My Thoughts on CrowdStrike

From PM Board Chair Morris Pearl

This is my perspective on the CrowdStrike debacle — from my perspective as a trained computer engineer.

Background:

All modern computer operating systems (Windows, Unix, Linux, Mac OS X, etc.) have two modes. They use different names, but I will just call them "kernel" and "application." The purpose of kernel mode is that there are a few things that normal applications (apps) are not allowed to do. For example sending information on the network involves actually changing the voltage of electricity in various wires. Normal apps are not allowed to do that. Another thing is memory management. Imagine a storage facility where each person stores a bunch of boxes. Erica can go to the desk, and say please give me box number 2. And the worker gives her her second box. And then Dylan asks for his box number 2. And the worker gives him his second box. The worker has a notebook, with a page for each person, and a list of where their boxes are. Erica's box number 2 is on a certain shelf somewhere, and Dylan's box number 2 is on a different shelf somewhere. That notebook is "special". No one is allowed to mess with it except for the specially trained workers.

Analogously the computer operating system has some tables of which portions of the memory chips are assigned to which app. The reason for all of this is that part of the job of the operating system is to prevent one app from either accidentally or maliciously interfering with another app. Just like Dylan is not allowed to have any of Erica's boxes, and Erica is not allowed to put stuff into any of Dylan's boxes, if you are running a Microsoft Excel spreadsheet, and you are watching video on your Chrome web browser — those two applications are not allowed to interfere with each other. Part of the job of the operating system is making sure that they do not interfere with each other. The operating system is analogous to the storage facility worker with their special notebook.

There are some exceptions. If a company manufactures some special hardware (say, some new kind of super-deluxe mouse kind of thing) the company can supply some special software that gets loaded and is allowed to run in "kernel" mode — because the software to operate the mouse needs to deal with the voltages in the wires, etc. Microsoft has a program wherein they carefully inspect software like this (they call them "device drivers") and approve them. There have always been device drivers. Recently the European Union has started doing some regulating to make sure that Microsoft is not using their approval process in an anti-competitive way.

Finally, we can get to CrowdStrike.

CrowdStrike is supposed to detect and monitor apps for malicious behavior on your computer. Imagine for a moment that you are worried about a vicious poodle hiding in a box in the storage facility, and this poodle then getting out of its box and running around and damaging other boxes. CrowdStrike would sell you a special box that has a microphone and a computer programmed to detect the sounds of the poodle barking, and set off an alarm, and therefore the same for viruses, malware, etc.

As mentioned above, in a computer the operating system normally prevents one app from knowing what another app is doing. CrowdStrike made a device driver (even though it does not sell hardware) and it got Microsoft to approve this device driver. When they find out about new malicious software, CrowdStrike wants to send new versions very quickly; they don't want to wait for Microsoft to approve new versions of their fix. So their response was to program their device driver (which is allowed to run in kernel mode) to check for new software released by CrowdStrike, and load the new software into kernel mode too.

Some big organizations have a policy that when ANY new software is delivered, it is only run on a few computers for the first week or so to prevent any system-wide errors. CrowdStrike believes that it is important to deploy its virus detecting software quickly when a new threat starts spreading (that is the service they advertise) so it bypasses that check too. There is also a provision in Windows that when a device driver fails, it will try to reboot the computer without that device driver. CrowdStrike, though, marked its software as essential, so as to bypass yet another check.

All of this was working well until that fateful Friday, July 19. CrowdStrike had detected a new computer virus spreading to some of its clients. It worked very quickly to develop and test a new addition to its software to detect malicious use of something called "named pipes." It then sent this new piece immediately to its clients. Unfortunately, when this was deployed, they seem to have accidentally sent a bug-ridden file to its clients. This file was loaded into kernel mode by the Cloudstrike software, and immediately caused the operating system to crash.

With Cloudstrike's ability to bypass various things to (ironically) try to prevent problems like this from propagating, those computers could not reboot themselves. It took many hours for technicians to manually go to each and every Windows computer (8.5 million devices were impacted), reboot it in a special mode so they could be repaired, and remove the offending file.

This took quite a while (the computers were located all over the place, in data centers, in airport kiosks, in automated signs, etc. etc.). Major US airlines canceled thousands of flights, disrupting the travel of hundreds of thousands of people. The cascading effect of the airline employees not traveling to the site of their next flights caused continued disruptions for several days after that. At Delta, my understanding is that they had particular difficulties with both computers used to do crew scheduling, and computers used to keep track of who is meeting children traveling by themselves — they ended up banning all children traveling without accompanying adults for about a week.

CrowdStrike then sent out gift cards for ten dollars off on Uber Eats. Several people are using the letter with those gift cards as an example of really bad corporate communications (the idea that sending the Delta employees ten dollar gift cards is somehow a suitable apology for a problem that probably cost their employer hundreds of millions of dollars is really dumb). The gift cards were flagged by Uber as fraud due to their high usage rates, adding a fitting coda to a frustrating and damaging day in our world's IT infrastructure.