

Amenaza mundial con el último virus informático

2009-02-15 18:22:11



Millones de usuarios de Windows en todo el mundo se enfrentan a la amenaza de un gusano informático que se propaga a través de redes de baja seguridad, memorias USB y computadores personales que no cuentan con las últimas actualizaciones de seguridad.

El programa dañino, conocido con los nombres de Conficker, Downadup o Kido, fue descubierto por primera vez en octubre de 2008. Aunque Microsoft lanzó un “parche” de seguridad, se piensa que el gusano ya ha infectado 3,5 millones de computadores.

Los expertos aseguran que esta cifra podría ser mucho mayor y afirman que los usuarios deberían tener programas antivirus actualizados e instalar el “parche” de Microsoft MS08-067.

Según Microsoft, el gusano informático funciona buscando un fichero ejecutable de Windows llamado “services.exe” y pasa a formar parte de ese código.

Entonces se copia a sí mismo en el sistema de ficheros de Windows como un fichero más del tipo conocido como “dll”. Se da a sí mismo un nombre de entre 5 y 8 caracteres, y modifica el registro, que enumera configuraciones clave de Windows para poner en funcionamiento el fichero infectado dll como un servicio.

Una vez está en marcha, el gusano hace un servidor HTTP, cambia el punto de restauración del sistema del computador (haciendo más difícil recuperar el sistema infectado) y entonces descarga ficheros del sitio de internet del pirata informático.

La mayoría de los programas dañinos utiliza uno de los pocos sitios desde los que puede descargar ficheros, haciendo que sean fáciles de localizar y cerrar. Pero Conficker funciona de manera diferente.

Según la firma de antivirus F-Secure, el gusano utiliza un complicado algoritmo para generar cientos de nombres de dominios diferentes cada día, tales como mphtfrxs.net, imctaef.cc y hcweu.org.

Tan sólo uno de estos será de hecho el sitio utilizado para bajar los ficheros del

pirata. Ante ello, será imposible rastrear ese sitio.

En cualquier caso, los técnicos han logrado revertir el gusano, de manera que pueden predecir alguno de los posibles nombres de los dominios. Ello no ayuda a descubrir quiénes son los responsables de la creación de Downadup, sin embargo al menos les permite saber cuantas máquinas están infectadas.

Windows afirma que el software dañino ha infectado computadores en muchas partes del mundo, siendo China, Brasil, Rusia e India los países con el mayor número de máquinas infectadas.

Via | [BBC Mundo](#)