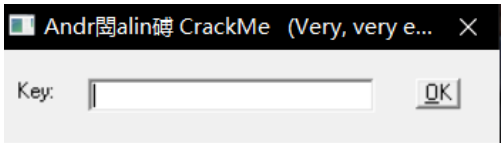
随风而逝的白色相簿

Crackme008

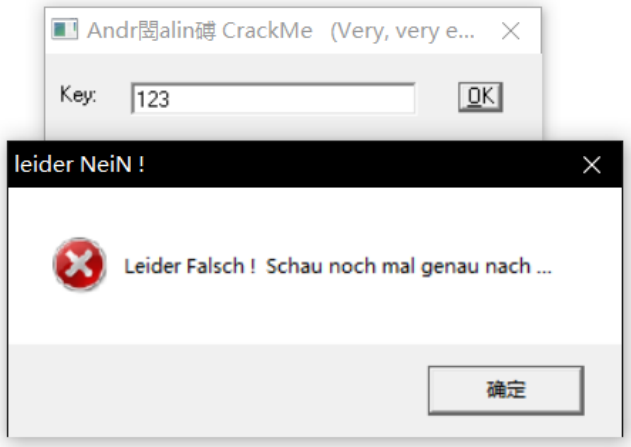
Crackme008 的逆向分析

1.观察程序



只有一个输入 Key 的输入框。

输入 123，点击 OK。

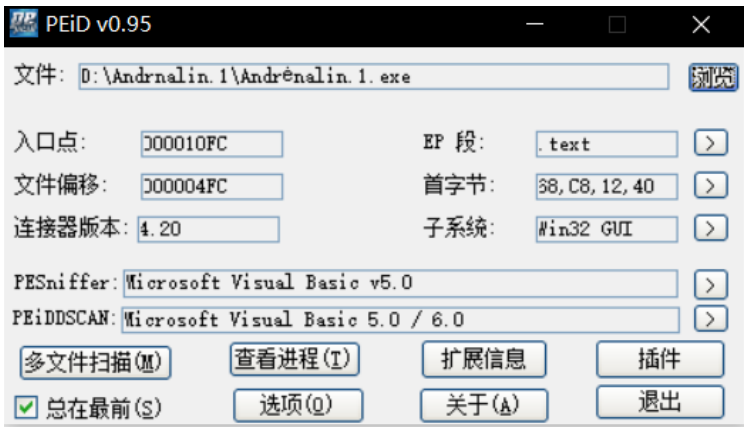


结果出现了奇怪的报错。上面的报错看不出来是啥意思。

于是使用百度翻译，结果发现居然是德语。

2.查壳

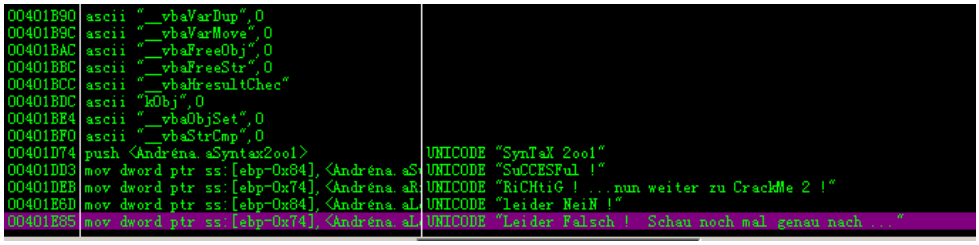
使用 PEiD 载入。可以看出是使用 VB 编写的程序，没有壳。



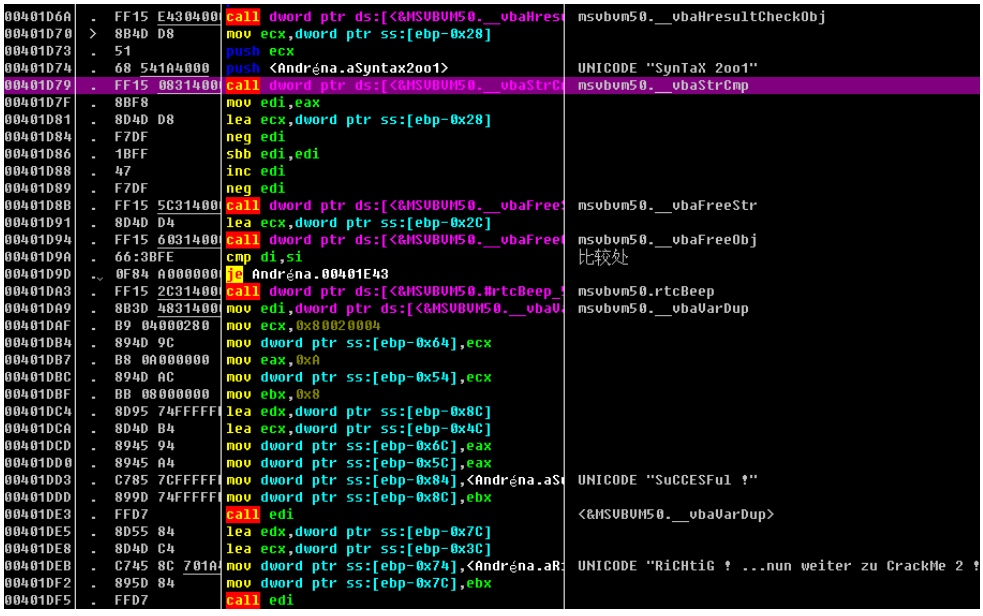
3.分析程序

使用 OD 载入程序。

搜索字符串，发现了报错的字符串，双击进入。



向上查找，发现了一个 cmp 和 je 语句。再 cmp 语句上面，还有一个 StrCmp 函数。



在 StrCmp 函数处下断点，输入 123，点击 OK。

程序断在了断点处。

```
00401D70  >  8B4D D8       mov ecx,dword ptr ss:[ebp-0x28]
00401D73  .  51            push ecx
00401D74  .  68 541A4000   push <Andrćna.aSyntax2oo1>          UNICODE "SynTaX 2oo1"
00401D79  .  FF15 0831400  call dword ptr ds:[<&MSVBVM50.__vbaStrC  msvbvm50.__vbaStrCmp
