

随风而逝的白色相簿

博客园

首页

新随笔

联系

订阅

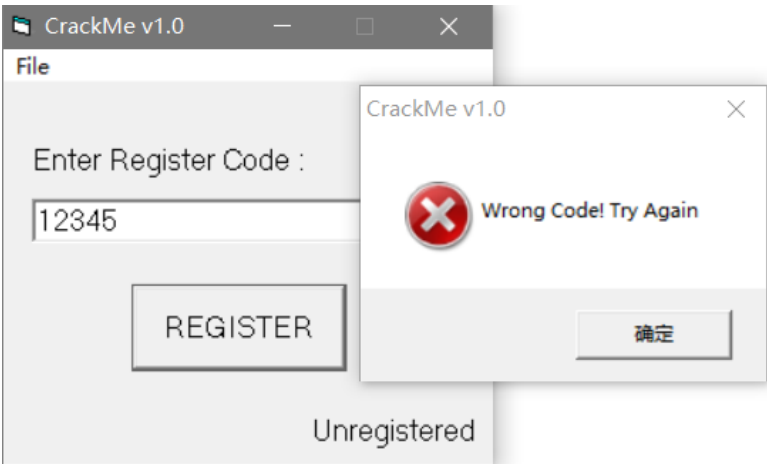
管理

随笔 - 12 文章 - 0 评论 - 1

CrackMe022

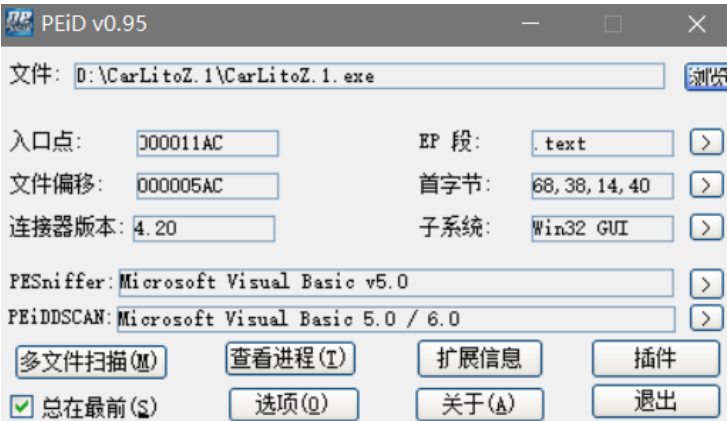
Crackme022 的逆向分析

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。

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	19	20	21
22	23		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(11)

随笔档案

2019年9月(11)
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(6984)
- 0 Crackme007(8)
- 推荐 Crackme009(7)
4. Crackme014(6)

中文搜索引擎		
地址	反汇编	文本字符串
00402B38	push CarLitoZ.00402240	c:\windows\MTR.dat
00402B3B	push CarLitoZ.0040226C	trv2156j0e
00402B3C	push CarLitoZ.00402288	REGISTERED
00402D05	mov dword ptr ss:[ebp-0x74],CarLitoZ.00402288	CrackMe v1.0
00402D07	mov dword ptr ss:[ebp-0x64],CarLitoZ.00402288	Registration Successful
00402E3D	push CarLitoZ.00402240	c:\windows\MTR.dat
00402E54	mov edx,CarLitoZ.0040226C	trv2156j0e
00402E53	push CarLitoZ.00402288	REGISTERED
00402F51	mov dword ptr ss:[ebp-0x64],CarLitoZ.00402288	Wrong Code! Try Again
00403085	push CarLitoZ.00402240	c:\windows\MTR.dat
004030A5	mov edx,CarLitoZ.00402364	oi
0040313A	push CarLitoZ.00402370	Unregistered

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

00402D9A	> 8D4E 34	lea ecx,dword ptr ds:[esi+0x34]	
00402D9D	. 8D55 94	lea edx,dword ptr ss:[ebp-0x6C]	
00402DA0	. 51	push ecx	var18 = 00155DAC
00402DA1	. 52	push edx	var28 = 0012F474
00402DA2	. C745 9C 0100	mov dword ptr ss:[ebp-0x64],0x1	
00402DA9	. C745 94 0280	mov dword ptr ss:[ebp-0x6C],0x8002	
00402DB0	. FF15 6C614000	call dword ptr ds:[<&MSUBUM50. __vbaVarTstEq	__vbaVarTstEq

