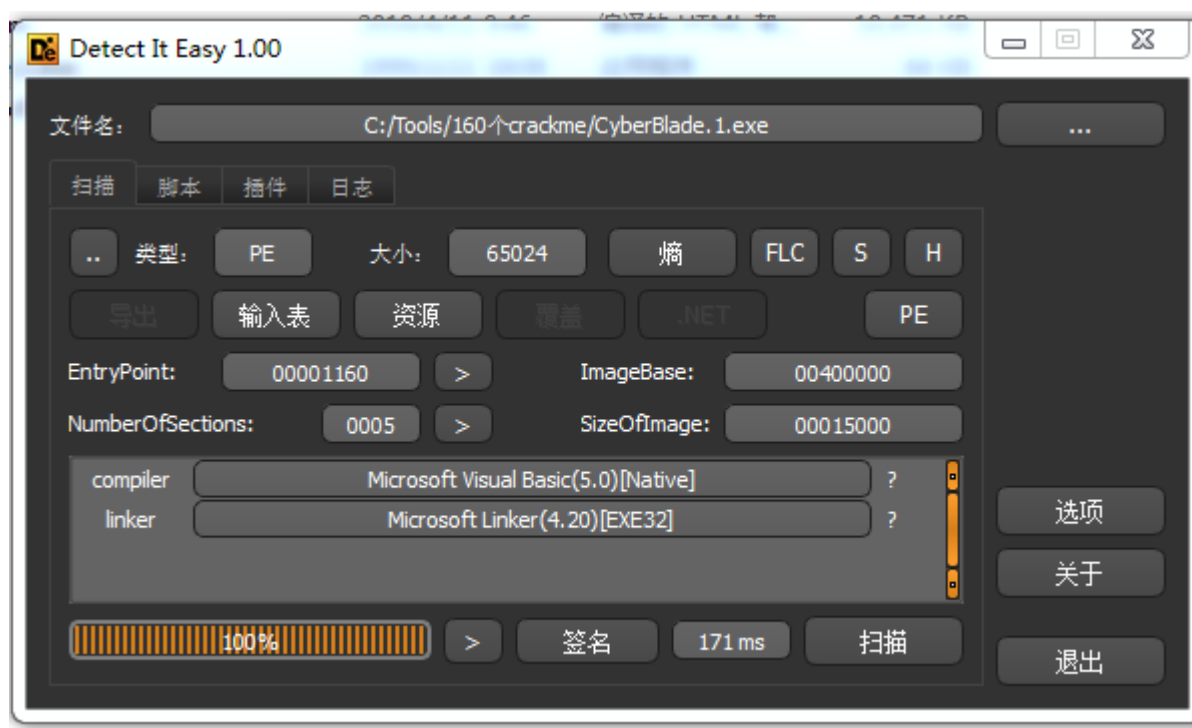


查壳  
分析程序  
验证结果

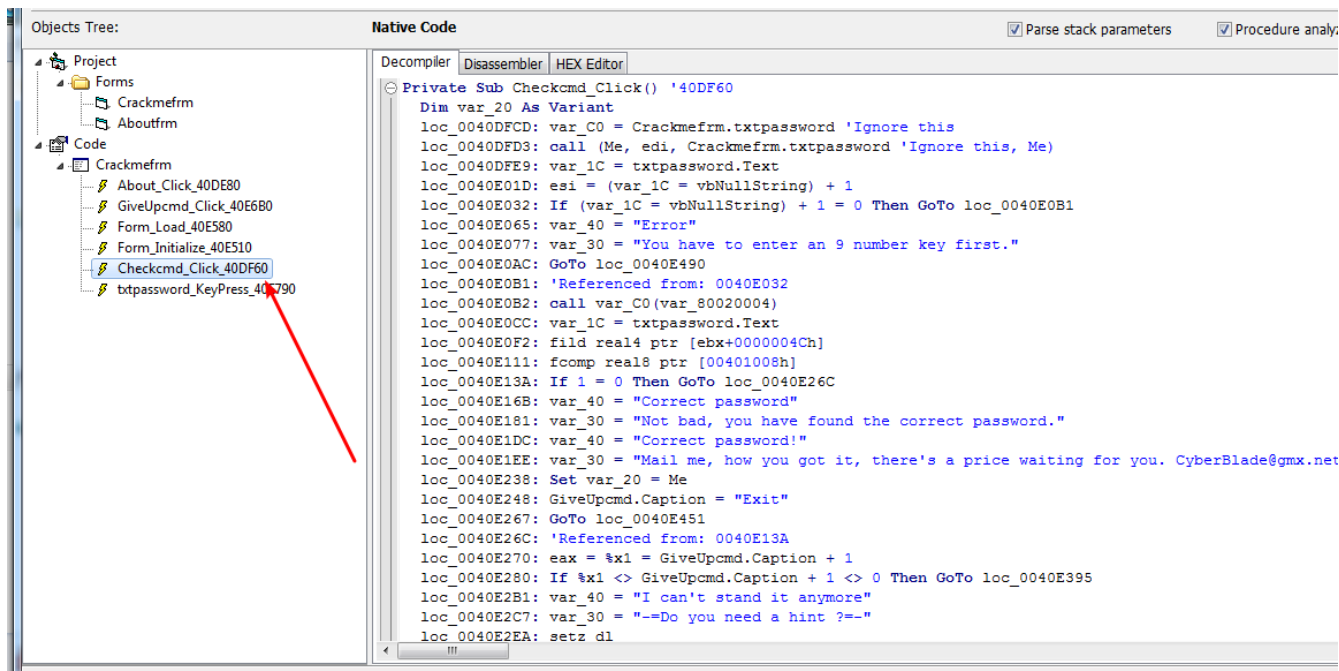
## 查壳



目标程序是用VB N-Code方式编译的，难度为一颗星，采用序列号保护方式

## 分析程序

这个程序的序列号保护方式是有算法的，单纯追踪注册码比较困难，所以直接用VB反编译工具查看按钮点击事件的RVA



直接在40DF60的位置下断点，随便输入一个序列号

地址	HEX 数据	反汇编	注释
0040DF4F	5F	pop edi	
0040DF50	5E	pop esi	
0040DF51	64:890D 000000	mov dword ptr fs:[0],ecx	
0040DF58	5B	pop ebx	
0040DF59	8BE5	mov esp,ebp	
0040DF5B	5D	pop ebp	
0040DF5C	C2 0400	ret 0x4	
0040DF5F	90	nop	
0040DF60	55	push ebp	
0040DF61	8BEC	mov ebp,esp	
0040DF63	83EC 0C	sub esp,0xC	
0040DF66	68 56104000	push <jmp.&MSVBVM50. __vbaB	
0040DF6B	64:A1 00000000	mov eax,dword ptr fs:[0]	
0040DF71	50	push eax	
0040DF72	64:8925 000000	mov dword ptr fs:[0],esp	
0040DF79	81EC B4000000	sub esp,0xB4	
0040DF7F	53	push ebx	
0040DF80	8B5D 08	mov ebx,dword ptr ss:[ebp+8]	
0040DF83	8BC3	mov ecx,ebx	

ebp=0018FF94

Try to find the correct password

About

password: 123456789

Check I give up

Crackme v1.00 written by CyberBlade (CyberBlade@gmx.net)

