

随风而逝的白色相簿

博客园

首页

新随笔

联系

订阅

管理

随笔 - 6 文章 - 0 评论 - 0

CrackMe011

Crackme011 的逆向分析

1.程序观察

CrackMe No.4 by Andr閤alin...Good Luck !

Serial: 123

123

456789*0#<-

Status: UNREGISTRIERT

If you should fail, ask me on Efnet #cug

可以看到，程序只有让输入的地方，没有确认按钮什么的。
在程序左侧，写着 Status: UNREGISTRIERT。

- 猜想：
1. 程序会根据输入框的变化事件来判断是否正确（其实是不正确的，到后面就知道了）。
 2. 输入正确的序列号程序旁边的 Status 会改变。

2.简单查壳



使用 VB 编写的程序，没有壳。

3.程序分析

使用 OD 载入程序，搜索字符串。

公告

昵称： 随风而逝的白色相簿
园龄： 1年9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		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

Q

g+

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(6)

随笔档案

2019年9月(6)
2018年10月(1)

阅读排行榜

1. PHP一句话木马(6604)
2. Crackme007(7)

0

推荐

```

00407CFE push <Andréna.aRegistriert> REGISTRIERT
00407FE3 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00407F1B push <Andréna.aRegistriert> REGISTRIERT
00408100 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408138 push <Andréna.aRegistriert> REGISTRIERT
00408111 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408355 push <Andréna.aRegistriert> REGISTRIERT
0040835A mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408572 push <Andréna.aRegistriert> REGISTRIERT
00408575 push <Andréna.aRegistriert> REGISTRIERT
0040878F push <Andréna.aRegistriert> REGISTRIERT
00408974 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
004089AC push <Andréna.aRegistriert> REGISTRIERT
00408B91 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408BC9 push <Andréna.aRegistriert> REGISTRIERT
0040918E mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
004091C3 push <Andréna.aRegistriert> REGISTRIERT
004093A8 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
004093E0 push <Andréna.aRegistriert> REGISTRIERT
004095C5 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
004095FD push <Andréna.aRegistriert> REGISTRIERT
004097E2 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040981A push <Andréna.aRegistriert> REGISTRIERT
004099FF mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00409A37 push <Andréna.aRegistriert> REGISTRIERT
00409C1C mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00409C54 push <Andréna.aRegistriert> REGISTRIERT
00409E39 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00409E71 push <Andréna.aRegistriert> REGISTRIERT
0040A05E mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040A08E push <Andréna.aRegistriert> REGISTRIERT
0040A273 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040A2AB push <Andréna.aRegistriert> REGISTRIERT
0040A490 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040A4C8 push <Andréna.aRegistriert> REGISTRIERT
0040A6AD mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040A6E5 push <Andréna.aRegistriert> REGISTRIERT
0040A8CA mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040A902 push <Andréna.aRegistriert> REGISTRIERT
0040AAE7 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040AB1F push <Andréna.aRegistriert> REGISTRIERT
0040AD04 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040AD3C push <Andréna.aRegistriert> REGISTRIERT
0040AF21 mov dword ptr ss:[ebp-0xAC], <Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
0040AF59 push <Andréna.aRegistriert> REGISTRIERT

