

随风而逝的白色相簿

博客园

首页

新随笔

联系

订阅

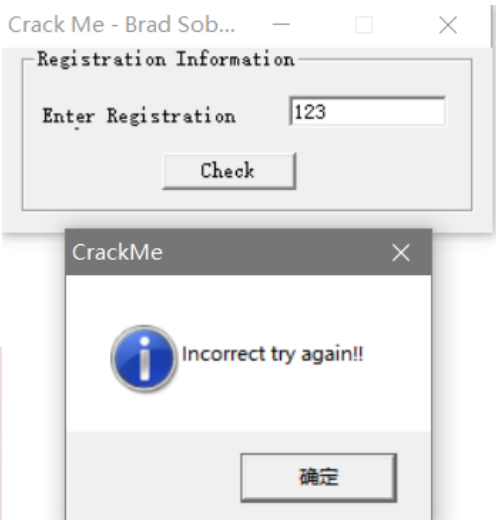
管理

随笔 - 9 文章 - 0 评论 - 1

Crackme018

Crackme018 的逆向分析

1.程序观察

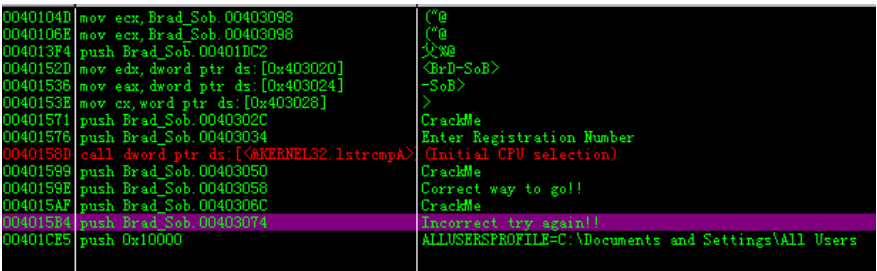


2.简单查壳



3.程序分析

OD 载入程序，搜索字符串。



公告

昵称： 随风而逝的白色相簿
园龄： 1年9个月
粉丝： 1
关注： 4

2019年9月						
日	一	二	三	四	五	六
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18		20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

搜索

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

随笔分类

160 Crackme(8)

随笔档案

2019年9月(8)
2018年10月(1)

最新评论

1. Re:Crackme014
写的真好

--随风而逝的白色相簿

阅读排行榜

1. PHP一句话木马(6701)
Crackme007(7)

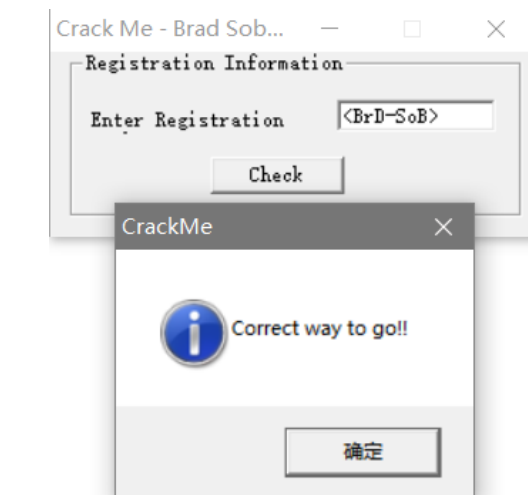
评论排行榜

跟进程序，发现一个比较函数。下断点，运行程序

```
0040155F . 50          push     eax
00401560 . FF15 04204000 call    dword ptr ds:[<&KERNEL32.1strlenA>] [String = 00000003 ???
00401566 . 8945 F0     mov     [local.4],eax [strlenA
00401569 . 837D F0 01  cmp     [local.4],0x1
0040156D . 73 16      jnb     short Brad_Sob.00401585
0040156F . 6A 40      push    0x40
00401571 . 68 2C304000 push    Brad_Sob.0040302C
00401576 . 68 34304000 push    Brad_Sob.00403034
0040157B . 8B4D E0     mov     ecx,[local.8]
0040157E . E8 7B050000 call    <jmp.&MFC42.#CWnd::MessageBoxA_4224
00401583 . EB 3C      jmp     short Brad_Sob.004015C1
00401585 . 8D4D E4     lea     ecx,[local.7]
00401588 . 51          push    ecx [String2 = "<BrD-SoB>"
00401589 . 8D55 F4     lea     edx,[local.3] [String1 = "123"
0040158C . 52          push    edx
0040158D . FF15 00204000 call    dword ptr ds:[<&KERNEL32.1strcmpA>] [strcmpA
00401593 . 85C0      test    eax,ebx
00401595 . 75 16      jnz     short Brad_Sob.004015AD
00401597 . 6A 40      push    0x40
00401599 . 68 50304000 push    Brad_Sob.00403050
0040159E . 68 50304000 push    Brad_Sob.00403058
004015A3 . 8B4D E0     mov     ecx,[local.8]
004015A6 . E8 53050000 call    <jmp.&MFC42.#CWnd::MessageBoxA_4224
004015AB . EB 14      jmp     short Brad_Sob.004015C1
004015AD . 6A 40      push    0x40
004015AF . 68 6C304000 push    Brad_Sob.0040306C
004015B4 . 68 74304000 push    Brad_Sob.00403074
004015B9 . 8B4D E0     mov     ecx,[local.8]
004015BC . E8 3D050000 call    <jmp.&MFC42.#CWnd::MessageBoxA_4224
004015C1 . 8BE5      mov     esp,ebp
004015C3 . 5D          pop     ebp
004015C4 . C3          retm

0012F884 . 0012F8A0 String1 = "123"
0012F888 . 0012F890 String2 = "<BrD-SoB>"
```

可以看到，参数1是我们输入的注册码，参数2是我们不认识的字符串，猜测是正确注册码。



非常朴实无华的018，和其它同为1星的妖艳贱货不一样

相关文件在我的 Github：<https://github.com/UnreachableLove/160-Crackme/tree/master/Crackme018>

2019-09-19 10:40:15

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: [Crackme017](#)







posted @ 2019-09-19 10:40 随风而逝的白色相簿 阅读(0) 评论(0) 编辑 收藏

0

👍 推荐

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