**WxBox - 详细需求分析文档**

**(v0.1.0)**

**修订历史记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 修改日期 | 版本  （指的是文档的版本号） | 说明 | 作者 |
| 2021-12-25 | v0.1.0 | 文档初始化 | 胡智钦 |
| 2021-12-29 | v0.1.1 | 迭代需求 | 胡智钦 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 引言 4](#_Toc91289430)

[2 WxBox项目 4](#_Toc91289431)

[2.1 非功能性需求 4](#_Toc91289432)

[2.2 功能性需求 4](#_Toc91289433)

[2.2.1 根据宏定义检测运行的操作系统【Proj-FR-1】 4](#_Toc91289434)

[3 WxBox模块 5](#_Toc91289435)

[3.1 非功能性需求 5](#_Toc91289436)

[3.2 功能性需求 5](#_Toc91289437)

[3.2.1 获取微信安装目录【WxBox-FR-1】 5](#_Toc91289438)

[3.2.2 获取微信版本号【WxBox-FR-2】 7](#_Toc91289439)

[3.2.3 获取系统进程列表【WxBox-FR-3】 7](#_Toc91289440)

[3.2.4 根据窗口句柄获取所在进程【WxBox-FR-4】 7](#_Toc91289441)

[4 WxBot模块 7](#_Toc91289442)

[4.1 非功能性需求 7](#_Toc91289443)

[4.2 功能性需求 7](#_Toc91289444)

# 引言

这个文档用于描述和记录WxBox模块与WxBot模块的需求，并对所有需求进行详细的分析以及设计。这个文档将不断的迭代，不需要一开始就全部补完。

# WxBox项目

## 非功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| Proj-NFR-1 |  |  |  |  |

## 功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| Proj-FR-1 | [识别操作系统](#_根据宏定义检测运行的操作系统) | 根据宏定义检测运行的操作系统 |  | 必须 |

### 根据宏定义检测运行的操作系统【Proj-FR-1】

这个通过meson.build构建脚本在configure的时候根据所在操作系统生成config.h文件，在项目中可以通过引入这个头文件，用WXBOX\_PLATFORM宏来判断是什么操作系统，这个宏是一个整型值，它的所有可能值如下：

|  |  |
| --- | --- |
| 宏 | 值 |
| WXBOX\_UNSUPPORT\_OS | 0 |
| WXBOX\_WINDOWS\_OS | 1 |
| WXBOX\_MAC\_OS | 2 |

# WxBox模块

## 非功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| WxBox-NFR-1 |  |  |  |  |

## 功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| WxBox-FR-1 | [获取微信安装目录](#_获取微信安装目录) | 获取微信安装目录，能应对正常和非常规安装微信的环境 |  | 必须 |
| WxBox-FR-2 | [检查微信安装目录是否有效](#_检查指定的安装路径是否有效【WxBox-FR-2】) | 检查指定的微信安装路径是否有效 | WxBox-FR-1 | 必须 |
| WxBox-FR-3 | [获取微信版本号](#_获取微信版本号) | 主要以关键模块的版本号来作为微信的版本号，比如Windows下使用WeChatWin.dll的文件版本号 | WxBox-FR-1 | 必须 |
| WxBox-FR-4 | [获取系统进程列表](#_获取系统进程列表) | 获取系统中所有进程的信息 |  | 必须 |
| WxBox-FR-5 | [识别窗口进程](#_根据窗口句柄获取所在进程) | 根据窗口的句柄获取它所属的进程信息 |  | 可选 |
| WxBox-FR-6 | [解除微信单例](#_解除微信单例【WxBox-FR-6】) | 通过WxBox启动新的微信实例 | WxBox-FR-3 | 必须 |
| WxBox-FR-7 | [定义Hook特征结构](#_定义Hook特征结构【WxBox-FR-7】) | 定义已知版本信息的Hook点与特征信息的存储方式 |  | 必须 |