```

可以看到有很多的很相似的字符串，还有很多个"REGISTRIERT"。

我们也不知道这是什么东西，随便双击一个进入代码。

```

004082C3 - 8D45 B4 lea eax,dword ptr ss:[ebp-0x4C]
004082C6 - 52 push edx
004082C7 - 8D4D B8 lea ecx,dword ptr ss:[ebp-0x48]
004082CA - 50 push eax
004082CB - 51 push ecx
004082CC - 6A 03 push 0x3
004082CE - FF15 9C104000 call dword ptr ds:[<8MSUBUH60.__vbaFreeStrList>]
004082D4 - 8D95 6CFFFFFF lea edx,dword ptr ss:[ebp-0x94]
004082D8 - 8D85 7CFFFFFF lea eax,dword ptr ss:[ebp-0x84]
004082E0 - 52 push edx
004082E1 - 8D4D 8C lea ecx,dword ptr ss:[ebp-0x74]
004082E4 - 50 push eax
004082E5 - 8D55 9C lea edx,dword ptr ss:[ebp-0x64]
004082E8 - 51 push ecx
004082E9 - 52 push edx
004082EA - 6A 04 push 0x4
004082EC - FF15 14104000 call dword ptr ds:[<8MSUBUH60.__vbaFreeVarList>]
004082F2 - 8D4C 24 add esp,0x24
004082F5 - 8D85 C8DFFFFF lea eax,dword ptr ss:[ebp-0x238]
004082F8 - 50 push eax
004082FC - 8D8D D8DFFFFF lea ecx,dword ptr ss:[ebp-0x228]
00408302 - 8D55 DC lea edx,dword ptr ss:[ebp-0x24]
00408305 - 51 push ecx
00408306 - 52 push edx
00408307 - FF15 C8104000 call dword ptr ds:[<8MSUBUH60.__vbaVarForNext>]
0040830D - E9 CFFFFFFF jmp Andréna.004081E1
00408312 - 8D45 CC lea eax,dword ptr ss:[ebp-0x34]
00408315 - 8D8D 4CFFFFFF lea ecx,dword ptr ss:[ebp-0x84]
00408318 - 50 push eax
0040831C - 51 push ecx
0040831D - C785 54FFFFFF mov dword ptr ss:[ebp-0xAC],<Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408327 - C785 4CFFFFFF mov dword ptr ss:[ebp-0x84],0x0000
00408331 - FF15 5C104000 call dword ptr ds:[<8MSUBUH60.__vbaVarForNext>]

```

可以发现，这代码和 009 和 010 非常相像。

都是先求得输入的长度，然后建立循环，最后再进行比较。

但是这里，一个代码块有很多的这样的组合。

这是为什么呢？

我们先在比较函数处下断点。

```

004082F2 - 8D4C 24 add esp,0x24
004082F5 - 8D85 C8DFFFFF lea eax,dword ptr ss:[ebp-0x238]
004082F8 - 50 push eax
004082FC - 8D8D D8DFFFFF lea ecx,dword ptr ss:[ebp-0x228]
00408302 - 8D55 DC lea edx,dword ptr ss:[ebp-0x24]
00408305 - 51 push ecx
00408306 - 52 push edx
00408307 - FF15 C8104000 call dword ptr ds:[<8MSUBUH60.__vbaVarForNext>]
0040830D - E9 CFFFFFFF jmp Andréna.004081E1
00408312 - 8D45 CC lea eax,dword ptr ss:[ebp-0x34]
00408315 - 8D8D 4CFFFFFF lea ecx,dword ptr ss:[ebp-0x84]
00408318 - 50 push eax
0040831C - 51 push ecx
0040831D - C785 54FFFFFF mov dword ptr ss:[ebp-0xAC],<Andréna.a0817E747D7AFF7C7F82836D74RR7A7F7E7B7C7D826D81KE7B7C>
00408327 - C785 4CFFFFFF mov dword ptr ss:[ebp-0x84],0x0000
00408331 - FF15 5C104000 call dword ptr ds:[<8MSUBUH60.__vbaVarForNext>]

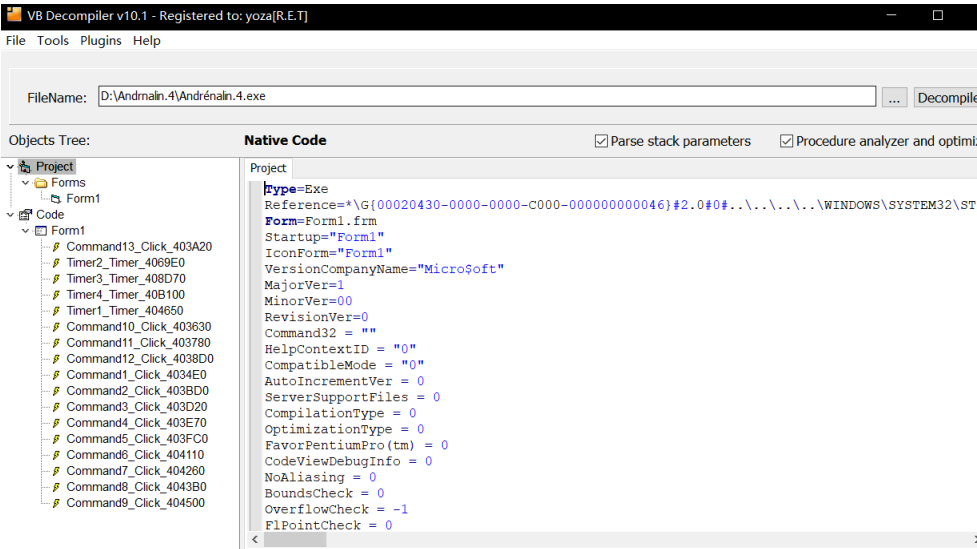
```

