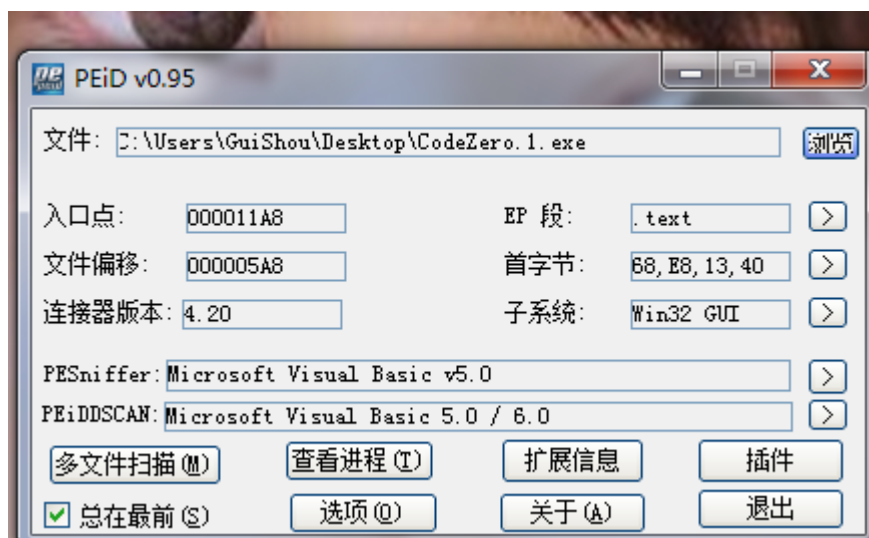


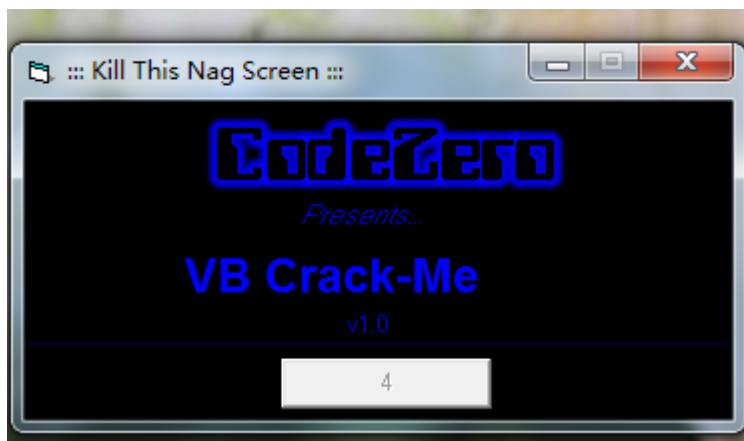
查壳
去Neg
追踪Serial

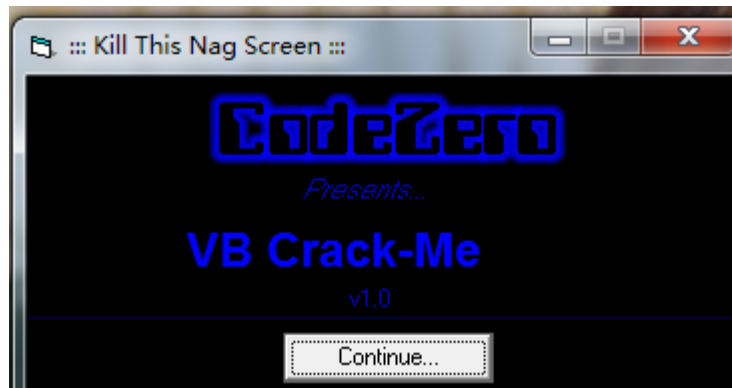
查壳