地址	HEX 数据	反汇编	注释
0040F000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0040F010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0018FF8C	765D33AA		返回到 kernel
0018FF90	7EFDE000		

校验过程如下

地址	HEX 数据	反汇编	注释
0040DFFE	50	push eax	
0040DFFF	FF15 F8104100	call dword ptr ds:[<&MSVBVM50. __vbaHresultCheckObj]	msvbvm50. __vbaHresultCheckObj
0040E005	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]	ecx=Serial
0040E008	51	push ecx	
0040E009	68 4C344000	push CyberBlade.0040344C	
0040E00E	FF15 28114100	call dword ptr ds:[<&MSVBVM50. __vbaStrCmp>]	检测字符串长度
0040E014	8BF0	mov esi,ecx	
0040E016	8D4D E4	lea ecx,dword ptr ss:[ebp-0x1C]	
0040E019	F7DE	neg esi	
0040E01B	1BF6	sbb esi,esi	
0040E01D	46	inc esi	
0040E01E	F7DE	neg esi	
0040E020	FF15 8C114100	call dword ptr ds:[<&MSVBVM50. __vbaFreeStr>]	msvbvm50. __vbaFreeStr
0040E026	8D4D E0	lea ecx,dword ptr ss:[ebp-0x20]	
0040E029	FF15 90114100	call dword ptr ds:[<&MSVBVM50. __vbaFreeObj>]	msvbvm50. __vbaFreeObj

