试试福昕吧

暂时没成功，各种RE，搁置。

10月3日更新

半夜开搞，而且基本上都花时间在OD的学习上，没多少内容。

好吧，一开始我先找到了几个Win32的API调用，因为是文件转换，我想应该有文件的读写，先是在IDA里去搜了CreateFile、ReadFile两个的调用，然后下断点，莫名不会执行……我也不知道为什么不会在断点停下，这点让我很郁闷，果然IDA还是适合静态反编译吗。

然后比较早就睡了。

10月4日更新

很郁闷，花了一晚上学习OD，实际上只是学习各种按键、功能而已……不过也算有点成效，虽然还是很不熟练，在第二天10月5日花了将近半天熟悉OD。

大概先是搜了"CreatFile"，没错，你没看错，"CreatFile"，我拼错了，自然没找到，所以直接去研究了ReadFile。

我没想到会用一天的时间在寻找PDF2WORD的核心转换代码（当然是找不到的……后来才发现……）。仍然，我先去搜了ReadFile的调用，不停进入函数、退出函数等等很容易就能找到一段代码，where （用个定语从句而已）执行5遍就会输出成品doc、docx文件，我大概在这上面不停调试花了半天时间，甚至进入系统调用一步一步分析反汇编……

```
630C7340    80BD DCFCFFFF   cmp     byte ptr [ebp-0x324], 0x0       转换部分循环开始
630C7347    0F85 74010000   jnz     beconv.630C74C1
630C734D    53              push    ebx
630C734E    8D8D B8FDFFFF   lea     ecx, [ebp-0x248]
630C7354    51              push    ecx
630C7355    8D8D CCFCFFFF   lea     ecx, [ebp-0x334]
630C735B    E8 20E9FEFF     call    beconv.630B5C80                 改变了flag的值
630C7360    8B8D BCFDFFFF   mov     ecx, [ebp-0x244]
630C7366    8B85 B8FDFFFF   mov     eax, [ebp-0x248]                mshtml.5B2DF816
630C736C    8BD1            mov     edx, ecx
630C736E    2BD0            sub     edx, eax                        UserSyst.5CB13D6F
630C7370    C645 FC 09      mov     byte ptr [ebp-0x4], 0x9
630C7374    83FA 0C         cmp     edx, 0xC
630C7377    75 7F           jnz     short beconv.630C73F8
630C7379    8138 00100000   cmp     dword ptr [eax], 0x1000         退出转换的flag
630C737F    75 77           jnz     short beconv.630C73F8           jnz short 5A0973F8
630C7381    8B08            mov     ecx, [eax]
630C7383    898D C0FCFFFF   mov     [ebp-0x340], ecx
630C7389    8B48 04         mov     ecx, [eax+0x4]
630C738C    8B40 08         mov     eax, [eax+0x8]
630C738F    85FF            test    edi, edi
630C7391    74 15           je      short beconv.630C73A8
630C7393    8B95 B0FCFFFF   mov     edx, [ebp-0x350]
630C7399    52              push    edx
630C739A    50              push    eax                             UserSyst.5CB13D6F
630C739B    8B47 04         mov     eax, [edi+0x4]
630C739E    51              push    ecx
630C739F    FFD0            call    eax                             UserSyst.5CB13D6F
630C73A1    83C4 0C         add     esp, 0xC
630C73A4    8BF0            mov     esi, eax                        UserSyst.5CB13D6F
630C73A6    EB 05           jmp     short beconv.630C73AD
630C73A8    BE 01000000     mov     esi, 0x1
630C73AD    8D8D 50FCFFFF   lea     ecx, [ebp-0x3B0]
630C73B3    E8 F8D5FEFF     call    beconv.630B49B0
630C73B8    8D8D 50FCFFFF   lea     ecx, [ebp-0x3B0]
630C73BE    E8 4DD5FEFF     call    beconv.630B4910
630C73C3    53              push    ebx
630C73C4    6A 04           push    0x4
630C73C6    8D8D E8FCFFFF   lea     ecx, [ebp-0x318]
630C73CC    51              push    ecx
630C73CD    8D8D CCFCFFFF   lea     ecx, [ebp-0x334]
630C73D3    8985 ECFCFFFF   mov     [ebp-0x314], eax                UserSyst.5CB13D6F
630C73D9    89B5 E8FCFFFF   mov     [ebp-0x318], esi
630C73DF    E8 BCE7FEFF     call    beconv.630B5BA0                 文件转换函数
630C73E4    8D8D B8FDFFFF   lea     ecx, [ebp-0x248]
630C73EA    C645 FC 08      mov     byte ptr [ebp-0x4], 0x8
630C73EE    E8 7D0BFFFF     call    beconv.630B7F70
630C73F3    E9 48FFFFFF     jmp     beconv.630C7340                 转换循环部分结束
```