这个Crackme是VB5写的 没有壳

去Neg

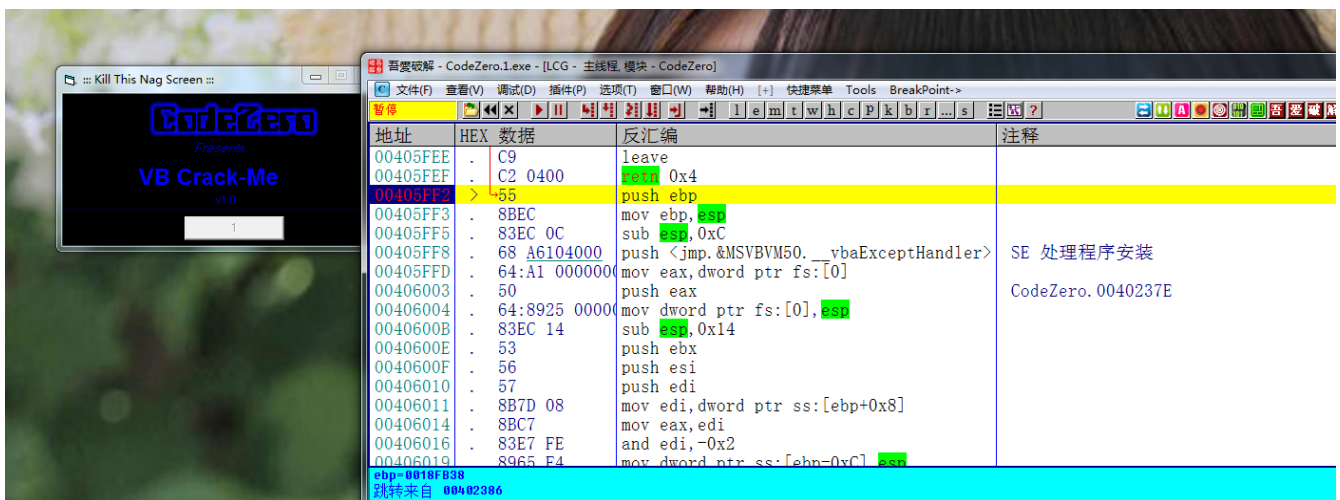




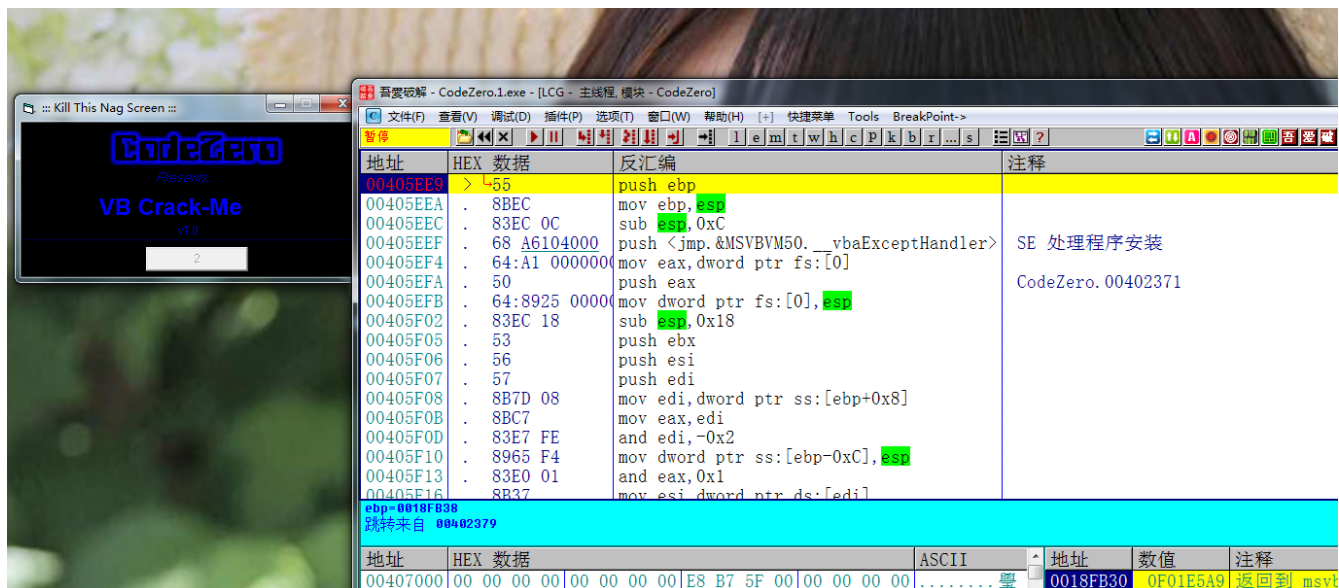
第一个任务就是去除这个倒计时五秒的Neg窗口，去除的思路就是通过字符串的提示向上找到窗体一的加载事件，然后去除

