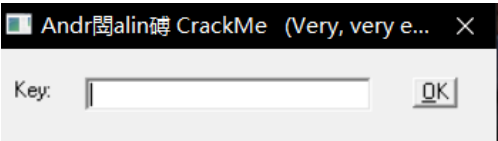


随风而逝的白色相簿

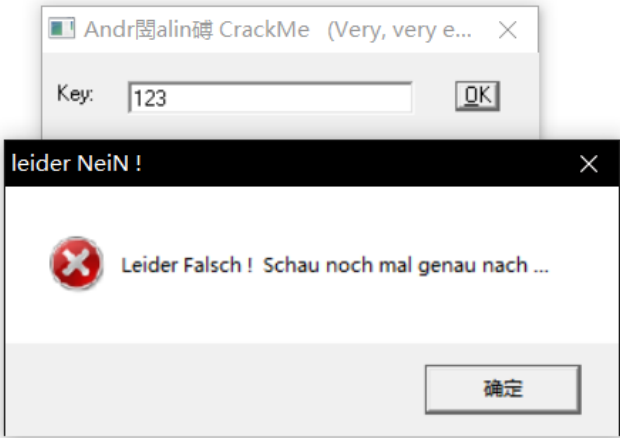
Crackme008

Crackme008 的逆向分析

1.观察程序



只有一个输入 Key 的输入框。
输入 123，点击 OK。



结果出现了奇怪的报错。上面的报错看出来是啥意思。
于是使用百度翻译，结果发现居然是德语。

2.查壳

使用 PEiD 载入。可以看出是使用 VB 编写的程序，没有壳。

公告

昵称： 随风而逝的白色相簿
园龄： 1年8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	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(2)

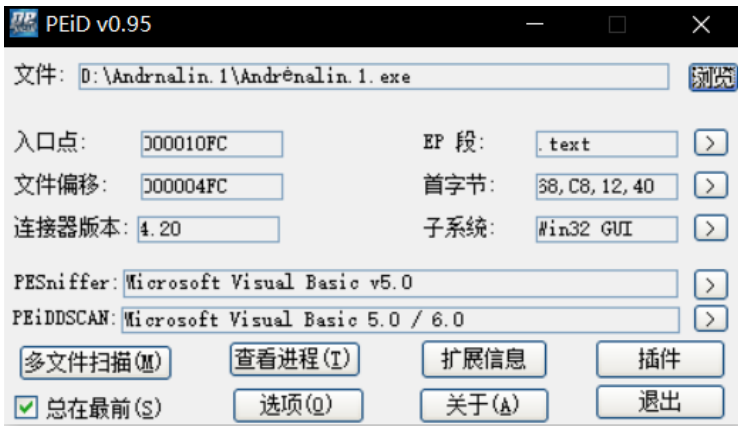
随笔档案

2019年9月(2)
2018年10月(1)

