El peligro que ocultan las memorias USB

09/10/2014

Da igual que sea de 32 gigas y esté lleno de películas, series o documentos, la gente que se lo lleva de nuestras casas por lo general se lo queda y se olvida de que no es suyo.

Pero esta práctica de lo más habitual en nuestros días debería dejar de existir. Y no solo por deferencia, sino por seguridad informática. Muchos de los virus que se han hecho famosos en las noticias empezaron infectando no a través del correo electrónico o de descargas en oscuras paginas web, sino a través de un inocente usb.

Conficker, el gusano que infectó a millones de ordenadores y los convirtió en una gigantesca red de zombies, se introdujo en los ordenadores de la Marina francesa y en los del ayuntamiento de Manchester (Inglaterra) y en los de otras muchas instituciones, y casi siempre a través de usb infectados.

En 2008, un virus llamado agent.btz entró dentro de uno de los sistemas a priori más seguros del planeta, los ordenadores de la marina de los Estados Unidos, y lo hizo de la misma forma que Conficker. Esta infección inició en una base americana en Oriente Medio, y los militares sospechan que se trató de un ataque de los servicio secretos de otro país.

Incluso algunos medios han relacionado los virus que paralizaron el ordenador central de seguridad de la aerolínea Spanair con un usb infectado. Si ese PC no hubiera tenido problemas, es probable que no hubiera

permitido que el vuelo JK5022 hubiera despegado de Madrid aquella fatídica tarde del 20 de agosto de 2008.

Los antivirus poco pueden hacer

Los virus que puedan transportar los USB también pueden servir para hacerse con el control del ordenador al que se están conectando. O en cuestión de segundos pueden robar información importante de nuestro disco duro.

Los antivirus son por norma general poco hábiles para detectar actividad extraña en estas unidades. Los ordenadores ven a las memorias usb como una unidad extraíble y si la escasean, lo hacen de manera superficial. Los programas maliciosos que puedan tener en su interior pueden camuflarse de manera mucho más fácil que si llegaran a través de un correo electrónico.

Y los usb no son el único problema. Los móviles Android también pueden transportar información maliciosa que nos puede meter en problemas. Un inocente '¿Puedo cargar mi móvil en tu ordenador?' puede ser el inicio de una pesadilla. Karsten Nohl, jefe de seguridad de la firma SRLabs asegura a la CNN que con tan solo bajarnos una app equivocada -y en Google Play existen varias de esas- puede hacer que nuestro móvil se infecte y el problema salte a nuestro pc cuando lo conectemos.

Así que la mejor manera de evitar que estos dispositivos nos creen problemas es tratarlos como si fueran nuestro cepillo de dientes. ¿A qué nunca lo prestaríamos a nadie? Pues eso.