首先检测字符长度是否匹配，不满足则提示错误

0040E039	BB 04000280	mov ebx,0x80020004	
0040E03E	897D A0	mov dword ptr ss:[ebp-0x60],edi	
0040E041	897D B0	mov dword ptr ss:[ebp-0x50],edi	
0040E044	8B3D 78114100	mov edi,dword ptr ds:[<&MSVBVM50. __vbaVarDup>]	msvbvm50. __vbaVarDup
0040E04A	BE 08000000	mov esi,0x8	
0040E04F	8D55 80	lea edx,dword ptr ss:[ebp-0x80]	
0040E052	8D4D C0	lea ecx,dword ptr ss:[ebp-0x40]	
0040E055	895D A8	mov dword ptr ss:[ebp-0x58],ebx	
0040E058	895D B8	mov dword ptr ss:[ebp-0x48],ebx	
0040E05B	C745 88 EC3440	mov dword ptr ss:[ebp-0x78],CyberBla. 004034EC	UNICODE "Error"
0040E062	8975 80	mov dword ptr ss:[ebp-0x80],esi	
0040E065	FFD7	call edi	
0040E067	8D55 90	lea edx,dword ptr ss:[ebp-0x70]	
0040E06A	8D4D D0	lea ecx,dword ptr ss:[ebp-0x30]	
0040E06D	C745 98 943440	mov dword ptr ss:[ebp-0x68],CyberBla. 00403494	UNICODE "You have to enter an 9 number key first."
0040E074	8975 90	mov dword ptr ss:[ebp-0x70],esi	
0040E077	FFD7	call edi	
0040E079	8D55 A0	lea edx,dword ptr ss:[ebp-0x60]	
0040E07C	8D45 B0	lea eax,dword ptr ss:[ebp-0x50]	
0040E07F	52	push edx	
0040E080	8D4D C0	lea ecx,dword ptr ss:[ebp-0x40]	

必须为9个字符

地址	HEX 数据	反汇编	注释	寄存器 (FPU)
0040E0C9	56	push esi		EAX 00000000
0040E0CA	8B16	mov edx,dword ptr ds:[esi]		ECX 2A9848A3
0040E0CC	FF92 A0000000	call dword ptr ds:[edx+0xA0]		EDX 0018F2A4
0040E0D2	3BC7	cmp eax,edi		EBX 005C88B8
0040E0D4	7D 12	ja short CyberBla. 0040E0E8		ESP 0018F364
0040E0D6	68 A0000000	push 0xA0		EBP 0018F438
0040E0DB	68 50344000	push CyberBla. 00403450		ESI 0228E5EC
0040E0E0	56	push esi		EDI 00000000
0040E0E1	50	push eax		EIP 0040E0F2 CyberBla. 0040E0F2
0040E0E2	FF15 F8104100	call dword ptr ds:[<&MSVBVM50. __vbaResultCheckObj>]	msvbvm50. __vbaResultCheckObj	C 0 ES 002B 32位 0 (FFFFFFFF)
0040E0E8	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]		P 1 CS 0023 32位 0 (FFFFFFFF)
0040E0EB	51	push ecx	ecx=Serial	A 0 SS 002B 32位 0 (FFFFFFFF)
0040E0EB	FF15 5C114100	call dword ptr ds:[<&MSVBVM50. __vbaR8Str>]	将序列号转为浮点数	Z 0 DS 002B 32位 0 (FFFFFFFF)
0040E0F2	DB43 4C	fild dword ptr ds:[ebx+0x4C]	将12D1FB78(315751288)转为浮点数	S 0 FS 0053 32位 7EFD0000 (FFF)
0040E0F5	DD9D 38FFFFFF	fistp qword ptr ss:[ebp-0xC8]	将序列号保存到[ebp-0xC8]	T 0 GS 002B 32位 0 (FFFFFFFF)
0040E0F8	DCA5 38FFFFFF	fsub qword ptr ss:[ebp-0xC8]	用序列号减去315751288	D 0
0040E101	DFE0	fstsw ax		O 0 LastErr ERROR_SUCCESS (00000000)
0040E103	A8 0D	test al,0xD		EFL 00000206 (NO, NB, NE, A, NS, PE, GE, G)
0040E105	0F85 EB030000	jnz CyberBla. 0040E4F6		ST0 valid 123456789.000000000000
0040E10B	FF15 14114100	call dword ptr ds:[<&MSVBVM50. __vbaFpR8>]	msvbvm50. __vbaFpR8	ST1 empty 0.0
0040E111	DC1D 08104000	comd word ptr ds:[0x401008]	比较ST0和[0x1008]	ST2 empty 0.0