### 获取微信安装目录【WxBox-FR-1】

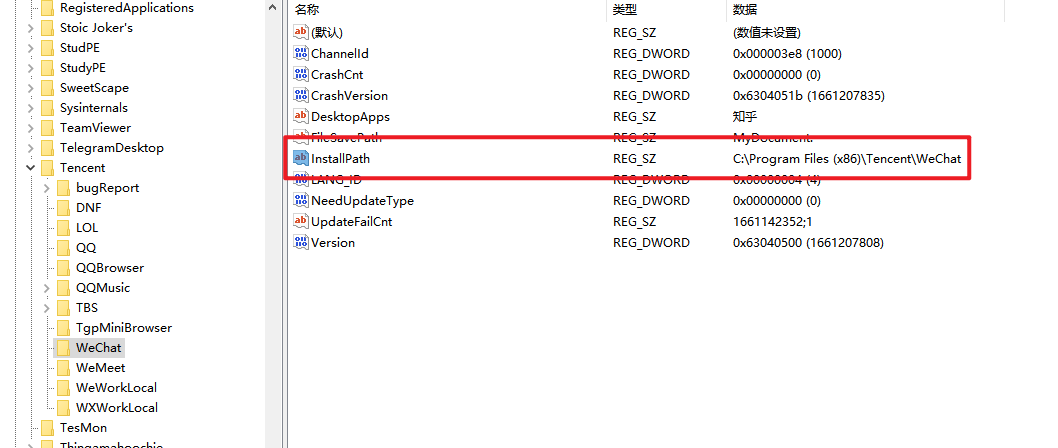
#### Windows

##### 正常安装

在Windows下如果是正常安装的话，可以在注册表的以下位置获取到微信的安装路径

HKEY\_CURRENT\_USER\SOFTWARE\Tencent\WeChat#InstallPath

这个InstallPath是一个REG\_SZ类型的值



【微信安装目录在注册表中的位置】

关于注册表的Windows API可以看MSDN文档：<https://docs.microsoft.com/zh-cn/windows/win32/sysinfo/registry-functions>。

主要使用的API是[RegGetValue](https://docs.microsoft.com/zh-cn/windows/win32/api/winreg/nf-winreg-reggetvaluea)。

##### 非常规安装

如果微信安装路径在注册表中找不到的话，可能是系统上并没有安装微信，也可能使用的不是常规的安装方法，比如绿色版之类的。这时候让用户手动指定微信的安装位置。

#### Mac OS

### 检查微信安装目录是否有效【WxBox-FR-2】

#### Windows

在Windows下检查安装目录是否存在WeChat.exe和WeChatWin.dll，以此来决定安装目录是否有效。

#### Mac OS

### 获取微信版本号【WxBox-FR-3】

#### Windows

在Windows下以WeChatWin.dll的文件版本来作为微信的版本号。相关函数API有：[GetFileVersionInfoSizeA](https://docs.microsoft.com/en-us/windows/win32/api/winver/nf-winver-getfileversioninfosizea)、[GetFileVersionInfo](https://docs.microsoft.com/en-us/windows/win32/api/winver/nf-winver-getfileversioninfoa)和[VerQueryValueA](https://docs.microsoft.com/en-us/windows/win32/api/winver/nf-winver-verqueryvaluea)。相关结构体：[VS\_FIXEDFILEINFO](https://docs.microsoft.com/en-us/windows/win32/api/verrsrc/ns-verrsrc-vs_fixedfileinfo)。

#### Mac OS

### 获取系统进程列表【WxBox-FR-4】

#### Windows

在Windows下可以用快照来获取进程列表，关键函数是CreateToolhelp32Snapshot，MSDN文档：[CreateToolhelp32Snapshot](https://docs.microsoft.com/en-us/windows/win32/api/tlhelp32/nf-tlhelp32-createtoolhelp32snapshot)。

#### Mac OS

### 根据窗口句柄获取所在进程【WxBox-FR-5】

#### Windows

在Windows下可以用WindowFromPoint来根据屏幕上的坐标来获取窗口句柄，用GetWindowThreadProcessId来获取该窗口句柄所属的进程，MSDN文档：[WindowFromPoint](https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-windowfrompoint)，[GetWindowThreadProcessId](https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getwindowthreadprocessid)。

