

[writeup]360-ctf-2014-re123

原创

hellotaqini 于 2016-03-13 20:28:24 发布 824 收藏

分类专栏: [ctf](#) 文章标签: [逆向 ctf](#)

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/hellotaqini/article/details/50879818>

版权



[ctf](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

2014年360 CTF 逆向分析 三道简单的题目

re1

输入错误密码后会提示Done

正确的会提示success

定位到success, 发现是明文比较 ==

C:\Documents and Settings\Administrator\桌面\some re\360-rel\CrackMe.exe - [*G.P.U* - main thread, module CrackMe]

File View Debug Plugins Options Window Help Tools BreakPoint->

Paused

Registers (FPU)

EAX 009639F0 ASCII "K\$q*a_+@xt"
ECX 00000024
EDX 00962824
EBX 00000001
ESP 0012F8E0
EBP 0012F90C
ESI 00963950 ASCII "1234567890"
EDI 0012FEA4
EIP 004014C6 CrackMe.004014C6
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
D 0
T 0 GS 0000 NULL
0 0 LastErr ERROR_SUCCESS (00000000)

Is:[00963951]=32 ('2')
Il=24 ('\$')

Address	Hex dump	ASCII
004014B5	8A 10	mov dl,byte ptr ds:[eax]
004014B7	8ACA	mov cl,dl
004014B9	3A 16	cmp dl,byte ptr ds:[esi]
004014BB	75 1C	jnz short CrackMe.004014D9
004014BD	84 C9	test cl,cl
004014BF	74 14	je short CrackMe.004014D5
004014C1	8A 50 01	mov dl,byte ptr ds:[eax+0x1]
004014C4	8ACA	mov cl,dl
004014C6	3A 56 01	cmp dl,byte ptr ds:[esi+0x1]
004014C9	75 0E	jnz short CrackMe.004014D9
004014CB	83 C0 02	add eax,0x2
004014CE	83 C6 02	add esi,0x2
004014D1	84 C9	test cl,cl
004014D3	75 E0	jnz short CrackMe.004014B5
004014D5	33 C0	xor eax,eax

