what Turning USB peripherals into where adUSB

USB devices are connected to – and in many cases even built into – virtually all computers. The interface standard conquered the world over the past two decades thanks to its versatility: Almost any computer peripheral, from storage and input gadgets to healthcare devices, can connect over the ubiquitous technology. And many more device classes connect over USB to charge their batteries.

This versatility is also USB's Achilles heel: Since different device classes can plug into the same connectors, one type of device can turn into a more capable or malicious type without the user noticing.

Reprogramming USB peripherals. To turn one device type into another, USB controller chips in peripherals need to be reprogrammed. Very widely spread USB controller chips, including those in thumb drives, have no protection from such reprogramming.

BadUSB – Turning devices evil. Once reprogrammed, benign devices can turn malicious in many ways, including:

1. A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.
2. The device can also spoof a network card and change the computer's DNS setting to redirect traffic.
3. A modified thumb drive or external hard disk can – when it detects that the computer is starting up – boot a small virus, which infects the computer's operating system prior to boot.

Defenses?

No effective defenses from USB attacks are known. Malware scanners cannot access the firmware running on USB devices. USB firewalls that block certain device classes do not (yet) exist. And behavioral detection is difficult,

since a BadUSB device's behavior when it changes its persona looks as though a user has simply plugged in a new device.

To make matters worse, cleanup after an incident is hard: Simply reinstalling the operating system – the standard response to otherwise ineradicable malware – does not address BadUSB infections at their root. The USB thumb drive, from which the operating system is reinstalled, may already be infected, as may the hardwired webcam or other USB components inside the computer. A BadUSB device may even have replaced the computer's BIOS – again by emulating a keyboard and unlocking a hidden file on the USB thumb drive.

Once infected, computers and their USB peripherals can never be trusted again.

More details are available in the slides of our talk at PacSec 2014. (An earlier version of the talk was presented at BlackHat 2014.) YouTube has a video of the BlackHat talk.

Proof-of-Concept. We are not yet releasing the modified USB controller firmwares. Instead we are providing a proof-of-concept for Android devices that you can use to test your defenses: BadAndroid-v0.1

Questions? – usb [you know what to put here] srlabs.de

> Imprint , Subscribe: RSS Atom