实验吧（逆向）：1000

原创

s0i1 于 2019-09-04 17:30:11 发布 123 收藏
分类专栏： 逆向工程

题目

答案格式：CTF{}

解题链接： http://ctf5.shiyanbar.com/misc/1000.exe

运行截图，1000有特殊含义：

运行程序之后，发现生成了一张图片 tip.jpg ：

可疑区：

```
00484D10  68 74 00 66 6C 61 67 2E  74 78 74 00 41 53 44 68  ht.flag.txt.ASDh
00484D20  65 67 79 64 62 48 46 38  38 37 4A 37 36 37 4A 44  egydbHF887J767JD
00484D30  36 00 01 00 00 00 00 00  00 00 5C 74 69 70 2E 6A  6.........\tip.j
00484D40  70 67 00 01 00 00 00 66  0D 00 00 FF D8 FF E0 00  pg.....f........
00484D50  10 4A 46 49 46 00 01 01  01 00 60 00 60 00 00 FF  .JFIF.....`.`...
00484D60  DB 00 43 00 08 06 06 07  06 05 08 07 07 07 09 09  ..C.............
00484D70  08 0A 0C 14 0D 0C 0B 0B  0C 19 12 13 0F 14 1D 1A  ................
00484D80  1F 1E 1D 1A 1C 1C 20 24  2E 27 20 22 2C 23 1C 1C  ......$.'·",#..
00484D90  28 37 29 2C 30 31 34 34  34 1F 27 39 3D 38 32 3C  (7),01444.'9=82<
00484DA0  2E 33 34 32 FF DB 00 43  01 09 09 09 0C 0B 0C 18  .342...C........
00484DB0  0D 0D 18 32 21 1C 21 32  32 32 32 32 32 32 32 32  ...2!.!222222222
00484DC0  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
00484DD0  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
00484DE0  32 32 32 32 32 32 32 32  32 FF C2 00 11 08 00 A1  222222222.......
00484DF0  00 90 03 01 22 00 02 11  01 03 11 01 FF C4 00 1A  ....".....
00484E00  00 01 01 01 01 01 01 01  00 00 00 00 00 00 00 00  ................
00484E10  00 00 05 04 03 01 02 06  FF C4 00 16 01 01 01 01  ................
00484E20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 02  ................
00484E30  FF DA 00 0C 03 01 00 02  10 03 10 00 00 01 FD 15  ................
```

函数入口 WinMain（没用）：

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  return sub_479638(hInstance, hPrevInstance, lpCmdLine, nShowCmd);
}
```

找到获取输入内容的函数 GetWindowTextA：

```
004834EC    EqualRect                   USER32
004834F0    UpdateWindow                USER32
004834F4    ValidateRect                USER32
004834F8    InvalidateRect              USER32
004834FC    GetClientRect               USER32
00483500    GetFocus                    USER32
00483504    GetWindowTextA              USER32
00483508    GetWindowTextLengthA        USER32
0048350C    CharUpperA                  USER32
00483510    GetWindowDC                 USER32
00483514    BeginPaint                  USER32
00483518    EndPaint                    USER32
0048351C    TabbedTextOutA              USER32
00483520    DrawTextA                   USER32
00483524    GrayStringA                 USER32
00483528    GetDlgItem                  USER32
```

找到设置函数，但是没有用因为找不到 lpString：

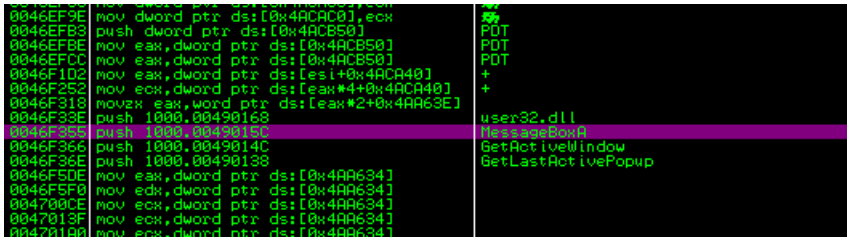
```
void __stdcall AfxSetWindowText(HWND hWnd, LPCSTR lpString)
{
  unsigned int v2; // esi
  CHAR String; // [esp+4h] [ebp-100h]

  v2 = lstrlenA(lpString);                      // 获取字符串长度,关键就是lpString
  if ( v2 > 256 || GetWindowTextA(hWnd, &String, 256) != v2 || lstrcmpA(&String, lpString) )// GetWindowTex
                                                // 运行成功，返回值是不包含结尾NULL字符的字符串长度;
                                                // 如果标题栏为空，又如果给定的句柄是无效的，那么返回值是0
                                                // lstrcmp 的比较区分大小写，前者大就返回正，后者大返回负，相等返回
    SetWindowTextA(hWnd, lpString);
}
```

动态分析　根据jpeg找到程序指令，下断点。

```
00452559  .  8D46 3C      lea eax,dword ptr ds:[esi+0x3C]
0045255C  .  B9 02000000  mov ecx,0x2
00452561  >  8958 F8      mov dword ptr ds:[eax-0x8],ebx
00452564  .  8918         mov dword ptr ds:[eax],ebx
00452566  .  83E8 04      sub eax,0x4
00452569  .  49           dec ecx
0045256A  .^ 75 F5        jnz short 1000.00452561
0045256C  .  895E 40      mov dword ptr ds:[esi+0x40],ebx
0045256F  .  895E 44      mov dword ptr ds:[esi+0x44],ebx
00452572  .  C746 48 5000 mov dword ptr ds:[esi+0x48],0x50
00452579  .  68 38614A00  push 1000.004A6138                JPEGMEM
0045257E  .  8977 04      mov dword ptr ds:[edi+0x4],esi
00452581  .  E8 1C130100  call 1000.004638A2
00452586  .  83C4 04      add esp,0x4
00452589  .  3BC3         cmp eax,ebx
0045258B  .  74 64        je short 1000.004525F1
0045258D  .  8D5424 14    lea edx,dword ptr ss:[esp+0x14]
00452591  .  8D4C24 0C    lea ecx,dword ptr ss:[esp+0xC]
```


根据1000就是数字8的消息找到，运行程序会有弹窗，锁定到 MessageBox 函数下断点，但是这个断点没有断，也不知道什么原因，没办法继续分析了。



搞了半天没有发现，最终的看了一下writeup，发现在用户文件夹下的收藏夹里。

```
1  G00dTh1sIske
```

加上最后的Y就对了， CTF{G00dTh1slskeY}

整理一下思路：

1、发现弹窗，寻找弹窗函数

2、根据jpg文件找线索