我们没有进行任何操作，程序就立刻中断了。

猜想程序可能使用了定时器。我们使用 VB Decompiler 加载程序

0

推荐



可以看到有4个定时器。

每个定时器代码块，里面都是很多个上面那样的代码。

0040B100	> 55	push esp	时钟4
0040B101	. 8BEC	mov ebp,esp	
0040B103	. 83EC 0C	sub esp,0xC	
0040B106	. 68 F6114000	push <jmp.&MSUBUM60.__vbaExceptionHandler>	SE 处理程序安装
0040B108	. 64:A1 000000	mov eax,dword ptr fs:[0]	
0040B111	. 50	push eax	
0040B112	. 64:8925 0000	mov dword ptr fs:[0],esp	
0040B119	. 81EC A003000	sub esp,0x3A0	
0040B11F	. 53	push ebx	msubum60.rtcLeftCharVar
0040B120	. 56	push esi	msubum60.__vbaStrVarUa1
0040B121	. 57	push edi	msubum60.__vbaVarMove
0040B122	. 8965 F4	mov dword ptr ss:[ebp-0xC],esp	
0040B125	. C745 F8 E011	mov dword ptr ss:[ebp-0x8],Andréna.0040	
0040B12C	. 8B7D 08	mov edi,dword ptr ss:[ebp+0x8]	
0040B12F	. 8BC7	mov eax,edi	msubum60.__vbaVarMove
0040B131	. 83E0 01	and eax,0x1	
0040B134	. 8945 FC	mov dword ptr ss:[ebp-0x4],eax	
0040B137	. 83E7 FE	and edi,-0x2	
0040B13A	. 57	push edi	msubum60.__vbaVarMove
0040B13B	. 897D 08	mov dword ptr ss:[ebp+0x8],edi	msubum60.__vbaVarMove
0040B13E	. 8B0F	mov ecx,dword ptr ds:[edi]	
0040B140	. FF51 04	call dword ptr ds:[ecx+0x4]	
0040B143	. 8B17	mov edx,dword ptr ds:[edi]	
0040B145	. 33F6	xor esi,esi	msubum60.__vbaStrVarUa1
0040B147	. 57	push edi	msubum60.__vbaVarMove
0040B148	. 8975 DC	mov dword ptr ss:[ebp-0x24],esi	msubum60.__vbaStrVarUa1
0040B14B	. 8975 CC	mov dword ptr ss:[ebp-0x34],esi	msubum60.__vbaStrVarUa1
0040B14E	. 8975 BC	mov dword ptr ss:[ebp-0x44],esi	msubum60.__vbaStrVarUa1

