Crashes in the I/O stack tend to occur in programs which do the most I/O

devblogs.microsoft.com/oldnewthing/20150813-00

August 13, 2015

Raymond Chen

A customer was diagnosing repeated blue screen errors on their system. They shared a few crash dumps, and they all had a similar profile: The crash occurred in the file system filter stack as the I/O request passed through the anti-virus software.

Some of the crashes reported `PROCESS_NAME: ngen.exe`. "Could `ngen.exe` be the problem?"

As a general rule, user-mode code cannot be responsible for blue-screen failures. It's the job of the kernel to be resistant to misbehavior in user-mode. Failures of the form `IRQL_NOT_LESS_THAN_OR_EQUAL` and `PAGE_FAULT_IN_NON_PAGED_AREA` are typically driver bugs or faulty hardware (for example, due to overheating or overclocking).

The application that happened to be active at the time of the failure is not typically interesting in and of itself, although it can give a clue as to what part of the kernel is misbehaving. The fact that `ngen` appears is more an indication that `ngen` performs a lot of disk I/O, so if there's a problem in the I/O stack, there's a good chance that `ngen` was involved, simply because `ngen` is involved in a lot of I/O requests.

- Bob goes to the beach very frequently.
- Every time there is a shark attack, Bob is at the beach.
- Conclusion: Bob causes shark attacks.

Blaming `ngen` for the kernel crash is like blaming Bob for the shark attacks.

Bonus chatter: Some of my colleagues came to different conclusions:

- Conclusion: Bob should stop going to the beach.
- Conclusion: Bob must be the shark.

Raymond Chen

Follow