00401D7F  .  8BF8          mov edi,eax
```

可以看出 StrCmp 函数有两个参数

```
0012F3FC   00401A54  UNICODE "SynTaX 2oo1"
0012F400   010F06F4  UNICODE "123"
```

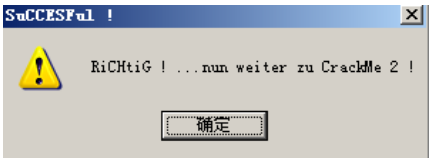
其中有一个是我们输入的 key，难道另一个就是正确的 key?

我们先执行该条指令，可以看到返回值不为 0

```
EAX FFFFFFFF
ECX 00000002
EDX 00050000
```

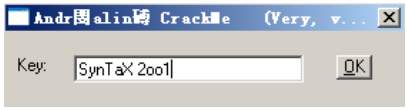
我们修改 EAX 的值为 0，让程序继续运行。

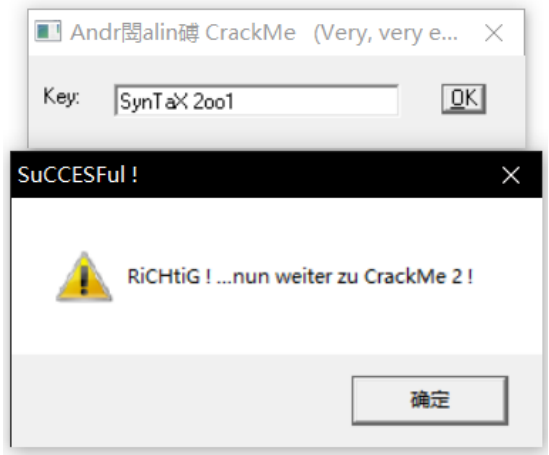
```
EAX 00000000
ECX 00000002
EDX 00050000
```



果然成功了。

接下来我们输入疑似为正确 key 的字符串，运行程序。





果然是正确的 key。

这个程序是一星的，所以很简单。

分类: 160 Crackme

好文要顶 关注我 收藏该文

随风而逝的白色相簿
关注 - 4
粉丝 - 1

« 上一篇： Crackme007

posted @ 2019-09-08 15:35 随风而逝的白色相簿 阅读(2) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

发表评论

昵称： 随风而逝的白色相簿

评论内容：

提交评论 退出

[Ctrl+Enter快捷键提交]

0
推荐