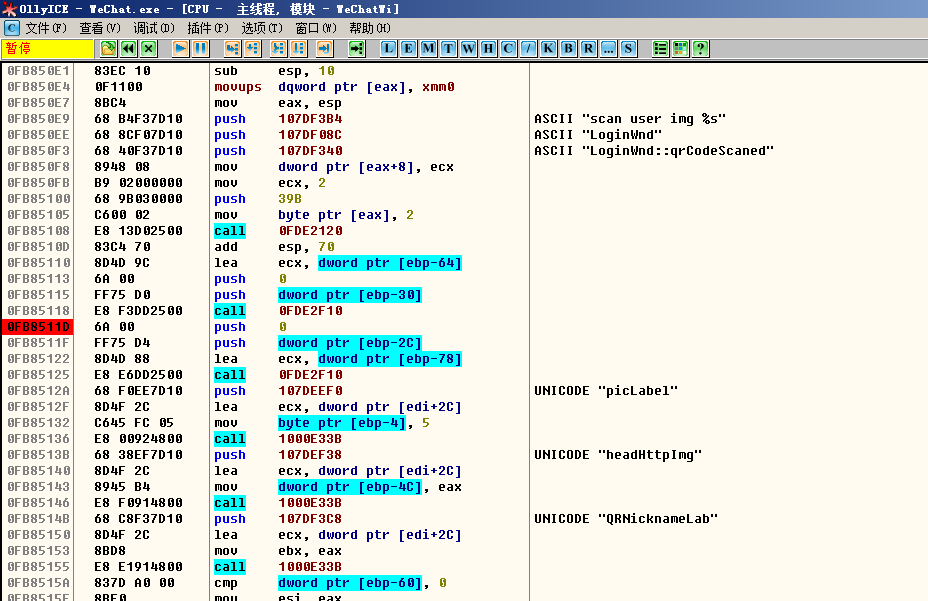
2.6.3.78版本分析：

登录前消息分析：

断点位置：WeChatWin.dll加载位置+ 0x1D511D

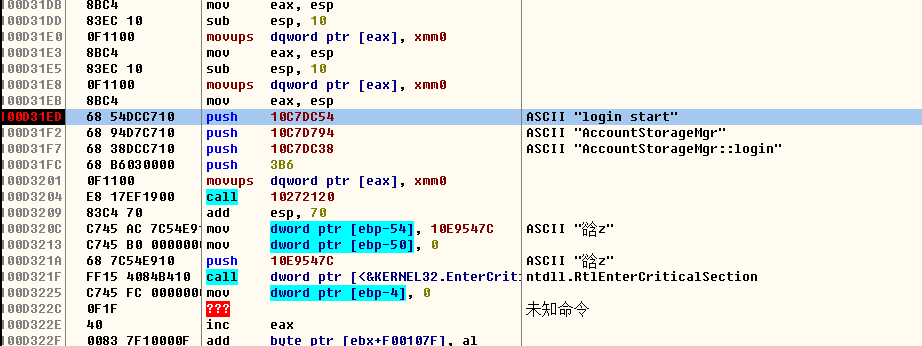
如图：



此处，堆栈下有个人图像URL。

断点位置：WeChatWin.dll加载位置+ 0x2931ED

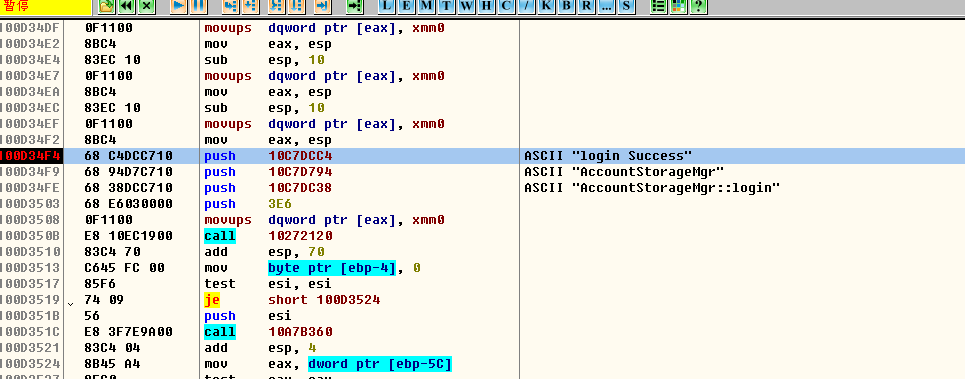
如图：



堆栈中出现微信号，wxid数据， "Everything is ok"数据，edi寄存器指向微信号。

断点位置：WeChatWin.dll加载位置+0x 2934F4

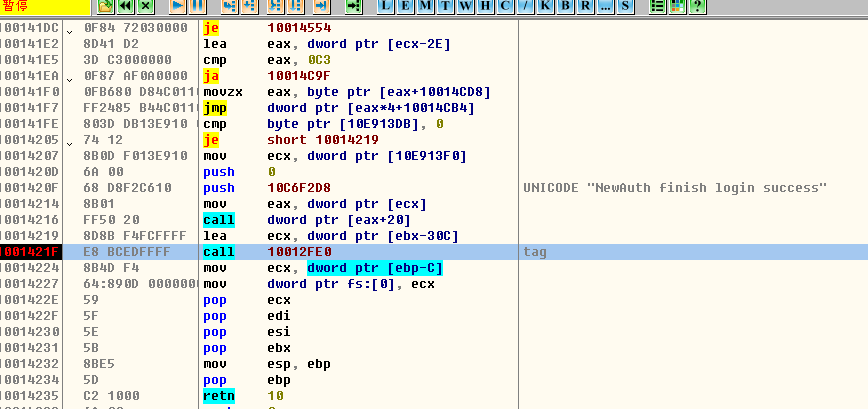
如图：



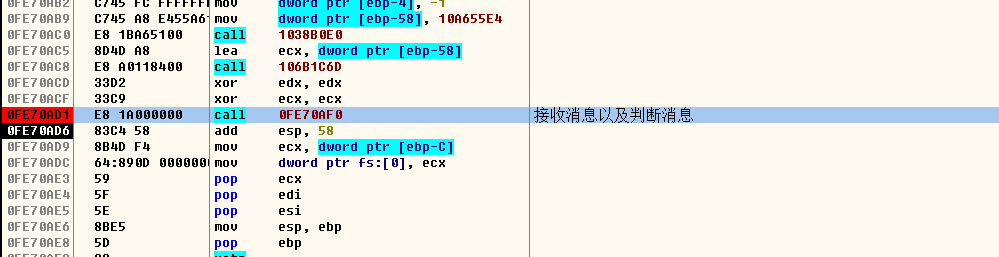
Esi和堆栈数据指向了微信号，堆栈中出现了wxid。