地址	HEX 数据	ASCII	地址	数值	注释
0040F000	00 00 00 00 00 00 00 00 60 A5 5E 00 00 00 00 00	.....星.	0018F364	0018F444	
0040F010	B8 88 5C 00 00 00 00 00 00 00 00 00 C0 A5 5E 00	.....星.	0018F368	0018F520	
0040F020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	0018F36C	0228E43C	

然后将输入的序列号转为浮点数

地址	HEX 数据	反汇编	注释	寄存器 (FPU)
0040E0C9	56	push esi		EAX 00000000
0040E0CA	8B16	mov edx,dword ptr ds:[esi]		ECX 2A9848A3
0040E0CC	FF92 A0000000	call dword ptr ds:[edx+0xA0]		EDX 0018F2A4
0040E0D2	3BC7	cmp eax,edi		EBX 005C88B8
0040E0D4	7D 12	ja short CyberBla. 0040E0E8		ESP 0018F364
0040E0D6	68 A0000000	push 0xA0		EBP 0018F438
0040E0DB	68 50344000	push CyberBla. 00403450		ESI 0228E5EC
0040E0E0	56	push esi		EDI 00000000
0040E0E1	50	push eax		EIP 0040E0F5 CyberBla. 0040E0F5
0040E0E2	FF15 F8104100	call dword ptr ds:[<&MSVBVM50. __vbaResultCheckObj>]	msvbvm50. __vbaResultCheckObj	C 0 ES 002B 32位 0 (FFFFFFFF)
0040E0E8	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]		P 1 CS 0023 32位 0 (FFFFFFFF)
0040E0EB	51	push ecx	ecx=Serial	A 0 SS 002B 32位 0 (FFFFFFFF)
0040E0EB	FF15 5C114100	call dword ptr ds:[<&MSVBVM50. __vbaR8Str>]	将序列号转为浮点数	Z 0 DS 002B 32位 0 (FFFFFFFF)
0040E0F2	DB43 4C	fild dword ptr ds:[ebx+0x4C]	将12D1FB78(315751288)转为浮点数	S 0 FS 0053 32位 7EFD0000 (FFF)
0040E0F5	DD9D 38FFFFFF	fistp qword ptr ss:[ebp-0xC8]	将序列号保存到[ebp-0xC8]	T 0 GS 002B 32位 0 (FFFFFFFF)
0040E0F8	DCA5 38FFFFFF	fsub qword ptr ss:[ebp-0xC8]	用序列号减去315751288	D 0
0040E101	DFE0	fstsw ax		O 0 LastErr ERROR_SUCCESS (00000000)
0040E103	A8 0D	test al,0xD		EFL 00000206 (NO, NB, NE, A, NS, PE, GE, G)
0040E105	0F85 EB030000	jnz CyberBla. 0040E4F6		ST0 valid 315751288.000000000000
0040E10B	FF15 14114100	call dword ptr ds:[<&MSVBVM50. __vbaFpR8>]	msvbvm50. __vbaFpR8	ST1 valid 123456789.000000000000
0040E111	DC1D 08104000	comd word ptr ds:[0x401008]	比较ST0和[0x1008]	ST2 empty 0.0

