

# 【reversing.kr逆向之旅】 Music Player的writeup

原创

iqiqiya 于 2018-11-01 16:48:30 发布 400 收藏

分类专栏: [我的逆向之路 -----reversing.kr](#) [我的CTF之路](#) 文章标签: [【reversing.kr逆向之旅】 Music Player reversing.kr Music Player的wri](#) [Music Player的writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xiangshangbashaonian/article/details/83621246>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[-----reversing.kr](#)

11 篇文章 0 订阅

订阅专栏

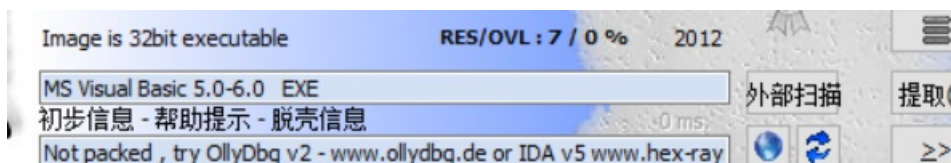


[我的CTF之路](#)

92 篇文章 5 订阅

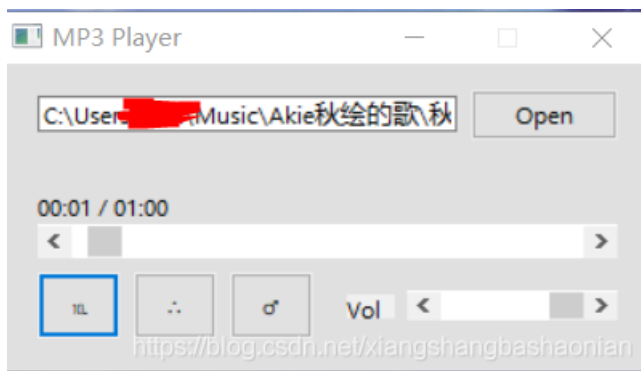
订阅专栏

VB写的程序 且没有加壳



运行看看 还真是一个音乐播放器 但是只能播放一分钟

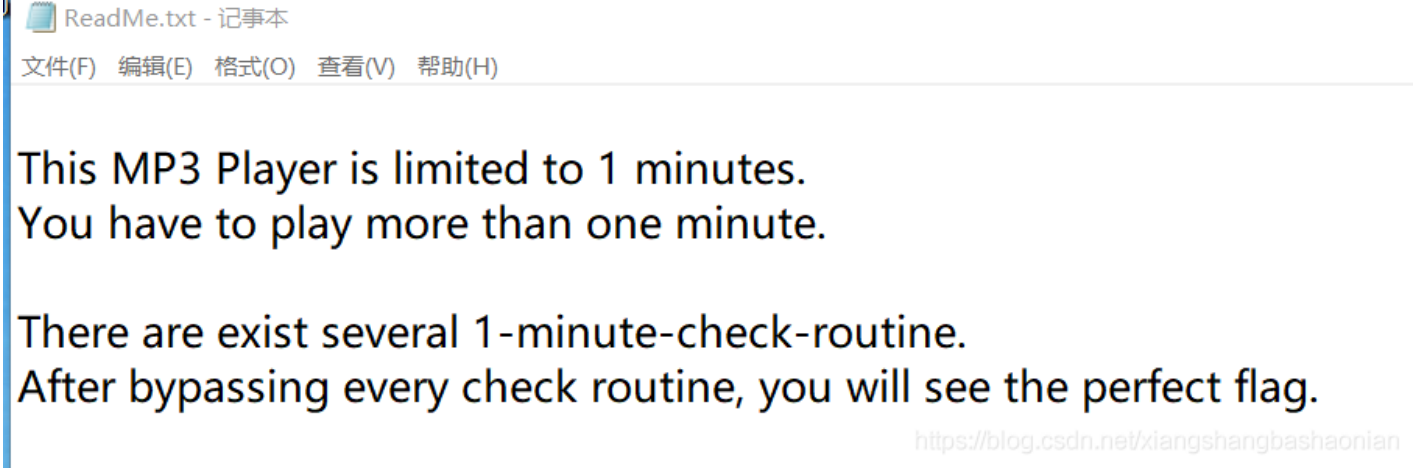
下面三个按钮据我分析 分别就是播放, 暂停, 重新开始播放



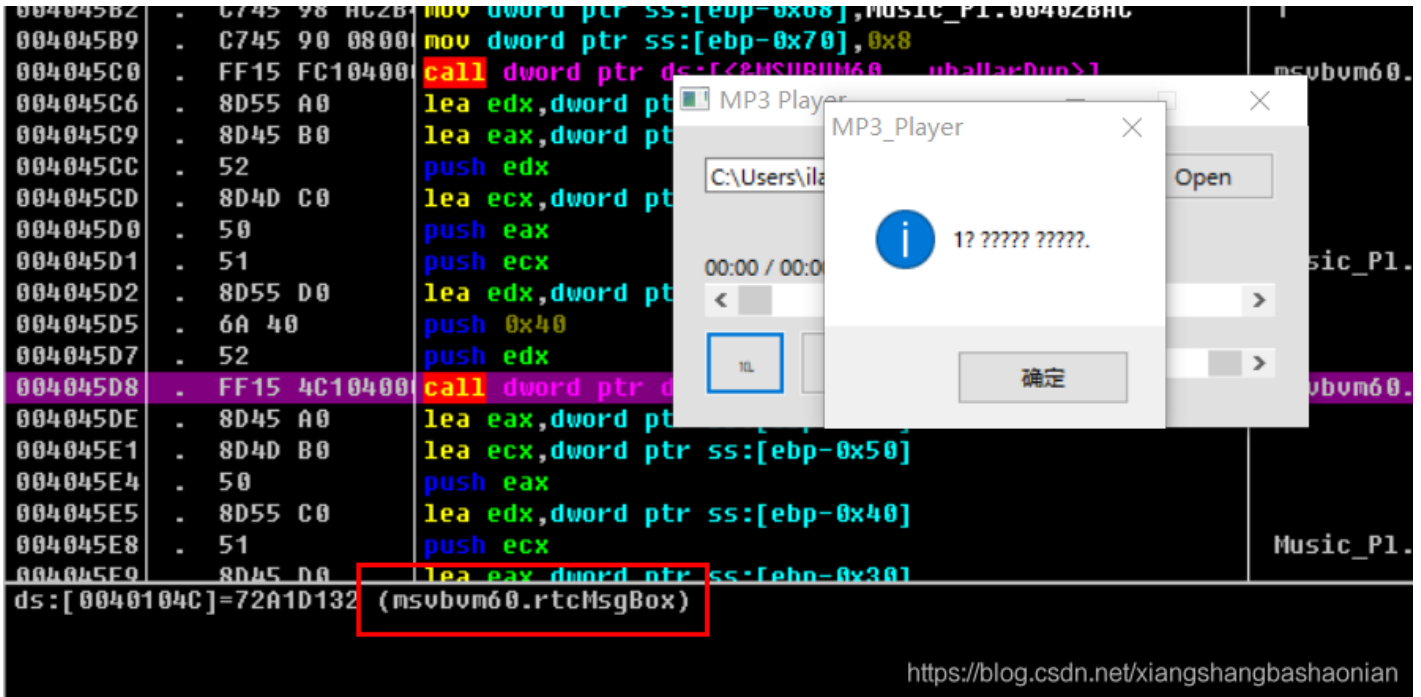
当滑动到1分钟时就会停止 并弹窗1? ??????



