Facilitar nuestros datos no debería significar un cheque en blanco para que hagan con ellos lo que se quiera. Pero esté seguro de que su rastro seguirá siendo olfateado allá por donde pase. Es solo el principio de lo que esta nueva mina de oro puede dar de sí. Y las mafias seguirán ahí, acechando su oportunidad para lucrarse a su costa. Así que mejor, ¡no baje la guardia!

amaia.arteta@capital.es