不要在意配色，这是我选中后的颜色。注释不止这么一点，我在很多函数里面也打了注释。

当然，试着改了很多参数，就是那个flag和计数器（我后来在内存区域看到flag边上有个值和我执行这段代码的次数相同，我猜测是计数器），不停地修改那些参数结果程序不停报错：Internal Error。然后我又不停地查MSDN的资料。以上，都是我在ReadFile里面遇到的坑，至今还没摆脱。

后来，大约又是10月5日的半夜时分，我再去搜索了一下创建File除了CreateFile一类函数还能有什么函数，找不到。最后我终于又去搜了一下CreateFile函数，在每个CreateFiles的头设置了断点一一尝试运行，pdf转换，发现只有一

个CreateFileW成功在断点处卡住，然而我貌似没有在栈列表里发现……我的pdf文件名？倒是发现另一个很神奇的可执行程序—存放在福昕同安装目录下的..\BCL Technologies\easyConverter SDK 4\Common\beconvlib.exe。

WHAT'S THAT???

我去网上搜了一下，马上搜到了这玩意儿……

> BCL easyConverter SDK是一款转换软件，能将pdf文档转word文档。
> BCL easyConverter SDK允许程序员将Adobe Acrobat兼容的PDF文档转换成Microsoft Word兼容的RTF文件。这些Word兼容的文件中的文本，图片，表格和列表能被编辑，修改或利用。
> BCL easyConverter SDK的使用方法和一般得转换器相似，先导入所需转换的pdf文件，然后根据导出的word文档所需的要求进行设置，最后导出文档即可。软件可免费试用，但试用只能转换五页，其后需要收费，是英语软件。

EXCUSE ME???

好了，搞了半天福昕转换器只是个外壳，我投翔，我投翔。

我试着自己调戏了一下那个可执行文件，改了一下文件名，好了福昕的不能转换了。试着自己运行了一下，发现不会用，于是去看了看官方文档……并且自己下了个样例代码来玩，成功转换了pdf……的一半。

对官方文档稍微有些理解之后又回去看了福昕转换器，又稍加调试，获得三段神秘代码。

```
********-****-****-****-************
****-****-****-****-****-****
{********-****-****-****-************}
```

