

查壳
分析程序
验证结果

查壳



这个Crackme跟上一个是同一个作者，VB写的。无，难度一颗星

分析程序

地址	HEX 数据	反汇编	注释	寄存器
005216B9	B8 0A000000	mov eax,0xA		EAX 7764
005216BE	894D AC	mov dword ptr ss:[ebp-0x54],ecx		ECX 0000
005216C1	894D BC	mov dword ptr ss:[ebp-0x44],ecx		EDX 0040
005216C4	894D CC	mov dword ptr ss:[ebp-0x34],ecx		EBX 7FF1
005216C7	8D55 94	lea edx,dword ptr ss:[ebp-0x6C]		ESP 0010
005216CA	8D4D D4	lea ecx,dword ptr ss:[ebp-0x2C]		EBP 0010
005216CD	8945 A4	mov dword ptr ss:[ebp-0x5C],eax	kernel32.BaseThreadInitThunk	ESI 0000
005216D0	8945 B4	mov dword ptr ss:[ebp-0x4C],eax	kernel32.BaseThreadInitThunk	EDI 0000
005216D3	8945 C4	mov dword ptr ss:[ebp-0x3C],eax	kernel32.BaseThreadInitThunk	EIP 0040
005216D6	C745 9C 7C0545	mov dword ptr ss:[ebp-0x64],cupofcof.0040507C	Incorrect password	C 0 ES
005216DD	C745 94 08000000	mov dword ptr ss:[ebp-0x6C],0x8		P 1 CS
005216E4	FF15 38415200	call dword ptr ds:[&MSVBVM50.__vbaVarDups]	msvbvm50.__vbaVarDup	A 0 SS
005216EA	8D55 A4	lea edx,dword ptr ss:[ebp-0x5C]		Z 1 DS
005216ED	8D45 B4	lea eax,dword ptr ss:[ebp-0x4C]		S 0 FS
005216F0	52	push edx	cupofcof.<ModuleEntryPoint>	T 0 GS
005216F1	8D4D C4	lea ecx,dword ptr ss:[ebp-0x3C]		D 0
005216F4	50	push eax	kernel32.BaseThreadInitThunk	O 0 La:
005216F5	51	push ecx		EFL 0000
005216F6	8D55 D4	lea edx,dword ptr ss:[ebp-0x2C]		ST0 emp1
005216F9	6A 10	push 0x10		ST1 emp1
005216FB	52	push edx	cupofcof.<ModuleEntryPoint>	ST2 emp1
0040507C=cupofcof.0040507C (UNICODE "Incorrect password")				
堆栈 ss:[0012FF30]-00000000				