地址	HEX 数据	ASCII	地址	数值	注释
005C8904	78 FB D1 12 01 00 00 00 A8 28 40 00 C4 28 40 00	x 1 ... ??.?.	0018F364	0018F444	
005C8914	20 29 40 00 B4 29 40 00 14 2A 40 00 60 2A 40 00	)?.??.??.*?.	0018F368	0018F520	

然后将315751288转为浮点数

Windows 7 x64			
CyberBlade.1.exe - [LCG - 主线程 - 模块 - CyberBla]			
文件(F) 查看(V) 调试(D) 操作(P) 选项(O) 窗口(W) 帮助(H) 快速菜单 Tools BreakPoint->			
地址 HEX 数据 反汇编 注释			
0040E0C9	56	push esi	
0040E0CA	8B16	mov edx,dword ptr ds:[esi]	
0040E0CC	FF92 A0000000	call dword ptr ds:[edx+0xA0]	
0040E0D2	3BC7	cmp eax,edi	
0040E0D4	7D 12	jge short CyberBla.0040E0E8	
0040E0D6	68 A0000000	push 0xA0	
0040E0DB	68 50344000	push CyberBla.00403450	
0040E0E0	56	push esi	
0040E0E1	50	push eax	
0040E0E2	FF15 F8104100	call dword ptr ds:[&MSVBVM50.__vbaHResultCheckObj]	msvbvm50.__vbaHResultCheckObj
0040E0E8	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]	
0040E0EB	51	push ecx	
0040E0EC	FF15 5C114100	call dword ptr ds:[&MSVBVM50.__vbaR8Str]	ecx=Serial
0040E0F2	DB43 4C	fld dword ptr ds:[ebx+0x4C]	将序列号转为浮点数
0040E0F5	DD9D 38FFFFFF	fstp qword ptr ss:[ebp-0xC8]	将12D1FB78(315751288)转为浮点数
0040E0FB	DCA5 38FFFFFF	fsb qword ptr ss:[ebp-0xC8]	将ST0保存到[ebp-0xC8]
0040E101	DFE0	fstsw ax	用序列号减去315751288
0040E103	A8 0D	test al,0xD	
0040E105	0F85 EB030000	jnz CyberBla.0040E4F6	
0040E10B	FF15 14114100	call dword ptr ds:[&MSVBVM50.__vbaFpR8]	msvbvm50.__vbaFpR8
0040E111	DC1D 08104000	fcomp qword ptr ds:[0x401008]	比较ST0和[401008]
地址 64 位双精度			
0018F370	315751288.0000000	1.888888711642293e-307	
0018F380	1.468965947963222e-305	2.121995793929666e-314	
0018F390	1.390671161567079e-309	3.470014837141519e-308	
0018F3A0	1.371260174809881e-19	3.470481676207891e-308	
地址 数值 注释			
0018F364	0018F444		
0018F368	0018F520		
0018F36C	0228E43C		
0018F370	78000000		