登录完成后经过的代码：

断点位置：WeChatWin.dll加载位置+0x 1D420D



接收消息（很多消息都过）：



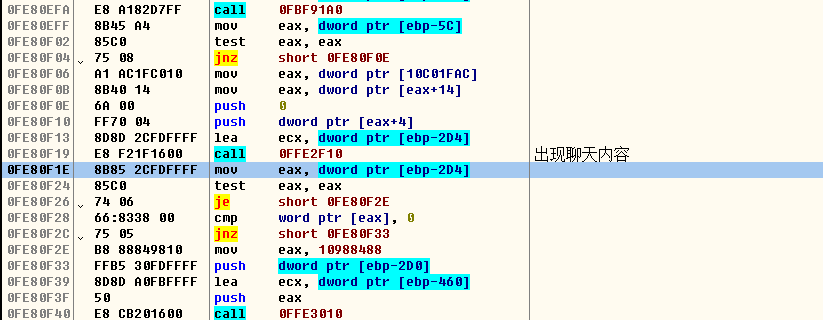
函数内部有：

0FE70CC1 68 409C9D10 push 109D9C40 ; UNICODE "@bottle:"

0FE70E39 68 1C669D10 push 109D661C ; UNICODE "officialaccounts"

0FE71073 68 C8249D10 push 109D24C8 ; ASCII "@chatroom"

接收消息（0FBB0000）：



位置在

0FE70E39 68 1C669D10 push 109D661C ; UNICODE "officialaccounts"

与

0FE71073 68 C8249D10 push 109D24C8 ; ASCII "@chatroom"

