

Forum:[Hack Forums](#)

Thread: [\[MRT-X\] Understanding Windows File Protection and Renaming System Files](#)

Tha Sneak - March 18, 2025, 12:32 am

Understanding Windows File Protection and Renaming System Files

1. Introduction

Windows File Protection (WFP) ensures that critical system files remain intact and unmodified. If a protected file is renamed or deleted, Windows automatically replaces it with a backup copy (if WFP is enabled).

This behavior only applies to .exe files and works only when Windows File Protection is switched on .

2. How Renaming a System File Works

Renaming a file does not change its function, but if Windows detects that a protected system file is missing, it replaces it with a backup copy stored on the system.

Example: If regedit.exe is renamed to regedit-old.exe, Windows detects that regedit.exe is missing.

A new copy of regedit.exe appears, restored from backup.

This behavior only works if Windows File Protection is enabled.

3. Replacing a Patched System File (e.g., winlogon.exe)

In some cases, malware modifies critical system files (e.g., winlogon.exe). There are two methods to restore a clean copy:

A. Using FRST (Replace:) The Replace: command in FRST forces the replacement of a patched system file.

This ensures that a clean version is used instead of an infected one.

B. Manual Renaming Method Rename winlogon.exe to winlogon-infected.exe.

If Windows File Protection is enabled, Windows automatically restores a clean copy of winlogon.exe .

This method works only if Windows File Protection is on.

4. When File Protection is Enabled

If Windows File Protection is switched on, renaming a system file will result in a new copy appearing next to the renamed file.

Example:Rename taskmgr.exe to taskmgr-old.exe.

Windows immediately creates a fresh copy of taskmgr.exe in the same location.

However, this does not work for every malware infection.

5. When This Won't Work (Virus/Sality Infections)

In cases of Virus or Sality infections, renaming system files does not help because:The backup files in Windows File Protection are also infected.

Windows restores an already compromised version of the file.

A clean Windows installation or system restore is required instead.

For more information, refer to:

<http://support.microsoft.com/kb/222193>

6. Checking If Windows File Protection is Disabled

The linked Microsoft article explains the SFCDisable registry setting:If SFCDisable is present, Windows File Protection is switched off.

If WFP is disabled, renaming system files will NOT trigger file replacement.

You can read more details on how SFC works, including registry settings, here:

<http://support.microsoft.com/kb/222473/>

7. How to Re-Enable Windows File Protection

If SFCDisable has been turned off (by malware or user action), you can re-enable it: Open Command Prompt (Admin) (Win + X > Command Prompt (Admin)).

Type:

Code `sfc /scannow`

Press Enter to restore system file integrity.

Restart your computer for changes to take effect.