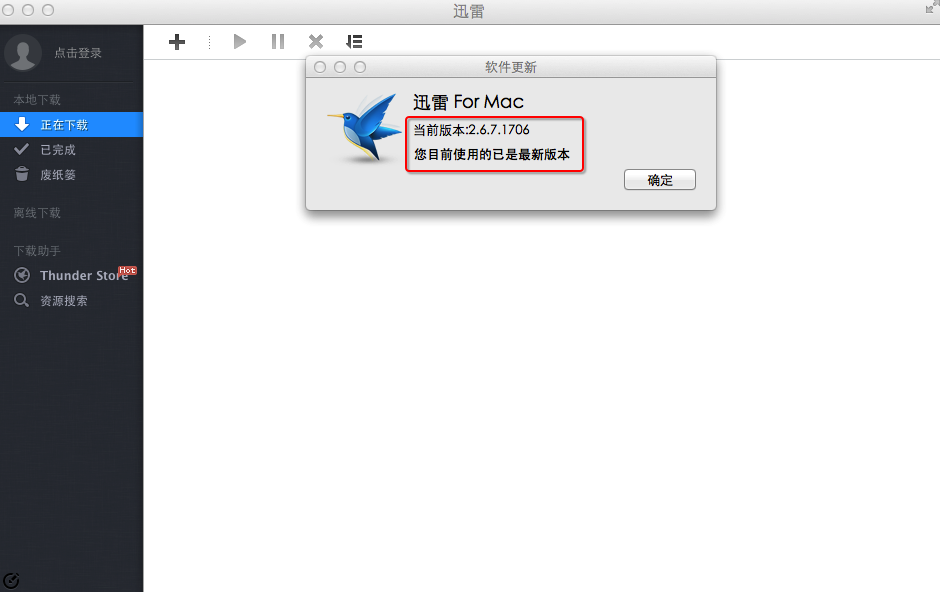
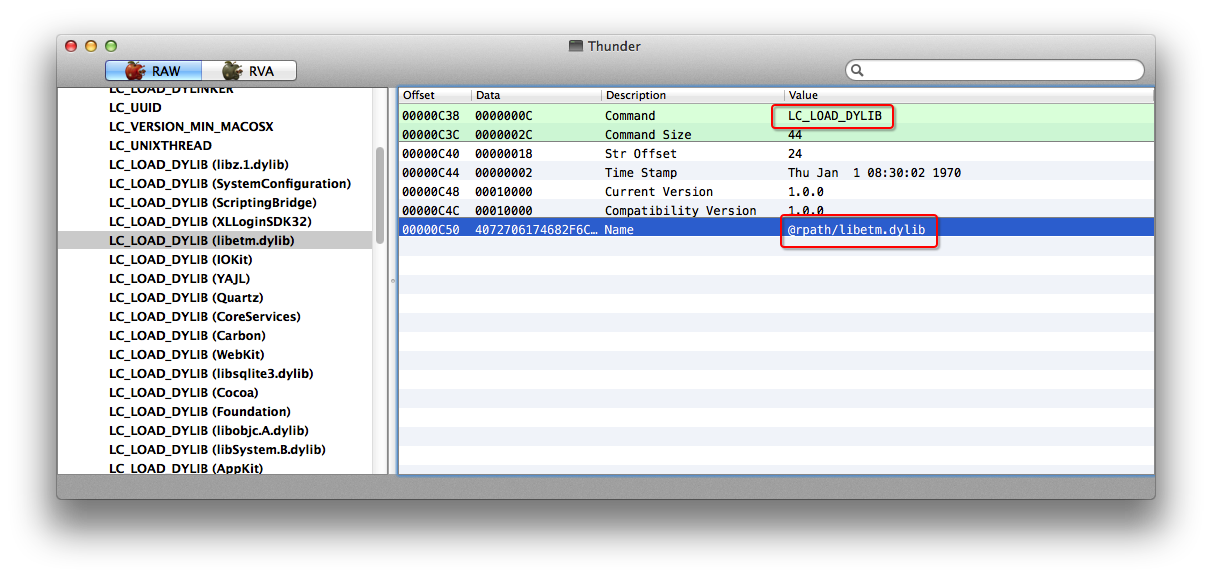
迅雷客户端dylib hijacking漏洞

