

strange file

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-05/0579.html

From: MAP (*anonymous_at_discussions.microsoft.com*)

Date: 05/04/04

Date: Tue, 4 May 2004 05:27:43 -0700

>-----Original Message-----

>what does the file rundll32.exe do? norton av keeps

>picking it up as a virus

>

>

Even though rundll32.exe is a valid application many viruses and worm will try to hide themselves by using the same name.If Norton says you have one then you most likely do.

Rundll32.exe

(Microsoft)

Microsoft's "Run a DLL as an App". A DLL is a Dynamic Link Library. In layman and [very] simplistic terms a DLL is a portion of a software program which is only used by the main program as and when specific features of the software are used by the end user (for instance the PRINT function in your wordprocessor). The main advantage is that, using this technique, programmers can develop software which does not end up gobbling up memory through the whole program loading in one go, but which instead only uses enough memory for the core functions of the program, with specific features, implemented in separate DLL files, only loaded as and when the end-user decides to use them (ie. The Print DLL will only be loaded into memory when the end-user clicks on PRINT). Another advantage is that the software developers can also have common features which they have implemented across a range of their programs, implemented just the one time as a shared DLL which is used by all that developer's programs. RUNDLL and RUNDLL32 are the Microsoft Windows programs that need to be used to load DLLs into memory so that they can be used by specific programs or by Windows.

Recommendation :

RUNDLL and RUNDLL32 do not normally appear in the Task List in Windows. In our experience they tend to appear only when you are already having problems of some sort with your PC, or a particular DLL is either misbehaving, is buggy, or is having problems, such as a Control Panel applet hanging for example. If you see RUNDLL or RUNDLL32 in your Task List persistently then you should be [slightly] worried (see below the other entry for RUNDLL32) – make sure you have good and up-to-date antivirus software, boot into Safe Mode, and run a full virus scan on your PC. If you do not have a virus and see either in your Task List, simply leave it alone. We are not sure as to the other times when the real RUNDLL or RUNDLL32 can sometimes suddenly appear in the Task List, but you should leave them alone in most cases provided, again, that you know you do not have a virus.

Rundll32

(2)

Rundll32.exe

(???)

You have one of the W32.Miroot.Worm / W32/Legemer.Worm / W32.HLLW.Sanker viruses (or another virus).