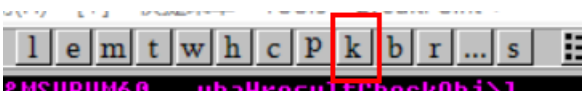
结合ReadMe中所述 必须跳过若干个在1分钟的检查 才可以看到flag



OD载入分析 F9运行 播放到1分钟时弹窗 这时候可以看到程序调用了rtcMsgBox



这时候点击k查看调用堆栈情况 可以看到有调用rtcMsgBox这个API



地址	堆栈	函数过程	调用来自	结构
0019F4DC	745F9004	win32u.NtUserWaitMessage	user32.745F8FFE	0019F518
0019F51C	745F4B0A	user32.745F8F01	user32.745F4B05	0019F518
0019F54C	74658A17	user32.745F4A2B	user32.74658A12	0019F548
0019F620	746578AD	user32.SoftModalMessageBox	user32.7465789B	0019F61C
0019F784	74657FD5	user32.746575F8	user32.74657FD0	0019F780
0019F814	562A2441	包含 apphelp.562A243F	apphelp.562A243F	0019F810
0019F830	562A3273	包含 apphelp.562A2441	apphelp.562A3271	0019F82C
0019F84C	729AF829	包含 apphelp.562A3273	msvbvm60.729AF827	0019F848
0019F86C	729AF6A5	包含 msvbvm60.729AF829	msvbvm60.729AF6A2	0019F868
0019F8B4	729AF9AD	msvbvm60.729AF58B	msvbvm60.729AF99B	0019F8B0
0019F8E4	729A3D68	msvbvm60.729AF90F	msvbvm60.729A3D63	0019F8E0
0019F948	72A1D22E	msvbvm60.729A3ADB	msvbvm60.72A1D229	0019F944
0019F9C0	004045DE	?msvbvm60.rtcMsgBox	Music_P1.https://blog.csdn.net/xiangshangbashaonian	0019F944

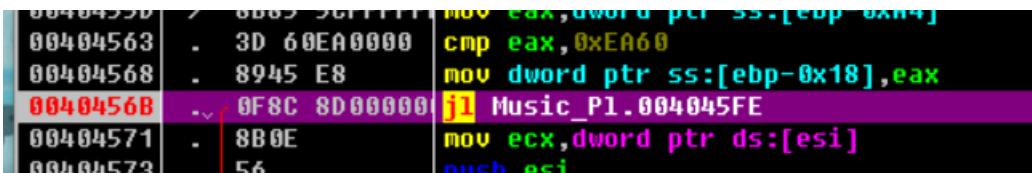
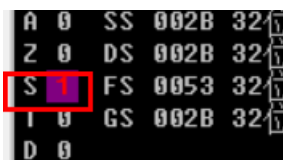
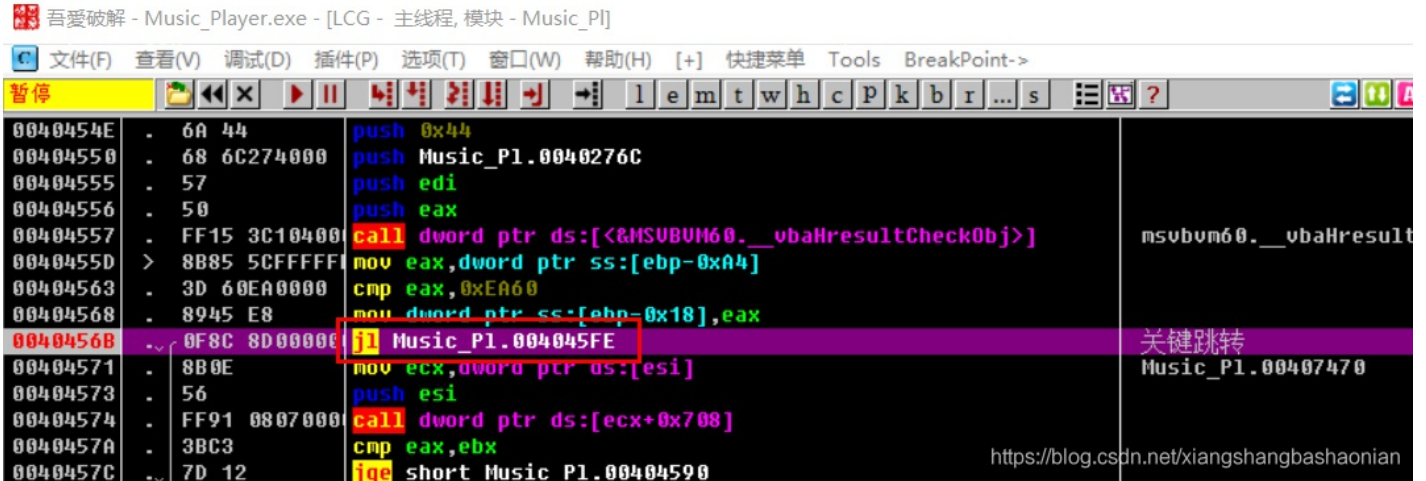
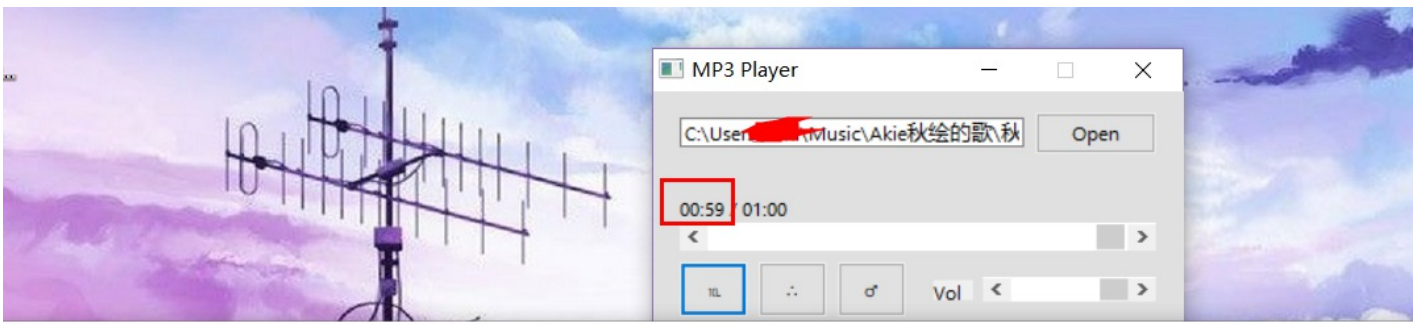
接着右键这一行 查看调用