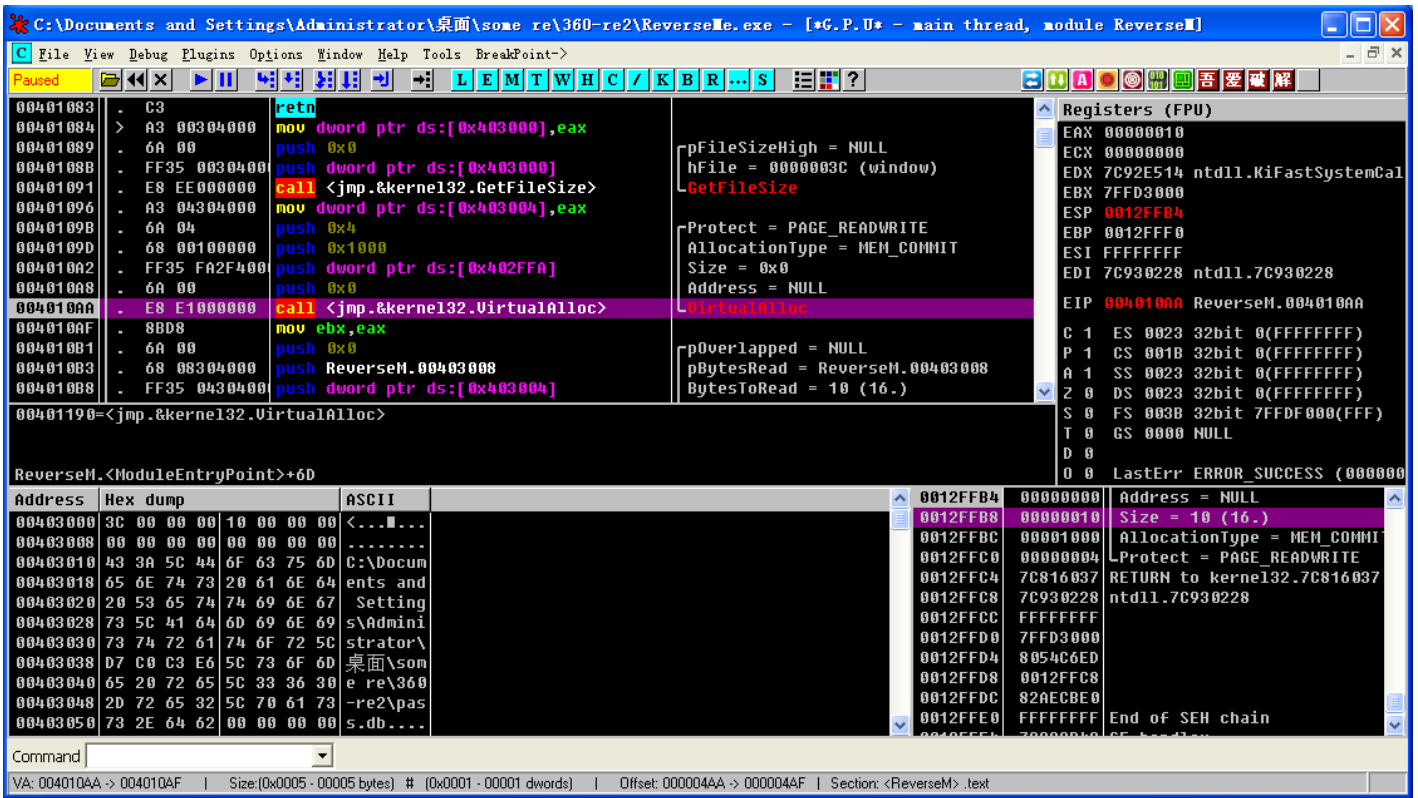
Command

Memory Window 1 Start: 0x44A000 End: 0x449FFF Size: 0x0 Value: 0x0

re2

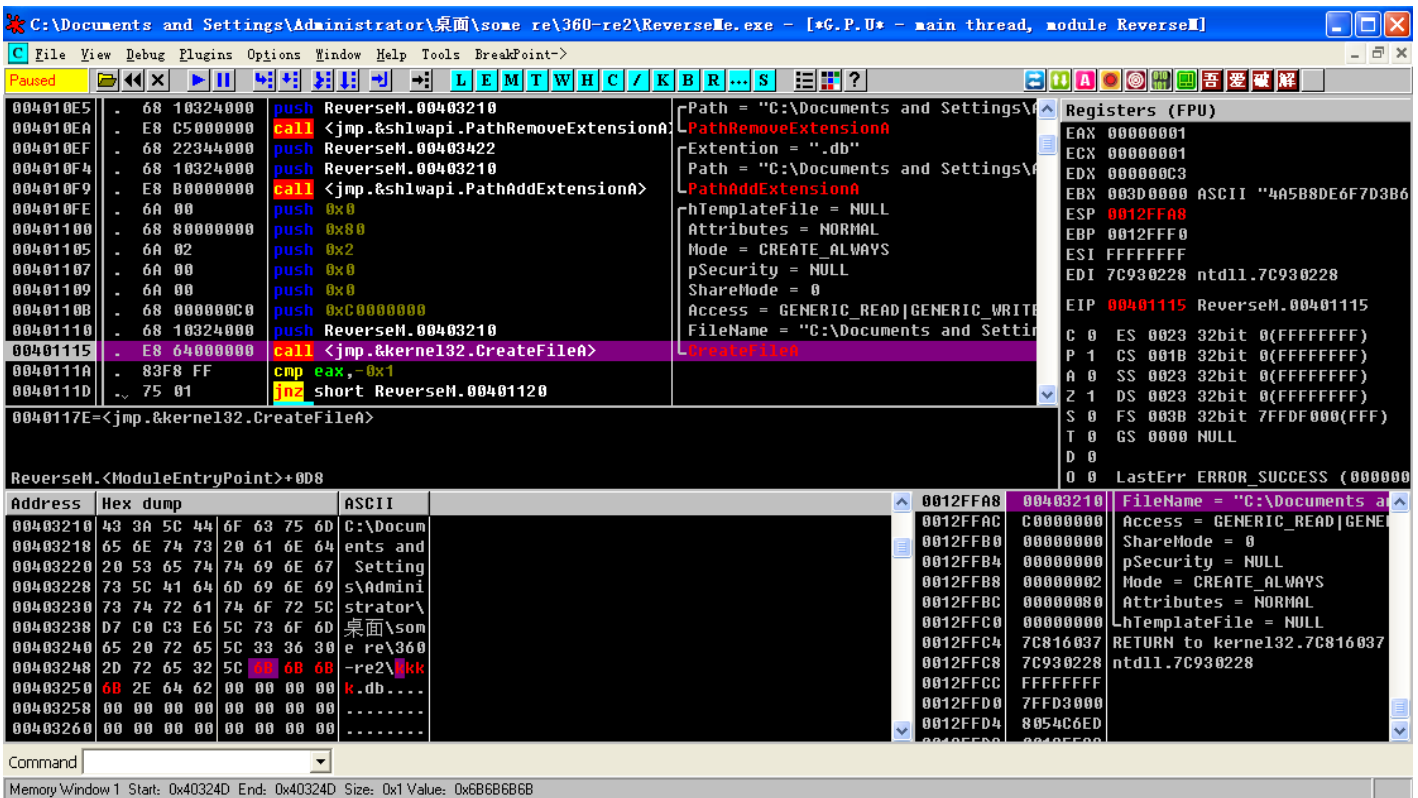
设置参数为pass.db, 用od载入

单步执行到VirtualAlloc, 发现函数没调用成功。



