Why does GetCommandLine give me a corrupted command line?

devblogs.microsoft.com/oldnewthing/20100113-00

January 13, 2010

Raymond Chen

A customer had the following problem:

> We're calling `GetCommandLine` to retrieve the command line, and the documentation says that it returns a single null-terminated string. However, when we call it in our application, we find that it is actually a *double*-null-terminated string. The buffer returned consists of a series of null-terminated strings, one string per word on the command line, all stored one after the other, and with two null terminators at the end. How do I get the original string?

Recall that the command line is just a conveniently-initialized variable in a process and once it's set up, the kernel doesn't really care about it any more. What is most likely happening is that somebody is taking the raw command line returned by `GetCommandLine` and writing to it. The customer can confirm this by dumping the command line just as the process starts, even before any DLLs get to run their `DllMain` s, and then setting a write breakpoint on the command line to see who is writing to it.

And in fact, the customer did find the culprit.

> It turns out it was some other part of the code (not written by me!) which was parsing the command line and writing into it in the process.

Raymond Chen

Follow