接着保存315751288到内存

Windows 7 x64			
CyberBlade.1.exe - [LCG - 主线程 - 模块 - CyberBla]			
文件(F) 查看(V) 调试(D) 操作(P) 选项(O) 窗口(W) 帮助(H) 快速菜单 Tools BreakPoint->			
地址 HEX 数据 反汇编 注释			
0040E0C9	56	push esi	
0040E0CA	8B16	mov edx,dword ptr ds:[esi]	
0040E0CC	FF92 A0000000	call dword ptr ds:[edx+0xA0]	
0040E0D2	3BC7	cmp eax,edi	
0040E0D4	7D 12	jge short CyberBla.0040E0E8	
0040E0D6	68 A0000000	push 0xA0	
0040E0DB	68 50344000	push CyberBla.00403450	
0040E0E0	56	push esi	
0040E0E1	50	push eax	
0040E0E2	FF15 F8104100	call dword ptr ds:[&MSVBVM50.__vbaHResultCheckObj]	msvbvm50.__vbaHResultCheckObj
0040E0E8	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]	
0040E0EB	51	push ecx	
0040E0EC	FF15 5C114100	call dword ptr ds:[&MSVBVM50.__vbaR8Str]	ecx=Serial
0040E0F2	DB43 4C	fld dword ptr ds:[ebx+0x4C]	将序列号转为浮点数
0040E0F5	DD9D 38FFFFFF	fstp qword ptr ss:[ebp-0xC8]	将12D1FB78(315751288)转为浮点数
0040E0FB	DCA5 38FFFFFF	fsb qword ptr ss:[ebp-0xC8]	将ST0保存到[ebp-0xC8]
0040E101	DFE0	fstsw ax	用序列号减去315751288
0040E103	A8 0D	test al,0xD	
0040E105	0F85 EB030000	jnz CyberBla.0040E4F6	
0040E10B	FF15 14114100	call dword ptr ds:[&MSVBVM50.__vbaFpR8]	msvbvm50.__vbaFpR8
0040E111	DC1D 08104000	fcomp qword ptr ds:[0x401008]	比较ST0和[401008]
地址 64 位双精度			
0018F370	315751288.0000000	1.888888711642293e-307	
0018F380	1.468965947963222e-305	2.121995793929666e-314	
0018F390	1.390671161567079e-309	3.470014837141519e-308	
0018F3A0	1.371260174809881e-19	3.470481676207891e-308	
0018F3B0	3.260234866299314e-310	3.47032889250033e-308	
0018F3C0	1.371260176034410e-19	1.742795143119777e-310	
0018F3D0	9.8856038106674e-315	7.639184847474979e-316	
0018F3E0	1.358077306301765e-312	2.121995790965272e-314	
0018F3F0	7.639184848265484e-313	0.0	
0018F400	8.079751945829408e-318	-NaN FFFFFFFF 00000000	
0018F410	0.0	6.764868287148777e-307	
0018F420	3.473155390904499e-308	3.469828103578593e-308	
0018F430	2.124070088030347e-314	2.198752365091618e-236	
地址 数值 注释			
0018F364	0018F444		
0018F368	0018F520		
0018F36C	0228E43C		
0018F370	78000000		
0018F374	41B2D1FB		
0018F378	0F10C358	msvbvm50.0F10C358	
0018F37C	0040FA6C	CyberBla.0040FA6C	
0018F380	00000000		
0018F384	00A4A180	UNICODE "Check"	
0018F388	00000000		
0018F38C	00000001		
0018F390	00000010		
0018F394	00010000		