根据pass.db长度把size改为0x10(16)，函数成功调用

继续单步执行，又碰到一个CreateFileA，文件名还是pass.db，修改文件名



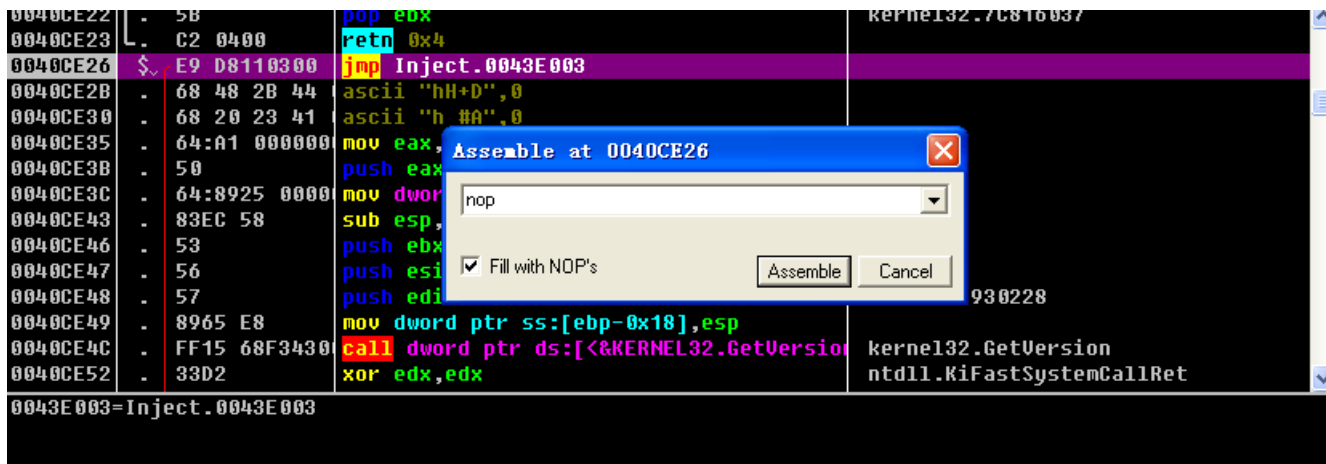
继续执行程序

打开生成的kkkk.db发现密码

...说是被病毒感染了

od载入程序后发现进入点有个jmp

直接nop掉



运行程序即可看到密码