简易上手 HID 攻击

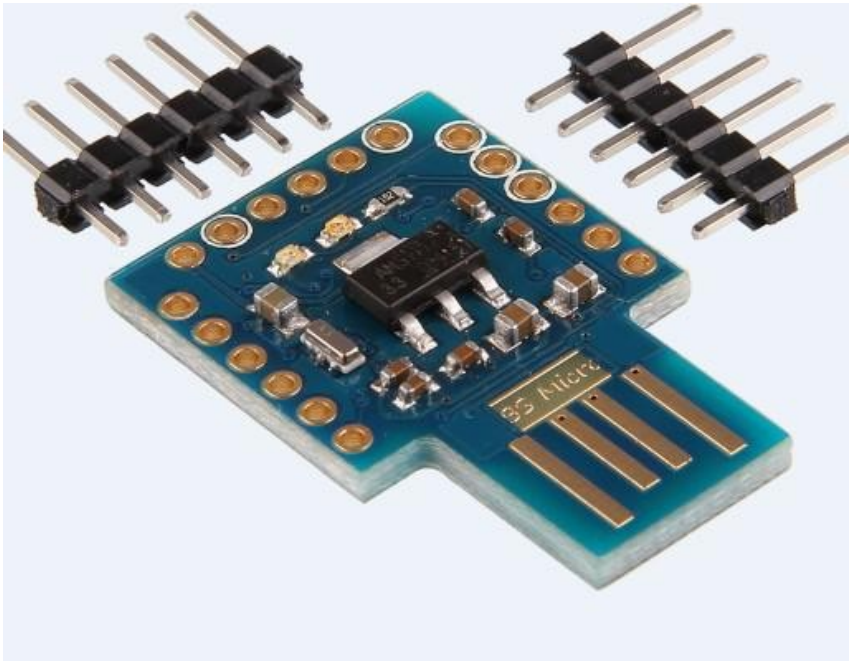
---by 豆@ATToT

HID 攻击是 badusb 的一种 ,通过 usb 接入硬件直接在目标操作系统上模拟键盘执行恶意代码的攻击方式。由于 usb 接口使用广泛，使这类攻击存在一定的利用价值。

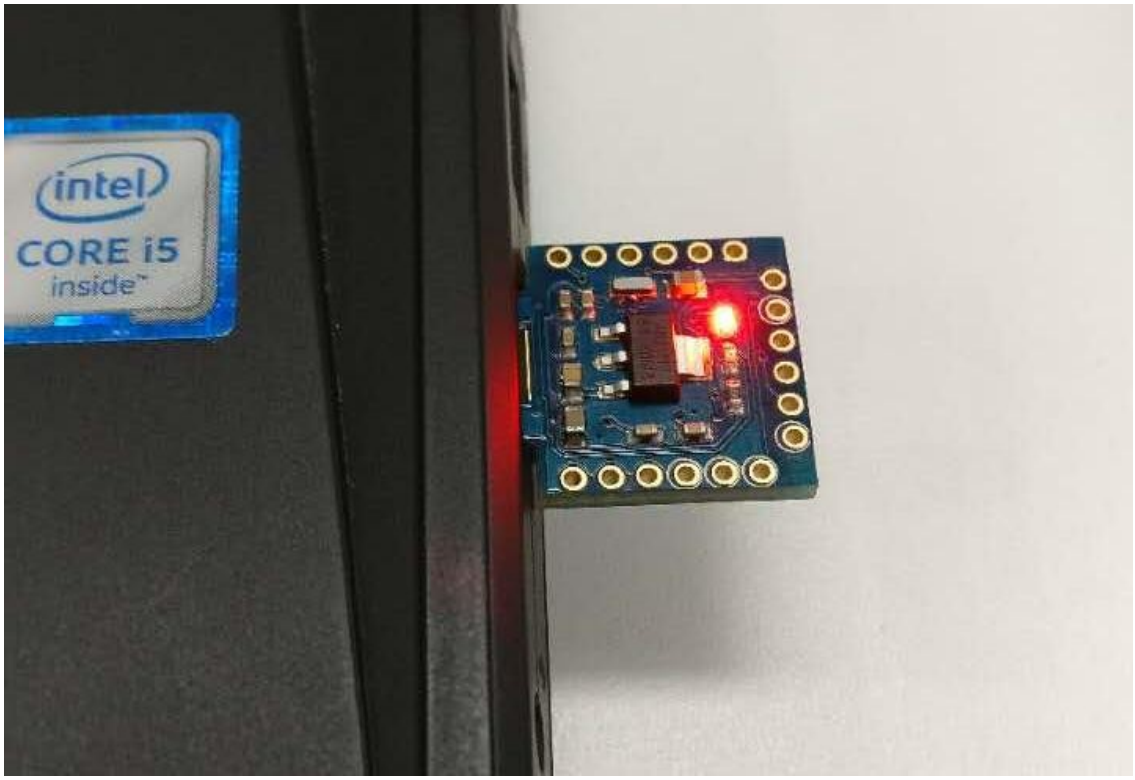
最早公开于 2014 年美国拉斯维加斯黑帽大会上,那会儿是曝光了群联主控芯片的一个漏洞，允许修改固件。但根据情报显示,早在 2008 年 NSA 就有此类攻击方案并且有成熟的硬件设备。

