Forum:Hack Forums

Thread: USB driver assembly code modification (WILL PAY IF YOU KNOW)

SkunT3llo - *January 30, 2019, 5:05 pm*

Hello everyone, I don't know if this is the right place for asking this but
is there anyone who know how to modify assembly code of usb driver and add function to run and decode base64?

So it looks like this in action?
youtube. com/watch?v=EZBDRhWpYvM

Please PM me if You know. ? ?

fireswap - *January 30, 2019, 8:45 pm*

Hi OP

This isn't a driver, but the USB's EEPROM (basically a tiny non-volatile storage device) being flashed to identify itself as a HID and emulate some input (kb/mouse). This wouldn't be driver modification, as the driver is what runs on the host itself.

You can very easily replicate this functionality yourself by purchasing a Rubber Ducky, as flashing the EEPROM with a modified firmware is probably a little more difficult than a device purpose-built for such a task.

If you wanted to go the longer route, you would probably need to get yourself Ida Pro, some ARM or MIPS assembly knowledge, and a SOIC8 clipper cable and EEPROM flasher. Ida Pro you can find a free version of, but the SOIC8 clipper cable you will probably need to order from Taiwan and wait to arrive by boat (lol).