找到这个错误提示之后往上翻，有一个比较函数，下断点等待程序断下之后，观察堆栈

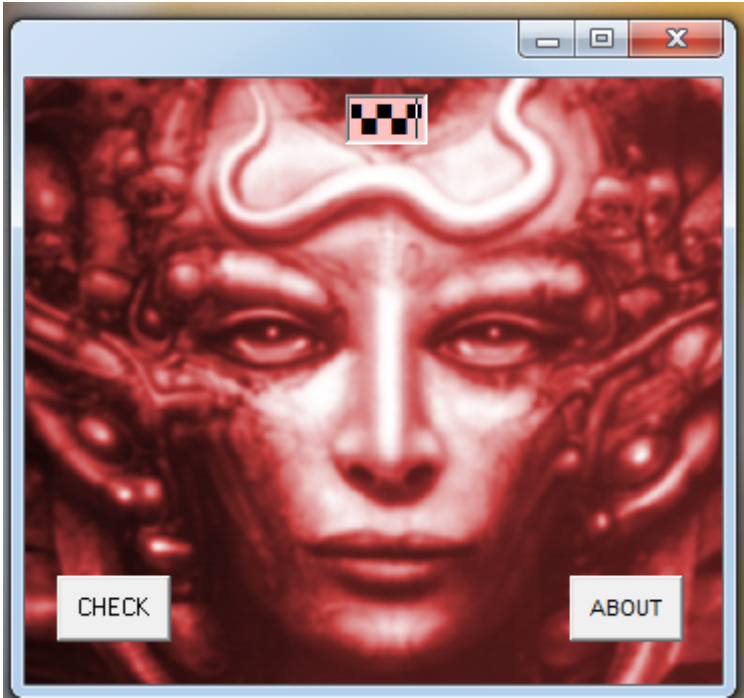
地址	HEX 数据	反汇编	注释	寄存器 (FPU)
00521677	68 4C054500	push cupofcof.0045054C		EAX 00000000
0052167C	56	push esi		ECX 00198754 UNICODE "111111111111"
0052167D	50	push eax		EDX 00000007
0052167E	FF15 D4405200	call dword ptr ds:[&MSVBVM50.__vbaFreeStr]	msvbvm50.__vbaFreeStrCmp	EBX 005231CC cupofcof.005231CC
00521684	8B4D E8	mov ecx,dword ptr ss:[ebp-0x18]		ESP 0012F3B0
00521687	51	push ecx		EBP 0012F474
00521688	68 60054500	push cupofcof.00450560		ESI 01495544
0052168B	FF15 F8405200	call dword ptr ds:[&MSVBVM50.__vbaFreeStr]	msvbvm50.__vbaFreeObj	EDI 00000000
00521693	8BF0	mov esi,eax		EIP 0052168D cupofcof.0052168D
00521695	8D4D E8	lea ecx,dword ptr ss:[ebp-0x18]		C 0 ES 0023 32位 0(FFFFFFFF)
00521698	F7DE	neg esi		P 1 CS 001B 32位 0(FFFFFFFF)
0052169A	1BF6	sbb esi,esi		A 0 SS 0023 32位 0(FFFFFFFF)
0052169C	F7DE	neg esi		Z 1 DS 0023 32位 0(FFFFFFFF)
0052169E	F7DE	neg esi		S 0 FS 003B 32位 7FFDF000(FFF)
005216A0	FF15 4C415200	call dword ptr ds:[&MSVBVM50.__vbaFreeStr]	msvbvm50.__vbaFreeObj	T 0 GS 0000 NULL
005216A6	8D4D E4	lea ecx,dword ptr ss:[ebp-0x1C]		D 0
005216A9	FF15 50415200	call dword ptr ds:[&MSVBVM50.__vbaFreeStr]	msvbvm50.__vbaFreeObj	O 0 LastErr ERROR_SUCCESS (00000000)
005216AF	66:3BF7	cmp si,di		EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE)
005216B2	74 6E	je short cupofcof.00521722		ST0 empty 0.0
005216B4	B9 04000280	mov ecx,0x80020004		ST1 empty 0.0
005216B9	B8 0A000000	mov eax,0xA		ST2 empty 0.0
ds:[00524150]=BF 01DC7F (msvbvm50.__vbaFreeObj)				

地址	HEX 数据	ASCII	地址	数值	注释
00450560	2E 00 2E 00 2E 00 2E 00 2E 00 2E 00 2E 00	0012F3B0	00450560	UNICODE "....."
00450570	2E 00 2E 00 00 00 00 00 24 00 00 00 49 00 6E 00\$.I.n.	0012F3B4	00198754	UNICODE "111111111111"
00450580	63 00 6F 00 72 00 72 00 65 00 63 00 74 00 20 00	c.o.r.r.e.c.t.	0012F3B8	0012F480	
00450590	70 00 61 00 73 00 73 00 77 00 6F 00 72 00 64 00	p.a.s.s.w.o.r.d.	0012F3BC	0012F55C	UNICODE "1"
004505A0	00 00 00 00 27 F6 04 EF A7 41 D3 11 A7 8D CF 4D	...'?按A? 蜥	0012F3C0	01495354	
004505B0	F1 08 27 07 3D F7 04 EF A7 41 D3 11 A7 8D CF 4D	?*=?按A? 蜥	0012F3C4	FFFFFFFF	
004505C0	F1 08 27 07 26 F6 04 EF A7 41 D3 11 A7 8D CF 4D	?*&?按A? 蜥	0012F3C8	0012F408	
004505D0	F1 08 27 07 3C F7 04 EF A7 41 D3 11 A7 8D CF 4D	?*<?按A? 蜥	0012F3CC	779056D9	返回到 user32.779056D9 来自 lpk.LpkDrawTextEx
004505E0	F1 08 27 07 0C 00 00 00 00 00 00 00 00 00 00	?*...@.....	0012F3D0	7701217B	shell32.7701217B
004505F0	2B F6 04 EF A7 41 D3 11 A7 8D CF 4D F1 08 27 07	+?按A? 蜥?*	0012F3D4	00000000	

