

Crack看雪论坛加解密的一个破解案例程序

原创

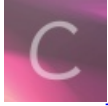
Cvjark 于 2019-03-19 21:59:27 发布 1209 收藏 3

分类专栏: [逆向学习](#) [读书笔记](#)

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/weixin_43084928/article/details/88674955

版权



[逆向学习](#) 同时被 2 个专栏收录

10 篇文章 2 订阅

订阅专栏



[读书笔记](#)

6 篇文章 0 订阅

订阅专栏

新手能力有限, 文章有什么错误还请各位前辈批正, 感激不尽~

运行程序, 了解下程序的大概流程:



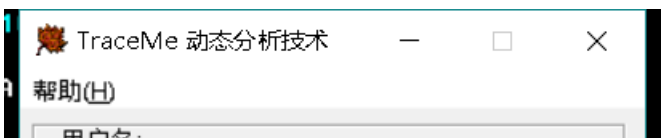
程序要求输入用户名于序列号, 点击check, 基于Windows的消息机制, 一般都从一些API入手, 读取输入的内容然后执行下一步, 因此我们可以以API作为切入点:

在OD中, 我们可以ctrl+G检索要跟随的API表达式, 读取内容一般是: `GetDlgItemTest (A/W)` 和 `GetWindowText (A/W)`

这个例子是: `GetDlgItemTextA`

755CB33F	CC	int3
755CB340	8BFF	mov edi,edi
755CB342	55	push ebp
755CB343	8BEC	mov ebp,esp
755CB345	FF75 0C	push dword ptr ss:[ebp+0xC]

在这个位置下断: F9, 我们停在这里, 此时回到程序界面, 输入信息





点击check，持续单步，留意消息框，会有惊喜：

```

004011D5  7C 71          [?] short TraceMe.00401248
004011D7  8D5424 4C     lea edx,dword ptr ss:[esp+0x4C]
004011DB  53           push ebx
004011DC  8D8424 A00000 lea eax,dword ptr ss:[esp+0xA0]
004011E3  52           push edx
004011E4  50           push eax
004011E5  E8 56010000  call TraceMe.00401340
004011EA  8B3D BC404000 mov edi,dword ptr ds:[<&USER32.GetDlgItemTextA]
004011F0  83C4 0C     add esp,0xC
004011F3  85C0        test eax,eax
004011F5  74 37       je short TraceMe.0040122E
004011F7  8D4C24 0C     lea ecx,dword ptr ss:[esp+0xC]
004011FB  51           push ecx
004011FC  68 E4544000  push TraceMe.004054E4
00401201  FF15 60404000 call dword ptr ds:[<&KERNEL32.lstrcpyA]
00401207  6A 00       push 0x0
00401209  6A 0E       push 0x0E
0040120B  56           push esi
0040120C  FFD7       call edi
0040120E  8B1D A4404000 mov ebx,dword ptr ds:[&USER32.EnableWindow]

```

堆栈地址=0019F788, (ASCII "! ")
edx=0019F78C, (ASCII "CrashInto")

https://blog.csdn.net/weixin_43084928

按照约定俗成，韩式调用返回通常把结果放在EAX中，即便长度不够的话，也还是会吧内容放在内存，取首地址放在EAX中，

```

004011F3  85C0        test eax,eax
004011F5  74 37       je short TraceMe.0040122E
004011F7  8D4C24 0C     lea ecx,dword ptr ss:[esp+0xC]
004011FB  51           push ecx

```

cString2 = "?"

这里做了校验函数结果的条件控制跳转，我们让它取反，改Z标志位...

```

004011F3  85C0        test eax,eax
004011F5  74 37       je short TraceMe.0040122E
004011F7  8D4C24 0C     lea ecx,dword ptr ss:[esp+0xC]
004011FB  51           push ecx
004011FC  68 E4544000  push TraceMe.004054E4
00401201  FF15 60404000 call dword ptr ds:[<&KERNEL32.lstrcpyA]
00401207  6A 00       push 0x0
00401209  6A 0E       push 0x0E
0040120B  56           push esi
0040120C  FFD7       call edi
0040120E  8B1D A4404000 mov ebx,dword ptr ds:[&USER32.EnableWindow]

```

跳转未实现
0040122E=TraceMe.0040122E

String2 = B95B4A0B ???
String1 = TraceMe.004054E4
lstrcpyA
Enable = FALSE
ControlID = 6E (110.)
hWnd = 002C05F4 ('TraceMe 动态分析技术',class
GetDlgItem
user32.EnableWindow

EIP 004011F5 TraceMe.004011F5
C 0 ES 002B 32位 0(FFFFFFFF)
P 1 CS 0023 32位 0(FFFFFFFF)
A 0 SS 002B 32位 0(FFFFFFFF)
Z 0 OF 002B 32位 0(FFFFFFFF)
S 0 FS 0053 32位 3D0000(FFF)
T 0 GS 002B 32位 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (0)
EFL 00000206 (NO,NB,NE,A,NS,P
ST0 empty 0.0
ST1 empty 0.0
SMBos99859.0000 netweixin_43084928

F8执行...

```

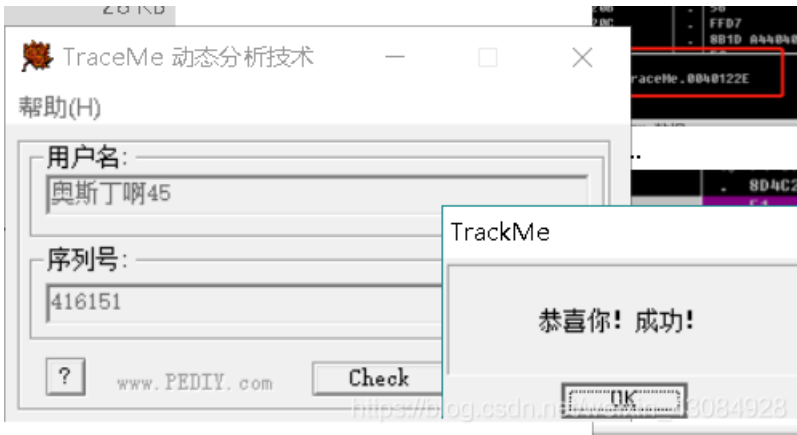
004011F7  8D4C24 0C     lea ecx,dword ptr ss:[esp+0xC]
004011FB  51           push ecx
004011FC  68 E4544000  push TraceMe.004054E4
00401201  FF15 60404000 call dword ptr ds:[<&KERNEL32.lstrcpyA]
00401207  6A 00       push 0x0
00401209  6A 0E       push 0x0E
0040120B  56           push esi
0040120C  FFD7       call edi
0040120E  8B1D A4404000 mov ebx,dword ptr ds:[&USER32.EnableWindow]

```

String2 = "恭喜你! 成功!"
String1 = TraceMe.004054E4
lstrcpyA
Enable = FALSE
ControlID = 6E (110.)
hWnd = 002C05F4 ('TraceMe 动态分析技术',cla
GetDlgItem
user32.EnableWindow



实现暴力破解，我们直接可以填充那个条件跳转指令用nop代替...然后保存到文件...:



少了校验判断，我们输入什么都会出现成功的信息...

程序[下载链接](#) 提取码: s237