然后用序列号减去315751288

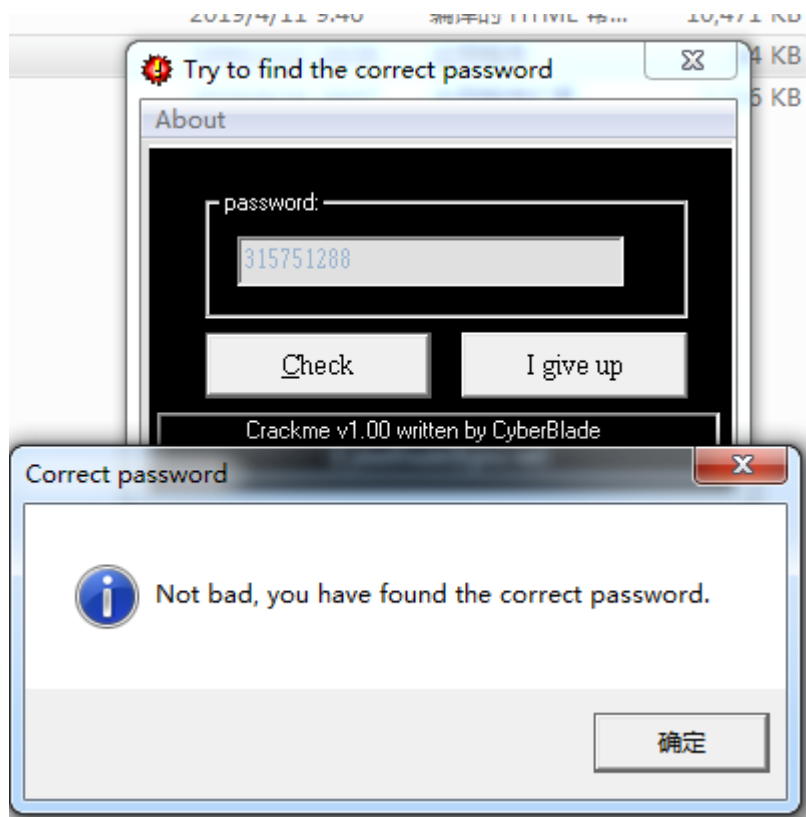
Windows 7 x64			
CyberBlade.1.exe - [LCG - 主线程 - 模块 - CyberBla]			
文件(F) 查看(V) 调试(D) 操作(P) 选项(O) 窗口(W) 帮助(H) 快速菜单 Tools BreakPoint->			
地址 HEX 数据 反汇编 注释			
0040E0D2	3BC7	cmp eax,edi	
0040E0D4	7D 12	jge short CyberBla.0040E0E8	
0040E0D6	68 A0000000	push 0xA0	
0040E0DB	68 50344000	push CyberBla.00403450	
0040E0E0	56	push esi	
0040E0E1	50	push eax	
0040E0E2	FF15 F8104100	call dword ptr ds:[&MSVBVM50.__vbaHResultCheckObj]	msvbvm50.__vbaHResultCheckObj
0040E0E8	8B4D E4	mov ecx,dword ptr ss:[ebp-0x1C]	
0040E0EB	51	push ecx	
0040E0EC	FF15 5C114100	call dword ptr ds:[&MSVBVM50.__vbaR8Str]	ecx=Serial
0040E0F2	DB43 4C	fld dword ptr ds:[ebx+0x4C]	将序列号转为浮点数
0040E0F5	DD9D 38FFFFFF	fstp qword ptr ss:[ebp-0xC8]	将12D1FB78(315751288)转为浮点数
0040E0FB	DCA5 38FFFFFF	fsb qword ptr ss:[ebp-0xC8]	将ST0保存到[ebp-0xC8]
0040E101	DFE0	fstsw ax	用序列号减去315751288
0040E103	A8 0D	test al,0xD	
0040E105	0F85 EB030000	jnz CyberBla.0040E4F6	
0040E10B	FF15 14114100	call dword ptr ds:[&MSVBVM50.__vbaFpR8]	msvbvm50.__vbaFpR8
0040E111	DC1D 08104000	fcomp qword ptr ds:[0x401008]	比较ST0和[401008]
0040E117	DFE0	fstsw ax	
0040E119	F6C4 40	test ah,0x40	
0040E11C	74 05	jbe short CyberBla.0040E123	
地址 64 位双精度			
00401008	0.0	3.000000000000000	
00401018	1.879400744366187e-307	1.879411326612980e-307	
00401028	1.879738566096157e-307	1.88024105465407e-307	
00401038	1.88058566815861e-307	1.880597549785062e-307	
00401048	1.880870863050165e-307	1.144926016128826e-125	
00401058	2.038740815764115e-225	1.898714653011130e-237	
00401068	1.144926015853662e-125	4.260429420441307e-227	
00401078	1.898891103060938e-307	1.144926016025639e-125	
地址 数值 注释			
0018F364	0018F444		
0018F368	0018F520		
0018F36C	0228E43C		
0018F370	78000000		
0018F374	41B2D1FB		
0018F378	0F10C358	msvbvm50.0F10C358	
0018F37C	0040FA6C	CyberBla.0040FA6C	
0018F380	00000000		

将两个数相减的结果和0进行比较，根据比较的结果提示是否正确注册。

结论：注册码很明显就是315751288了。

## 验证结果

输入315751288,



提示正确，破解完成。需要相关文件可以到我的Github下载:

<https://github.com/TonyChen56/160-Crackme>