

Re: Windows 2000 WFP

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.setup_upgrade/2005-08/msg00022.html

- *From:* "Jim Nugent" <njim2k-nntp@xxxxxxxxxx>
 - *Date:* Wed, 17 Aug 2005 08:55:18 -0500
-

Thanks, Dave.

It sounds like WFP simply consults the dllcache and servicepackfiles directories. Think that to be rather non-robust I decided on an experiment — dropping a replacement file into dllcache. But first I just wanted to verify that things were working properly: I made a copy of notepad.exe on my desktop, and renamed it to calc.exe. Then copied and pasted the "bogus" calc.exe into c:\winnt\system32.

1. It stayed there, and clicking on it brought up notepad.
2. It copied the bogus calc.exe into dllcache!

I noted that if I DELETE the file from system32, it will pull it from dllcache, but not if I replace it. Assuming malware or a misguided install tries to replace a system file, I find this behavior analogous to the following:

1. WFP does not restore modified system file = watchdog is sound asleep.
2. WFP(?) copies modified file into dllcache = watchdog dog comes running to thief with your wallet in its mouth.

What am I missing? Do you have to run SFC to get WFP to act?

—

Jim

"Be right back... Godot"

"Dave Patrick" <DSPatrick@xxxxxxxxxxxxxxxxxx> wrote in message <news:OmMJjntoFHA.2976@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

> When updates are installed the \servicepackfiles and \dllcache folders are updated with the new versions. SFC pulls from these.

>

>

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/system_file_checker.mspx

>

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/system_file_protection.mspx

>

>

> --

> Regards,
>
> Dave PatrickPlease no email replies – reply in newsgroup.
> Microsoft Certified Professional
> Microsoft MVP [Windows]
> <http://www.microsoft.com/protect>
>
> "Jim Nugent" wrote:
> | In all my W2k research, I have never come across what it is (catalog?
> | database?) that WFP consults to determine if a system file is the
> | "correct
> | one." Obviously, msi files have to update this information since they
> | are
> | allowed to replace these files.
> |
> | But how can I repair it if something goes wrong. For example, if I were
> | to
> | do an sfc /scannow right now, I believe it would "break" some hot fixes
> | by
> | undoing some file replacements. I'd like to tell it what I believe to be
> | the
> | correct files. How do I do that?
> | --
> | Jim
> | "Be right back... Godot"
> |
> |
> |
> |
> |

• *Follow-Ups:*

- ◆ **[Re: Windows 2000 WFP](#)**
 ◇ From: Dave Patrick

• *References:*

- ◆ **[Windows 2000 WFP](#)**
 ◇ From: Jim Nugent
- ◆ **[Re: Windows 2000 WFP](#)**
 ◇ From: Dave Patrick

- Prev by Date: **[Re: Windows 2000 WFP](#)**
- Next by Date: **[Windows 2000 server problem](#)**
- Previous by thread: **[Re: Windows 2000 WFP](#)**
- Next by thread: **[Re: Windows 2000 WFP](#)**
- Index(es):
 - ◆ **[Date](#)**

Re: Windows 2000 WFP

◆ *Thread*