

Re: Has been file replaced?

Re: Has been file replaced?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2008-09/msg03135.html>

- *From:* "Pegasus \ (MVP)" <I.can@xxxxxxxxxxx>
 - *Date:* Thu, 18 Sep 2008 12:55:32 +0200
-

Here are the details for c:\windows\system32\setup.exe on my WinXP Pro machine:

--a-- W32i APP ENU 5.1.2600.5512 shp 23,040 04-14-2008 setup.exe

Perhaps your file is hidden. If it is really missing then you can restore it from the i386 folder of your WinXP installation CD. In this case the Windows File Protection mechanism won't interfere.

"Santander" <santander@xxxxxxxxxxxxxxxx> wrote in message [news:%23Hqd\\$XGJHA.1268@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:%23Hqd$XGJHA.1268@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I find no setup.exe in windows system32 folder, there is setupapi.dll v. 5.1.2600.5512 setupdll.dll v. 5.1.2600.0
The application is old HHD Sector Scan utility (Floppy Version) 3.0 from SalvationDATA Technology Inc. File name hsr3.0floppysetup.exe is SFX RAR archive.

Not clear why this utility tried to replace setup. Probably virus??
I checked file on online scanner, <http://www.virustotal.com>, and few antiviruses show that there is a virus:

Avast 4.8.1195.0 2008.09.17 Win32:Spyware-gen
eSafe 7.0.17.0 2008.09.17 Suspicious File
Ikarus T3.1.1.34.0 2008.09.18 Virus.Win32.Spyware
eSafe 7.0.17.0 2008.09.17 Suspicious File

NOD32 and Kaspersky does not detected anything. Is this false positive?
But we know new viruses appears every day. Please give the advice.

"ju.c" <bibidybubidyboop@xxxxxxxxxxxxxxxx> wrote in message <news:OvCfwBXGJHA.768@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Re: Has been file replaced?

The Windows file "setup.exe" is located in 'C:\WINDOWS\system32'.

"file version of the system file is 5.1.2600.5512"

That is correct for WinXP SP3. 'Windows File Protection' has done its job. Everything looks fine.

ju.c

"Santander" <santander@xxxxxxxxxxxxxxxx> wrote in message
news:erUoA4WGJHA.4056@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Someone run untested self-extracting archive (executable)
on work PC. I
checked Event Viewer tasks and find there:

System -> Source: Windows File Protection

Event Type: Information
Event Source: Windows File Protection
Event Category: None
Event ID: 64002
Date: 2008.09.17.
Time: 9:59:49
User: N/A
Computer: UserName
Description:
File replacement was attempted on the protected system file
setup.exe.
This
file was restored to the original version to maintain system
stability.
The
file version of the system file is 5.1.2600.5512.
For more information, see Help and Support Center at
<http://go.microsoft.com/fwlink/events.asp>.

Has been replaced this system file or not?(is if was restored).
What is
this file and where?

Thanks.

Re: Has been file replaced?