writeup - bamboofox2021

Ransomware

Getting Started

- Firstly, I opened an archive file(download them at here) containing some source files of this challenge. There are a compiled byte-code (.pyc extension) of python script(**task.pyc**) and an encrypted data file(**flag.enc**).
- Using uncompyle6(installing here) to decompile **task.pyc**, I get the original python-script as below:

```
$ uncompyle6 task.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.5 (default, Jul 28 2020, 12:59:40)
# [GCC 9.3.0]
# Embedded file name: task.py
# Compiled at: 2021-01-14 21:13:24
# Size of source mod 2**32: 420 bytes
(lambda data, key, iv: if len(data) != 0:
(lambda key, iv, data, AES: open('flag.enc', 'wb').write(AES.new(key, AES.
# okay decompiling task.pyc
```

Solve

- After achieving original python-script, I'm confused with it because the script is mess and looks like unreadable code. So, I needed to ***petrus's*** support*(a crypto-player of my team)* and he send me to python-script, which can be based-on decompiled code in order to decrypt **flag.enc**:

solve.py

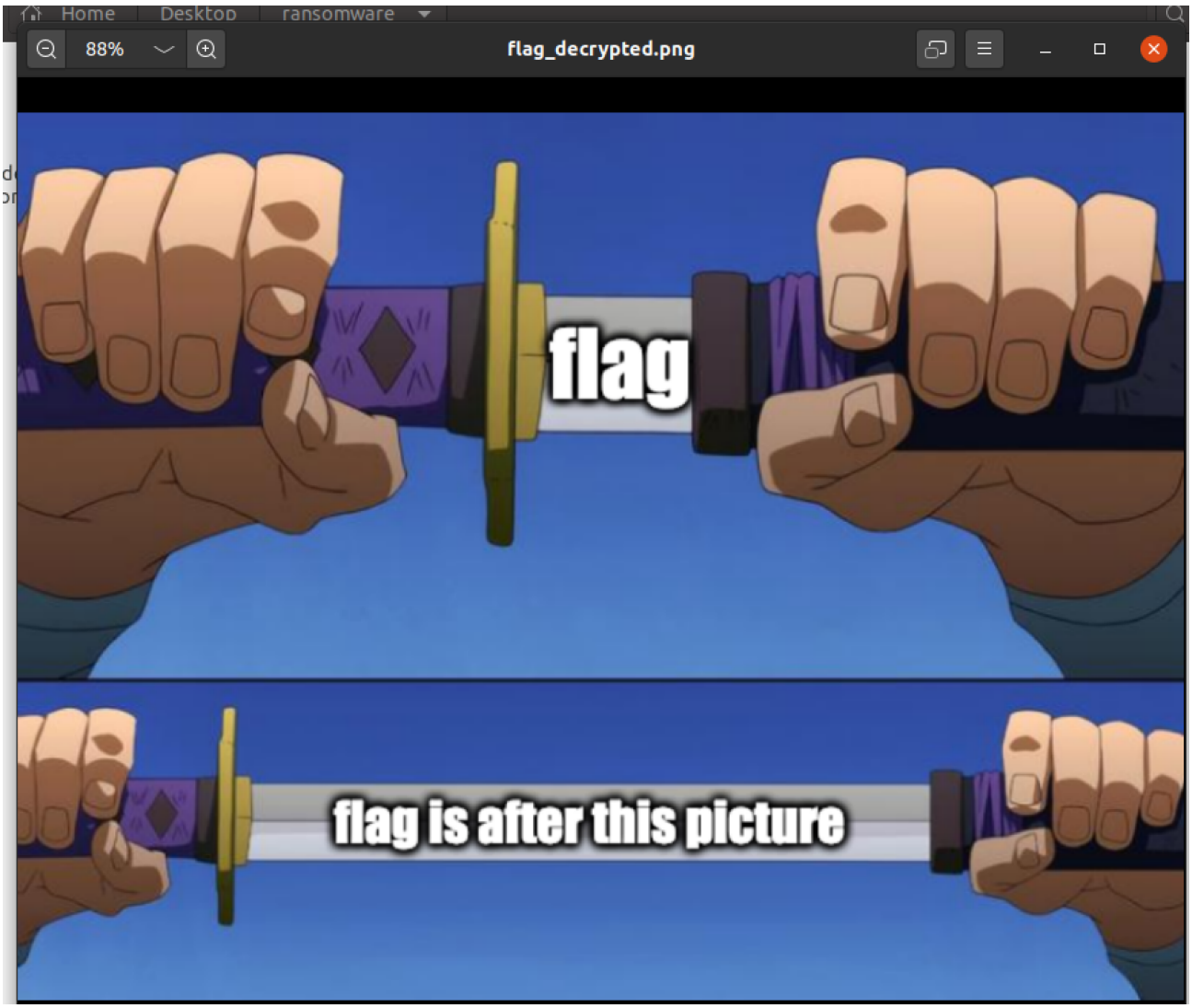
```
import requests
from Crypto.Cipher import AES

data = requests.get('https://ctf.bamboofox.tw/rules').text.encode()
```

```
key = data[99:99+16]
iv = data[153:153+16]

with open('flag.enc','rb') as f1:
  ciphertext = f1.read()

plaintext = AES.new(key, AES.MODE_CBC, iv).decrypt(ciphertext)
with open('flag_decrypted', 'wb') as f2:
  f2.write(plaintext)
```

