171107 逆向-SWPU（Re300-解密）

原创

奈沙夜影 于 2017-11-07 23:41:52 发布 270 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/whklhhhh/article/details/78473965

1625-5 王子昂 总结《2017年11月7日》【连续第403天总结】

A. 08067CTF-re300

B.

上文说到看到一个非常复杂的算法

扒了一半想起来就算正向实现了这么复杂也没可能做出逆向的啊……

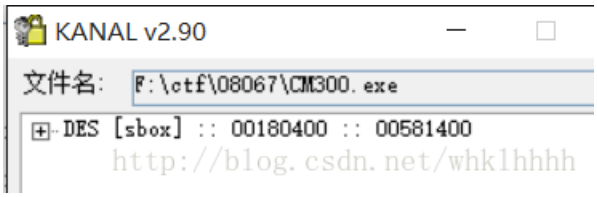
果断放弃

参考官方WriteUp得知是DES加密，通过工具分析或者代码特征发现都可以

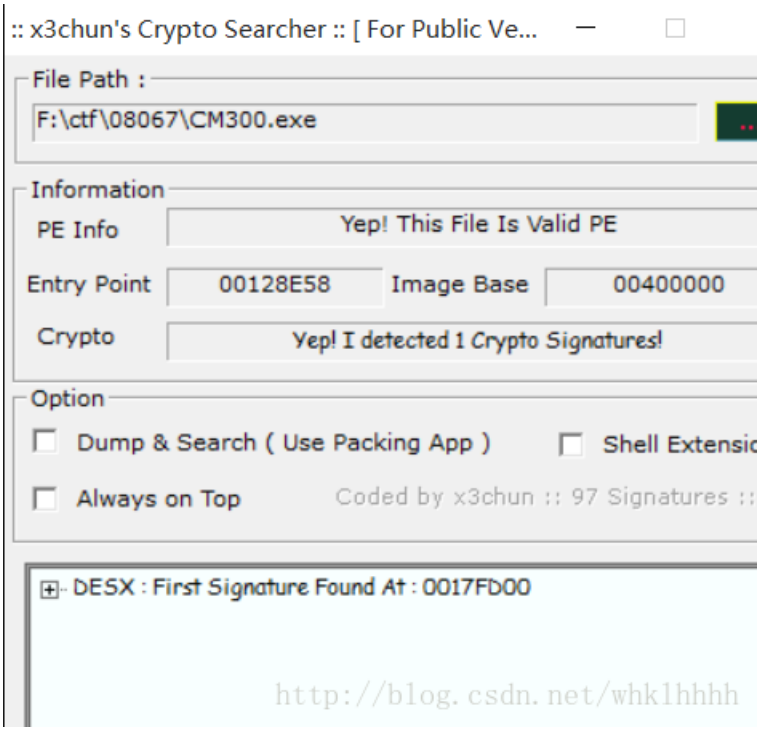
后者需要熟悉DES加密的算法，我对现代密码学都很苦手……

找了几个工具试下，最后只有两个能查到：

PEiD中附带的，最新版的kanal（v2.9）：



CryptoSearcher：



确认是DES算法的话就好办了，DES的解密算法就是加密算法将轮密钥逆序
轮密钥是16个64位的值，合在一起长度为0x80，就是memcpy来的v9，值存在0x5A1308中