0406032	. 8B86 00030000	mov eax,dword ptr ds:[esi+0x300]	
0406038	. 8365 E8 00	and dword ptr ss:[ebp-0x18],0x0	
040603C	. 57	push edi	
040603D	. FFD0	call eax	CodeZero.00401DA2
040603F	. 50	push eax	CodeZero.00401DA2
0406040	. 8D45 E8	lea eax,dword ptr ss:[ebp-0x18]	
0406043	. 50	push eax	CodeZero.00401DA2
0406044	. E8 17B1FFFF	call <jmp.&MSVBVM50.__vbaObjSet>	
0406049	. 8BD8	mov ebx,eax	CodeZero.00401DA2
040604B	. 68 B0294000	push CodeZero.004029B0	Continue...
0406050	. 53	push ebx	
0406051	. 8B03	mov eax,dword ptr ds:[ebx]	
0406053	. FF50 54	call dword ptr ds:[eax+0x54]	
0406056	. 85C0	test eax,eax	CodeZero.00401DA2
0406058	. 7D 0E	jge short CodeZero.00406068	
040605A	. 6A 54	push 0x54	
040605C	. 68 8C294000	push CodeZero.0040298C	
0406061	. 53	push ebx	

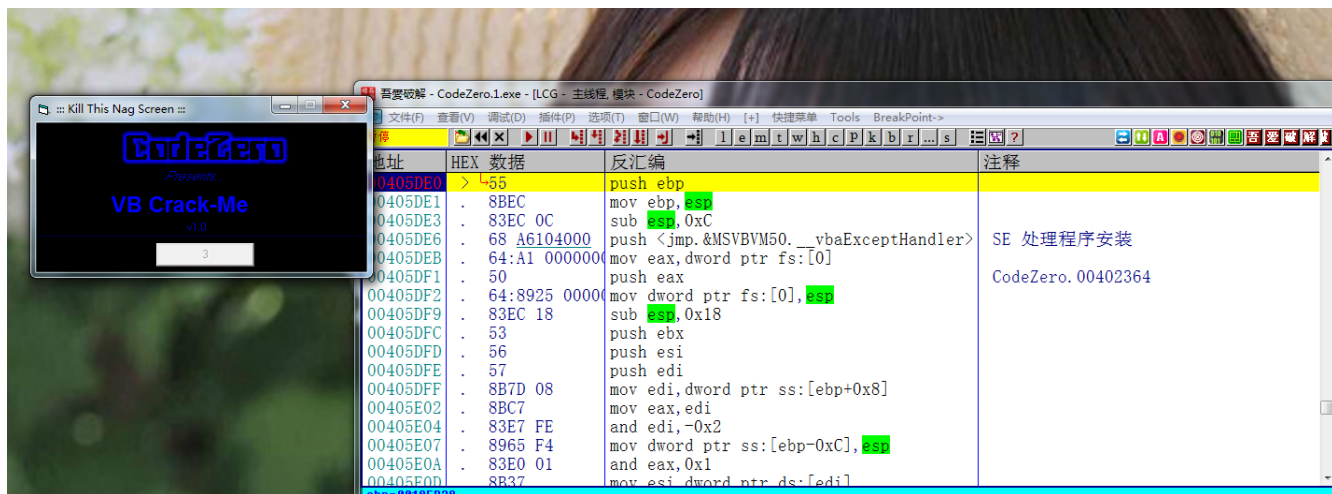
首先来到字符串的提示的地方，向上滚找到函数开头，下断点



程序断下来时倒计时为1秒，窗体加载完成，所以这里肯定不是，所以我们需要继续往上翻，再找到上一个函数，下断点



断下之后，倒计时为2秒，继续往上找函数头，下断点



断下之后，倒计时为3秒，也不是这，但是我们显然已经找到了规律，每经过一个函数，倒计时减一，继续往上找，直到达到这个地方，程序断下时，窗体还没有加载出来

00405900	. 5D	pop eax	MSVBVM50. 0F01E5A9
00405901	. C9	leave	
00405902	. C2 0400	ret 0x4	
00405905	. 55	push ebp	
00405906	. 8BEC	mov ebp, esp	
00405908	. 83EC 0C	sub esp, 0xC	
0040590B	. 68 A6104000	push <jmp.&MSVBVM50. vbaExceptionHandler>	SE 处理程序安装
00405910	. 64:A1 00000000	mov eax, dword ptr fs:[0]	
00405916	. 50	push eax	CodeZero. 00401DA2
00405917	. 64:8925 0000	mov dword ptr fs:[0], esp	
0040591E	. 83EC 10	sub esp, 0x10	
00405921	. 53	push ebx	
00405922	. 56	push esi	
00405923	. 57	push edi	