向上翻 可以很明显发现cmp

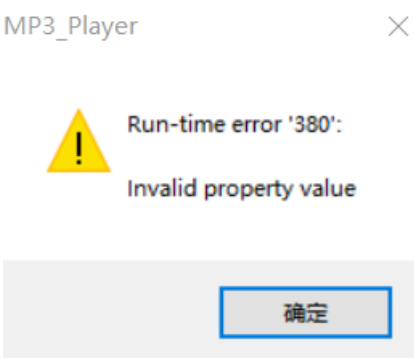
0xEA60 就是60000毫秒 正好就是1分钟 而且这个跳转正好跳过.rtcMsgBox 猜测这个就是关键跳

00404556	- 50	push eax	
00404557	- FF15 3C10400	call dword ptr ds:[&MSUBUM60.__vbaHres	msvbvm60.__vbaHresultCheckObj
0040455D	> 8B85 5CFFFFFF	mov eax,dword ptr ss:[ebp-0xA4]	
00404563	- 3D 60EA0000	cmp eax,0xEA60	
00404568	- 8945 E8	mov dword ptr ss:[ebp-0x18],eax	
0040456B	0F8C 8D000000	jl Music_P1.004045FE	关键跳转
00404571	- 8B0E	mov ecx,dword ptr ds:[esi]	
00404573	- 56	push esi	
00404574	- FF91 0807000	call dword ptr ds:[ecx+0x708]	
0040457A	- 3BC3	cmp eax,ebx	
0040457C	7D 12	jge short Music_P1.00404590	
0040457E	- 68 08070000	push 0x708	
00404583	- 68 C0254000	push Music_P1.004025C0	
00404588	- 56	push esi	
00404589	- 50	push eax	
0040458A	- FF15 3C10400	call dword ptr ds:[&MSUBUM60.__vbaHres	msvbvm60.__vbaHresultCheckObj
00404590	> B9 04000280	mov ecx,0x80020004	
00404595	- B8 0A000000	mov eax,0xA	
00404599	- 8B4D 00	mov dword ptr ss:[ebp-0xF9],eax	https://blog.csdn.net/xiangshangbashaonian

