Then again, it might not be overclocking after all

devblogs.microsoft.com/oldnewthing/20060421-12

April 21, 2006

Raymond Chen

While it’s true that there’s an awful lot of overclocking out there, it’s also true that not everything that looks like overclocking actually is. Last Thanksgiving, I helped one of my relatives upgrade their computer by scavenging parts from another unused computer (installing more memory and replacing a broken CD drive). When I took the front panel off the machine, I was greeted with a wall of dust. A little wrangling with a vacuum cleaner was called for before I got around to yanking the broken CD drive and installing the replacement. When we go through the failure reports that people submit, we find a lot of single-bit errors, where the correct value and the actual value differ in only one bit position. If these problems are systematic, then that would be the sign of some sort of software problem, but the ones we saw were one-time events, isolated single-bit errors. We had no proof, but we suspected flakey memory, possibly the result of an overheated machine. People often stick their computers in out-of-the-way locations, against walls, on a carpeted floor, in a closet. While that’s very convenient for home decor, the computer itself suffers because the flow of air through the computer has been impaired. The accumulation of dust impedes the cooling effect further. So make sure the vents on your computer are clean and unobstructed, or you too may find yourself on the short end of a memory glitch caused by overheating. Jeremy Kelly from the Exchange Server team was part of the team that investigated a crash that looked just like overclocking, except it wasn’t. The program crashed on a `mov eax, 0x20` instruction, an instruction that merely loads a constant into a register. It doesn’t access memory; it’s not a privileged instruction; there’s no reason why the instruction could fail. Yet it did. This looked like overclocking, but the problem was consistently reproducible (atypical of overclocking), and besides, companies that pay tens of thousands of dollars for an Exchange server system aren’t going to skimp on a few hundred by overclocking it. The Exchange server team were fortunate enough to be able to capture a live debug session, which permitted them to investigate the problem both on the user-mode side and on the kernel-mode side, and that revealed the true cause: The Exchange server had been infected with a rootkit.

The rootkit was lying to the user-mode debugger about what code was executing. It told the debugger that the instruction was the harmless one, when in fact the rootkit was doing something else. Looking at the problem from the kernel-mode side allowed our investigators to identify the true cause of the problem: A crashing bug in the rootkit itself.

Raymond Chen

Follow