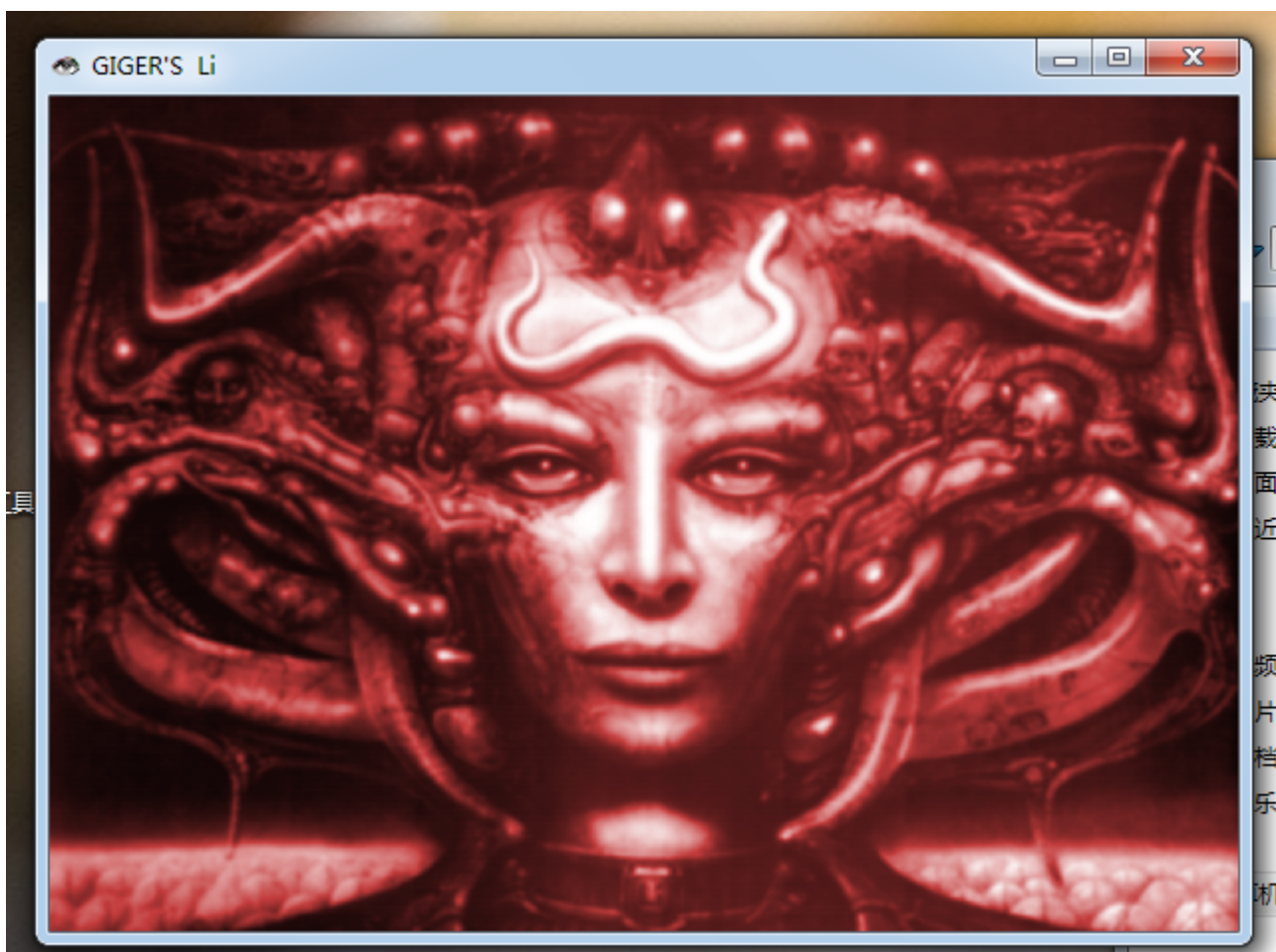
序号号还是十个点，跟上一个一样。只不过程序换了个界面而已

验证结果

输入英文状态下的十个点



点击CHECK



图片变大，破解完成

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