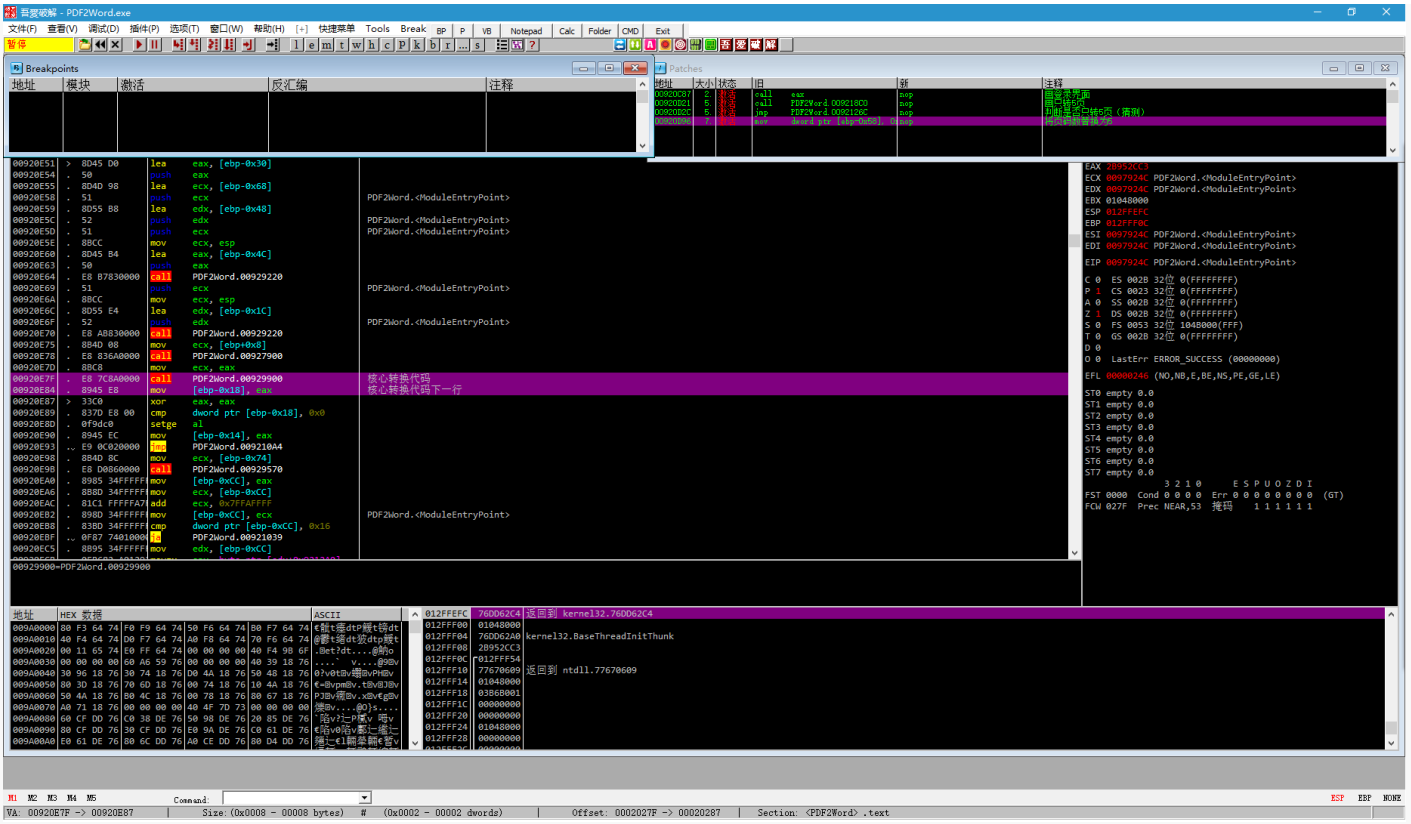
猜测第二个是激活码，亦即，福昕这货买了它的产品，然后自己做了个外壳。

阿普戴特：感觉人家商业软件放出来不太好，比赛结束后修改了一下这文档，隐藏掉了……有兴趣自己找，不难。

阿普黛特啊普代特：别问我阿普戴特是什么玩意儿，大声念出来。

10月5日更新

昨晚搞得比较迟，睡了，今天大约下午一点才醒来。顺着思路找到了页码数保存在哪里，然后在边上发现几个诡异的立即数0x05。尝试NOP掉一处之后成功转换全篇pdf，并且找到了核心的转换函数。



到此为止，基本上已经完成了，剩下的，解决掉那个要求登录的就可以了。其实那个之前就已经找到了，不过没有进入过研究而已。

瞬间搞掉要求登录的页面，还剩一个只转5页的选择框，虽然不搞掉应该也可以……

……很简单地搞掉了只转5页的选择框

好吧，剩下还有个小问题就是路径移动之后就没法用了，我试着破一下Init……

后记

花了一天多了，生活全都乱了。

也算是搞了出来，感觉重点还是在于找到那个核心转换代码（也就是调用BCL的dll的代码……）

我因为安装在C:\Program Files (x86)\，到时候检查应该也需要放在那里……不管了。

PS

我用这个pdf2word转了一下我的WriteUp猜发生了什么？

神tmd Microsoft的PDF打印机就是把页面转成图片然后变成pdf出来啊？？？