What are these ghost drivers named dump_diskdump.sys and other dump_*.sys that didn't come from any file?

devblogs.microsoft.com/oldnewthing/20160913-00

September 13, 2016

Raymond Chen

Run Process Explorer with administrative privileges, select Options, Verify Signatures, pick the System process, then open the DLL view. In that view, you'll find some drivers with names like `dump_diskdump.sys`, `dump_dumpfve.sys`, and `dump_storahci.sys`. The Verified Signer column says "An error occurred while reading or writing to a file," these drivers have no description, no company name, and their reported path points to nonexistent files like `C:\Windows\System32\Drivers\dump_diskdump.sys`. What are these things? Does the computer have a virus?

These are virtual drivers that are used for creating crash dumps.[1]

Creating a crash dump is a bit of a catch-22: When the crash occurs, the system is in an unknown state, which means that you can't trust anything, not even the file system or block device drivers. After all, the crash may have been in one of those drivers!

When the system starts up, it preallocates space on the hard drive to record crash dump information, in case that becomes necessary. It also clones the drivers needed to write to the disk. If a crash occurs, the kernel doesn't trust the drivers that were running the show. Instead, it asks these clones to step in and write the crash data. The theory here is that these clone drivers have been kept in a state of suspended animation immediately after they've been initialized, in order to minimize the chance that they have gotten into a corrupted state that would prevent them from doing their job.[2]

These virtual drivers show up in Process Explorer with no description or other metadata because Process Explorer takes the reported path and extracts the metadata from that path. But these drivers weren't loaded from a file, so there is nothing to show.

Bonus chatter: Most of the driver names are self-explanatory. The one that may not be obvious is `dumpfve`: "fve" is short for Full Volume Encryption, more commonly known as BitLocker.

[1] Also hibernation files, but crash dumps are the interesting part of the story.

[2] Of course, if a driver is so buggy that it can't even initialize itself without corrupting itself, then you're screwed. Let's hope that by the time a driver passes WHQL, it can at least initialize itself without corrupting itself.

Raymond Chen

Follow