00405924	. 8B7D 08	mov edi, [arg. 1]	
00405927	. 8BC7	mov eax, edi	
00405929	. 83E7 FE	and edi, -0x2	
0040592C	. 8965 F4	mov [local. 3], esp	

函数尾的位置是ret 0x4

地址	HEX 数据	反汇编	注释
004059A5	. 8B45 08	mov eax,[arg.1]	
004059A8	. 50	push eax	CodeZero.00
004059A9	. 8B08	mov ecx,dword ptr ds:[eax]	
004059AB	. FF51 08	call dword ptr ds:[ecx+0x8]	
004059AE	. 8B4D EC	mov ecx,[local.5]	CodeZero.00
004059B1	. 8B45 FC	mov eax,[local.1]	
004059B4	. 5F	pop edi	msvbvm50.0F
004059B5	. 5E	pop esi	msvbvm50.0F
004059B6	. 64:890D 0000	mov dword ptr fs:[0],ecx	
004059BD	. 5B	pop ebx	msvbvm50.0F
004059BE	. C9	leave	
004059BF	. C2 0400	retn 0x4	

所以只要把函数头的位置修改位retn 0x4，保存文件即可，修改后如下

地址	HEX 数据	反汇编	注释
004058E8	. 8B45 08	mov eax,[arg.1]	
004058EB	. 50	push eax	CodeZero.00402364
004058EC	. 8B08	mov ecx,dword ptr ds:[eax]	
004058EE	. FF51 08	call dword ptr ds:[ecx+0x8]	
004058F1	. 8B4D EC	mov ecx,[local.5]	CodeZero.00401050
004058F4	. 8B45 FC	mov eax,[local.1]	
004058F7	. 5F	pop edi	msvbvm50.0F01E5A9
004058F8	. 5E	pop esi	msvbvm50.0F01E5A9
004058F9	. 64:890D 0000	mov dword ptr fs:[0],ecx	
00405900	. 5B	pop ebx	msvbvm50.0F01E5A9
00405901	. C9	leave	
00405902	. C2 0400	retn 0x4	
00405905	. C2 0400	retn 0x4	
00405908	. 83EC 0C	sub esp,0xC	
0040590B	. 68 A6104000	push <jmp.&MSVBVM50.__vbaExceptionHandler>	SE 处理程序安装
00405910	. 64:A1 00000000	mov eax,dword ptr fs:[0]	
00405916	. 50	push eax	CodeZero.00402364
00405917	. 64:8925 0000	mov dword ptr fs:[0],esp	
0040591E	. 83EC 10	sub esp,0x10	
00405921	. 53	push ebx	
00405922	. 56	push esi	

