第16天：红帽杯2019-easyRE

原创

S1lenc3 于 2019-11-15 18:47:06 发布 1295 收藏 1
分类专栏： CTF

复现easyRE

看了几篇writeup我始终没弄懂是怎么找到真正的加密算法的。

搜索字符串，看到you found me。交叉引用来到主函数。

```
v50 = 0;
if ( sub_424BA0(v48) == 36 )
{
  for ( i = 0; i < (unsigned __int64)sub_424BA0(v48); ++i )
  {
    if ( (unsigned __int8)(v48[i] ^ i) != *(&v12 + i) )
    {
      result = 4294967294LL;
      goto LABEL_13;
    }
  }
  sub_410CC0("continue!");
  memset(&v51, 0, 0x40uLL);
  v53 = 0;
  sub_4406E0(0LL, &v51, 64LL);
  v52 = 0;
  if ( sub_424BA0(&v51) == 39 )
  {
    v1 = sub_400E44(&v51);
    v2 = sub_400E44(v1);
    v3 = sub_400E44(v2);
    v4 = sub_400E44(v3);
    v5 = sub_400E44(v4);
    v6 = sub_400E44(v5);
    v7 = sub_400E44(v6);
    v8 = sub_400E44(v7);
    v9 = sub_400E44(v8);
    v10 = sub_400E44(v9);
    if ( !(unsigned int)sub_400360(v10, off_6CC090) )
    {
```


这串代码首先对给出的明文加密，加密后的结果是Info:The first four chars are `flag`。

然后是十次同一个函数加密，最后和明文比较，查看明文很像base64加密的，所以base64解密十次得到了https://bbs.pediy.com/thread-254172.htm

然后，，，，发现被耍了，我就想这几百个函数，我怎么知道哪个是正确的，直接放弃。

赛后看writeup知道是主函数的上下两个函数才是关键。

```
if ( ((unsigned __int8)v3 ^ byte_6CC0A0[0]) == 'f' && (HIBYTE(v6) ^ (unsigned __int8)byte_6CC0A3) == 'g' )
{
  for ( j = 0; j <= 24; ++j )
  {
    v0 = (unsigned __int8)(byte_6CC0A0[j] ^ *((_BYTE *)&v6 + j % 4));
    sub_410E90(v0);
  }
}
v2 = __readfsqword(0x28u);
result = v2 ^ v7;
if ( v2 != v7 )
  sub_444020(v0);
return result;
```


判断密钥第一个和第四个是不是f和g，那就猜测这四个字符是flag。

然后循环24次做异或操作。

```
s = [0x40,0x35,0x20,0x56,0x5D,0x18,0x22,0x45,0x17,0x2F,0x24,0x6E,0x62,
     0x3C,0x27,0x54,0x48,0x6C,0x24,0x6E,0x72,0x3C,0x32,0x45,0x5B]
s1 = 'flag'
key = ''
flag = ''
for k in range(4):
    key += chr(s[k] ^ ord(s1[k]))
for i in range(len(s)):
    flag += chr(s[i] ^ ord(key[i%4]))
print(flag)
```