Evr_Q

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Bin
Challenge | 2017 | HCTF | Bin | Evr_Q

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

- *TLS*
- *反调试*

解题思路

写在前面

这题一开始是准备TLS+SMC+反调试的，发现放在第一题有些不太合适，就把SMC的调用部分删掉了。

其实留下了彩蛋，smc的实现我没有删XD

设计思路

用TLS检测工具进程和调试器，进入主函数后先检测用户名，通过后检测StartCode(即flag)，最后输入'Y'确认CM。

部分细节

Win10的TLS在vs17上有点小Bug，只能在Debug模式下跑起来，于是没有选择Release版本，如果给大家带来困扰这里十分抱歉。 用户名注册存在多解，原因是我把进位值舍去了（输入'I'也能通过username验证哦） StartCode部分先验证长度为35 Step1: 全体 xor 0x76 Step2: [7:14]每个字节先异或0xAD, 再将0b10101010位与0b01010101位互换 Step3: [14:21]每个字节先异或0xBE, 再将0b11001100位与0b00110011位互换 Step4: [21:28]每个字节先异或0xAD, 再将0b11110000位于0b00001111位互换 Step2~4加密前先调用ntdll!NtQueryInformationProcess, 各检查1种标志(7, 30，31) 比较简单的做法直接用ida看了，cuz没有造成任何静态反编译的难度

EXP

```
import random
import os
import hashlib

enc_flag = [30, 21, 2, 16, 13, 72, 72, 111, 221, 221, 72, 100, 99, 215, 46, 44, 254, 106, 109, 42, 242, 111, 154, 77, 139, 75, 30, 30, 14, 14, 14, 14, 14, 14, 11]
dec_flag = [0] * len(enc_flag)

#////////////////////////////////////////////////
def dec0_f(dec_t, enc_t, num):
    for i in range(num):
        dec_t[i] = chr(enc_t[i] ^ 0x76)
    return dec_t
#////////////////////////////////////////////////
def dec1_f(dec_t, enc_t, num):
    for i in range(num):
        v1 = (enc_t[i] & 0x55) << 1
        v2 = (enc_t[i] >> 1) & 0x55
        enc_t[i] = v1 | v2
        dec_t[i] = enc_t[i] ^ 0xAD
    return dec_t
#////////////////////////////////////////////////
def dec2_f(dec_t, enc_t, num):
    for i in range(num):
        v1 = (enc_t[i] & 0x33) << 2
        v2 = (enc_t[i] >> 2) & 0x33
        enc_t[i] = v1 | v2
        dec_t[i] = enc_t[i] ^ 0xBE
    return dec_t
#////////////////////////////////////////////////
def dec3_f(dec_t, enc_t, num):
    for i in range(num):
        v1 = (enc_t[i] & 0xF) << 4
        v2 = (enc_t[i] >> 4) & 0xF
        enc_t[i] = v1 | v2
        dec_t[i] = enc_t[i] ^ 0xEF
    return dec_t
#////////////////////////////////////////////////
def dec_f(dec_flag, enc_flag):
    for i in range(len(enc_flag)):
        dec_flag[i] = enc_flag[i]
    dec_flag[21:28] = dec3_f(dec_flag[21:28], enc_flag[21:28], 7)
    dec_flag[14:21] = dec2_f(dec_flag[14:21], enc_flag[14:21], 7)
    dec_flag[7:14] = dec1_f(dec_flag[7:14], enc_flag[7:14], 7)
    dec_flag = dec0_f(dec_flag, dec_flag, 35)
#////////////////////////////////////////////////

dec_f(dec_flag, enc_flag)

print ''.join(dec_flag)
```

Flag

```
hctf{>>D55_CH0CK3R_B0o0M!-xxxxxxxx}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Bin/rHmvVC6fT6Z8X6VVhMwkb2.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2017 # HCTF # Bin
A true man can play a palo one hundred time
ez_crackme