- Running the above script, and I see that the new file "flag_decrypted" is generated. Examining it using **file** command:

```
$ file flag_decrypted
flag_decrypted: PNG image data, 980 x 746, 8-bit/color RGBA, non-interlace
```

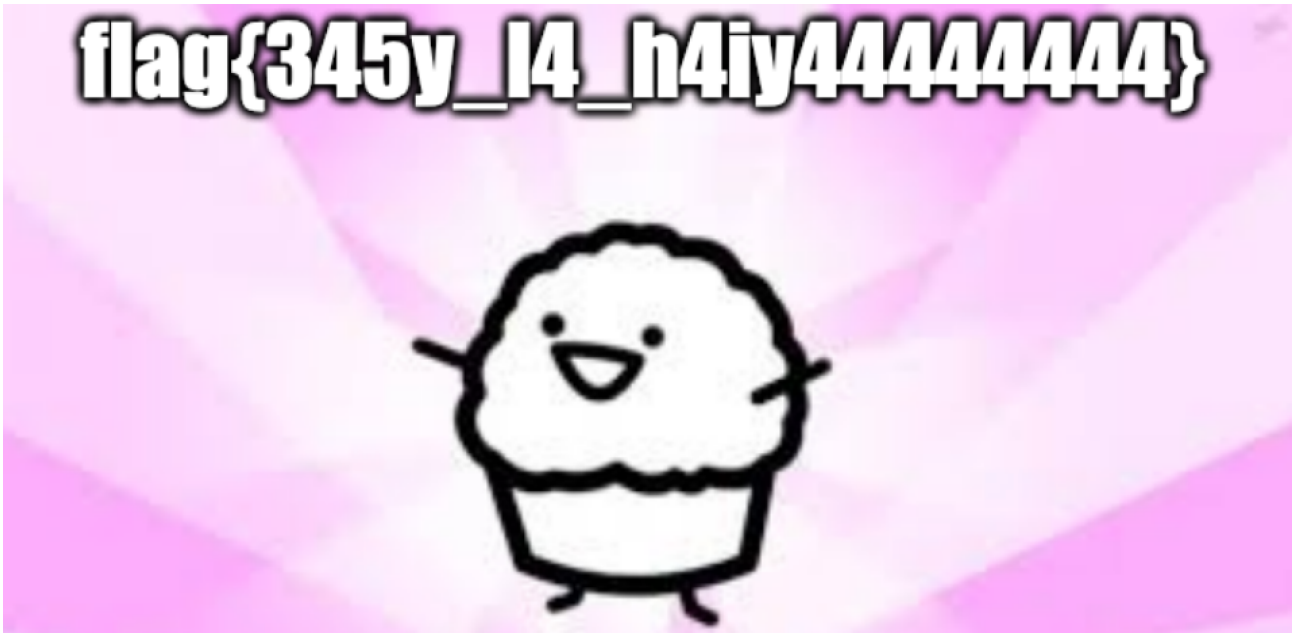
- Adding an extension(.png) to new file and opening it:



- In this stage, I also confused when I don't have an idea to get the flag :(. I needed to the ***Stirring's*** support to get the final image, which contains the flag's content:

```
$ binwalk flag_decrypted.png --dd='.*'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 980 x 746, 8-bit/color RGBA, non-
41            0x29            Zlib compressed data, default compression
808562        0xC5672         PNG image, 980 x 492, 8-bit/color RGBA, non-
808603        0xC569B         Zlib compressed data, default compression
```

- Maybe I guess that the second image having offset as 0xC5672 is flag-image. Opening and wow, it's real flag:


flag{345y_l4_h4iy444444444}