阅读排行榜

1. PHP一句话木马(6349)

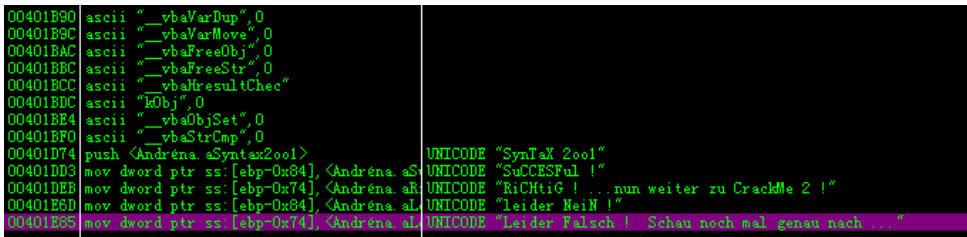




3.分析程序

使用 OD 载入程序。

搜索字符串，发现了报错的字符串，双击进入。

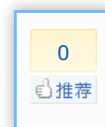


向上查找，发现了一个 `cmp` 和 `je` 语句。再 `cmp` 语句上面，还有一个 `StrCmp` 函数。

000401D6A	FF15 E4304000	call dword ptr ds:[<&MSUBUM50._vbaHres	msvbvm50._vbaHresultCheckObj
000401D70	> 8B4D D8	mov ecx,dword ptr ss:[ebp-0x28]	
000401D73	51	push ecx	
000401D74	68 541A0400	push <Andréna.aSyntax2oo1>	UNICODE "SynTaX 2oo1"
000401D79	FF15 08314000	call dword ptr ds:[<&MSUBUM50._vbaStrC	msvbvm50._vbaStrCmp
000401D7F	8BF8	mov edi,eax	
000401D81	8D4D D8	lea ecx,dword ptr ss:[ebp-0x28]	
000401D84	F7DF	neg edi	
000401D86	1BFF	sbb edi,edi	
000401D88	47	inc edi	
000401D89	F7DF	neg edi	
000401D80	FF15 5C314000	call dword ptr ds:[<&MSUBUM50._vbaFree	msvbvm50._vbaFreeStr
000401D91	8B4D D8	lea ecx,dword ptr ss:[ebp-0x2C]	
000401D94	FF15 6B314000	call dword ptr ds:[<&MSUBUM50._vbaFree	msvbvm50._vbaFreeObj
000401D9A	66:3BFE	cmp di,si	比較处
000401D9D	0F84 A0000000	jc Andréna.000401E43	
000401DA3	FF15 2C314000	call dword ptr ds:[<&MSUBUM50.rtcBeep	msvbvm50.rtcBeep
000401DA9	8B3D 48314000	mov edi,dword ptr ds:[<&MSUBUM50._vbaU	msvbvm50._vbaVarDup
000401DAF	B9 04000280	mov ecx,0x80020004	
000401DB4	894D 9C	mov dword ptr ss:[ebp-0x64],ecx	
000401DB7	B8 0A000000	mov eax,0xA	
000401DBC	894D AC	mov dword ptr ss:[ebp-0x54],ecx	
000401DBF	BB 08000000	mov ebx,0x8	
000401DC4	8D95 74FFFFFF	lea edx,dword ptr ss:[ebp-0x8C]	
000401DCA	8D4D B4	lea ecx,dword ptr ss:[ebp-0x4C]	
000401DCD	8945 94	mov dword ptr ss:[ebp-0x6C],eax	
000401DD0	8945 A4	mov dword ptr ss:[ebp-0x5C],eax	
000401DD3	C785 7CFFFFFF	mov dword ptr ss:[ebp-0x84],<Andréna.aS	UNICODE "SuCCeSsFu1 !"
000401DDD	899D 74FFFFFF	mov dword ptr ss:[ebp-0x8C],ebx	
000401DE3	FFD7	call edi	<&MSUBUM50._vbaVarDup>
000401DE5	8D55 84	lea edx,dword ptr ss:[ebp-0x7C]	
000401DE8	8D4D C4	lea ecx,dword ptr ss:[ebp-0x3C]	
000401DEB	C745 8C 701A	mov dword ptr ss:[ebp-0x74],<Andréna.aR	UNICODE "RiChTiG ! ...nun weiter zu CrackMe 2 !
000401DF2	895D 84	mov dword ptr ss:[ebp-0x7C],ebx	
000401DF5	FFD7	call edi	

在 StrCmp 函数处下断点，输入 123，点击 OK。

程序断在了断点处。



00401D70	> 8B4D D8	mov ecx,dword ptr ss:[ebp-0x28]	
00401D73	. 51	push ecx	
00401D74	. 68 541A4000	push <Andréna.aSyntax2001>	Unicode "SynTaX 2001"
00401D79	. FF15 08314000	call dword ptr ds:[&H\$V080H50.vbaStrC	msvbvm50.vbaStrCmp
00401D7E	. 8BF8	mov edi,ecx	

可以看出 StrCmp 函数有两个参数

0012F3FC	00401A54	Unicode "SynTaX 2001"
0012F400	010F06F4	Unicode "123"

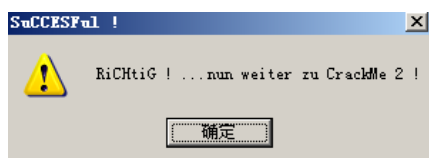
其中有一个是我们输入的 key，难道另一个就是正确的 key？

我们先执行该条指令，可以看到返回值不为 0

```
EAX 00000002
ECX 00000002
EDX 00050000
```

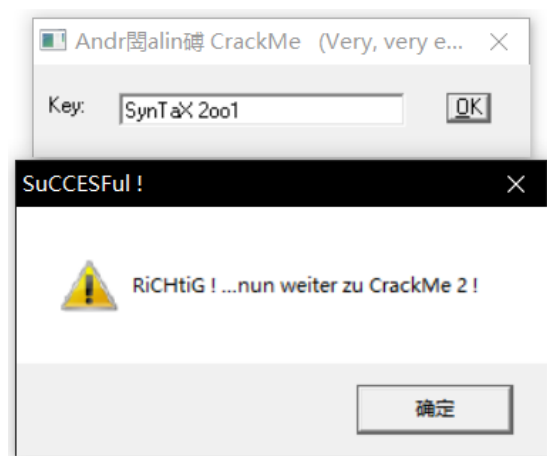
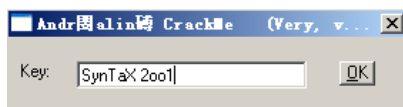
我们修改 EAX 的值为 0，让程序继续运行。

```
EAX 00000000
ECX 00000002
EDX 00050000
```



果然成功了。

接下来我们输入疑似为正确 key 的字符串，运行程序。



果然是正确的 key。

这个程序是一星的，所以很简单。

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: [Crackme007](#)

posted @ 2019-09-08 15:35 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