
Delete Virus Jamban dan Flash10

(Tuesday, 09 October 2007) - Written by Administrator - Last Updated (Tuesday, 09 October 2007)

Use HijackThis to scan and then remove the entries that contain Flash.10.exe, JambaMu.com, MSN.msn

Enable Folder Options that disabled by the malware:

Go to Run -> Type gpedit.msc -> Expand "User Configuration" -> Expand "Administrative Templates" -> Expand "Windows Components" -> Select "Windows Explorer" -> Double click "Removes the Folder Options menu item from the Tools menu" in the right panel -> Select Disabled

Folder Options should be appeared now, go to Folder Options -> Select "show hidden files and folders" & uncheck "hide protected operating system files"

Go to C:\Windows\System32, delete Flash.10.exe, JambanMu.com, regedit.com, cmd.com, msconfig.com, ping.com, dxdiag.com

Delete My Secret.fold in My Documents, New Song.lagu & New Video.vidz in My Music, aweks.pikz & seram.pikz in My Pictures

Delete C:\Program Files\Common Files\Microsoft Shared\DAO\MSN.msn

Delete C:\Program Files\Common Files\Microsoft Shared\Macromedia.10.exe

- If you cannot delete the files and get messages like "cannot read from the source disk" or others that similar, probably your antivirus has blocked the access to these files, that's why you cannot move, delete or rename the files. Disable your antivirus and try again.

*regedit.exe and cmd.exe actually stay intact, it just disabled by the malware.

Enable regedit that disabled by the malware:

Go to Run -> Type gpedit.msc -> Expand "User Configuration" -> Expand "Administrative Templates" -> Select "System" -> Double click "Prevent access to registry editing tools" in the right panel -> Select Disabled

Enable command prompt(cmd) that disabled by the malware:

Go to Run -> Type gpedit.msc -> Expand "User Configuration" -> Expand "Administrative Templates" -> Select "System" -> Double click "Prevent access to the command prompt" in the right panel -> Select Disabled