**PC微信v3.6.0.18改动分析记录**

**(windows-3.6.0.18 version)**

**修订历史记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 修改日期 | 版本 | 说明 | 作者 |
| 2022/03/19 | windows-3.6.0.18 |  | 胡智钦 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 引言 5](#_Toc98619532)

[2 Hook点改动 5](#_Toc98619533)

[2.1 CheckAppSingleton 5](#_Toc98619534)

[2.1.1 RVA 5](#_Toc98619535)

[2.2 FetchGlobalContactContextAddress 5](#_Toc98619536)

[2.2.1 RVA 5](#_Toc98619537)

[2.2.2 变化 5](#_Toc98619538)

[2.3 InitWeChatContactItem 5](#_Toc98619539)

[2.3.1 RVA 5](#_Toc98619540)

[2.4 DeinitWeChatContactItem 6](#_Toc98619541)

[2.4.1 RVA 6](#_Toc98619542)

[2.5 FindAndDeepCopyWeChatContactItemWrapper 6](#_Toc98619543)

[2.5.1 RVA 6](#_Toc98619544)

[2.6 FetchGlobalProfileContext 6](#_Toc98619545)

[2.6.1 RVA 6](#_Toc98619546)

[2.6.2 变化 6](#_Toc98619547)

[2.7 HandleRawMessages 6](#_Toc98619548)

[2.7.1 RVA 6](#_Toc98619549)

[2.7.2 逻辑变化 6](#_Toc98619550)

[2.8 HandleReceivedMessages 7](#_Toc98619551)

[2.8.1 RVA 7](#_Toc98619552)

[2.9 WXSendTextMessage 7](#_Toc98619553)

[2.9.1 RVA 7](#_Toc98619554)

[2.10 FetchGlobalSendMessageContext 7](#_Toc98619555)

[2.10.1 RVA 7](#_Toc98619556)

[2.11 WXSendFileMessage 7](#_Toc98619557)

[2.11.1 特征 7](#_Toc98619558)

[2.11.2 RVA 8](#_Toc98619559)

[2.12 CloseLoginWnd 8](#_Toc98619560)

[2.12.1 特征 8](#_Toc98619561)

[2.12.2 RVA 8](#_Toc98619562)

[2.13 LogoutAndExitWeChat 8](#_Toc98619563)

[2.13.1 RVA 8](#_Toc98619564)

[2.14 Logouted 9](#_Toc98619565)

[2.14.1 RVA 9](#_Toc98619566)

[2.15 LogoutedByMobile 9](#_Toc98619567)

[2.15.1 RVA 9](#_Toc98619568)

[2.16 Logined 9](#_Toc98619569)

[2.16.1 RVA 9](#_Toc98619570)

[2.17 WeChatEventProc 9](#_Toc98619571)

[2.17.1 RVA 9](#_Toc98619572)

[2.17.2 触发退出登录事件的变化 9](#_Toc98619573)

[3 数据结构变化 10](#_Toc98619574)

[3.1 Profile 10](#_Toc98619575)

[3.2 MessageStructure 10](#_Toc98619576)

# 引言

记录PC微信3.6.0.18版本的改动。

# Hook点改动

## CheckAppSingleton

特征相比上一个版本没有发生变化

### RVA

wechatwin.dll:$CD64F8

## FetchGlobalContactContextAddress

特征相比上一个版本没有发生变化

### RVA

wechatwin.dll:$9A000

### 变化

## InitWeChatContactItem

### RVA

wechatwin.dll:$659840

## DeinitWeChatContactItem

### RVA

wechatwin.dll:$65A340

## FindAndDeepCopyWeChatContactItemWrapper

### RVA

wechatwin.dll:$4024A0

## FetchGlobalProfileContext

### RVA

wechatwin.dll:$9E560

### 变化

## HandleRawMessages

特征没有变化

### RVA

wechatwin.dll:$4E7000

### 逻辑变化

g\_wechat\_raw\_message\_type\_point\_offset的偏移需要继续往回三个节。这个补充到feature中。



## HandleReceivedMessages

### RVA

wechatwin.dll:$4EDDA0

## WXSendTextMessage

### RVA

wechatwin.dll:$4BE7B0

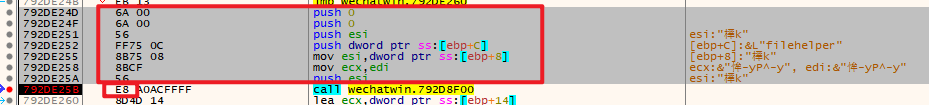
## FetchGlobalSendMessageContext

### RVA

wechatwin.dll:$9A1C0

## WXSendFileMessage

### 特征



先定位到这串调用WXSendFileMessage的指令

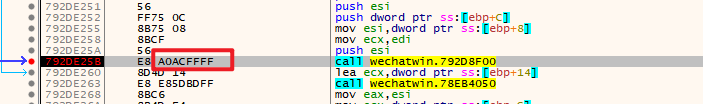
扫描十六进制流：

{

0x6A, 0x00, 0x6A, 0x00, 0x56, 0xFF, 0x75, 0x0C, 0x8B, 0x75, 0x08, 0x8B, 0xCF, 0x56, 0xE8

};

可以获取到WxSendFileMessage函数，距离call的下一条指令的相对距离



取得相对距离后，上面用call指令的下一条指令的地址加上这个偏移就能够得到WxSendFileMessage的入口地址了。

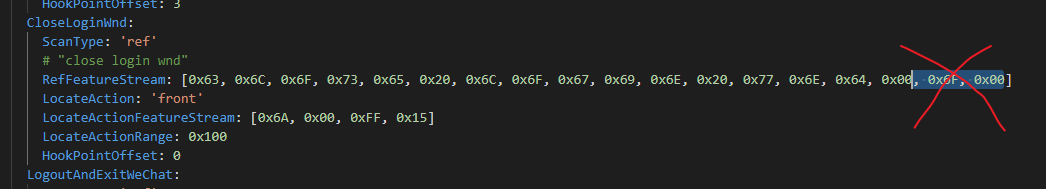
### RVA

wechatwin.dll:$4B8F00

## CloseLoginWnd

### 特征

扫描特征没有发生变化，但是需要把3.5.0.46版本的特征的后两个字节去掉，这是多余的部分。



### RVA

wechatwin.dll:$319025

## LogoutAndExitWeChat

### RVA

wechatwin.dll:$330C20

## Logouted

特征与旧版本相同

### RVA

wechatwin.dll:$326D8A

## LogoutedByMobile

特征与旧版本相同

### RVA

wechatwin.dll:$325DF7

## Logined

特征与旧版本相同

### RVA

wechatwin.dll:$319930

## WeChatEventProc

### RVA

wechatwin.dll:$325B60

### 触发退出登录事件的变化

当前版本改为**0x321**

# 数据结构变化

## Profile

context+offset 0xBC：用户昵称，这个不变

context+offset **0x510**：登录的微信号，如果首字节为0说明退出登录

context+offset **0x528**：存放wxid字符串地址

## MessageStructure

大小发生变换，变为**0x298**