Neg完美去除

追踪Serial

运行	HEX 数据	反汇编	注释
0040578E	. 8D45 B4	lea eax,dword ptr ss:[ebp-0x4C]	
00405791	. 50	push eax	
00405792	. 8D45 C4	lea eax,dword ptr ss:[ebp-0x3C]	
00405795	. 50	push eax	
00405796	. 6A 40	push 0x40	
00405798	. EB 28	jmp short CodeZero.004057C2	
0040579A	> E8 A3B9FFFF	call <jmp.&MSVBVM50.__vbaVarDup>	
0040579F	. C745 9C 1027	mov dword ptr ss:[ebp-0x64],CodeZero.004057C2	Invalid unlock code, please try again.
004057A6	> 8D55 94	lea edx,dword ptr ss:[ebp-0x6C]	
004057A9	. 8D4D D4	lea ecx,dword ptr ss:[ebp-0x2C]	
004057AC	. 8975 94	mov dword ptr ss:[ebp-0x6C],esi	
004057AF	. E8 8EB9FFFF	call <jmp.&MSVBVM50.__vbaVarDup>	
004057B4	. 8D45 A4	lea eax,dword ptr ss:[ebp-0x5C]	
004057B7	. 50	push eax	
004057B8	. 8D45 B4	lea eax,dword ptr ss:[ebp-0x4C]	
004057BB	. 50	push eax	
004057BC	. 8D45 C4	lea eax,dword ptr ss:[ebp-0x3C]	
004057BF	. 50	push eax	
004057C0	. 6A 10	push 0x10	
004057C2	> 8D45 D4	lea eax,dword ptr ss:[ebp-0x2C]	
004057C5	. 50	push eax	
00401142	< jmp.&MSVBVM50.__vbaVarDup>		
跳转来自 0040576E			

