Beware the Image File Execution Options key

devblogs.microsoft.com/oldnewthing/20051219-11

December 19, 2005

Raymond Chen

Beware the Image File Execution Options key (more). Its power can be used for evil as well as for good.

Its intended use is to force a program to run under a debugger regardless of how it is launched (and secondarily to alter how the system treats the program). It's handy if you need to debug a program "in the wild" rather than under the controlled environment of your favorite IDE. For example, you can use it if you want to debug how a program runs when it is launched by some other program you can't debug.

Two things people often forget:

- If you err in specifying the debugger, the program won't launch at all. For example, if you get the path to the debugger wrong or if you subsequently uninstall the debugger, you'll get ERROR_FILE_NOT_FOUND when you try to run the target program since the system can't find the debugger.
- Remember to delete the entry for your program when you no longer need it. Otherwise you'll wonder why the debugger keeps launching for no apparent reason.

Evil can be done with the Image File Execution Options key. Malware can install themselves as the "debugger" for a frequently-run program (such as Explorer) and thereby inject themselves into the execution sequence.

Note that the ability to use the Image File Execution Options key for evil purposes is not a security hole. To modify the key in the first place requires administrator permissions. Consequently, anybody who can exploit this feature already owns your machine.

Raymond Chen

Follow