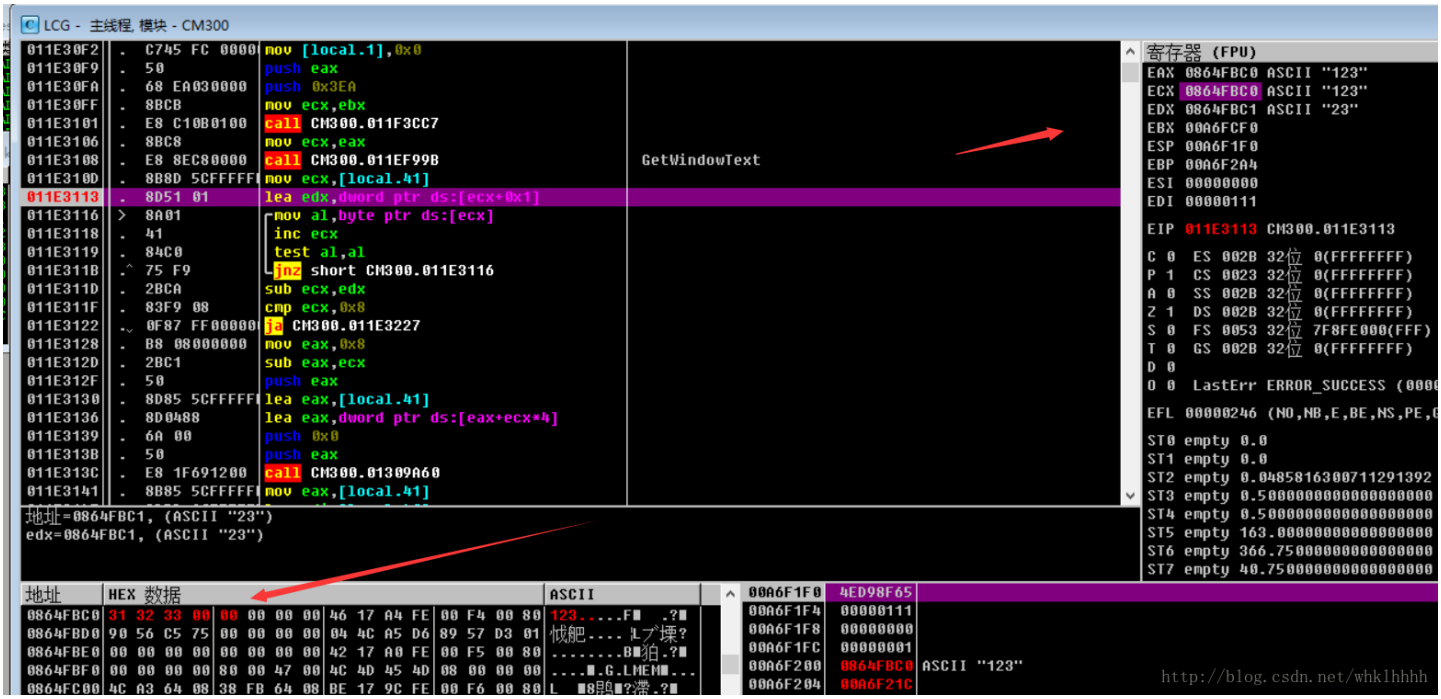
```
if ( v2 <= 8 )
{
  memset(&input + v2, 0, 8 - v2);               // 用0补齐8个字节
  i58 = *(_DWORD *)(input + 4);                 // 后4个字符
  i04 = *(_DWORD *)input;                       // 前4个字符
  i58_ = i58;
  v10 = BYTE3(i04) | ((BYTE2(i04) | ((BYTE1(i04) | ((unsigned __int8)i04 << 8)) << 8)) << 8);
  v11 = BYTE3(i58) | ((BYTE2(i58) | ((BYTE1(i58_) | ((unsigned __int8)i58 << 8)) << 8)) << 8);// 字符串转整数
  qmemcpy(&v9, &unk_5A1308, 0x80u);             // 密钥复制
  sub_401B20((int)&v10, (int)&v9);              // 加密变换
  LOBYTE(i04) = BYTE3(v10);
  BYTE1(i04) = BYTE2(v10);
  BYTE2(i04) = BYTE1(v10);
  BYTE3(i04) = v10;
  LOBYTE(i58_) = BYTE3(v11);
  BYTE1(i58_) = BYTE2(v11);
  BYTE2(i58_) = BYTE1(v11);
  BYTE3(i58_) = v11;
  v10 = i04;
  v11 = i58_;                                   // 整数转回字符串
  v4 = 0;
  while ( *((_BYTE *)&v10 + v4) == byte_581500[v4] )// 校验结果
  {
    if ( ++v4 >= 8 )
```



```
A8 13 9C DB 0E A5 9C 6C
```

