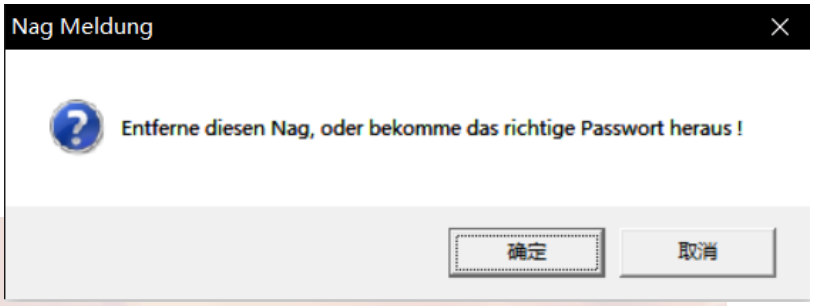
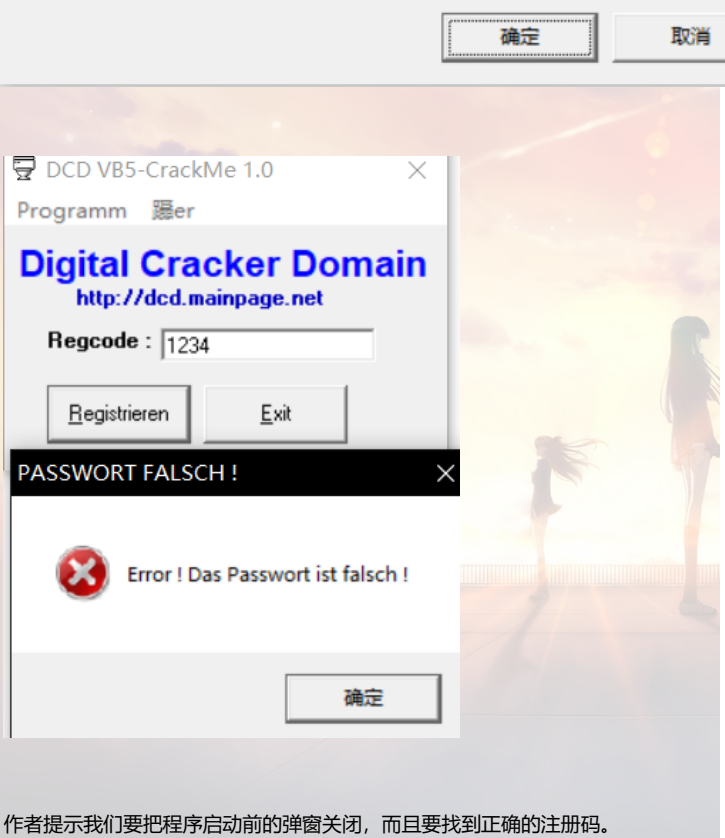
随风而逝的白色相簿

