# It rather involved being on the other side of this airtight hatchway: Surreptitious file access by administrator

devblogs.microsoft.com/oldnewthing/20140703-00

July 3, 2014

Raymond Chen

A security report was received that went something like this:

> A user can bypass file sharing locks by opening a read-only handle to the physical volume containing the file in question. This allows the user to extract the contents of protected files by reading the corresponding sectors directly from the disk. Since this operation requires administrator access, any user with administrator access can extract data from files that are normally inaccessible due to file locks, such as the SAM database.

Yes, that’s right. An attacker who gains administrator privileges can extract data from any file on the computer. But so what? The attacker is already on the other side of the airtight hatchway. They already pwn your machine. That a pwned machine can be pwned is not really all that surprising. That some files are not accessible due to file locks is not a security measure. It is a consequence of, um, file access. Besides, once you gain administrator access, a much easier way to steal the SAM is to merely grab a backup copy. What, you can’t find a backup copy? No problem. After all, you’re the administrator. One of your job responsibilities is to maintain regular system backups. So create a backup of the SAM file. Of course the system will let you do this. It is your job after all. For example, you can use the Volume Shadow Service to create a volume snapshot, then mount the snapshot and extract the SAM file. Bingo, instant copy of the SAM database.

Just doing your job.

Raymond Chen

**Follow**