密文为0x581500处存的，即

重新运行，在OD中将明文改为上述内容（要在字符串转整数之前，不然需要手动转换）

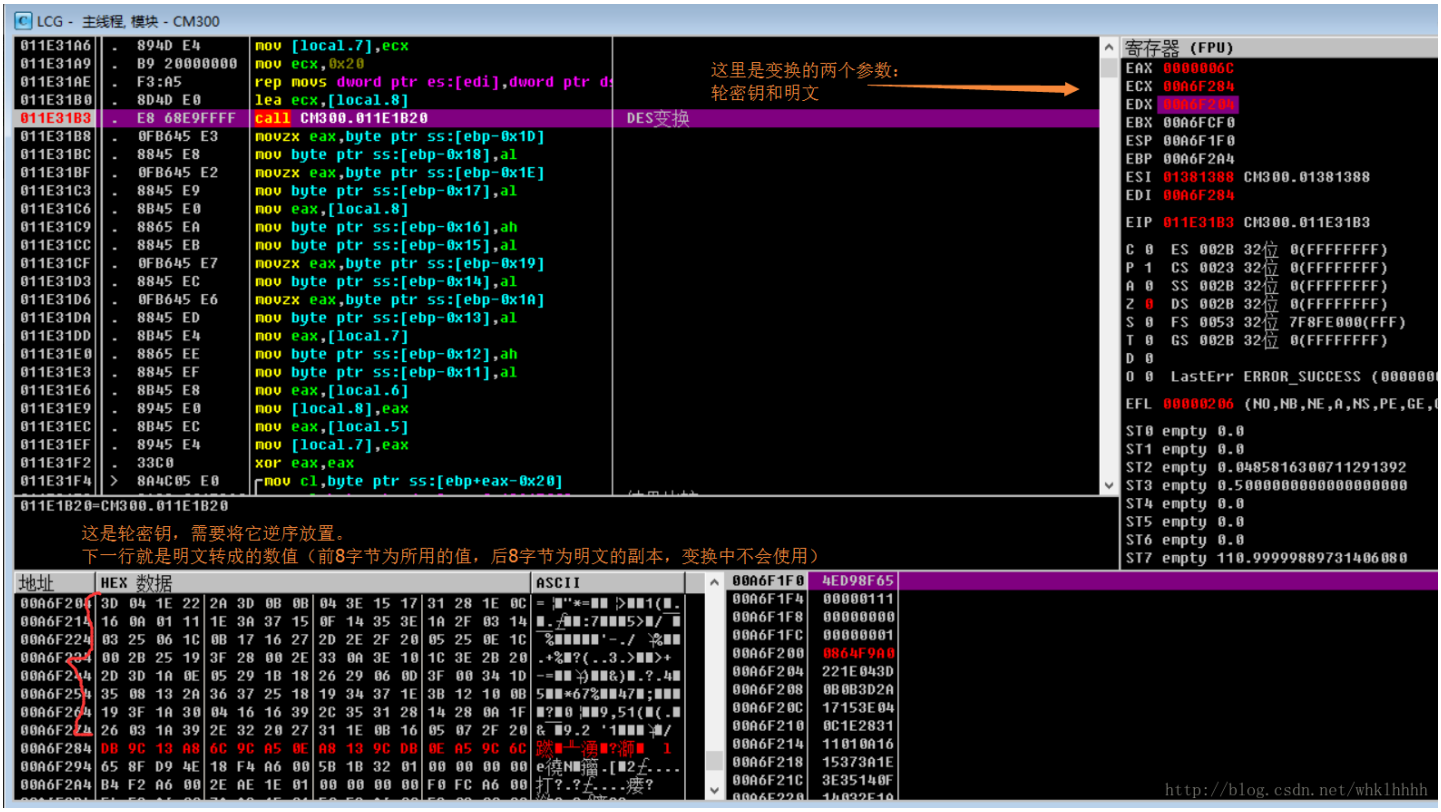


这里断到GetWindowTextA的缓冲区，直接修改它的值就可以了
（注意明文长度为8，后一个比特要改为00，作为字符串结束标志，否则复制时将认为字符串超长而直接终止）

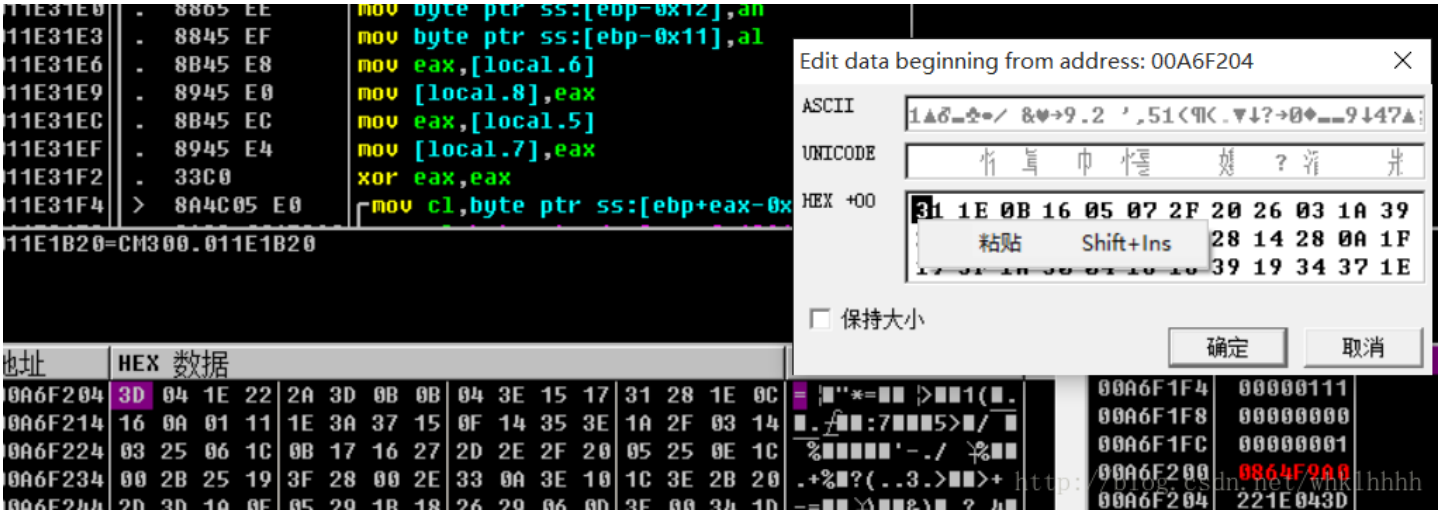
然后修改轮密钥，k1~k16改为k16~k1

```
31 1E 0B 16 05 07 2F 20 26 03 1A 39 2E 32 20 27
2C 35 31 28 14 28 0A 1F 19 3F 1A 30 04 16 16 39
19 34 37 1E 3B 12 10 0B 35 08 13 2A 36 37 25 18
26 29 06 0D 3F 00 34 1D 2D 3D 1A 0E 05 29 1B 18
33 0A 3E 10 1C 3E 2B 20 00 2B 25 19 3F 28 00 2E
2D 2E 2F 20 05 25 0E 1C 03 25 06 1C 0B 17 16 27
0F 14 35 3E 1A 2F 03 14 16 0A 01 11 1E 3A 37 15
04 3E 15 17 31 28 1E 0C 3D 04 1E 22 2A 3D 0B 0B
```

