SR Labs research to expose BadUSB next week in Vegas

July 31 2014, by Nancy Owano

USB logo

A Berlin-based security research and consulting company will reveal how USB devices can do damage that can conduct two-way malice, from computer to USB or from USB to computer, and can survive traditional "cleaning" protective measures.

SR Labs chief scientist Karsten Nohl and security researcher Jakob Lell are to deliver their presentation, "Bad USB – On Accessories that Turn Evil," at Black Hat in Las Vegas next week. The risks, noted Andy Greenberg in a report on their work in Wired, has to do with the very core of how they are made. This, said Reuters, is a form of malware that can operate from controller chips inside the USB devices. The two researchers from SR Labs said their talk is to demonstrate a full system compromise from USB and a self-replicating USB virus not detectable with current defenses. The name of their firmware-residing malware is BadUSB, and it is capable of taking control over a PC.

Nohl and Lell spent months, said Wired, reverse-engineering the firmware running communication functions of the USB devices, and finding out that the firmware can be reprogrammed to hide attack code. Devices not "sticks" is a word used intentionally here, since other devices such as keyboards and mice could also serve as attack conduits. A modified thumb drive, for example, can, when it detects that the computer is starting up, boot a small virus, which infects the computer's operating system. Nohl and Lell said the malware can even impersonate a USB keyboard to suddenly start typing commands. The malware can spoof a network card and change the network's DNS settings to redirect traffic. Any time a USB stick is plugged into a computer, its firmware could be reprogrammed by malware on that PC, and likewise, any USB device could silently infect a user's computer.

Fixing this risk is not easy; there are no known patches; it is not as if one can "clean up" the problem by deleting files. Anti-virus programs are designed to scan for software written onto memory. As the report in Reuters pointed out, "bugs in software used to run tiny electronics components that are invisible to the average computer user can be extremely dangerous when hackers figure out how to exploit them."

One short-term solution to avoid such an attack might be, said Wired, to not connect your USB device to computers you do not own or do not have good reason to trust and, on the reverse, not to plug untrusted USB devices into your own computer.

More information: srlabs.de/