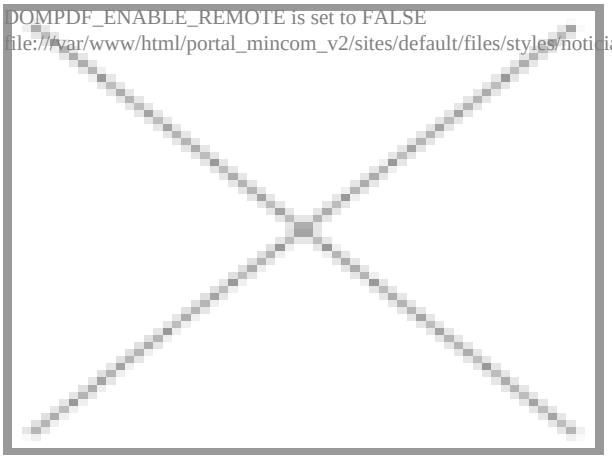

Source:
Siliconweek

Ciberterrorismo, phishing, ataques a la nube… El nuevo año empieza tal y como acabó el anterior: con empresas e individuos temerosos de que sus sistemas o dispositivos sean vulnerables.

¿Y de dónde pueden venir los ataques? Bruce Goslin, director ejecutivo de K2 Intelligence [1], intenta responder a esta pregunta señalando las **cinco tendencias que marcarán las pautas en el ámbito de la ciberseguridad y la ciberdefensa durante los próximos 12 meses**. Son estas:

1. Aumento de ataques patrocinados por estados, de la guerra digital y del ciberespionaje. Debido al éxito de las técnicas y tácticas del ciberespionaje y actividades de ciberguerra utilizadas por algunos gobiernos, otros países querrán desarrollar sus propios programas de ciberespionaje, particularmente en países con altas previsiones de crecimiento económico.

“Un ciberataque en instalaciones industriales puede causar estragos en un país y originar daños extremos. Por ejemplo, la **interrupción del servicio eléctrico**; esto no sólo afecta a la vida cotidiana, sino que también ocasiona una gran cantidad de pérdidas económicas a muchos niveles. Creemos que esta es una de las razones por las que crecerá la guerra cibernética en 2015, ya que los ciberterroristas intentarán provocar una mayor cantidad de daños en el territorio al que se dirijan”, señala Goslin en un comunicado distribuido por su compañía.

2. Aumento en el robo de información sensible y confidencial, como tarjetas de crédito o historiales médicos. Los historiales médicos contienen una gran cantidad de información personal que puede ser utilizada en una multitud de ataques y varios tipos de fraude. Por este motivo, desde K2 Intelligence esperan un mayor número de ciberataques contra esta industria.

Con el aumento constante de la seguridad por parte de las empresas, **los cibercriminales harán del phishing su vector de ataque preferido**, a la vez que introducirán y diseñarán nuevas técnicas de evasión de *e-mail* altamente sofisticadas y realizarán un reconocimiento más específico de los objetivos para que los correos tengan una apariencia cada vez más creíble y consigan una mayor tasa de clics.

4. A medida que aumenta el valor de los nombres de usuarios, contraseñas y credenciales robadas, también lo hace su valor en el mercado negro, propiciando que **emerjan más mercados negros todavía ocultos**.

5. Un aumento en ataques a la nube y móviles. Otra de las previsiones de K2 Intelligence para 2015 es el **aumento de las violaciones de seguridad en cuanto a nombres de usuario y contraseñas almacenadas en la nube**, ya que cada vez más datos de las organizaciones se están llevando a los servidores externos.

Por una parte, los nombres de usuario y contraseñas de cuentas con privilegios y de administrador son, básicamente, las “llaves del castillo”, como se pudo probar en los grandes ataques a bases de datos como el que sufrió la cadena de supermercados Target, con alto valor en el mercado negro.

Por otra, **los dispositivos móviles serán cada vez más objeto de ataques de robo de credenciales o autenticación** que se utilizarán en una fecha posterior. Estos ataques usarán el teléfono como un punto de entrada a las aplicaciones y datos empresariales basados en la nube a los que los dispositivos acceden libremente.

Disponible en:

http://www.siliconweek.es/security/los-ciberdelincuentes-no-daran-tregua... [2]

Links
[1] http://www.k2intelligence.com/es/
[2] http://www.siliconweek.es/security/los-ciberdelincuentes-no-daran-tregua-en-2015-73359#Zqdgy4m81pmvVWFu.99