#### Mac OS

### 解除微信单例【WxBox-FR-6】

#### Windows

在Windows下，做法是这样的：首先需要获取微信的安装目录并确保安装目录是有效的，根据安装目录可以拼接出WeChat.exe的绝对路径，然后通过CreateProcess以DEBUG\_ONLY\_THIS\_PROCESS模式来启动一个WeChat.exe进程并Attach住，这里需要注意因为微信是多进程模式的，所以必须用DEBUG\_ONLY\_THIS\_PROCESS而不是DEBUG\_PROCESS。

Attach住之后就可以进入调试循环了，需要关心的只有一个事件，那就是LOAD\_DLL\_DEBUG\_EVENT事件，即dll的加载事件，这是因为WeChatWin.dll是动态加载的，而我们要做解除微信单例，需要到操作就在WeChatWin.dll上，所以在LOAD\_DLL\_DEBUG\_EVENT事件处识别到加载WeChatWin.dll模块，就可以执行解除操作了。

接下来分为两种情况：一种是对于已知版本，这种是知道了修改点的；第二种是未知版本，需要用特征去定位修改点。

这里以第二种情况来说明做法，首先使用TitanEngine的FindEx方法来在WeChat.exe进程的WeChatWin.dll模块上去搜索特征字符串“**\_WeChat\_App\_Instance\_Identity\_Mutex\_Name**”的VA地址，接下来继续在WeChatWin.dll模块上用FindEx方法搜索引用这个VA地址的地方，这里需要补充说明一下，“**\_WeChat\_App\_Instance\_Identity\_Mutex\_Name**”这种全局字符串在push、mov这些指令的使用方式是这样的，编译生成的exe文件，push、mov后跟的是全局变量的一个RVA地址，在PE可执行文件加载到内存后，这个RVA地址会被重定位成一个VA地址，所以我们在内存上搜索的是VA地址而不是RVA。

定位到引用“**\_WeChat\_App\_Instance\_Identity\_Mutex\_Name**”的位置后，还需要往回定位到这个函数的入口点，找到后那么修改点就找到了。

接下来使用frida-gum的GumX86Writer来生成机器指令，汇编代码是move eax, 0; ret（对于这里其实不需要用到GumX86Writer，直接使用[0xB8, 0x00, 0x00, 0x00, 0x00,0xC3]就可以了）。

最后就是把机器指令替换到找到的函数入口点上，然后脱离WeChat.exe的调试（这里暂时来看必须使用这种调试挂起的方式）。

相关API文档资料：

* [CreateProcess](https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa)
* [Process Creation Flags](https://docs.microsoft.com/en-us/windows/win32/procthread/process-creation-flags)
* [Creating a Basic Debugger](https://docs.microsoft.com/en-us/windows/win32/debug/creating-a-basic-debuggerhttps:/docs.microsoft.com/en-us/windows/win32/debug/creating-a-basic-debugger)
* [Writing the Debugger's Main Loop](https://docs.microsoft.com/en-us/windows/win32/debug/writing-the-debugger-s-main-loop)
* [WaitForDebugEvent](https://docs.microsoft.com/en-us/windows/win32/api/debugapi/nf-debugapi-waitfordebugevent)
* [ContinueDebugEvent](https://docs.microsoft.com/en-us/windows/win32/api/debugapi/nf-debugapi-continuedebugevent)
* [LOAD\_DLL\_DEBUG\_INFO structure](https://docs.microsoft.com/en-us/windows/win32/api/minwinbase/ns-minwinbase-load_dll_debug_info)
* [x64dbg/TitanEngine](https://github.com/x64dbg/TitanEngine)
* [gumx86writer](https://github.com/frida/frida-gum/blob/main/gum/arch-x86/gumx86writer.h)

#### Mac OS

### 定义Hook特征结构【WxBox-FR-7】

所有的预定义的特征信息使用yaml存储起来。

#### 存储已知微信版本的Hook点方式

对于已知版本的微信的所有Hook点，直接存储对应Hook点的RVA，例如：以下存储Windows微信版本3.4.5.27的Hook点信息。

absolute:

  '3.4.5.27':

    CheckAppSingleton:

      EntryRVA: 0x00C45E20

    FetchGlobalContactContextAddress:

      EntryRVA: 0x00406540

    InitWeChatContactItem:

