

随风而逝的白色相簿

博客园

首页

新随笔

联系

订阅

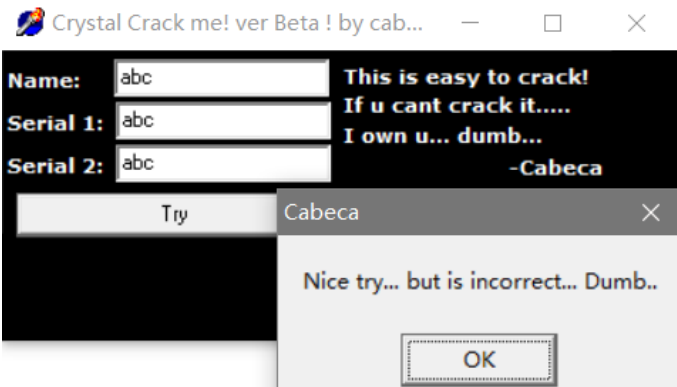
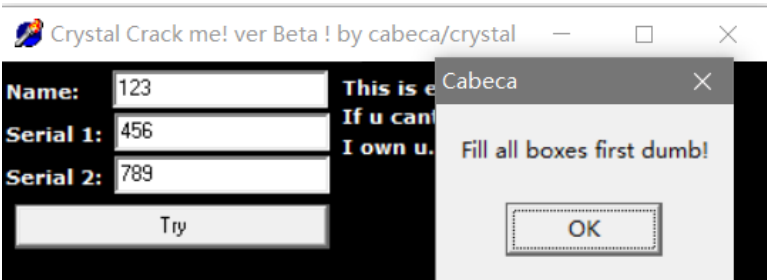
管理

随笔 - 12 文章 - 0 评论 - 1

Crackme021

Crackme021 的逆向分析

1.程序观察



可以看到，name 其实是让输入英文的，输入数字就会出现像图1那样的弹窗。
只有输入英文字母的时候，程序才会真正开始验证输入的是否正确，而且一个用户名是有两个验证码的。

2.简单查壳

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

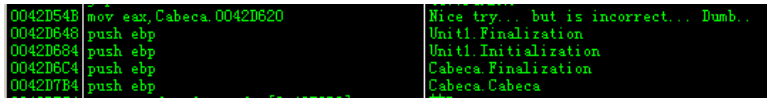
1. PHP一句话木马(6970)
- 0 Crackme007(8)
- 推荐 Crackme009(6)



