It rather involved being on the other side of this airtight hatchway: Booting into another operating system

devblogs.microsoft.com/oldnewthing/20200318-00

March 18, 2020

Raymond Chen

A security vulnerability report came in that went roughly like this:

- Create a malicious program and copy it to a USB thumb drive.
- Boot from recovery media.
- Ask for a recovery console.
- Go to the C: drive and replace file X with the malicious version from the USB thumb drive.
- Reboot the computer.
- Result: System is compromised.

Well, yeah. It's compromised because you compromised it.

Booting off custom media is equivalent to removing the hard drive and inserting it into a different computer. You are treating the hard drive as a secondary storage device relative to some other operating system. At that point, the other operating system has full control over the hard drive and can read and write any sectors it wishes.

Consider the following variation:

- Create a malicious program and copy it to a USB thumb drive.
- Boot from a linux bootable DVD.
- Mount the Windows boot volume.
- Replace file X with the malicious version from the USB thumb drive.
- Reboot the computer.
- Result: System is compromised.

This is basically the same thing as the previous attack, just using different recovery media.

And this variation demonstrates that you are already starting on the other side of the airtight hatchway: It assumes physical access to the system to run a different operating system entirely. This runs afoul of the third immutable law of security: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

You can't expect Windows to protect you when it isn't even running. Physical access is a level of access even beyond Administrator. At least Administrators still play within the operating system's rules. But with physical access, you can leave the game entirely, and the rules no longer apply.

It's like saying that you found a way to beat Roger Federer at tennis: Bribe the scorekeeper so that no matter what happens on the court, the point is credited to you. Sure, you beat Roger Federer, but you did so by going outside the game itself, so you didn't so much beat him at tennis as you did beat him at "the ritual playing of a tennis match."

If you are concerned about attacks from users with physical access, you can add another layer of protection by employing full disk encryption like BitLocker. That way, even if somebody gets physical access and boots to a different operating system (or removes the drive and puts it into another computer), all they will be able to read is encrypted data. They may be able to corrupt the hard drive, but they won't be able to replace one file with a malicious version, since they won't know how to encrypt the malicious version.

Bonus chatter: BitLocker uses the TCG Reset Attack Mitigation (Memory Overwrite Request) to protect against keys being extracted from RAM when rebooting into a new operating system. The Memory Overwrite Request (MOR) instructs the firmware to wipe memory upon any unexpected hardware reset.

Raymond Chen

Follow