Windows Defender Discussion

To prevent your CAMS system from running unnecessarily slow due to Windows Defender Real-Time scanning, you can disable "just the CAMS directories". Some may wonder if this makes the CAMS system vulnerable to security related attacks. This document attempts to share an email discussion about this.

Introduction

This issue was discovered while monitoring a new system using the Windows Resource Monitor. When observing a CAMS system operate, the **MsMpEng.exe** process kept showing up. This is the Windows Defender process. During normal operation, Windows Defender should not scan so often. As it turns out, every time a CAMS FF file or other CAMS files were touched, MsMpEng.exe was scanning those files. This slowed down the CAMS operations a lot. An example is that the three CAMS post-capture processing functions that take the most amount of time are: FTP_ValidateFFfiles.exe, FTP_MeteorCal_AutoUpdate.exe, and FTP_DetectMultipleFF.exe. However, what follows are the reasons that disabling realtime scanning for the CAMS directories is safe:

1. Real-time scanning is not the best way to protect your system. Ideally, files only need to be scanned once – when they are placed on your system. If the files are clean then, then record a hash for the file and compare that hash when a program is run. It's much more reliable than trying to keep the entire world caught up on virus database updates and broadcasting them.
2. I agree that it is risky if a virus gets into any of the FTP_*.exe or other programs, such as du.exe, process.exe, FindAndReplace.exe, etc., and you are right to always use caution and stay aware of security risks.
3. However, since these programs are placed on your system through a network interface, they are ALWAYS SCANNED. We are only recommending to disable the on-access scanning for files that are already on the system (or created by CAMS programs), but we leave all other scanning enabled.
4. Most virus scanners will scan the FF files and all the other files created by the CAMS programs and scripts. There is no reason to scan the files created during capture or post-capture processing, since those are created by already-scanned programs on your computer. These are essentially data files and they don't include executable code in them.
5. .BAT files are essentially text files. They can be infected by someone adding lines that create code and run it, but these files would also be scanned whenever these scripts are copied to your computer across the network.
6. You might be also worried about transmitting viruses when you upload to SETI. Well, since the FF*.bin files are created on your system, there is no reason to scan them for on-access, such as during autocal or detection. The zip files they are in will be scanned when they are transmitted.

Therefore, disabling on-access scanning for the CAMS directories, while leaving it enabled for other things, will improve performance (possibly by double) and still keep the system safe.

This topic should remain open for discussion.