根据字符串提示找到跳转到错误提示的地址，跟进去

地址	HEX 数据	反汇编	注释	寄存器
00405712	. 68 00264000	push CodeZero.00402600		EAX 00000000
00405717	. 56	push esi		ECX 0000000B
00405718	. 50	push eax		EDX 0000000A
00405719	. E8 3CBAFFFF	call <jmp.&MSVBVM50. __vbaHresultCheckOb>		EBX 00000000
0040571E	> FF75 E8	push dword ptr ss:[ebp-0x18]		ESP 0018F374
00405721	. 68 A4264000	push CodeZero.004026A4	55555	EBP 0018F438
00405726	. E8 3BBAFFFF	call <jmp.&MSVBVM50. __vbaStrCmp>		ESI 004761CC
0040572B	. 8BF0	mov esi,eax		EDI 00000000
0040572D	. 8D4D E8	lea ecx,dword ptr ss:[ebp-0x18]		EIP 00405726 CodeZero.004026A4
00405730	. F7DE	neg esi		C 0 ES 002B 32位 0 (FFFFFFFF)
00405732	. 1BF6	sbb esi,esi		P 1 CS 0023 32位 0 (FFFFFFFF)
00405734	. 46	inc esi		A 0 SS 002B 32位 0 (FFFFFFFF)
00405735	. F7DE	neg esi		Z 1 DS 002B 32位 0 (FFFFFFFF)
00405737	. E8 18BAFFFF	call <jmp.&MSVBVM50. __vbaFreeStr>		S 0 FS 0053 32位 7EFD0000
0040573C	. 8D4D E4	lea ecx,dword ptr ss:[ebp-0x1C]		T 0 GS 002B 32位 0 (FFFFFFFF)
0040573F	. E8 0ABAFFFF	call <jmp.&MSVBVM50. __vbaFreeObj>		D 0
00405744	. 6A 0A	push 0xA		O 0 LastErr ERROR_SUCCESS
00405746	. 66:3BF3	cmp si,bx		EFL 00000246 (NO, NB, E, BE, N)
00405749	. 58	pop eax		ST0 empty 0.0
0040574A	. B9 04000280	mov ecx,0x80020004	CodeZero.004026A4	ST1 empty 0.0
0040574F	. 6A 08	push 0x8		ST2 empty 0.0
00405750	. 55	push 0x5		
00405751	. 5A	push 0xA		
00405752	. 59	push 0x9		
00405753	. 58	push 0x8		
00405754	. 57	push 0x7		
00405755	. 56	push 0x6		
00405756	. 55	push 0x5		
00405757	. 54	push 0x4		
00405758	. 53	push 0x3		
00405759	. 52	push 0x2		
0040575A	. 51	push 0x1		
0040575B	. 50	push 0x0		
0040575C	. 4F	push 0xF		
0040575D	. 4E	push 0xE		
0040575E	. 4D	push 0xD		
0040575F	. 4C	push 0xC		
00405760	. 4B	push 0xB		
00405761	. 4A	push 0xA		
00405762	. 49	push 0x9		
00405763	. 48	push 0x8		
00405764	. 47	push 0x7		
00405765	. 46	push 0x6		
00405766	. 45	push 0x5		
00405767	. 44	push 0x4		
00405768	. 43	push 0x3		
00405769	. 42	push 0x2		
0040576A	. 41	push 0x1		
0040576B	. 40	push 0x0		
0040576C	. 3F	push 0xF		
0040576D	. 3E	push 0xE		
0040576E	. 3D	push 0xD		
0040576F	. 3C	push 0xC		
00405770	. 3B	push 0xB		
00405771	. 3A	push 0xA		
00405772	. 39	push 0x9		
00405773	. 38	push 0x8		
00405774	. 37	push 0x7		
00405775	. 36	push 0x6		
00405776	. 35	push 0x5		
00405777	. 34	push 0x4		
00405778	. 33	push 0x3		
00405779	. 32	push 0x2		
0040577A	. 31	push 0x1		
0040577B	. 30	push 0x0		
0040577C	. 2F	push 0xF		
0040577D	. 2E	push 0xE		
0040577E	. 2D	push 0xD		
0040577F	. 2C	push 0xC		
00405780	. 2B	push 0xB		
00405781	. 2A	push 0xA		
00405782	. 29	push 0x9		
00405783	. 28	push 0x8		
00405784	. 27	push 0x7		
00405785	. 26	push 0x6		
00405786	. 25	push 0x5		
00405787	. 24	push 0x4		
00405788	. 23	push 0x3		
00405789	. 22	push 0x2		
0040578A	. 21	push 0x1		
0040578B	. 20	push 0x0		
0040578C	. 1F	push 0xF		
0040578D	. 1E	push 0xE		
0040578E	. 1D	push 0xD		
0040578F	. 1C	push 0xC		
00405790	. 1B	push 0xB		
00405791	. 1A	push 0xA		
00405792	. 19	push 0x9		
00405793	. 18	push 0x8		
00405794	. 17	push 0x7		
00405795	. 16	push 0x6		
00405796	. 15	push 0x5		
00405797	. 14	push 0x4		
00405798	. 13	push 0x3		
00405799	. 12	push 0x2		
0040579A	. 11	push 0x1		
0040579B	. 10	push 0x0		
0040579C	. 0F	push 0xF		
0040579D	. 0E	push 0xE		
0040579E	. 0D	push 0xD		
