

Este tipo de virus ya ha infectado a más 8,9 millones de PCs en varios países

Los gusanos informáticos invaden los ordenadores desprotegidos de todo el mundo

En los últimos días se han disparado las infecciones de un gusano informático que se propaga a través de las redes de baja seguridad, memorias USB y ordenadores 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.

[Fax Press/BBC Mundo/La Razón](#) .- La empresa antivirus F-Secure estima que ya hay 8,9 millones de computadores infectados en todo el mundo. Los expertos advierten que las cifras podrían aumentar y aconsejan a los usuarios a actualizar los programas antivirus e instalar el "parche" de Microsoft MS08-067.

Según asegura en su página de internet la compañía F-Secure, el número de infecciones basado en sus cálculos se ha "disparado" y que la situación "está emperorando". Graham Culley, consultor de tecnología de la empresa antivirus Sophos, aseguró que la magnitud del contagio no se había visto en mucho tiempo.

"Microsoft hizo una buena labor actualizando los computadores personales, pero el virus continúa infectando a las empresas que no han instalado el parche. La reducción del personal técnico durante las vacaciones no ayudó y la aplicación de un parche a un gran número de computadores no es cosa fácil", aseguró Culley.

"Además, si los usuarios utilizan contraseñas vulnerables, como 12345, el virus las puede descifrar rápidamente", añadió. "Pero como el virus se puede propagar a través de las memorias USB, aunque se aplique el parche de Windows no hay seguridad. Para eso se necesita tener un programa antivirus", concluyó.

Método

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 crea 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 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.

Variante

Según Eddy Willems, analista de seguridad de la firma Kaspersky Lab, una nueva cepa del virus está complicando la situación. "Apareció hace menos de dos semanas y es la que está causando la mayor parte de los problemas", explicó Willems.

"Lo métodos que utiliza para replicarse son bastante buenos. Además, usa múltiples mecanismos, incluyendo memorias USB, con lo que puede pasar de un computador a otro a través de esas memorias portátiles", agregó.

Según el experto, el problema es que la gente no ha protegido sus computadores. Si utilizaran los "parches" de seguridad no tendrían que preocuparse. Los técnicos han logrado revertir el gusano, de manera que pueden predecir alguno de los posibles nombres de los dominios. Ello no ayuda a averiguar quiénes son los responsables de la creación de Downadup, pero al menos les permite saber cuantas máquinas están infectadas.

"Estamos viendo cómo cientos de miles de direcciones IP únicas se conectan a los dominios que hemos registrado", dijo en un comunicado Tony Kovunen, de la compañía F-Secure. "Podemos verlos pero no podemos desinfectarlos, ya que sería considerado como un uso no autorizado".

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.

Fecha artículo: 2009-01-20 09:22:39 - url artículo: <http://www.internautas.org/html/4430.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org