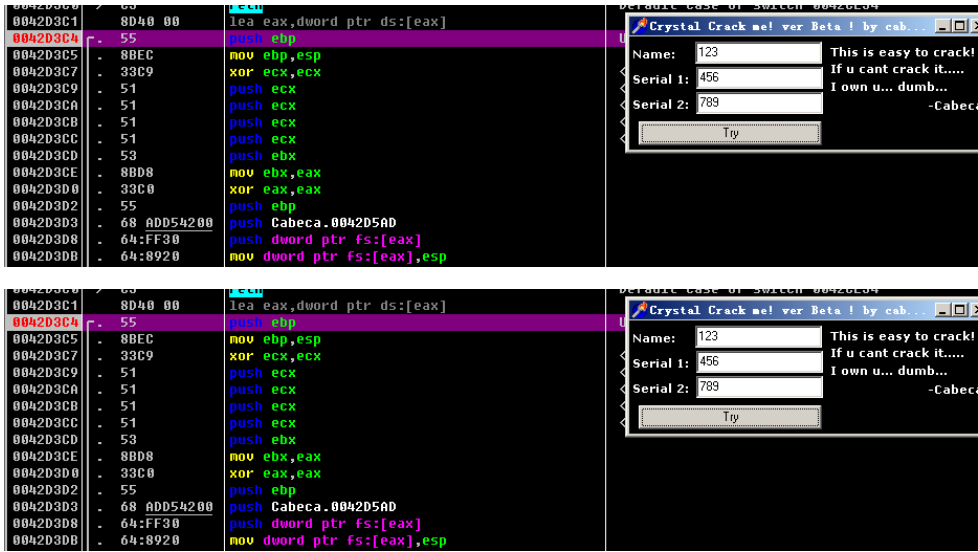
程序使用 Delphi 编写，无壳。

3.程序分析

OD 载入程序，搜索字符串。



进入代码，来到代码块开头，下断点，点击 Try 按钮，程序就断了下来



程序会比较内存42F714和内存42F718处的值，如果是0，就会弹窗报错



0042D3DE	- 833D 14F7420	cmp dword ptr ds:[0x42F714],0x0	内存 42F714 处是否为 0
0042D3E5	74 45	jc short Cabeca.0042D42C	为 0 错误, 跳转
0042D3E7	- 833D 18F7420	cmp dword ptr ds:[0x42F718],0x0	内存 42F718 处是否为 0
0042D3EE	74 3C	jc short Cabeca.0042D42C	为 0 错误, 跳转
0042D3F0	- 8D55 FC	lea edx,[local.1]	
0042D3F3	- 8B83 E001000	mov eax,dword ptr ds:[ebx+0x1E0]	
0042D3F9	- E8 E2C9FEFF	call <Cabeca.Controls.TControl.GetText>	获得 edit1 内容
0042D3FE	- 837D FC 00	cmp [local.1],0x0	
0042D402	74 28	jc short Cabeca.0042D42C	
0042D404	- 8D55 F8	lea edx,[local.2]	
0042D407	- 8B83 E401000	mov eax,dword ptr ds:[ebx+0x1E4]	
0042D40D	- E8 CEC9FEFF	call <Cabeca.Controls.TControl.GetText>	获得 edit2 内容
0042D412	- 837D F8 00	cmp [local.2],0x0	
0042D416	74 14	jc short Cabeca.0042D42C	
0042D418	- 8D55 F4	lea edx,[local.3]	
0042D41B	- 8B83 EC01000	mov eax,dword ptr ds:[ebx+0x1EC]	
0042D421	- E8 BAC9FEFF	call <Cabeca.Controls.TControl.GetText>	获得 edit3 内容
0042D426	- 837D F4 00	cmp [local.3],0x0	
0042D42A	75 44	jnz short Cabeca.0042D470	
0042D42C	> -B8 C4D54200	mov eax,Cabeca.0042D5C4	Fill all boxes first dumb
0042D431	- E8 56F6FFFF	call <Cabeca.Dialogs.ShowMessage>	

如果都不为0, 才会进行接下来的验证程序。

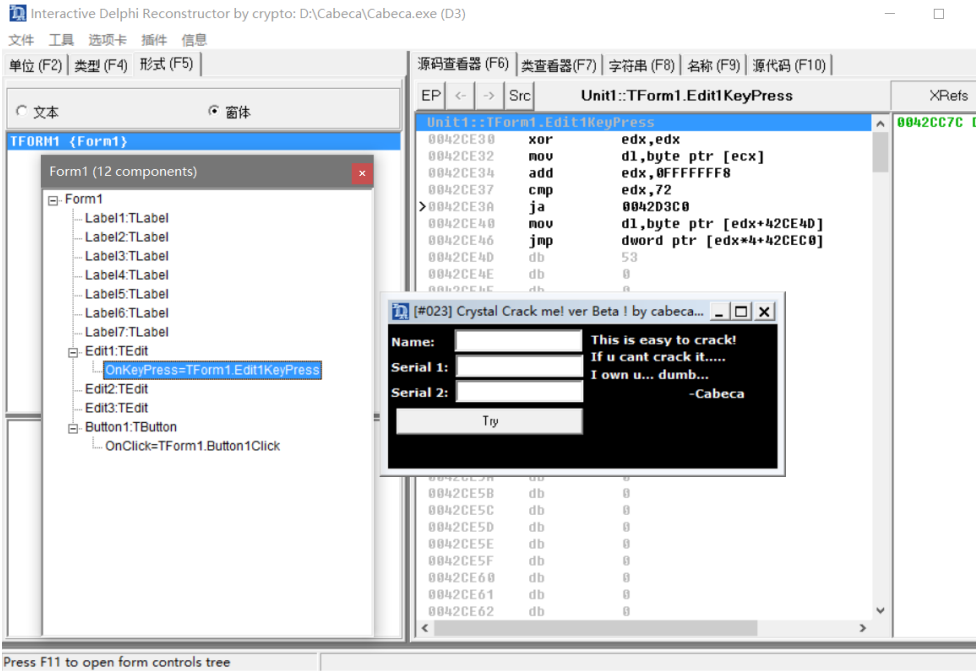
1. 程序获取三个输入框的值, 比较是否为0
2. 再次比较两个内存处的值是否为0
3. 依次将内存 42F714 和内存 42F718 处的值转化为字符串, 再和两个序列号进行比较, 全部相同, 就会提示正确