Crackme015

Crackme015 的逆向分析

1.程序观察





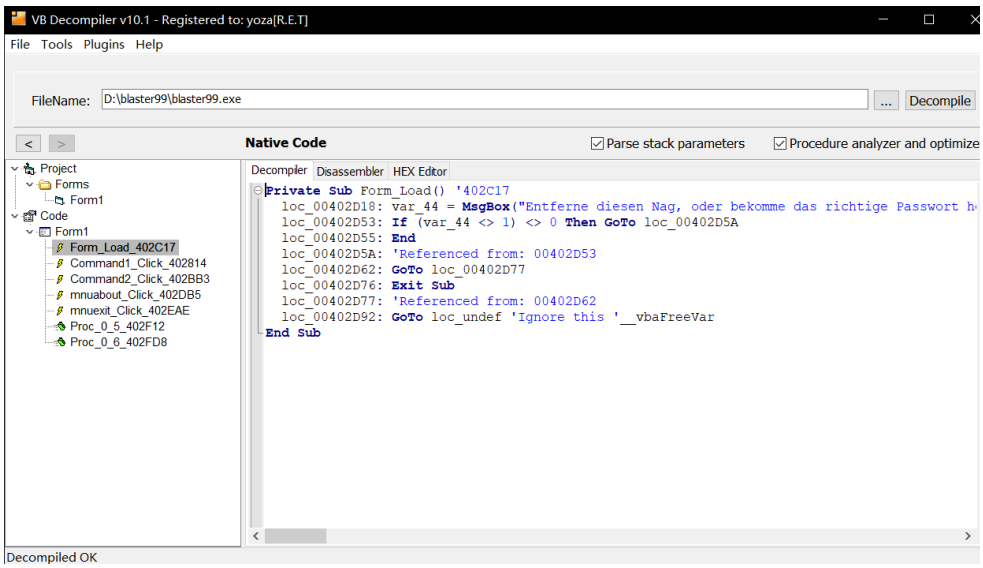
作者提示我们要把程序启动前的弹窗关闭，而且要找到正确的注册码。

2.简单查壳

程序使用 VB5 编写，无壳。

3.程序分析

首先要去除启动时的弹窗。
使用 VB Decompiler 载入程序



从反编译的代码，我们可以看到加载的时候，程序在调用 MsgBox 函数弹窗之后，会验证返回值，如果不符合条件就会退出。
我们查看相对应的汇编代码

```
00402C85  .  C745 84 F01E  mov dword ptr ss:[ebp-0x7C],blaster9.00  UNICODE "Entferne diesen Nag, oder bekomme das richtige Pas"
00402C8C  .  899D 7CFFFFFF mov dword ptr ss:[ebp-0x84],ebx
00402C92  .  E8 95E4FFFF   call <jmp.&MSVBVM50.__vbaVarCopy>
00402C97  .  6A 03         push 0x3
00402C99  .  8D95 7CFFFFFF lea edx,dword ptr ss:[ebp-0x84]
00402C9F  .  5F            pop edi                                 0012FAAC
00402CA0  .  8D4D DC       lea ecx,dword ptr ss:[ebp-0x24]
00402CA3  .  C745 84 2100  mov dword ptr ss:[ebp-0x7C],0x21
00402CAA  .  897D 7CFFFFFF mov dword ptr ss:[ebp-0x84],edi
00402CB0  .  E8 71E4FFFF   call <jmp.&MSVBVM50.__vbaVarMove>
00402CB5  .  8D95 7CFFFFFF lea edx,dword ptr ss:[ebp-0x84]
00402CBB  .  8D4D CC       lea ecx,dword ptr ss:[ebp-0x34]
00402CBE  .  C745 84 781F  mov dword ptr ss:[ebp-0x7C],blaster9.00  UNICODE "Nag Meldung"
00402CC5  .  899D 7CFFFFFF mov dword ptr ss:[ebp-0x84],ebx
00402CCB  .  E8 5CE4FFFF   call <jmp.&MSVBVM50.__vbaVarCopy>
00402CD0  .  6A 0A         push 0xA
00402CD2  .  B9 04000280   mov ecx,0x80020004
00402CD7  .  58            pop eax                                 0012FAAC
00402CD8  .  894D 94       mov dword ptr ss:[ebp-0x6C],ecx         msvbvm50.7403BDC0
00402CDB  .  8945 8C       mov dword ptr ss:[ebp-0x74],eax
00402CDE  .  8945 9C       mov dword ptr ss:[ebp-0x64],eax
00402CE1  .  8D45 8C       lea eax,dword ptr ss:[ebp-0x74]
00402CE4  .  894D A4       mov dword ptr ss:[ebp-0x5C],ecx         msvbvm50.7403BDC0
00402CE7  .  50            push eax
00402CE8  .  8D45 9C       lea eax,dword ptr ss:[ebp-0x64]
00402CEB  .  50            push eax
00402CEC  .  8D45 CC       lea eax,dword ptr ss:[ebp-0x34]
00402CEF  .  50            push eax
00402CF0  .  8D45 DC       lea eax,dword ptr ss:[ebp-0x24]
00402CF3  .  50            push eax
00402CF4  .  E8 21E4FFFF   call <jmp.&MSVBVM50.__vbaI4Var>
00402CF9  .  50            push eax
00402CFA  .  8D45 AC       lea eax,dword ptr ss:[ebp-0x54]
00402CFD  .  50            push eax
00402CFE  .  E8 1DE4FFFF   call <jmp.&MSVBVM50.#rtcMsgBox_595>
```

```
00402D2C  .  83C4 0C      add esp,0xC
00402D2F  .  8D45 BC      lea eax,dword ptr ss:[ebp-0x44]
00402D32  .  C745 84 0100 mov dword ptr ss:[ebp-0x7C],0x1
00402D39  .  C785 7CFFFFF mov dword ptr ss:[ebp-0x84],0x8003
00402D43  .  50           push eax                          ┌var18 = 0012FAAC
00402D44  .  8D85 7CFFFFF lea eax,dword ptr ss:[ebp-0x84]   │
00402D4A  .  50           push eax                          └var28 = 0012FAAC
00402D4B  .  E8 BEE3FFFF  call <jmp.&MSVBVM50.__vbaVarTstEq>  └__vbaVarTstEq
00402D50  .  66:85C0      test ax,ax
00402D53  .v 75 05        jnz short blaster9.00402D5A
00402D55  .  E8 AEE3FFFF  call <jmp.&MSVBVM50.__vbaEnd>
```

