



Название:	Лазанья
Категория:	Реверс-инжиниринг
Уровень:	Лёгкая
Очки:	200
Описание:	В реверсе, иногда, как в готовке. Шифрование может быть словно слои лазаньи 😊
Теги:	Python, PyInstaller, побитовое шифрование
Автор:	ROP

Прохождение:

Изучаем файл через Detect It Easy.

Detect It Easy v3.09 [Windows 10 Version 2009] (x86_64)

Имя файла: C:\Users\rop\Documents\Temp\lasagna.exe

Тип файла: PE64 | Размер файла: 6.70 Миб

Сканировать: Автоматически | Порядок байт: LE | Режим: 64-битный | Архитектура: AMD64 | Тип: Консоль

Продвинутый

PE64

- Операционная система: Windows(Server 2003)[AMD64, 64-битный, Консоль]
- Линковщик: Microsoft Linker(14.36.33135)
- Компилятор: Microsoft Visual C/C++(19.36.33135)[C]
- Язык: C/C++
- Инструмент: Visual Studio(2022 version 17.6)
- Упаковщик: PyInstaller ←

Оверлей: Binary

- Данные: ZLIB data[ZLIB compression best]
- Архивная запись[unpacked]: Binary

Сигнатуры | Рекурсивный скан | Глубокий анализ | Эвристический скан | Подробно | Сканировать

Папка | Журнал | Все типы | 349 мс | Выход

Видно, что используется Pyinstaller.

Распакуем EXE через <https://github.com/extremecoders-re/pyinstxtractor>.

```
PS C:\Users\rop\Documents\Temp> .\pyinstxtractor.py .\lasagna.exe  
PS C:\Users\rop\Documents\Temp> |
```

Декомпилируем PYC-файл через uncompyle6 :

```

r += sc
else:
    r += c
else:
    return r

def e(i):
    s = 13
    c_e = c(i, s)
    b_e = base64.b64encode(c_e.encode()).decode()
    x_k = 65
    x_e = strxor_c(b_e.encode(), x_k)
    a_k = b'KEYrf87ijoasd8j1'
    a_i = b'IV89jf9198fj8912'
    cipher = AES.new(a_k, AES.MODE_CBC, a_i)
    a_e = cipher.encrypt(pad(x_e, AES.block_size))
    return a_e

print(l)
u_i = input("Enter the encryption flag: ")
e_t = e(u_i)
if e_t == t:
    print("This is your flag! :)")
else:
    print("That's not it...")

# okay decompiling .\lasagna.py

```

Программа делает следующее с вводом:

1. Шифр Цезаря
2. Base64
3. XOR с ключом 0x41
4. AES с ключом "KEYrf87ijoasd8j1" и IV "IV89jf9198fj8912"

Затем происходит проверка зашифрованного ввода с:

```
t = b'B\\xcc,\\xdc\\xafA\\x193\\x9f\\xb5Z\\x80\\xa8\\xa0\\xaar\\xacT%\\xc9\\xa4\\x9aeg\\xe4\\xeb\\x87\\x87\\xc
d\\xd0]\\xf8\\xb6\\xdb\\xe0h\\x0e\\xc6!\\xc4\\x8aq\\x82\\xa7'
```

Исходя из этого можно расшифровать значение переменной `t`.

[https://cyberchef.org/#recipe=AES_Decrypt\({option:'UTF8','string':'KEYrf87ijoasd8j1'},{'option':'UTF8','string':'IV89jf9198fj8912'},'CBC','Hex','Raw',{'option':'Hex','string':''},{'option':'Hex','string':''}\)XOR\({'option':'Hex','string':'41'},'Standard',false\)From Base64\('A-Za-z0-
%2B/%3D',true,false\)ROT13\(true,true,false,13\)&input=MHg0MiwgMHHhDOCwgMHgzRSwgMHhDQywgMHgyQywqMHhE
C](https://cyberchef.org/#recipe=AES_Decrypt({option:'UTF8','string':'KEYrf87ijoasd8j1'},{'option':'UTF8','string':'IV89jf9198fj8912'},'CBC','Hex','Raw',{'option':'Hex','string':''},{'option':'Hex','string':''})XOR({'option':'Hex','string':'41'},'Standard',false)From Base64('A-Za-z0-
%2B/%3D',true,false)ROT13(true,true,false,13)&input=MHg0MiwgMHHhDOCwgMHgzRSwgMHhDQywgMHgyQywqMHhE
C)