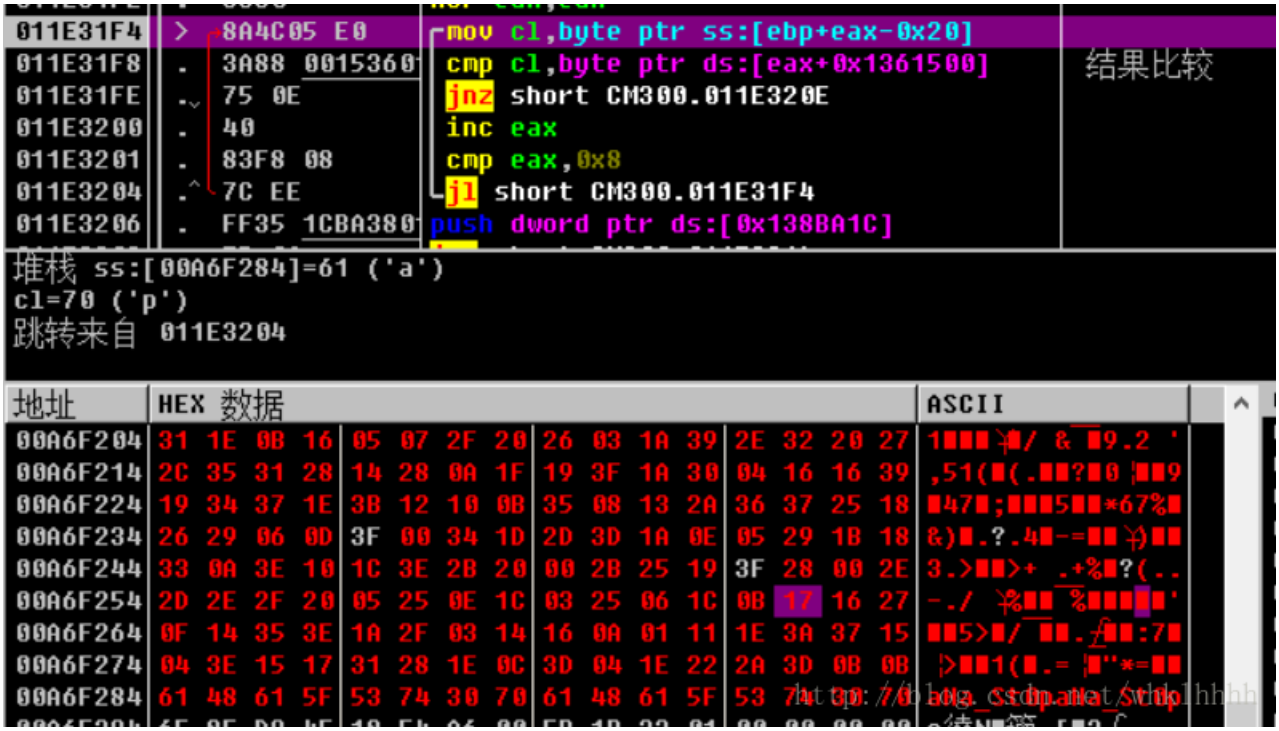
将它覆盖轮密钥，密文覆盖原明文：



覆盖的双击弹窗修改窗口，取消保持大小的勾以后直接粘贴就行了



运行DES函数以后，数据窗口就出现了flag, 不过这时候还是数值顺序的，要再往下走到比较结果的地方：



轮密钥后面就出现了flag：`aHa_St0p`

C. 明日计划

Re200和400