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

00402D65	. 56	push esi	
00402D66	. 897D E8	mov dword ptr ss:[ebp-0x18],edi	
00402D69	. 897D E4	mov dword ptr ss:[ebp-0x1C],edi	
00402D6C	. 897D D4	mov dword ptr ss:[ebp-0x2C],edi	
00402D6F	. 897D C4	mov dword ptr ss:[ebp-0x3C],edi	
00402D72	. 897D B4	mov dword ptr ss:[ebp-0x4C],edi	
00402D75	. 897D A4	mov dword ptr ss:[ebp-0x5C],edi	
00402D78	. 897D 94	mov dword ptr ss:[ebp-0x6C],edi	
00402D7B	. 897D 84	mov dword ptr ss:[ebp-0x7C],edi	
00402D7E	. FF93 F8060000	call dword ptr ds:[ebx+0x6F8]	CarLitoZ.00401F11
00402D84	. 3BC7	cmp eax,edi	
00402D86	. 7D 12	jge short CarLitoZ.00402D9A	
00402D88	. 68 F8060000	push 0x6F8	
00402D8D	. 68 0C224000	push CarLitoZ.0040220C	
00402D92	. 56	push esi	
00402D93	. 50	push eax	
00402D94	. FF15 34614000	call dword ptr ds:[&MSUBUM50. __vbaHresu	msubum50. __vbaHresultC
00402D9A	> 8D4E 34	lea ecx,dword ptr ds:[esi+0x34]	
00402D9D	. 8D55 94	lea edx,dword ptr ss:[ebp-0x6C]	
00402DA0	. 51	push ecx	var18 = 00155D78
00402DA1	. 52	push edx	var28 = NULL
00402DA2	. C745 9C 0100	mov dword ptr ss:[ebp-0x64],0x1	
00402DA9	. C745 94 0280	mov dword ptr ss:[ebp-0x6C],0x8002	
00402DB0	. FF15 6C614000	call dword ptr ds:[<&MSUBUM50. __vbaVarTstEq	__vbaVarTstEq

断点处就是真正的比较函数所在处。

进入函数里面

00403230	> 55	push ebp	rgr_403230
00403231	. 8BEC	mov ebp,esp	
00403233	. 83EC 0C	sub esp,0xC	
00403236	. 68 66104000	push <jmp.&MSUBUM50. __vbaExceptionHandler>	SE 处理程序安装
0040323B	. 64:AT 000000	mov eax,dword ptr fs:[0]	
00403241	. 50	push eax	
00403242	. 64:8925 0000	mov dword ptr fs:[0],esp	
00403249	. 81EC 54030000	sub esp,0x354	
0040324F	. 8B45 08	mov eax,dword ptr ss:[ebp+0x8]	CarLitoZ.00404A68
00403252	. 53	push ebx	
00403253	. 56	push esi	
00403254	. 57	push edi	
00403255	. 8B08	mov ecx,dword ptr ds:[eax]	
00403257	. 8965 F4	mov dword ptr ss:[ebp-0xC],esp	
0040325A	. 33F6	xor esi,esi	
0040325C	. C745 F8 4010	mov dword ptr ss:[ebp-0x8],CarLitoZ.00404010	
00403263	. 50	push eax	
00403264	. 8975 FC	mov dword ptr ss:[ebp-0x4],esi	
00403267	. 898D 98FCFF	mov dword ptr ss:[ebp-0x368],ecx	
0040326D	. FF51 04	call dword ptr ds:[ecx+0x4]	
00403270	. A1 24404000	mov eax,dword ptr ds:[0x404024]	

在下面才是真正的比较函数

00403886	. 50	push eax	var28 = 0012F1D0
00403887	. FF15 6C614000	call dword ptr ds:[<&MSUBUM50. __vbaVarTstEq	__vbaVarTstEq

评论排行榜

1. Crackme014(1)

0

推荐

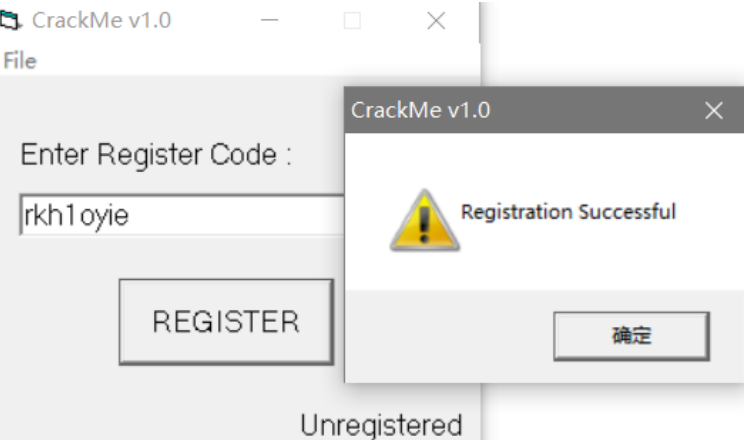
函数的参数

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 68 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 rkhl0yie 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: [Crackme021](#)

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