0040B398	. 8D45 BC	lea eax,dword ptr ss:[ebp-0x44]	
0040B39B	. 52	push edx	
0040B39C	. 8D4D 9C	lea ecx,dword ptr ss:[ebp-0x64]	
0040B39F	. 50	push eax	
0040B3A0	. 51	push ecx	
0040B3A1	. 89B5 4CFFFFFF	mov dword ptr ss:[ebp-0x84],esi	
0040B3A7	. 89B5 3CFFFFFF	mov dword ptr ss:[ebp-0xC4],esi	
0040B3AD	. FF15 30104000	call dword ptr ds:[<&MSUBUM60.__vbaLenU	
0040B3B3	. 50	push eax	
0040B3B4	. 8D95 3CFFFFFF	lea edx,dword ptr ss:[ebp-0xC4]	
0040B3BA	. 8D85 08FFFFFF	lea eax,dword ptr ss:[ebp-0xF8]	
0040B3C0	. 52	push edx	
0040B3C1	. 8D8D 18FFFFFF	lea ecx,dword ptr ss:[ebp-0xE8]	
0040B3C7	. 50	push eax	
0040B3C8	. 8D55 DC	lea edx,dword ptr ss:[ebp-0x24]	
0040B3CB	. 51	push ecx	
0040B3CC	. 52	push edx	
0040B3CD	. FF15 30104000	call dword ptr ds:[<&MSUBUM60.__vbaVarF	
0040B3D3	. 8B35 80104000	mov esi,dword ptr ds:[<&MSUBUM60.__vbaS	
0040B3D9	. 8B1D B4104000	mov ebx,dword ptr ds:[<&MSUBUM60.WrtcLe	
0040B3DF	> 85C0	test eax,eax	
0040B3E1	~ 0F84 29010000	je Andréna.0040B510	
0040B3E7	. 8D45 BC	lea eax,dword ptr ss:[ebp-0x44]	
0040B3EA	. 6A 01	push 0x1	
0040B3EC	. 8D4D 8C	lea ecx,dword ptr ss:[ebp-0x74]	
0040B3EF	. 50	push eax	
0040B3F0	. 51	push ecx	
0040B3F1	. FF03	call ebx	msubum60.rtcLeftCharVar
0040B3F3	. 8D55 8C	lea edx,dword ptr ss:[ebp-0x74]	
0040B3F6	. 8D45 B0	lea eax,dword ptr ss:[ebp-0x50]	
0040B3F9	. 52	push edx	
0040B3FA	. 50	push eax	
0040B3FB	. FF06	call esi	msubum60.__vbaStrVarUa1
0040B3FD	. 50	push eax	
0040B3FE	. FF15 08104000	call dword ptr ds:[<&MSUBUM60.WrtcR8Ua1	msubum60.rtcR8Ua1FromBstr
0040B404	. DD0D 34FFFFFF	ret qword ptr ss:[ebp-0xCC]	

先分析程序的算法



00406470	-	8040 BC	lea ecx,dword ptr ss:[ebp-0x44]	Step8 = 0012FB44
0040647C	-	50	push eax	
0040647D	-	8055 9C	lea edx,dword ptr ss:[ebp-0x64]	
00406480	-	51	push ecx	
00406481	-	52	push edx	
00406482	-	FF15 30104000	call dword ptr ds:[&MSUBUM60._vbaLenU]	End8 = 0012FB44
00406488	-	50	push eax	
00406489	-	8085 3CFFFFFF	lea eax,dword ptr ss:[ebp-0xC4]	
0040648F	-	8080 68DFFFF	lea ecx,dword ptr ss:[ebp-0x298]	
00406495	-	50	push eax	
00406496	-	8095 78DFFFF	lea edx,dword ptr ss:[ebp-0x288]	
0040649C	-	51	push ecx	
0040649D	-	80A5 DC	lea eax,dword ptr ss:[ebp-0x24]	
004064A0	-	52	push edx	
004064A1	-	50	push eax	
004064A2	-	FF15 38104000	call dword ptr ds:[&MSUBUM60._vbaVarF]	
004064A8	>	85C0	test eax,edx	
004064AA	-	0F84 29010000	je Andrena.004065D9	
004064B0	-	8040 BC	lea ecx,dword ptr ss:[ebp-0x44]	
004064B3	-	6A 02	push 0x2	取得字符数
004064B5	-	8055 8C	lea edx,dword ptr ss:[ebp-0x74]	
004064B8	-	51	push ecx	
004064B9	-	52	push edx	
004064BA	-	FFD3	call ebx	取左边 2 个字符
004064BC	-	8045 8C	lea eax,dword ptr ss:[ebp-0x74]	
004064BF	-	8040 B0	lea ecx,dword ptr ss:[ebp-0x50]	
004064C2	-	50	push eax	
004064C3	-	51	push ecx	
004064C4	-	FFD6	call esi	
004064C6	-	50	push eax	
004064C7	-	FF15 D8104000	call dword ptr ds:[&MSUBUM60.#rtcR80all	
004064CD	-	DD9D 34FFFFFF	fstp qword ptr ss:[ebp-0xC]	转化为字符串 转化为浮点数 将 ST 弹出到指定内存
004064D3	-	8055 9C	lea edx,dword ptr ss:[ebp-0x64]	
004064D6	-	8045 DC	lea eax,dword ptr ss:[ebp-0x24]	
004064D9	-	52	push edx	
004064DA	-	50	push eax	