0042D470	> 833D 14F7420	cmp dword ptr ds:[0x42F714],0x0	
0042D477	74 6C	jc short Cabeca.0042D4E5	
0042D479	- 833D 18F7420	cmp dword ptr ds:[0x42F718],0x0	
0042D480	74 63	jc short Cabeca.0042D4E5	
0042D482	- 8D55 F0	lea edx,[local.4]	
0042D485	- A1 14F74200	mov eax,dword ptr ds:[0x42F714]	将内存 42F714 处的值转换为字符串
0042D48A	- E8 C190DFFF	call <Cabeca.SysUtils.IntToStr>	
0042D49F	- 8B45 F0	mov eax,[local.4]	
0042D4A2	- 59	push eax	
0042D4A3	- 8D55 FC	lea edx,[local.1]	
0042D4A6	- 8B83 E401000	mov eax,dword ptr ds:[ebx+0x1E4]	
0042D4A9C	- E8 3FC9FEFF	call <Cabeca.Controls.TControl.GetText>	得到序列号 1
0042D4B1	- 8B55 FC	mov edx,[local.1]	0012FA98 比较
0042D4B4	- 58	pop eax	
0042D4B5	- E8 2664DFFF	call <Cabeca.System.@LStrCmp>	
0042D4BA	- 75 39	jnz short Cabeca.0042D4E5	
0042D4BC	- 8D55 F0	lea edx,[local.4]	
0042D4BF	- A1 18F74200	mov eax,dword ptr ds:[0x42F718]	将内存 42F718 处的值转换为字符串
0042D4B4	- E8 9790DFFF	call <Cabeca.SysUtils.IntToStr>	
0042D4B9	- 8B45 F0	mov eax,[local.4]	
0042D4BC	- 58	push eax	
0042D4BD	- 8D55 FC	lea edx,[local.1]	
0042D4C0	- 8B83 EC01000	mov eax,dword ptr ds:[ebx+0x1EC]	
0042D4C6	- E8 15C9FEFF	call <Cabeca.Controls.TControl.GetText>	得到序列号 2
0042D4CB	- 8B55 FC	mov edx,[local.1]	0012FA98 比较
0042D4CE	- 58	pop eax	
0042D4CF	- E8 FC63DFFF	call <Cabeca.System.@LStrCmp>	
0042D4D4	- 75 BF	jnz short Cabeca.0042D4E5	
0042D4D6	- 00 E8D54200	mov eax,Cabeca.0042D5E8	Hmmn.... Cracked... Congratulations idiot! :-)
0042D4D0	- E8 AC57FFFF	call <Cabeca.Dialogs.ShowMessage>	跳转到结束
0042D4E0	~ E9 A5000000	jmp Cabeca.0042D580	

那么内存 42F714 和内存 42F718 处的值从哪里来的呢?
其实是在我们输入用户名的时候, 程序就计算出来的。
使用 IDR 载入程序, 可以看到有一个键盘输入事件

0

推荐



0042CE30	- 33D2	xor edx,edx	Unit1.TForm1.Edit1KeyPress
0042CE32	- 8A11	mov dl,byte ptr ds:[ecx]	得到输入的值
0042CE34	- 83C2 F8	add edx,-0x8	Switch (cases 8..7A)
0042CE37	- 83FA 72	cmp edx,0x72	是否小于 z
0042CE3A	- 0F87 8005000	ja Cabeca.0042D3C0	
0042CE40	- 8A92 4DCE420	mov dl,byte ptr ds:[edx*0x42CE40]	
0042CE46	- FF2495 C0CE4	jmp dword ptr ds:[edx*4*0x42CEC0]	Cabeca.0042CF98
0042CE4D	- 35	db 35	分支 0042CEC0 索引表

