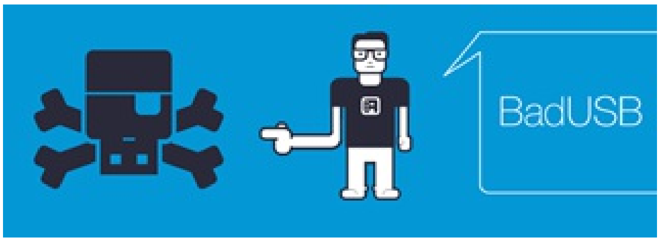
BadUSB: The unusual suspect

September 23, 2014

BadUSB: The unusual suspect



When security research like the most recent findings regarding BadUSB announced by SR Labs appears, security experts and vendors usually take two sides. There are the ones who immediately try to find a solution and others that undermine the threats.

As a device control and data loss prevention (DLP) vendor, we are aware of USB device threats to data security and until now, the most dangerous scenarios included unauthorized data transfers and possible malware infections. With device control and DLP solutions, this is perfectly controllable. However, when it comes to the firmware that controls the basic functions of USB devices, this is another story, as the media has also noted.

According to SR Labs, USB devices can be reprogrammed to act like a keyboard or any other devices to manipulate your computer. This is possible through the firmware of the micro-controller, which is hidden from the user. The firmware can be reverse-engineered and since the anti-virus solution or the operating system cannot verify the firmware, BadUSB is a latent threat and can seriously damage entire networks by completely taking over command.

The main idea here is that SR Labs scenario is perfectly believable taking into account that USB micro-controllers and the firmware that controls them are not built with security in mind. They are being mass-produced in order to reach the market as fast as possible and they are meant to do one job - facilitate the communication between the device and the computer. Maybe a strong point in the future for micro-controller manufacturers would be to include security features to their offerings.

Another point that is important to touch on is that until now there are no actual known attacks “in the wild” and, if we think about the number of firmware versions of USB devices, reprogramming is pretty difficult to achieve. It is not impossible, though. Thinking a little bit further to include also household electronics like Smart TVs that operate on firmware, or Wi-Fi access points, this subject becomes more and more “interesting.” The spectrum of use for these firmware-manipulated devices can be even broader. People with malicious intent might have access to firmware in advance for mass shipments and manipulate in their interest USB and other devices in order to intercept data transfers or to control targeted organizations.

Taking a step back to the SR Labs research, it is clear that this is a USB vulnerability, which is not solved with the recently, very popular USB 3.0. Hopefully, upcoming versions or the USB standard will address it. Until then, we have already formed a team to investigate possible solutions to include in our device control product, so our next releases should bring good news to the community. One should take into consideration that we will likely see more firmware-based threats in the near future.