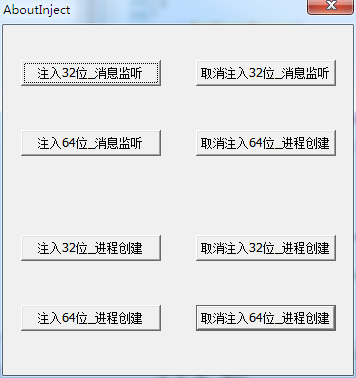
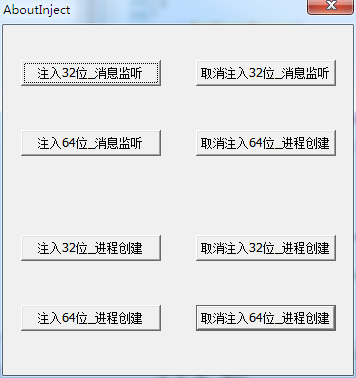


Inject32工程：32位exe，注入方。



Inject64工程：64位exe，注入方。



MsgHook工程：64位dll，注入到64位进程中，。安装消息钩子，可以监听指定窗口的位置改变消息。

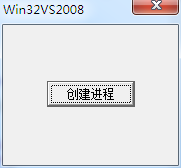
MsgHook32工程：32位dll，注入到32位进程中。安装消息钩子，可以监听指定窗口的位置改变消息。

MuteHook工程：64位dll，注入到64位进程中。Hook进程创建函数(如CreateProcessA/W, CreateProcessInternalW)，是实现进程树监控的基础。

MsgHook32工程：32位dll，注入到64位进程中。Hook进程创建函数(如CreateProcessA/W, CreateProcessInternalW)，是实现进程树监控的基础。

Win32VS2008工程：32位exe。

Win32VS2008工程： 32位exe



Win64VS2008工程： 64位exe



Wow64Ext工程: 32位dll，32位注入64位的辅助dll。

参考文档：

VS 2008的64位编译环境的安装和使用

<http://blog.163.com/danshiming@126/blog/static/10941274820165243411771/>

DLL/PIC Injection on Windows from Wow64 process

<https://modexp.wordpress.com/2015/11/19/dllpic-injection-on-windows-from-wow64-process/>

Mixing x86 with x64 code

<http://blog.rewolf.pl/blog/?p=102>

windows 64编程中寄存器的使用

<https://blog.csdn.net/a1875566250/article/details/11619637>

Windows 7 64位 HookApi例子

<https://blog.csdn.net/caoshiying/article/details/51881787>

Programming Guide for 64-bit Windows

<https://msdn.microsoft.com/en-us/library/windows/desktop/bb427430(v=vs.85).aspx>

核心注入文件

Inject32\injectHelper32: 用于32位程序注入dll的导出函数到指定的32位进程中。

Inject32\InjectHelper64: 用于32位程序注入dll的导出函数到指定的64位进程中。

Inject64\injectHelper32: 用于64位程序注入dll的导出函数到指定的32位进程中。

Inject64\InjectHelper64: 用于64位程序注入dll的导出函数到指定的64位进程中。