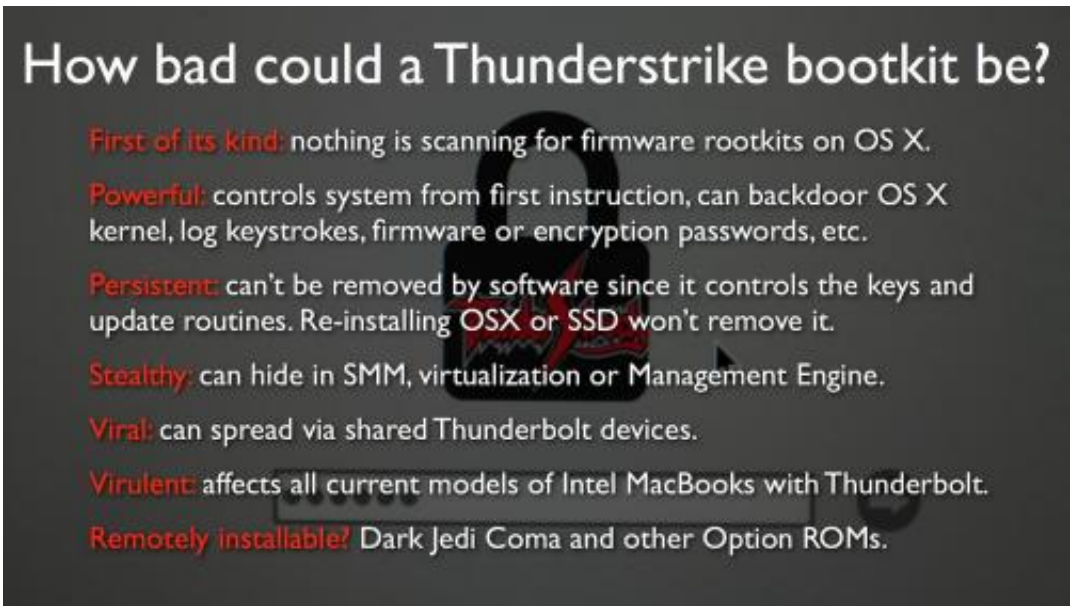
Reverse engineer creates Thunderstrike bootkit able to exploit vulnerability in OS X boot ROM

January 9 2015, by Bob Yirka



Credit: Trammell Hudson

Trammell Hudson, an employee of Two Sigma Investments has found a way to hack into computers running OS X, using a pre programmed hardware device. He calls the software that runs from the device a bootkit because it allows for gaining unprecedented access to Mac computers prior to the point where the operating system is loaded—he has named it Thunderstrike after Mac's Thunderbolt interface.

In many respects, it is surprising that the vulnerability was not found before. Hudson found that the option ROMs on Mac computers are leftover remnants of machines from the 80's—they are blocks of memory set aside for holding information (data or code) used by peripheral devices. He found that they were initialized prior to booting the operating system, which meant that if code were placed in those memory blocks, they could be disguised and thus not seen by operating system security features. Option ROMs hook into the operating system to allow for communications between a peripheral and the OS. Thus, if code is placed into such blocks, it can run quietly in the background, executing commands at will, leaving the computer open to all manner of hacking options. Worse, because it loads first, malware running in an option ROM can replace the RSA encryption key that Mac computers use to make sure only authorized firmware is installed, giving the malware complete control.

Fortunately, there is some good news—the hack can only be carried out if the person making the attempt is able to gain physical access to the computer—for a few minutes. All it takes is for the peripheral device to be plugged into a port, and then for the machine to be cold booted. Because of that little necessity, it would appear that most people would not be at risk from this particular vulnerability for two main reasons. The first is that it is not likely that others have made the hardware device to carry out the hack. The second is that for most people, there is a lack of incentive on the part of hackers. Such a hack would mostly likely be targeted at high profile computer users such as government employees, spies, etc.

In retrospect, it appears it is possible that the vulnerability has been discovered before, but went unreported—information leaked by Edward Snowden revealed that government agents had been engaging in planting "hidden" code in computers sent by manufactures and intercepted prior to their arrival at a "suspect" site, allowing for monitoring everything the

user was doing on or with the computer.

Credit: Trammell Hudson

More information: Trammell Hudson: trmm.net/Thunderstrike

via Arstechnica

Citation: Reverse engineer creates Thunderstrike bootkit able to exploit vulnerability in OS X boot ROM (2015, January 9) retrieved 19 April 2024 from https://techxplore.com/news/2015-01-reverse-thunderstrike-bootkit-exploit-vulnerability.html