A few stray notes on Windows patching and hot patching

devblogs.microsoft.com/oldnewthing/20130102-00

January 2, 2013

Raymond Chen

Miscellaneous notes, largely unorganized.

- A lot of people questioned the specific choice of `MOV EDI, EDI` as the two-byte NOP, with many people suggesting alternatives. The decision to use `MOV EDI, EDI` as the two-byte NOP instruction came after consulting with CPU manufacturers for their recommendations for the best two-byte NOP. So if you think something better should have been used, go take it up with the CPU manufacturers. They're the ones who came up with the recommendation. (Though I suspect they know more about the best way to optimize code for their CPUs than you do.)
- You can enable hotpatching on your own binaries by passing the `/hotpatch` flag to the compiler.
- The primary audience for hotpatching is server administrators who want to install a security update without having to reboot the computer.
- There were some people who interpreted the presence of hotpatch points as a security hole, since it makes it easier for malware to redirect OS code. Well, yes, but it didn't enable anything that they didn't already know how to do. If malware can patch your process, then it has already made it to the other side of the airtight hatchway. And besides, malware authors aren't going to bother carefully patching code to avoid obscure race conditions. They're just going to patch the first five bytes of the function without regard for safety, because that'll work 99% of the time. (It's not like the other 1% are going to call the virus authors when the patch fails.)

Raymond Chen

Follow