Trend Micro Provides “Fix-it” Tool for Victims of PE_NIMDA.A Virus

Submitted by: Text 100 London
Thursday, 20 September 2001

New fix-it tool and updated pattern file available at www.trendmicro.co.uk

Marlow, England – 20 September 2001 – Trend Micro (NASDAQ: TMIC; TSE: 4704), a worldwide leader in network antivirus and Internet content security solutions, announced the availability of a “fix-it” tool for PE_NIMDA.A, also known as the Nimda virus. Trend Micro has also released an updated pattern file, #942, to detect and remove this worm.

This pattern file is available for download from Trend Micro’s Web site at www.trendmicro.co.uk

Customers can also download the fix-it tool from Trend Micro’s Web site at www.trendmicro.co.uk

The tool will repair damage that’s already taken place on the client systems by restoring the integrity of their system files. The tool is designed to run on Windows NT, 2000, 9x and ME machines. Before using this new tool, Trend Micro recommends that end users scan their system for the NIMDA virus first by using Trend Micro’s free online virus scanner called HouseCall available at http://housecall.antivirus.com/housecall/start_pcc.asp

If HouseCall determines that the user’s system is infected by PE_NIMDA.A, the user should disconnect their computers from the network to prevent further infection and download and run the fix-it tool, FIX_NIMDA.EXE, from a clean disk.

PE_NIMDA.A has three modes of spreading: through email, network-shared drives or through servers with IIS installed. When spreading through email, the attachment usually is named “readme.exe.” However, there have also been customer reports of file attachments with extensions .wav and .com.

Since the file name and extension of the attachment changes, customers are advised to use Trend Micro's InterScanä eManager™ and ScanMailä eManager to block all executables files and all non-business-related files.

PE_NIMDA.A can propagate via email using its own SMTP engine and also through additional messaging application program interfaces (APIs). The worm carrying email may be executed automatically when it is opened using Microsoft Outlook or Outlook Express. Trend Micro is recommending that end users on Windows 9x, NT, 2000, and ME machines install the most recent patch form Microsoft to ensure that their client systems are no longer susceptible to this particular vulnerability.

To download this patch go to Microsoft’s Web site at http://www.microsoft.com/technet/

This new threat also uses the IIS Web Directory Traversal exploit, also known as the Unicode Web Traversal IIS exploit. A patch to address this particular vulnerability is available for download at http://www.microsoft.com/technet/

The worm can also propagate through shared-network drives. Similar to PE_FUNLOVE.4099, the worm searches the network to which the infected machine belongs for shared folders with write access. If one is found, a randomly named Newsgroup posting (NWS) or EML file is dropped. These dropped files also contain the worm as an attachment.

For more information regarding PE_NIMDA.A, please go to http://www.antivirus.com/vinfo/

“We don't yet have a real idea of the extent of damage related to this worm, but we do know that this virus is creating quite a lot of commotion worldwide,” said Joe Hartmann, director of North American virus research with Trend Micro. “Already PE_NIMDA.A has jumped to number one on our virus tracking map with over 26,000 infected computers worldwide.”

About Trend Micro

Trend Micro is a leader in network antivirus and Internet content security software and services. The Tokyo-based corporation has its European headquarters in Marlow, England, and business units worldwide. Trend Micro products are sold through corporate, value-added resellers and managed service providers.

For additional information and evaluation copies of all Trend Micro products, visit: http://uk.antivirus.com or www.trendmicro.co.uk

For additional information contact:

Europe

Anna Wright
Trend Micro European Marcoms
Tel: + 44 (0)1628 400534
anna_wright@trendmicro.co.uk