004064DB	-	C745 A4 0100	mov dword ptr ss:[ebp-0x5C],0x1	
004064E2	-	C745 9C 0200	mov dword ptr ss:[ebp-0x64],0x2	
004064E9	-	FF15 AC104000	call dword ptr ds:[&MSUBUM60._vbaI4Uar	msubum60._vbaI4Uar
004064EF	-	8D4D BC	lea ecx,dword ptr ss:[ebp-0x44]	
004064F2	-	50	push eax	
004064F3	-	8D55 B8	lea edx,dword ptr ss:[ebp-0x48]	
004064F6	-	51	push ecx	
004064F7	-	52	push edx	
004064F8	-	FFD6	call esi	转化为字符串
004064FA	-	50	push eax	
004064FB	-	FF15 4C104000	call dword ptr ds:[&MSUBUM60.#rtcMidCh	取一个字符
00406501	-	8BD0	mov edx,eax	edx = 取得字符
00406503	-	8D4D B4	lea ecx,dword ptr ss:[ebp-0x4C]	
00406506	-	FF15 BC104000	call dword ptr ds:[&MSUBUM60._vbaStrM	msubum60._vbaStrMove
0040650C	-	50	push eax	String = "-"
0040650D	-	FF15 20104000	call dword ptr ds:[&MSUBUM60.#rtcAnsiU	转化为十六进制
00406513	-	0FBFC0	movsx eax,ax	
00406516	-	8985 60CFFFF	mov dword ptr ss:[ebp-0x3A0],eax	
0040651C	-	8D8D 7CFFFFFF	lea ecx,dword ptr ss:[ebp-0x84]	
00406522	-	DB85 60CFFFF	fild dword ptr ss:[ebp-0x3A0]	将hex转化为16进制弹出到ST6
00406528	-	51	push ecx	
00406529	-	C785 7CFFFFFF	mov dword ptr ss:[ebp-0x84],0x5	
00406533	-	DD9D 58CFFFF	fstp qword ptr ss:[ebp-0x3A8]	将 ST0 弹回该地址
00406539	-	DD85 58CFFFF	fild qword ptr ss:[ebp-0x3A8]	
0040653F	-	DC85 34FFFFFF	fadd qword ptr ss:[ebp-0xCC]	加上前两个字符的浮点数
00406545	-	DD5D 84	fstp qword ptr ss:[ebp-0x7C]	相加的值保存在该地址
00406548	-	DFF0	fstsw ax	
0040654A	-	A8 0D	test al,0xD	
0040654C	-	0F85 7A040000	jnz Andrena.004069CC	
00406552	-	FF15 94104000	call dword ptr ds:[&MSUBUM60.#rtcHexBs	将相加的值转化为hex
00406558	-	8985 74FFFFFF	mov dword ptr ss:[ebp-0x8C],eax	
0040655E	-	8D55 CC	lea edx,dword ptr ss:[ebp-0x34]	
00406561	-	8D85 6CFFFFFF	lea eax,dword ptr ss:[ebp-0x94]	
00406567	-	52	push edx	
00406568	-	8D8D 5CFFFFFF	lea ecx,dword ptr ss:[ebp-0xA4]	

