72：Whitzard OJ逆向--Validator3000

原创

S1lenc3 于 2020-02-10 22:58:33 发布 121 收藏
分类专栏： CTF
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/qq_41858371/article/details/104256431
版权


CTF 专栏收录该内容
25 篇文章 1 订阅
订阅专栏

直接IDA分析，

找到关键处，

```
if ( v6 )
{
  v7 = FindResourceW(0, (LPCWSTR)0x82, &Type);
  v8 = v7;
  v9 = SizeofResource(0, v7);
  v10 = v9;
  if ( v8
    && v9
    && (v11 = LoadResource(0, v8)) != 0
    && (v12 = LockResource(v11)) != 0
    && (v13 = (int (__stdcall *)(_DWORD, signed int, LPVOID *))sub_401510(v12, v10)) != 0 )
  {
    if ( v13(0, 8, &lpAddress) && lpAddress )
    {
      if ( ((int (*)(void))lpAddress)() )
        SetWindowTextW(::hWnd, L"Congratulations, you won!");
      else
        SetWindowTextW(::hWnd, L"Bad flag");
    }
    CloseHandle(v6);
    if ( v13(0, 6, &lpAddress) )
      VirtualFree(lpAddress, 0, 0x8000u);
  }
  else
  {
    SetWindowTextW(::hWnd, L"Checker module is not available");
    CloseHandle(v6);
  }
}
```

https://blog.csdn.net/qq_41858371

猜测就是通过sub_401510对一段代码进行解密，解密代码是用的windowsAPI库函数写的，看不懂，想着可以通过动态调试，然后发现还有防御，动调的话程序就不能正常执行了。根据题意和提示：

The flag check is a simple strcmp, but we hide it with unbreakable shields. Can you find a way to break it or bypass it?

flag format: ctfzone{}

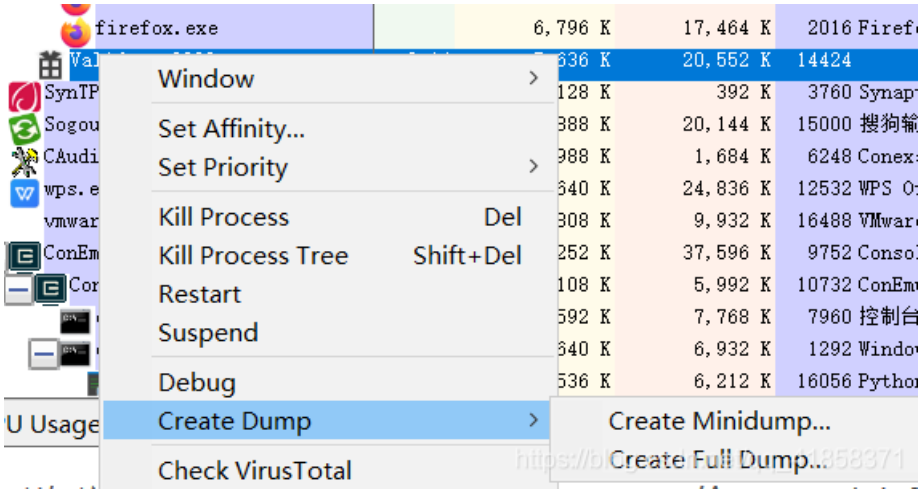
Estimated difficulty: easy or hard

hint: You can dump the memory to solve it easily

hint2: unicode

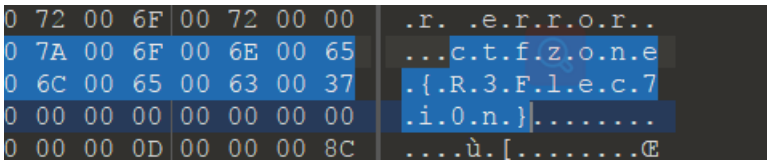
https://blog.csdn.net/qq_41858371

可以知道，只要把程序跑起来，就能拿到flag，hint给了dump内存和unicode，使用软件procexp转储内存。



然后IDA打不开，windbg也不会用，想了想查找字符串那就用010editor试试。

提示unicode，那就按照unicode格式搜索 ctfzone看看。



有经验的话，很快就能做出来，我还分析了好长时间。。。

还做了一道题，processor师傅出的一道入群题，第一次看的时候压根没看懂，今天又试了试，解出来了。哈哈。

入群题，不方便写writeup。

做逆向还是要静心、耐心、细心，继续努力。