

西普学院 writeup 逆向工程 该题不简单

原创

taotiaolong99234 于 2015-08-14 16:05:39 发布 1353 收藏

分类专栏: [ctf](#) 文章标签: [writeup](#) [ctf](#) [西普学院](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/taotiaolong99234/article/details/47663179>

版权



[ctf 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

跳跳龙

逆向的话主要就是IDA和OD的混合使用。两者各有优势, 不过这道题用IDA就够了, 而且OD的话貌似还调试不了, 貌似加了保护。

IDA逆向的结果如下: IDA对windowsAPI逆的真心不错。

故事发生在这个函数:

```
10  __int16 v7; // [sp+45h] [bp-23h]@1
11  char v8; // [sp+47h] [bp-21h]@1
12  CHAR String1; // [sp+48h] [bp-20h]@1
13  char v10; // [sp+49h] [bp-1fh]@1
14  __int16 v11; // [sp+65h] [bp-3h]@1
15  char v12; // [sp+67h] [bp-1h]@1
16
17  String[0] = 0;
18  memset(&String[1], 0, 0x1Cu);
19  v3 = 0;
20  v4 = 0;
21  String1 = 0;
22  memset(&v10, 0, 0x1Cu);
23  v11 = 0;
24  v12 = 0;
25  String2 = 0;
26  memset(&v6, 0, 0x1Cu);
27  v7 = 0;
28  v8 = 0;
29  if ( GetDlgItemTextA(hDlg, 1000, String, 16) >= 5 )
30  {
31  GetDlgItemTextA(hDlg, 1001, &String1, 16);
32  v1 = 0;
33  if ( strlen(String) != 0 )
34  {
35  do
36  {
37  *(&String2 + v1) = (v1 + v1 * String[v1] * String[v1]) % 66 + 33;
38  ++v1;
39  }
40  while ( v1 < strlen(String) );
41  }
42  strcpy(String, "Happy@");
43  lstrcatA(String, &String2);
44  result = lstrcpnA(&String1, String) != 0;
45 }
```

我就不解释了, 加密的算法还是很清楚的, 然后我用py简单写了一下:

```
C:\Users\tangtianlong\Desktop\math.py - Sublime Text 2 (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences H
ctf3.py x ctfmima1.py x ctf.py — Desktop x ctf2.py — Des
1 #coding=utf-8
2
3 str="hello"
4 str2=[]
5 for i in range(5):
6     x=(i+i*ord(str[i])*ord(str[i])%66+33)
7     c=chr(x)
8     str2.append(c)
9
10 print ''.join(str2)
11
12     http://blog.csdn.net/
13
14
15
16
17
18
19
20
21
!GA0U
[Finished in 0.2s]
```

再看一下IDA，结果是拼接了一下，大家要对WINDOWS的API熟悉。答案就是Happy@!GA0U