之间。

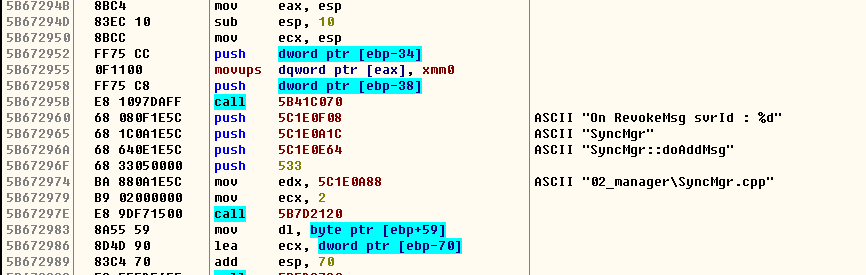
接收文本消息分析：

断点位置：WeChatWin.dll加载位置+0x2D2C1D

如图：



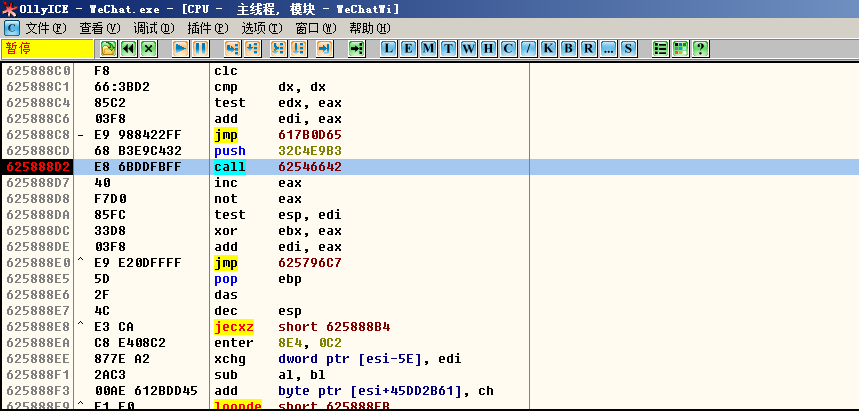
其上含有字符串标志：



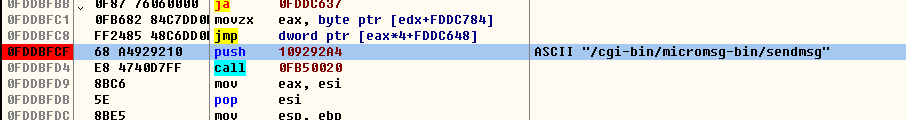
接收小视频消息分析：

断点位置：WeChatWin.dll加载位置+0x11388D2

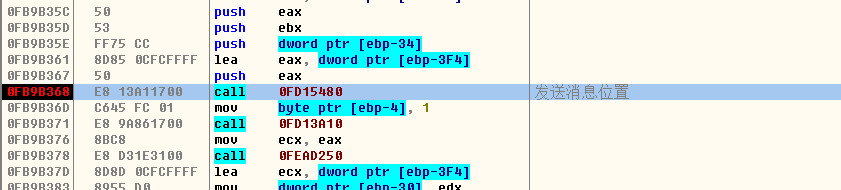
如图：



发送消息位置（模块基地址：0FAE0000）：

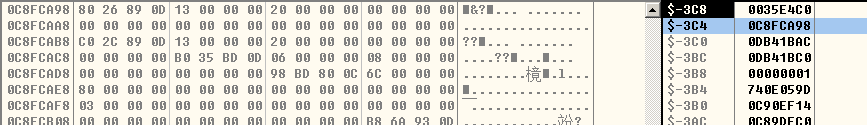


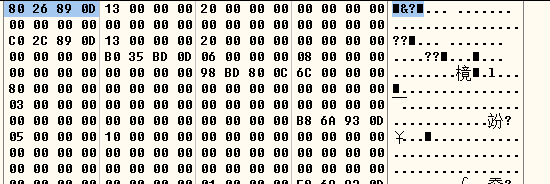
从这个位置下断点，然后往前回溯，直到：



此时，堆栈中

Ebp+4位置：





转到地址保存了接收方wxid

Ebp+8位置保存了发送内容，ebx也指向此处。