0042CE30	- 33D2	xor edx,edx	Unit1.TForm1.Edit1KeyPress
0042CE32	- 8A11	mov dl,byte ptr ds:[ecx]	得到输入的值
0042CE34	- 83C2 F8	add edx,-0x8	Switch (cases 8..7A)
0042CE37	- 83FA 72	cmp edx,0x72	是否小于 z
0042CE3A	- 0F87 8005000	ja Cabeca.0042D3C0	
0042CE40	- 8A92 4DCE420	mov dl,byte ptr ds:[edx*0x42CE40]	
0042CE46	- FF2495 C0CE4	jmp dword ptr ds:[edx*4*0x42CEC0]	Cabeca.0042CF98
0042CE4D	- 35	db 35	分支 0042CEC0 索引表

程序会得到输入的字符，然后进行比较，是否为非法字符串，如果是，就跳转走；如果不是，就来到给内存 42F714 和内存 42F718 赋值的地方

0042CF98	> 8105 14F7420	add dword ptr ds:[0x42F714],0x37	Case 61 of switch 0042CE34
0042CFA2	- 8305 18F7420	add dword ptr ds:[0x42F718],0x79	
0042CFA9	- C3	retn	
0042CF9A	> 8105 14F7420	add dword ptr ds:[0x42F714],0x68C	Case 62 of switch 0042CE34
0042CFB4	- 8305 18F7420	add dword ptr ds:[0x42F718],0x6F	
0042CFBB	- C3	retn	
0042CFBC	> 8105 14F7420	add dword ptr ds:[0x42F714],0x491	Case 63 of switch 0042CE34
0042CFD6	- 8105 18F7420	add dword ptr ds:[0x42F718],0x2E2	
0042CFD0	- C3	retn	
0042CFD1	> 8105 14F7420	add dword ptr ds:[0x42F714],0x4740	Case 64 of switch 0042CE34
0042CFD8	- 8105 18F7420	add dword ptr ds:[0x42F718],0x2FA	
0042CFE5	- C3	retn	
0042CFE6	> 8105 14F7420	add dword ptr ds:[0x42F714],0x400	Case 65 of switch 0042CE34
0042CFF0	- 8305 18F7420	add dword ptr ds:[0x42F718],0xE	
0042CFF7	- C3	retn	
0042CFF8	> 8105 14F7420	add dword ptr ds:[0x42F714],0x6D0	Case 66 of switch 0042CE34
0042D002	- 8305 18F7420	add dword ptr ds:[0x42F718],0xD	
0042D009	- C3	retn	
0042D00A	> 8105 14F7420	add dword ptr ds:[0x42F714],0x67D	Case 67 of switch 0042CE34
0042D014	- 8305 18F7420	add dword ptr ds:[0x42F718],0xC	
0042D01B	- C3	retn	
0042D01C	> 8105 14F7420	add dword ptr ds:[0x42F714],0x750	Case 68 of switch 0042CE34
0042D026	- 8305 18F7420	add dword ptr ds:[0x42F718],0xB	
0042D02D	- C3	retn	
0042D02E	> 8105 14F7420	add dword ptr ds:[0x42F714],0x43C	Case 69 of switch 0042CE34
0042D038	- 8305 18F7420	add dword ptr ds:[0x42F718],0x63	
0042D03F	- C3	retn	
0042D040	> 8105 14F7420	add dword ptr ds:[0x42F714],0x764	Case 6A of switch 0042CE34
0042D04A	- 8105 18F7420	add dword ptr ds:[0x42F718],0x378	
0042D054	- C3	retn	
0042D055	> 8105 14F7420	add dword ptr ds:[0x42F714],0xC0	Case 6B of switch 0042CE34
0042D05F	- 8305 18F7420	add dword ptr ds:[0x42F718],0x40	

根据输入不同的字母，给两处内存加上不同的值。
因为程序内有固定的表，所以也不用写注册机了，自己算一算就行了。



相关文件在我的 Github: <https://github.com/UnreachableLove/160-Crackme/tree/master/Crackme021>

2019-09-23 21:55:50

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: [Crackme019](#)







posted @ 2019-09-23 21:56 随风而逝的白色相簿 阅读(3) 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