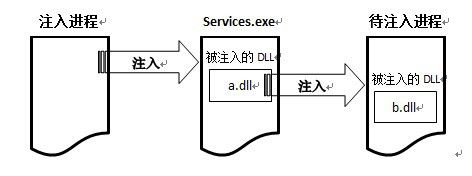
DLL注入技术之依赖可信进程注入

    依赖可信进程注入原理是利用Windows 系统中Services.exe这个权限较高的进程，首先将a.dll远线程注入到Services.exe中，再利用a.dll将b.dll远线程注入到待注入进程中。具体过程如下图所示：



    这里提供一个小技巧，当注入到Services.exe里的DLL时，想在做完事情后悄无声息的将自己释放掉，在Windows 中有这样的一个API函数FreeLibraryAndExitThread()，它可以把自己卸载掉并且退出线程，具体代码如下：

1. DWORD ThreadProc(CMfcServicesInjectDLLApp\* pThis)
2. {
3. //切换mfc模块
4. AFX\_MANAGE\_STATE(AfxGetStaticModuleState());
5. pThis->m\_InjectObj.Attach(
6. \_T("calc.exe"),
7. \_T("D:\\MyDll\\RelyServicesInject\\Debug\\MfcExeInjectDLL.dll"));
8. //在线程中卸载掉自己并且退出线程
9. FreeLibraryAndExitThread(pThis->m\_hInstance,0);
10. return 0;
11. }
12. // CMfcServicesInjectDLLApp 初始化
13. BOOL CMfcServicesInjectDLLApp::InitInstance()
14. {
15. DWORD dwThreadId;
16. m\_hThread = ::CreateThread(NULL, NULL,
17. (LPTHREAD\_START\_ROUTINE)ThreadProc,
18. this, NULL,&dwThreadId);
19. return TRUE;
20. }

复制代码

依赖可信进程注入其实就是远线程注入的增强版，它利用了系统较高权限的进程进行远程注入，大大提高了注入的成功率，并在注入完毕后释放掉自己，降低了被查杀的可能性。