

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] HijackThis: F0, F1, F2, and F3 Entries \[Legacy Tool\] \[Optional\]](#)

Tha Sneak - February 14, 2025, 12:48 am

HijackThis!: What Do All Those Numbers Mean?: F0, F1, F2, F3 Entries

In this section, we will evaluate the entries that correspond to programs loaded from your .INI files, such as system.ini and win.ini.

F0 Entries

An F0 entry corresponds to the "Shell=" statement under the [Boot] section of the system.ini file. This setting determines what shell program (e.g., Explorer.exe) Windows will use as the graphical user interface.

Example Entry:

Code F0 - system.ini: Shell=Explorer.exe

Files Used: "C:\Windows\System.ini"

Windows ME and below use this file, but Windows XP, 2000, and later versions use the registry equivalent instead.

Malware can modify this setting to run additional programs at startup, such as:

Code F0 - system.ini: Shell=Explorer.exe badprogram.exe This means both Explorer.exe and badprogram.exe will launch at startup.

F1 Entries

An F1 entry corresponds to the "Run=" or "Load=" statements in the win.ini file. These settings were mainly used in Windows 3.1, 95, 98, and ME to auto-run programs at startup.

Example Entries:

Code F1 - win.ini: load=bad.pif

F1 - win.ini: run=evil.pif

Files Used: "C:\Windows\Win.ini"

If you find F1 entries on a Windows XP or later system, this is a huge red flag, as these versions do not use the win.ini file to execute programs.

The "load=" statement was originally used to load hardware drivers, but on modern Windows versions, these entries are ignored.

F2 Entries

F2 entries correspond to the Windows NT-based registry equivalent of F0 and F1. These entries are found in Windows XP, 2000, and NT and use IniFileMapping instead of the traditional system.ini and win.ini.

HijackThis! will only show F2 entries if it detects a non-whitelisted or potentially malicious value in these registry keys:

Code HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Example Entries:

Code F2 - REG:system.ini: UserInit=userinit.exe,nddeagnt.exe

F2 - REG:system.ini: Shell=explorer.exe beta.exe

- UserInit determines what program runs immediately after a user logs in.

- The default value is:

- Code C:\Windows\System32\userinit.exe,

- If additional programs are listed, such as:

- Code C:\Windows\System32\userinit.exe, C:\Windows\badprogram.exe -> This could indicate malware.

- Shell determines which program loads the Windows GUI (normally Explorer.exe).

- If the value is Shell=Explorer.exe something.exe, malware may be hiding inside.

? Warning: If F2 entries appear in your HijackThis log, they likely indicate an infection. Always research unknown values!

F3 Entries

F3 entries function similarly to F2, but instead affect user-specific settings in the registry.

These entries are found under:

Code HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run

Example Entries:

Code F3 - REG:win.ini: load=chocolate.exe

F3 - REG:win.ini: run=beer.exe

These registry keys allow programs to run at startup for specific users. If unknown or suspicious programs appear here, research them before deleting.

How to Analyze and Fix These Entries

? For F0 Entries:

- If the Shell= statement only contains Explorer.exe, it is safe.

- If additional programs are listed (e.g., Shell=Explorer.exe malware.exe), investigate and remove them.

? For F1 Entries:

- Modern programs do not use win.ini, so if an entry appears on a Windows XP or newer system, it's a red flag.
- Google unknown entries to check if they are legitimate.

? For F2 Entries:

- If UserInit=userinit.exe (with or without nddeagnt.exe), it's safe.
- If there's another program listed alongside userinit.exe, investigate it, as it could be malware.
- If Shell=explorer.exe alone, it's safe; if another program is present, research before deleting.

? For F3 Entries:

- If an unknown program appears under load= or run=, it may be a threat.

Important Notes

? HijackThis does NOT delete the files associated with these entries

- When you fix an entry in HijackThis, it only removes the registry reference.
- You must manually delete the actual file from your system.

? Best Practices

- Always research unknown entries before removing them.
- Use safe mode to delete suspicious files.
- Combine HijackThis with other malware removal tools like:
 - [Malwarebytes](#)
 - [AdwCleaner](#)
 - [FRST \(Farbar Recovery Scan Tool\)](#)

Conclusion

Understanding F0, F1, F2, and F3 entries is essential for identifying potential malware in HijackThis logs. These entries indicate startup modifications, some of which are legitimate, but many can be malicious.

Always analyze carefully, research unknown values, and manually delete any associated malware files to ensure complete removal.

Tha Sneak - March 1, 2025, 8:33 pm

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak