crackme

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Reverse
Challenge | 2019 | 安洵杯 | Reverse | crackme

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6912

题目考点

解题思路

1.main函数之前

程序HOOK了MessageBoxW函数，让其执行一个自己写的函数

2.main函数

输入一串字符串，并且执行了MessageBoxW函数，由于函数被IAT HOOK，执行了自己写的一个函数，在函数之中，改变了BASE64的字母表（大 小写互换）并且添加了异常VEH向量。
执行完函数之后，程序注册了一个SEH，并且触发异常。

3.异常

VEH
异常触发首先执行VEH向量，VEH向量进行了SM4的密钥初始化，并且注册了UnhandledExceptionFilter

SEH
进行了SM4加密

UnhandledExceptionFilter
改变了比较的结果，并且进行变种base64加密

异常回调
执行main函数的比较函数

解密脚本

```
from pysm4 import encrypt,decrypt
import base64

mk = 0x77686572655F6172655F755F6E6F773F
base_now="yzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/abcdefghijklmnopqrstuvwxi!"
base_init="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/i="

clear="1UTAOIkpyOSWGv/mOYFY4R!!"
clear_re=""
for i in range(len(clear)):
    if(i%2==0):
        clear_re+=clear[i+1]
    else:
        clear_re+=clear[i-1]
c=""
for i in range(len(clear_re)):
    b=base_now.find(clear_re[i])
    c+=base_init[b]
c=base64.b64decode(c)
c=int(c.encode("hex"),16)
clear_num=decrypt(c,mk)
clear_num=hex(clear_num)[2:-1].decode("hex")
print clear_num
```

Flag

 # Challenge # Reverse # 2019 # 安洵杯
membershop
Easy Encryption