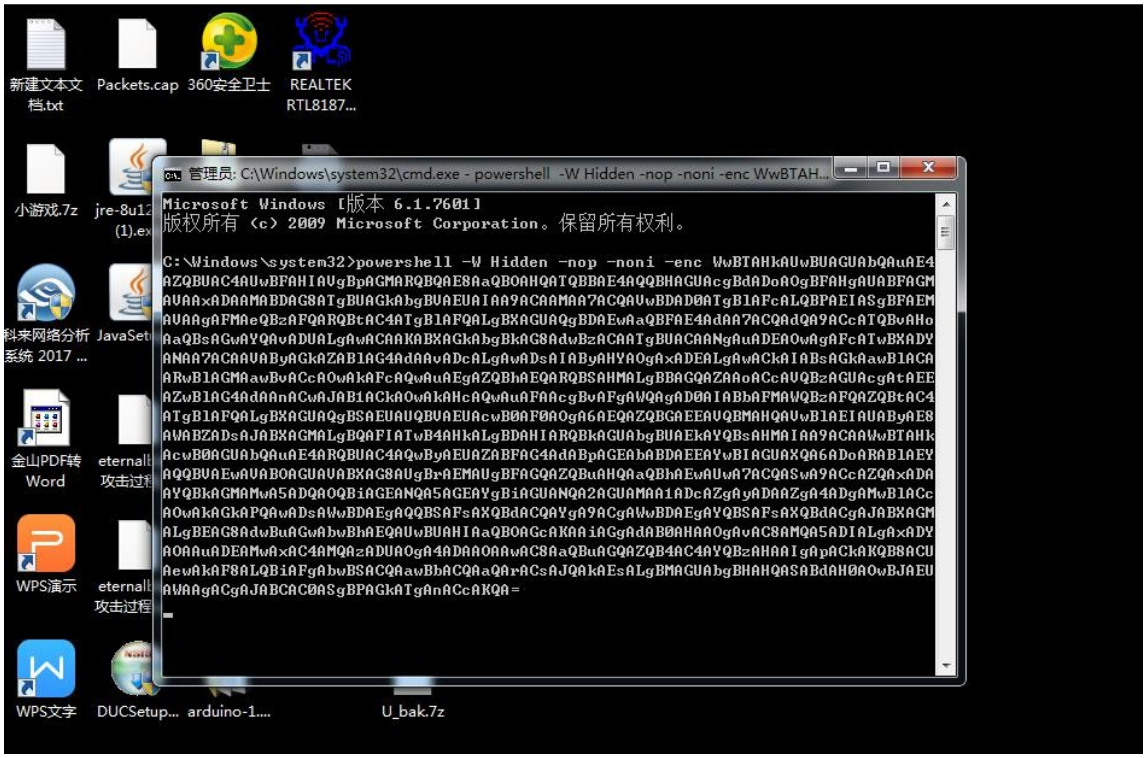
今天主要介绍大家都玩儿的起的

首先推荐 CJMCU-Beetle arduino Leonardo USB ATMEGA32U4 开发板（为什么推荐这个？便宜实惠啊，功能简单容易上手，不过仅限 HID 攻击）