所以想要去除弹窗，首先要去除 MsgBox 函数，还要使之不退出。

我们可以把 MsgBox 函数 和 End 函数的调用代码全部使用 nop 覆盖掉。

接下来寻找正确的注册码

地址 402B14 处是注册按钮点击事件，我们进入代码内部。

```
00402814  > 55            push ebp                          注册按钮
00402815  .  8BEC         mov ebp,esp
00402817  .  83EC 0C      sub esp,0xC
0040281A  .  68 66104000  push <jmp.&MSVBVM50.__vbaExceptHandler>  SE 处理程序安装
0040281F  .  64:A1 000000 mov eax,dword ptr fs:[0]
00402825  .  50           push eax                          blaster9.0040263C
00402826  .  64:8925 0000 mov dword ptr fs:[0],esp
0040282D  .  81EC B000000 sub esp,0xB0
00402833  .  53           push ebx
00402834  .  8B5D 08      mov ebx,dword ptr ss:[ebp+0x8]
00402837  .  8BC3         mov eax,ebx
00402839  .  56           push esi
0040283A  .  83E3 FE      and ebx,-0x2
0040283D  .  57           push edi
0040283E  .  8965 F4      mov dword ptr ss:[ebp-0xC],esp
00402841  .  83E0 01      and eax,0x1
00402844  .  8B3B         mov edi,dword ptr ds:[ebx]
00402846  .  C745 F8 0010 mov dword ptr ss:[ebp-0x8],blaster9.004
0040284D  .  53           push ebx
0040284E  .  8945 FC      mov dword ptr ss:[ebp-0x4],eax    blaster9.0040263C
00402851  .  895D 08      mov dword ptr ss:[ebp+0x8],ebx
00402854  .  FF57 04      call dword ptr ds:[edi+0x4]       blaster9.0040263C
00402857  .  8BBF 0403000 mov edi,dword ptr ds:[edi+0x304]  user32.77D2A013
0040285D  .  33F6         xor esi,esi
0040285F  .  53           push ebx
00402860  .  8975 DC      mov dword ptr ss:[ebp-0x24],esi
00402863  .  8975 CC      mov dword ptr ss:[ebp-0x34],esi
00402866  .  8975 BC      mov dword ptr ss:[ebp-0x44],esi
00402869  .  8975 AC      mov dword ptr ss:[ebp-0x54],esi
0040286C  .  8975 A8      mov dword ptr ss:[ebp-0x58],esi
0040286F  .  8975 A4      mov dword ptr ss:[ebp-0x5C],esi
00402872  .  8975 94      mov dword ptr ss:[ebp-0x6C],esi
00402875  .  8975 84      mov dword ptr ss:[ebp-0x7C],esi
00402878  .  89B5 74FFFFF mov dword ptr ss:[ebp-0x8C],esi
0040287E  .  89B5 54FFFFF mov dword ptr ss:[ebp-0xAC],esi
00402884  .  89BD 3CFFFFF mov dword ptr ss:[ebp-0xC4],edi
```

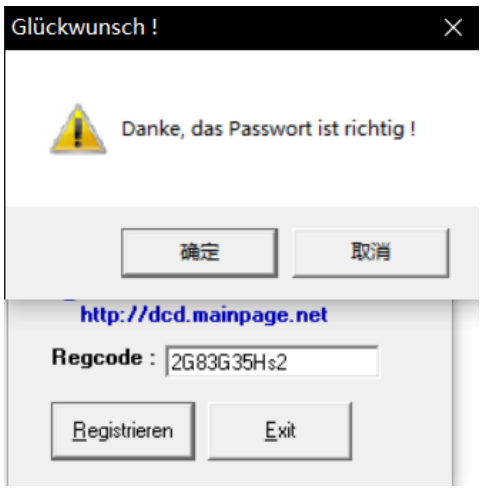
向下查看代码，可以看到有一个比较函数

```
004028BA  >  FF75 A8      push dword ptr ss:[ebp-0x58]
004028BD  .  68 DC1D4000  push blaster9.00401DDC            UNICODE "2G83G35Hs2"
004028C2  .  E8 83E8FFFF  call <jmp.&MSVBVM50.__vbaStrCmp>
```

查看参数，发现其中一个参数正是我们输入的假的注册码

```
0012F408  00401DDC  UNICODE "2G83G35Hs2"
0012F40C  001833BC  UNICODE "12345"
```

那 "2G83G35Hs2" 可能就是真的注册码了



2019-09-17 11:47:51

相关文件在我的 Github：https://github.com/UnreachableLove/160-Crackme/tree/master/Crackme015

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： Crackme014

posted @ 2019-09-17 11:48 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