



Colegio de Abogados del Departamento Judicial de Dolores.
Belgrano N° 160 - 7100 Dolores (Bs. As)- Tel-Fax: (02245) 441592
E mail: colabdol@fairweb.com.ar

CIRCULAR N° 46

Dolores, 25 de septiembre de 2.001.-
UNREGISTERED
REF: "Su Colegio le Informa".-
Created by Unregistered Version

NOTICIA DIFUNDIDA

Jueves, 20 de septiembre de 2001

Un supervirus provoca el contagio más rápido de la historia de Internet

El patógeno, de origen chino, se propaga de tres formas distintas

HÉCTOR BARCA | Madrid

UNREGISTERED

Created by Unregistered Version

La seguridad en Internet vuelve a estar en entredicho. Desde ayer, actividades teóricamente inocuas como visitar una página *web* o leer un mensaje de correo electrónico pueden propiciar un ataque vírico. La culpa la tiene *Nimda* (*admin* al revés), un gusano informático que en apenas unas horas ha sido capaz de encaramarse a la cabeza de las listas de prevalencia mundial, tras contagiar miles de ordenadores en Norteamérica y Europa.

La velocidad expansiva de *Nimda* se debe al hecho de que combina las técnicas de propagación empleadas por *Código rojo*, *Sircam* y *BubbleBoy*, tres de los virus más recientes e insidiosos de los últimos dos años.

Han sido cerca de 30.000 los casos recogidos por el centro de seguimiento vírico de la compañía Trend Micro a lo largo de las últimas 24 horas, por poco más de 3.000 de *Sircam*, el antiguo líder de tan dudosa clasificación.

Entre las víctimas conocidas hasta el momento destacan el Ministerio de Agricultura japonés, la multinacional germana Siemens y el portal financiero de los correos suizos, amén de cerca de 15.000 compañías europeas y más de 130.000 servidores norteamericanos de páginas *web*.

Precisamente Estados Unidos ha sido el país en el que *Nimda* ha impactado con especial incidencia, registrando más de un 80% de las infecciones totales. Ante este fenómeno, el secretario de Justicia, John Ashcroft, ha asegurado que no existe relación alguna entre la aparición de este espécimen y los atentados terroristas contra las Torres Gemelas y el Pentágono.

Las infecciones provocadas por *Nimda* pueden contraerse de tres formas: visitando páginas *web* infectadas, leyendo *e-mails* portadores, o trabajando en red con ordenadores contagiados. Las infecciones se producen a partir de un grave agujero de seguridad en Internet Explorer, descubierto por el especialista español Juan Carlos García Cuartango a mediados de marzo. A pesar de que Microsoft publicó a los pocos días un parche que solucionaba el problema, parece evidente que han sido muy pocos los usuarios que se han preocupado de proteger su sistema ante posibles ataques.

UNREGISTERED

Cuando *Nimda* se transmite por correo electrónico se presenta en forma de archivo anexo, llamado 'README.EXE', junto a *e-mails* que llevan como remitente el nombre del internauta infectado. En caso de que el destinatario lea el mensaje portador con el programa de correo Outlook, el patógeno se instalará en su sistema, y en el de todos los ordenadores a los que éste se encuentre conectado en red, si los hubiere.

Created by Unregistered Version

En las máquinas que albergan un servidor *web* bajo Windows NT o 2000, *Nimda* incluye en las páginas de todos los usuarios el código necesario para que quienes las visiten se infecten con una copia del gusano. Además, este espécimen modifica los parámetros de seguridad de los servidores afectados, permitiendo así la entrada de atacantes o infectivos oportunistas.

Nimda completa su ciclo expansivo enviándose a las direcciones que encuentra entre la correspondencia y las páginas *web* almacenadas en el disco duro del usuario infectado.

Se trata, pues, del primer patógeno capaz de propagarse de tres maneras distintas: entre usuarios de un servidor *web*, entre máquinas de una red de trabajo, y vía *e-mail* o páginas *web*.

La medida de prevención más efectiva frente a *Nimda* pasa por descargar el parche de Microsoft, disponible en la dirección <http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp>.

Carlos...

Dr. Francisco S. Repetto.-
Secretario.-

Dr. Adrián Rubén Lamacchia.-
Presidente.-