ConnectIT e-news Daily
26-January-2004

New virus hits high outbreak level

by Mark Cox

A new virus, W32/Mydoom@MM, also known as Mydoom, made its appearance on Monday, and quickly earned itself a high outbreak assessment from Network Associates' McAfee AVERT (Anti-Virus and Vulnerability Emergency Response Team).

"AVERT says it's receiving a very large number of samples from corporate and home users alike," said Jack Sebbag, Canadian General Manager and Vice President of Network Associates. "That's why it's been raised from medium to high. The infection is spreading at a very rapid rate."

Mydoom is a mass mailer. Despite the ominous name, it won't delete files. And it requires you to click proactively on the attachment, which isn't even disguised in a particularly cunning fashion. But Sebbag noted that there always seem to be people with too much time on their hands who manage to trigger the virus.

There doesn't seem to be a clear pattern in the subject lines or text, It arrives in an email message as follows:

From: (spoofed)

Subject: (Random)

Body: (Varies, such as)

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Attachment: (varies [.exe, .pif, .cmd, .scr]. It often arrives in a ZIP archive. The icon used by the file tries to make it appear as if the attachment is a text file. The one thing that is constant, Sebbag said, is its size, 22,528 bytes.

When this file is run it copies itself to the local system with the following filenames:

c:\Program Files\KaZaA\My Shared Folder\activation_crack.scr

c:\WINDOWS\Desktop\Document.scr

c:\WINDOWS\SYSTEM\taskmon.exe

It also uses a DLL that it creates in the Windows System directory:

c:\WINDOWS\SYSTEM\shimgapi.dll (4,096 bytes)

It creates the following registry entry to hook Windows startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows_ CurrentVersion\Run "TaskMon" =
%SysDir%\taskmon.exe

The worm opens a connection on TCP port 3127, suggesting remote access capabilities.

"It may have keystroke logging attached to it to let someone take over your OS," Sebbag said. "It does have that capability."

Upon executing the virus, Notepad is opened, filled with nonsense characters. The file will try to spread via email and by copying itself to the shared directory for Kazaa clients if they are present.