0040656E	- 50	push eax	
0040656F	- 51	push ecx	
00406570	- C785 6CFFFFFF	mov dword ptr ss:[ebp-0x94],0x8	
0040657A	- FF15 84104000	call dword ptr ds:[<&MSUBUM60.__vbaVarCat	msvbum60.__vbaVarCat
00406580	- 8BD0	mov edx,eax	
00406582	- 8D4D CC	lea ecx,dword ptr ss:[ebp-0x34]	
00406585	- FFD7	call edi	msvbum60.__vbaVarMove
00406587	- 8D55 B0	lea edx,dword ptr ss:[ebp-0x50]	
0040658A	- 8D45 B4	lea eax,dword ptr ss:[ebp-0x4C]	
0040658D	- 52	push edx	
0040658E	- 8D4D B8	lea ecx,dword ptr ss:[ebp-0x48]	
00406591	- 50	push eax	
00406592	- 51	push ecx	
00406593	- 6A 03	push 0x3	
00406595	- FF15 9C104000	call dword ptr ds:[<&MSUBUM60.__vbaFreeS	msvbum60.__vbaFreeStrLis
0040659B	- 8D95 6CFFFFFF	lea edx,dword ptr ss:[ebp-0x94]	
004065A1	- 8D85 7CFFFFFF	lea eax,dword ptr ss:[ebp-0x84]	
004065A7	- 52	push edx	
004065A8	- 8D4D 8C	lea ecx,dword ptr ss:[ebp-0x74]	
004065AB	- 50	push eax	
004065AC	- 8D55 9C	lea edx,dword ptr ss:[ebp-0x64]	
004065AF	- 51	push ecx	
004065B0	- 52	push edx	
004065B1	- 6A 04	push 0x4	
004065B3	- FF15 14104000	call dword ptr ds:[<&MSUBUM60.__vbaFreeS	msvbum60.__vbaFreeVarLis
004065B9	- 83C4 24	add esp,0x24	
004065BC	- 8D85 68FDFFFF	lea eax,dword ptr ss:[ebp-0x298]	
004065C2	- 50	push eax	
004065C3	- 8D8D 78FDFFFF	lea ecx,dword ptr ss:[ebp-0x288]	
004065C9	- 8D55 DC	lea edx,dword ptr ss:[ebp-0x24]	
004065CC	- 51	push ecx	
004065CD	- 52	push edx	
004065CE	- FF15 C8104000	call dword ptr ds:[<&MSUBUM60.__vbaVarF	msvbum60.__vbaVarForNext
004065D4	- ^ E9 CFFFFFFFFF	jmp Andrena.004064A8	
004065D9	- > 8D45 CC	lea eax,dword ptr ss:[ebp-0x34]	
004065DC	- 8D8D 4CFFFFFF	lea ecx,dword ptr ss:[ebp-0xB4]	

004065E2	- 50	push eax	
004065E3	- 51	push ecx	
004065E4	- C785 54FFFFFF	mov dword ptr ss:[ebp-0xAC],<Andrena.a0	var10 = 0012FB44
004065EE	- C785 4CFFFFFF	mov dword ptr ss:[ebp-0xB4],0x0000	var28 = 0012FAC4
004065F8	- FF15 5C104000	call dword ptr ds:[<&MSUBUM60.__vbaVarT	0017E747D7A7D7C7F82836D74747A7F7E7B7C7D826D817E7B7C

1. 程序先计算出我们输入的序列号的长度
2. 建立循环，循环次数是序列号的长度
3. 在循环中，程序取得我们输入序列号的前两个字符，将其转化为浮点数，保存在内存中
4. 然后程序依次取得序列号的单个字符，将其转化为使用10进制表示的 ASCII 码
5. 将上述两个值相加，再转化为十六进制
6. 将每个字符和前两个字符相加的值连接起来

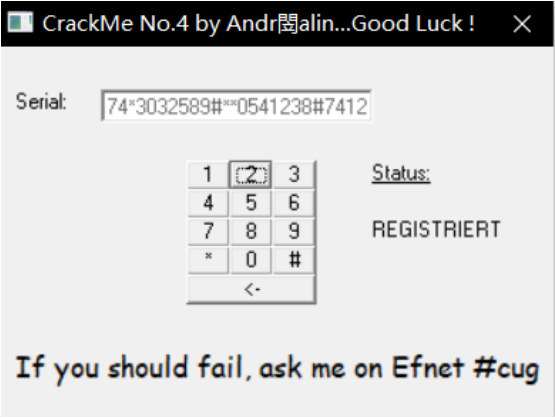
最后程序将这个字符串和一串字符串相比较，相同就注册成功。

由于我们输入的序列号最后转化的字符串是十六进制表示的，所以相比较的字符串也应该是在 0-9，A-F 范围内的，这样我们很容易就确定了真正的用来比较的字符串："081 7E 74 7D 7A 7D 7C 7F 82 83 6D 74 74 7A 7F 7E 7B 7C 7D 82 6D 8H 7E 7B 7C"。

由于最后生成的字符串，是和我们输入的序列号的前两位息息相关的。
前两位越大，最后每个字符相对应的也就越大。
前两位不一样，最后每个数字相对应的也就不一样。

根据正确的比较码，我们可以反推出正确的序列号：
74*3032589#**0541238#7412





相关文件在我的 Github: <https://github.com/UnreachableLove/160-Crackme/tree/master/Crackme011>

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: [Crackme010](#)

posted @ 2019-09-12 11:02 随风而逝的白色相簿 阅读(5) 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