      EntryRVA: 0x005B7460

    DeinitWeChatContactItem:

      EntryRVA: 0x005B7D40

    FindAndDeepCopyWeChatContactItemWithWXIDWrapper:

      EntryRVA: 0x005BD9A0

    FetchGlobalProfileContext:

      EntryRVA: 0x0009C7B0

    HandleRawMessages:

      EntryRVA: 0x0046BF93

    HandleReceivedMessages:

      EntryRVA: 0x0047152C

    WXSendTextMessage:

      EntryRVA: 0x00442540

    FetchGlobalSendMessageContext:

      EntryRVA: 0x000989A0

    WXSendFileMessage:

      EntryRVA: 0x0043DC20

#### 定义特征信息

特征信息是给未知微信版本定位Hook点用的。分为两步：第一步（扫描）是根据“扫描”特征进行扫描定位到Hook点附近的位置；第二步（定位）是根据“定位”特征从第一步找到的位置来实际定位到Hook点。

##### 扫描（Scan）

扫描方式（ScanType）分为三种：

* ref：例如：根据字符串提供的二进制流，定位到引用这个字符串的位置
* multiPushRef：例如：根据多个字符串的连续引用（连续的push <字符串地址>指令），定位到这个连续引用的起始位置
* instruction：例如：直接根据指令的二进制流，定位到这段指令的起始位置

ref和multiPushRef需要的扫描需要执行两次，而instruction只需要一次。

所有扫描方式的共同参数

|  |  |
| --- | --- |
| 参数名 | 说明 |
| ScanType[必须]<string> | 扫描方式 |

不同类型各自独有的参数：

|  |  |  |
| --- | --- | --- |
| 类型 | 参数说明 | |
| ref | 参数名 | 说明 |
| RefFeatureStream[必须]<uint8\_t[]> | 引用的字节流，例如：单字节字符串的字节流，宽字节字符串的字节流 |
| RefBackExtralInstruction[可选] <uint8\_t[]> | 在找到的VA前附加指令作为Scan的新模式 |
| RefFrontExtralInstruction[可选] <uint8\_t[]> | 在找到的VA后附加指令作为Scan的新模式 |
| multiPushRef | 参数名 | 说明 |
| PushInstruction[必须]<uint8\_t[]> | push指令前缀，这里固定是[0x68] |
| RefFeatureStreams[必须]<uint8\_t[][]> | 引用的多个字节流数组，这是个二维数组，例如：多个字符串字节流的数组 |
| RefFeatureStreamsOffset [必须]<uint8\_t[]> | 给找到的FeatureStreams的偏移 |
| instruction | 参数名 | 说明 |
| InstructionFeatureStream[必须]<uint8\_t[]> | 指令的二进制流 |

##### 定位（Locate）

定位动作（LocateAction）分为四种：

* back：往低地址定位
* front：往高地址定位
* backThenFront：分两步，先往低地址定位，然后再往高地址定位，这里用到两个特征
* backMultiTimes：使用相同的特征，多次往低地址定位

所有定位动作的共同参数

|  |  |
| --- | --- |
| 参数名 | 说明 |
| LocateAction[必须]<string> | 定位动作类型 |
| LocateActionFeatureStream[必须]<uint8\_t[]> | 定位使用的字节流 |
| LocateActionRange[必须]<int> | 定位动作的范围 |
| HookPointOffset[必须]<int> | 定位执行到最后，进行偏移然后得到实际的Hook点 |

不同类型各自独有的参数：

|  |  |  |
| --- | --- | --- |
| 类型 | 参数说明 | |
| back | 参数名 | 说明 |
|  |  |
| front | 参数名 | 说明 |
|  |  |
| backThenFront | 参数名 | 说明 |
| ThenLocateActionFeatureStream[必须]<uint8\_t[]> | 执行front定位使用的字节流 |
| backMultiTimes | 参数名 | 说明 |
| LocateActionExecuteTimes [必须]<int> | back定位动作的重复执行次数 |

# WxBot模块

## 非功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| WxBot-NFR-1 |  |  |  |  |

## 功能性需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能名称 | 简要描述 | 依赖 | 优先级 |
| WxBot-FR-1 |  |  |  |  |