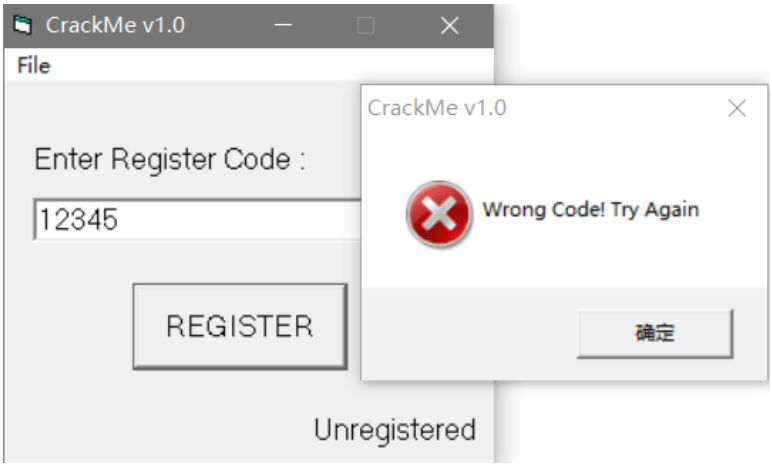
# 随风而逝的白色相簿



## CrackMe022

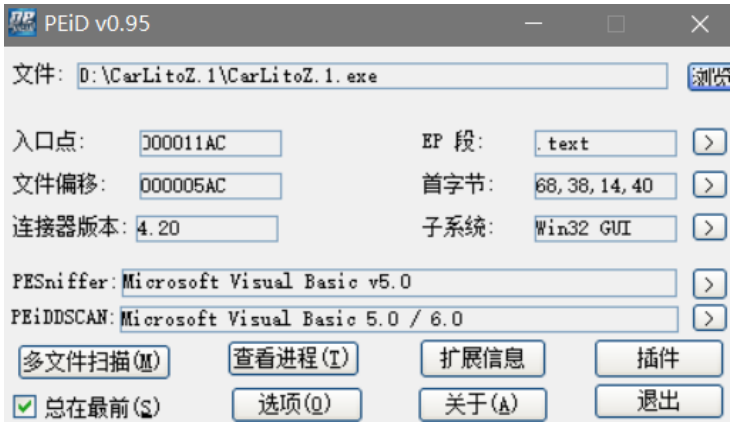
### Crackme022 的逆向分析

#### 1.程序观察




程序只有一个输入框，看起来只有一个注册码的亚子。

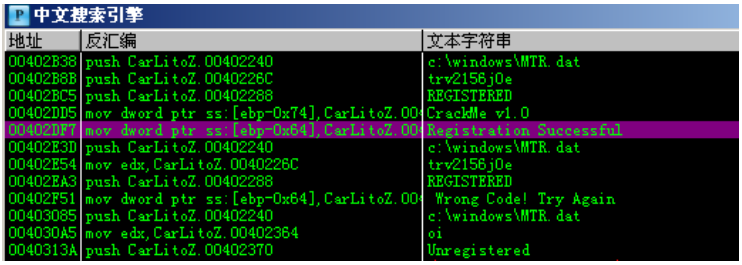
#### 2.简单查壳



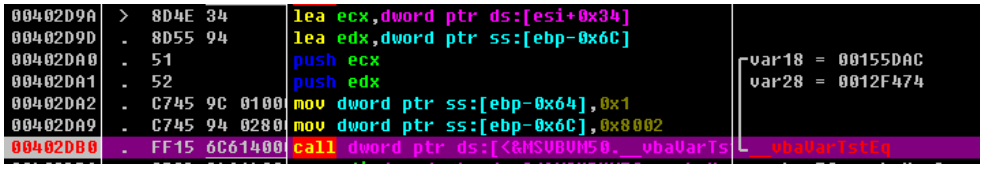

使用 VB5 编写，无壳。

#### 3.程序分析

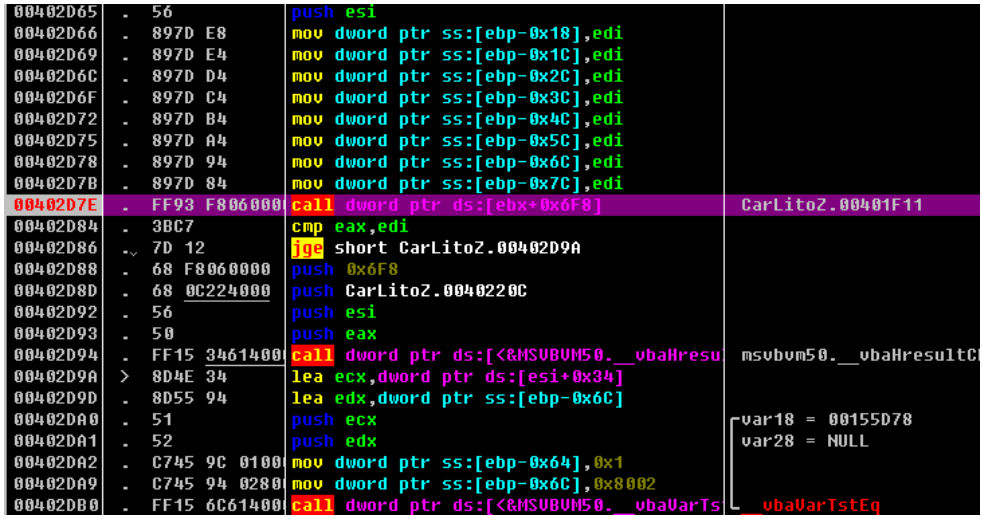
使用 OD 载入程序，搜索字符串。




在字符串上面有一个比较函数，但函数的参数并没有我们输入的注册码

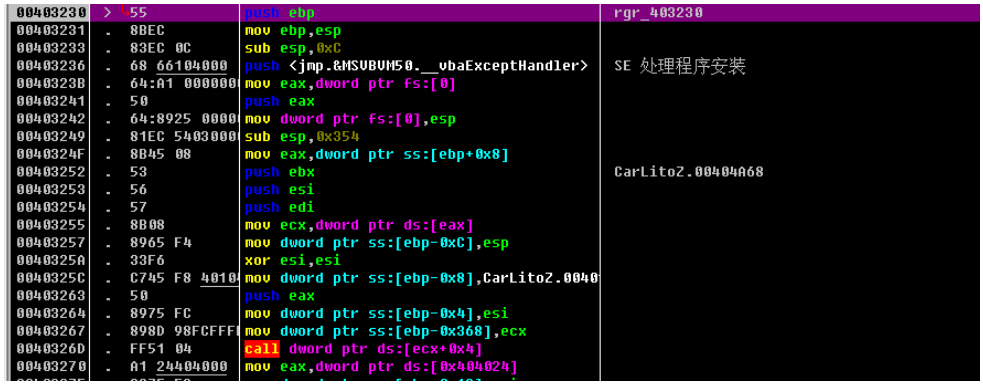



分析代码可以看出来，参数2的值固定为1，所以在别的代码处肯定还要有比较和为参数1赋值的代码。
真正的比较函数其实在上方不远




断点处就是真正的比较函数所在处。

进入函数里面




在下面是真正的比较函数

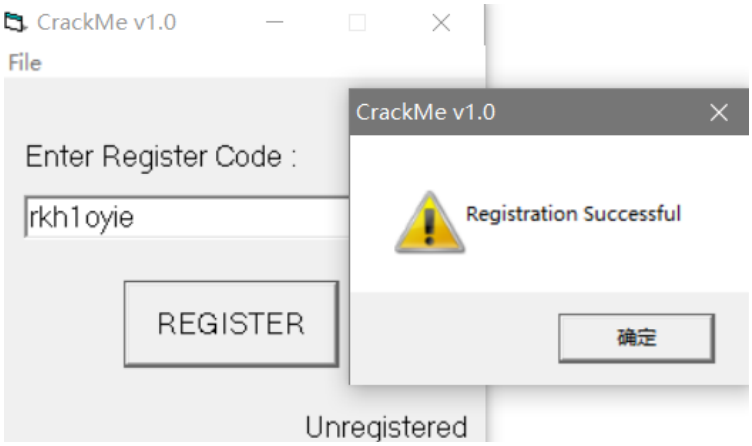
函数的参数

```
0012F0A0  0012F1D0  var28 = 0012F1D0
0012F0A4  0012F1C0  var18 = 0012F1C0
```

```
01112ACC  31 00 32 00  33 00 00 00  6B 00 4D 00  65 00 20 00  1.2.3...k.M.e. .
```

```
011045F4  72 00 6B 00  68 00 31 00  6F 00 79 00  69 00 65 00  r.k.h.1.o.y.i.e.
```

可以看到一个参数 123 是我们输入的注册码，而 rkh1oyie 就是真正的注册码。




相关文件在我的 Github：https://github.com/UnreachableLove/160-Crackme/upload/master/Crackme022

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： Crackeme021

posted @ 2019-09-24 20:19 随风而逝的白色相簿 阅读(1) 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