Subject: Warning: Spy Virus Spreading
Posted by Xtrm2Matt on Fri, 30 Jan 2004 07:42:25 GMT
View Forum Message <> Reply to Message

This virus is also known as "MyDoom".

Quote:Why We Are Issuing This Alert
At 9:00 A.M. Pacific Time on Wednesday, January 28, 2004, Microsoft began investigating reports of a variant of a new worm named "Mydoom" or "Novarg," known as Mydoom.B. This variant reportedly blocks access to some websites, including some Microsoft.com websites. The worm attempts to entice e-mail recipients into opening a message that has a file attachment. If the attached file is opened, the worm installs malicious code on the computer user's system and sends itself to all contacts in the user's address book.

http://www.microsoft.com/security/antivirus/mydoom.asp

Also, Symantec have made a tool to quickly remove this virus from your PC. They call it the "W32.Novarg.A@mm Removal Tool".

Quote:The W32.Novarg.A@mm Removal Tool does the following:

Terminates the W32.Novarg.A@mm viral processes.
Terminates the viral thread running under Explorer.exe.
Deletes the W32.Novarg.A@mm files.
Deletes the registry values added by the worm.

http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.removal.tool.html

And if your not sure if you have the virus, then do this:

Quote:If you use Windows XP

To find out if a computer is infected, do the following:

Click Start, and then click Search.
In the What do you want to search for? box, click All files and folders.
In the All or part of the file name box, type ctfmon.dll. If that file exists on the computer, the computer is infected with Mydoom.B, and you need to follow the steps below. Otherwise, the computer is not infected with that variant of the virus.

If you use Windows 2000 or Windows NT 4.0

To check for the worm yourself, do the following:

Click Start, and then click Run.
In the Open box, type cmd

Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.
Click the cursor, type dir ctfmon.dll /a /s and then press ENTER.
Wait a few moments:
If the results show File Not Found, the computer is not infected with Mydoom.B.

If you use Windows 98 or Windows 95

Click Start, and then click Run.
In the Open box, type command
Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.
Click the cursor, type dir ctfmon.dll /a /s and then press ENTER.
Wait a few moments:
If the results show File Not Found, the computer is not infected with Mydoom.B.

If any of the above actions actually find this .DLL file, i strongly advise you use the "W32.Novarg.A@mm Removal Tool" OR the steps below:

What to Do If Your Computer Is Infected

If your computer is infected, first try going to the website of your antivirus-software vendor to get the latest updates and information. If you are unable to access your antivirus-software vendor's site and need to fix the infection yourself, follow these steps:

Quote:Click Start, and then click Run.

In the Open box, type cmd.

Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.

Click the cursor and:
Type del /F %systemroot%\system32\drivers\etc\hosts
Press ENTER.

Type echo # Temporary HOSTS file >%systemroot%\system32\drivers\etc\hosts
Press ENTER.

Type attrib +R %systemroot%\system32\drivers\etc\hosts
Press ENTER.

After typing these commands, do one of the following:
If you use Windows NT 4.0, restart your computer.
If you use Windows XP or Windows 2000, do not restart your computer.

Instead, do the following:
Type ipconfig /flushdns
Press ENTER.

Hope this helps