0040579F	. 0C	push 0xC		
004057A0	. 0B	push 0xB		
004057A1	. 0A	push 0xA		
004057A2	. 09	push 0x9		
004057A3	. 08	push 0x8		
004057A4	. 07	push 0x7		
004057A5	. 06	push 0x6		
004057A6	. 05	push 0x5		
004057A7	. 04	push 0x4		
004057A8	. 03	push 0x3		
004057A9	. 02	push 0x2		
004057AA	. 01	push 0x1		
004057AB	. 00	push 0x0		
004057AC	. 00	push 0x0		
004057AD	. 00	push 0x0		
004057AE	. 00	push 0x0		
004057AF	. 00	push 0x0		
004057B0	. 00	push 0x0		
004057B1	. 00	push 0x0		
004057B2	. 00	push 0x0		
004057B3	. 00	push 0x0		
004057B4	. 00	push 0x0		
004057B5	. 00	push 0x0		
004057B6	. 00	push 0x0		
004057B7	. 00	push 0x0		
004057B8	. 00	push 0x0		
004057B9	. 00	push 0x0		
004057BA	. 00	push 0x0		
004057BB	. 00	push 0x0		
004057BC	. 00	push 0x0		
004057BD	. 00	push 0x0		
004057BE	. 00	push 0x0		
004057BF	. 00	push 0x0		
004057C0	. 00	push 0x0		
004057C1	. 00	push 0x0		
004057C2	. 00	push 0x0		
004057C3	. 00	push 0x0		
004057C4	. 00	push 0x0		
004057C5	. 00	push 0x0		
004057C6	. 00	push 0x0		
004057C7	. 00	push 0x0		
004057C8	. 00	push 0x0		
004057C9	. 00	push 0x0		
004057CA	. 00	push 0x0		
004057CB	. 00	push 0x0		
004057CC	. 00	push 0x0		
004057CD	. 00	push 0x0		
004057CE	. 00	push 0x0		
004057CF	. 00	push 0x0		
004057D0	. 00	push 0x0		
004057D1	. 00	push 0x0		
004057D2	. 00	push 0x0		
004057D3	. 00	push 0x0		
004057D4	. 00	push 0x0		
004057D5	. 00	push 0x0		
004057D6	. 00	push 0x0		
004057D7	. 00	push 0x0		
004057D8	. 00	push 0x0		
004057D9	. 00	push 0x0		
004057DA	. 00	push 0x0		
004057DB	. 00	push 0x0		
004057DC	. 00	push 0x0		
004057DD	. 00	push 0x0		
004057DE	. 00	push 0x0		
004057DF	. 00	push 0x0		
004057E0	. 00	push 0x0		
004057E1	. 00	push 0x0		
004057E2	. 00	push 0x0		
004057E3	. 00	push 0x0		
004057E4	. 00	push 0x0		
004057E5	. 00	push 0x0		
004057E6	. 00	push 0x0		
004057E7	. 00	push 0x0		
004057E8	. 00	push 0x0		
004057E9	. 00	push 0x0		
004057EA	. 00	push 0x0		
004057EB	. 00	push 0x0		
004057EC	. 00	push 0x0		
004057ED	. 00	push 0x0		
004057EE	. 00	push 0x0		
004057EF	. 00	push 0x0		
004057F0	. 00	push 0x0		
004057F1	. 00	push 0x0		
004057F2	. 00	push 0x0		
004057F3	. 00	push 0x0		
004057F4	. 00	push 0x0		
004057F5	. 00	push 0x0		
004057F6	. 00	push 0x0		
004057F7	. 00	push 0x0		
004057F8	. 00	push 0x0		
004057F9	. 00	push 0x0		
004057FA	. 00	push 0x0		
004057FB	. 00	push 0x0		
004057FC	. 00	push 0x0		
004057FD	. 00	push 0x0		
004057FE	. 00	push 0x0		
004057FF	. 00	push 0x0		

找到这个比较函数，下断点，看参数，那么序列号已经很明了，就是55555

地址	反汇编	文本字符串
004056D0	mov dword ptr ss:[ebp-0x74],CodeZero.004026A4	VB Crack-Me 1.0 by CodeZero
004056DF	mov dword ptr ss:[ebp-0x64],CodeZero.004026A4	Please enter the registration code.
00405721	push CodeZero.004026A4	55555
00405726	call <jmp.&MSVBVM50. __vbaStrCmp>	(Initial CPU selection)
0040575E	mov dword ptr ss:[ebp-0x74],CodeZero.004026A4	VB Crack-Me 1.0 by CodeZero
0040577B	mov dword ptr ss:[ebp-0x64],CodeZero.004026A4	Congratulations! you've really made it :-)
0040579F	mov dword ptr ss:[ebp-0x64],CodeZero.004026A4	Invalid unlock code, please try again.
0040604B	push CodeZero.004029B0	Continue...
00406165	mov dword ptr ss:[ebp-0x3C],CodeZero.004026A4	start.exe http://users2.lomag.net/~code/rE/

其实一开始在字符串里就搜到了，只不过不确定而已 哈哈

最后，需要相关文件的可以到我的Github下载：<https://github.com/TonyChen56/160-Crackme>