Issued 5/1/18

A Malicious USB Stick Could Crash your Windows PC, Even if it's Locked

Plugging a USB drive containing a malformed NTFS image into a Windows machine can cause it to bluescreen in mere seconds, according to Marius Tivadar of BitDefender. Tivadar recently published his NTFS image on GitHub after dissatisfaction with Microsoft's response. He initially reported the bug in July 2017, and "they did not want to assign CVE for it nor even to write me when they fixed it," Tivadar said. The important point to this threat is that there's a serious security risk in Windows systems: Autoplay will mount any volume inserted into the system, even if the machine is locked. Tivadar gives a thorough breakdown of the technical aspects of his proof-of-concept (link) exploit in a PDF accompanying the POC's GitHub project. Using a 10MB NTFS image with some modified root directory names, Tivadar was were locked or not—Autoplay mounted the image and crashed the screen in seconds. Autoplay, which is enabled by default in all versions of Windows, is the root of the problem here. Disabling Autoplay can prevent the NTFS image from automatically crashing Windows systems, but manually opening it has the same result. Manually crashing the system is still troubling, and Microsoft should act to prevent the NTFS exploits Tivadar used from crashing Windows, but it isn't the key issue—Autoplay is. "It is not necessary to have an usb stick," Tivadar said. "A malware for example could drop a tiny NTFS image and mount it somehow, thus triggering the crash." If that malware was properly coded it could do

more than just crash Windows: It could unleash other exploits as the system reboots or do things that can only be speculated on, and it could do them all because Microsoft failed to see the bigger, more serious, picture behind Tivadar's particular discovery.