这里的话修改下s标志位 使跳转成立



接着发现还是会报错



也是醉了

猜测下面还有校验判断的地方 重新来一次 这次修改过s标志位后 单步向下 看看到底是何方神圣。。

然后很明显可以看到当经过这个call后 就会弹窗报错

还可以看到上边有一个jge跳转 这时候我们可以把它改为jmp 或者再次修改s标志位

```
004046B9 . FF15 3C104000 call dword ptr ds:[&MSVBVM60.__vbaHresultCheckObj] ; msvbvm60.__vbaHr
```

```

0040467C - 50      push eax
0040467D - 8D45 E0  lea eax,dword ptr ss:[ebp-0x20]
00404680 - 50      push eax
00404681 - FF15 48104000 call dword ptr ds:[&MSUBUM60.__vbaObjSet]
00404687 - 8BF8    mov edi,eax
00404689 - 8BCB    mov ecx,ebx
0040468B - 8B17    mov edx,dword ptr ds:[edi]
0040468D - 8995 40FFFFFF mov dword ptr ss:[ebp-0xC0],edx
00404693 - FF15 84104000 call dword ptr ds:[&MSUBUM60.__vbaI2I4]
00404699 - 8B8D 40FFFFFF mov ecx,dword ptr ss:[ebp-0xC0]
0040469F - 50      push eax
004046A0 - 57      push edi
004046A1 - FF91 BC000000 call dword ptr ds:[ecx+0xBC]
004046A7 - 85C0    test eax,eax
004046A9 - DBE2    fcllex
004046AB - 7D 12   jgc short Music_P1.004046BF
004046AD - 68 BC000000 push 0xBC
004046B2 - 68 582B4000 push Music_P1.00402B58
004046B7 - 57      push edi
004046B8 - 50      push eax
004046B9 - FF15 3C104000 call dword ptr ds:[&MSUBUM60.__vbaHresultCheckObj]
004046BF - 8D4D E0  lea ecx,dword ptr ss:[ebp-0x20]
004046C2 - FF15 28114000 call dword ptr ds:[&MSUBUM60.__vbaFreeObj]
004046C8 - 33DB    xor ebx,ebx
004046CA - 8B46 34  mov eax,dword ptr ds:[esi+0x34]
004046CD - 8D7E 34  lea edi,dword ptr ds:[esi+0x34]

```

跳转未实现  
004046BF=Music\_P1.004046BF

https://blog.csdn.net/xiangshangbashaonian

我还是选择修改s标志位(ps:建议直接改成jmp吧)

```

004046A7 - 85C0    test eax,eax
004046A9 - DBE2    fcllex
004046AB - 7D 12   jgc short Music_P1.004046BF
004046AD - 68 BC000000 push 0xBC
004046B2 - 68 582B4000 push Music_P1.00402B58
004046B7 - 57      push edi
004046B8 - 50      push eax
004046B9 - FF15 3C104000 call dword ptr ds:[&MSUBUM60.__vbaHresultCheckObj]
004046BF - 8D4D E0  lea ecx,dword ptr ss:[ebp-0x20]
004046C2 - FF15 28114000 call dword ptr ds:[&MSUBUM60.__vbaFreeObj]

```

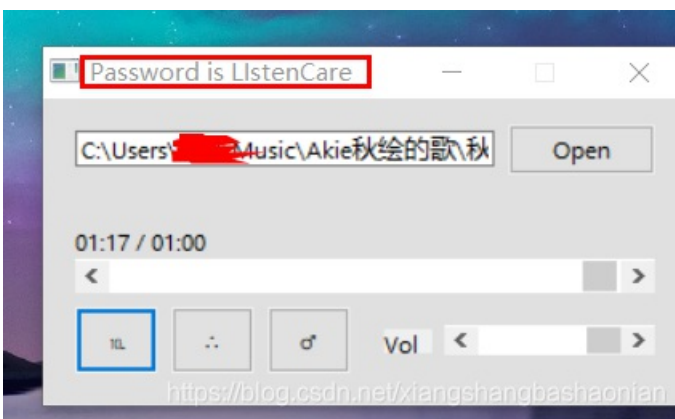
寄存器窗口显示: S FS 0053 32位 222000(FFF)

标题就是flag

ListenCare

我把两处都改成jmp并且保存了一份 哈哈

终于可以安静的听秋绘女神唱歌啦



总结: VB程序中, rtcMsgBox 用于弹出一个消息框,类似于WINDOWS API中的MessageBoxA/MessageBoxExA 函数