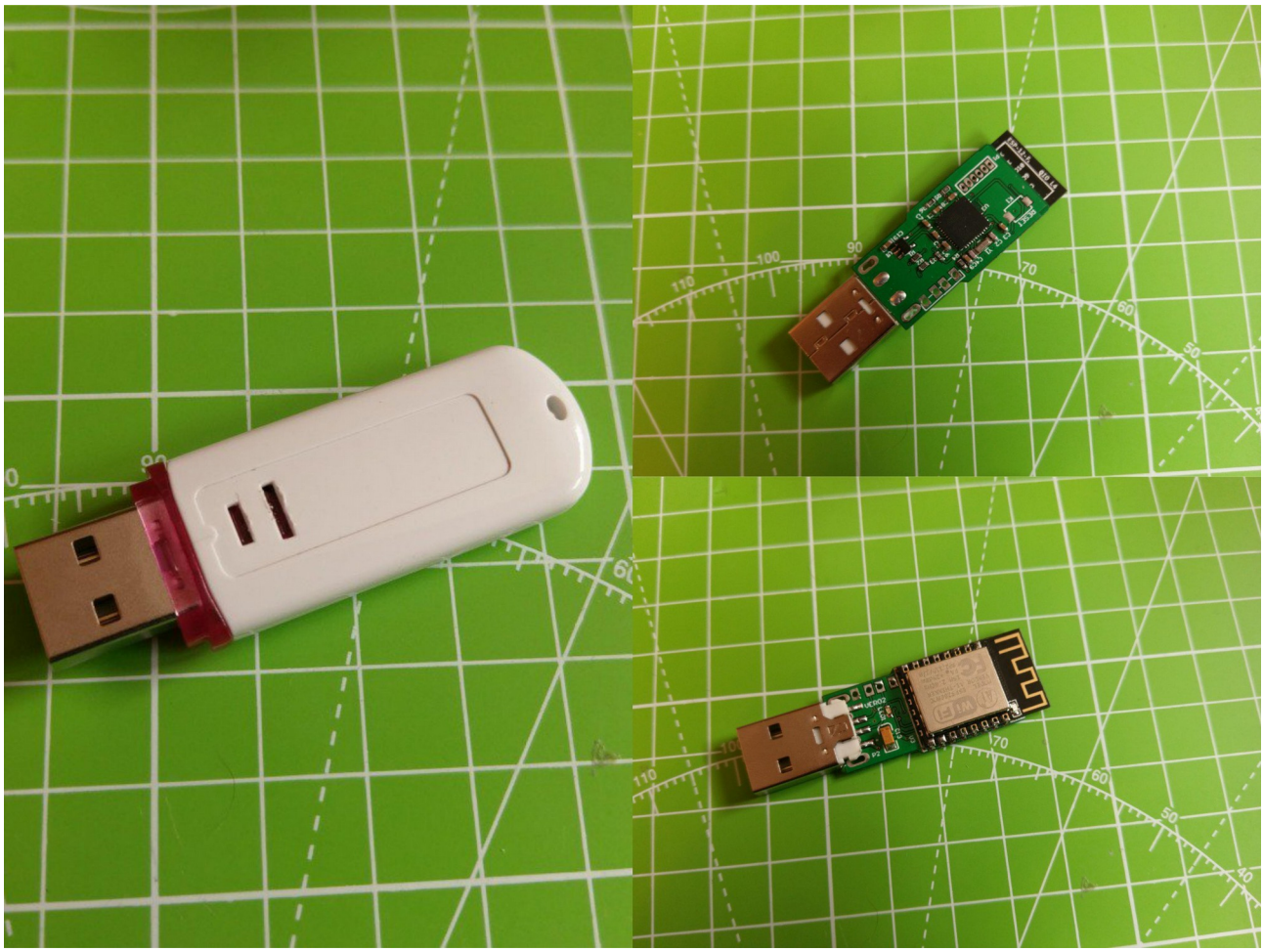
一旦接入目标机器就会自动执行恶意代码





How to
http://www.freebuf.com/sectool/107242.html
(板子规格不一样，但是操作是一样的)

下面这个硬件逼格高点，带有无线功能,



插入目标机器后可建立加密且隐藏 SSID 的 wifi 通信,攻击者只要在信号范围内就可以随时在目标机器上通过该设备提供的 web 页面执行命令,可从远程 C&C 下载木马也可直接偷取机密文件,通过无线传输

How to
https://github.com/whid-injector/WHID
（设备从哪儿买？在 howto 里找啦）

再贴近实战一点的姿势，你想，现在好多人都知道了 badusb 是不是？大家都有警戒心了，想要提高成功几率可以改造一个鼠标，把它武器化

毕竟鼠标这么人畜无害的东西，是吧?

How to
http://securityaffairs.co/wordpress/60019/hacking/weaponize-mouse-whid-injector-fun-w00t.html