Robos de información plantean necesidad de repensar cómo se protegen datos que circulan en internet.

El robo de más de 1.200 millones de contraseñas, que, de confirmarse, sería el mayor ataque llevado a cabo por piratas informáticos hasta ahora, vuelve a encender las alarmas sobre cuán protegidos están los datos que recorren la red, y se convierte en el más reciente de una lista de episodios que ponen de relieve la considerable vulnerabilidad de los sistemas de información en el mundo.

Pero, además de la magnitud (420.000 sitios fueron vulnerados por lo que se cree es una banda de una docena de hackers rusos), lo preocupante de este último ataque es la relativa simplicidad de los medios empleados. En lugar de misteriosas agencias estatales con tecnología de punta, los golpes de hoy los asestan ladrones que trabajan desde computadoras portátiles y que hallan formas sencillas de conducir ataques a gran escala.

En el caso de la pandilla rusa, los hackers infectaron docenas de computadoras personales para crear una botnet, una red de 'robots', en los que básicamente su computadora trabaja para los criminales sin que usted lo sepa. La red instruyó a sus terminales 'esclavas' para detectar fallas en cada sitio web visitado por el usuario. Si hallaban alguna, realizaban un ataque dirigido. Es una técnica que expertos comparan con ir de carro en carro en un parqueadero mirando si alguno tiene las puertas sin seguro.

El problema es que la mayoría de los sistemas de seguridad que se emplean hoy en día se basan en contraseñas alfanuméricas. Consideradas como virtualmente infalibles hace dos o más décadas, las contraseñas son cada día más susceptibles a ataques a gran escala que, a su vez, son más fáciles de realizar a medida que los equipos de cómputo ganan en poder y velocidad.

Datos de la firma Verizon sugieren que dos de cada tres violaciones de sistemas de seguridad involucran el uso de contraseñas robadas. Pedirles a los usuarios que las cambien

o que las hagan más complejas no ha demostrado tener efecto en las estadísticas.

En abril, el mundo se sorprendió con 'Heartbleed', un fallo informático que permite a los hackers abrir una puerta en OpenSSL, el sistema que encripta los datos sensibles de dos tercios de los sitios web en el planeta, y extraer piezas de información como contraseñas y nombres de usuario. Aunque se denunció como una seria vulnerabilidad, esta semana demuestra que poco o nada se ha hecho para solucionarla y que el 97 por ciento de los sitios vulnerables siguen en riesgo.

¿El fin de las contraseñas?
Eso ha llevado a muchas voces de la industria a plantear la necesidad de evolucionar hacia sistemas más complejos para proteger datos. Un camino natural es remplazar las contraseñas con métodos físicamente asociados al usuario, como los datos biométricos. La premisa es que a un ciberladrón le resultaría inservible tener su dirección de correo si además necesita su huella digital o el patrón de su retina.

Otra opción es sencillamente encriptar toda la red, para que los datos solo puedan ser descifrados una vez llegan a su legítimo destinatario. Yahoo, uno de los mayores proveedores de servicios de correo electrónico del mundo, anunció el jueves que permitirá a sus usuarios encriptar los mensajes que envíen mediante un sistema de encriptación PGP, una modalidad contra la que todos los ataques de los hackers hasta la fecha han resultado infructuosos.

PGP trabaja sobre una clave de encriptación única que cada usuario guarda en su ordenador, tableta y teléfono móvil. De esta manera, no será Yahoo (o Google, que también anunció en junio la adopción de un sistema similar) el que posea las claves de encriptación, sino que cada usuario generará sus propias claves, y sólo él y el receptor del mensaje podrán descifrarlo. Facebook, por su parte, adquirió recientemente la firma PrivateCore, que produce software para proteger información.