在CanSecW 2015安全会议上，国外安全人员Patrick Wardle公布了由其发现的OS X系统下的dylib hijacking漏洞。经过测试发现，最新的Thunder客户端存在此漏洞，并实现了简单验证。

使用最新版进行测试，如下：



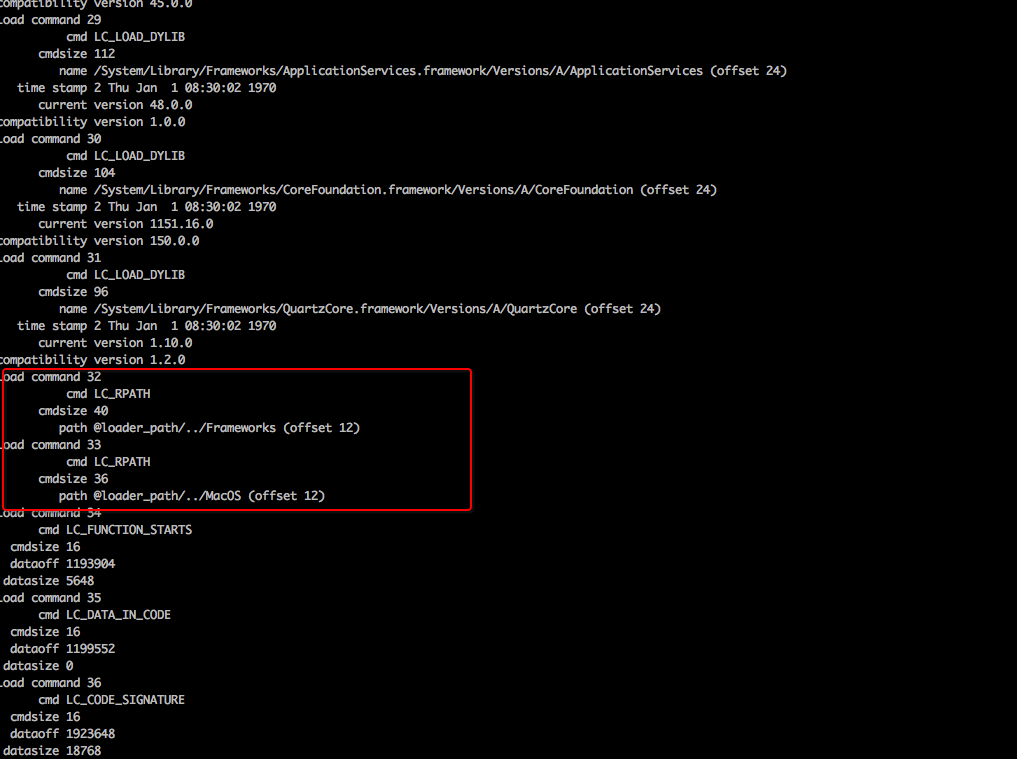
使用工具分析可执行文件Thunder可知，程序启动后会动态加载库文件libetm.dylib，该文件位于/Applications/Thunder.app/Contents/MacOS/目录下，但是在实现加载的过程中，其采用了@rpath方式加载，即会对多个路径进行搜索，而搜索又受到LC\_RPATH命令控制。

 通过执行命令otool –l Thunder，可以看到其32、33号命令都是LC\_RPATH，及包含两个搜索路径为：

1、/Applications/Thunder.app/Contents/Frameworks/

2、/Applications/Thunder.app/Contents/MacOS/

而根据命令先后顺序可知，首先会搜索1中的路径，因此存在dylib劫持漏洞。攻击者将精心制作的包含恶意代码的同名动态库（libetm.dylib）放在1中，应用程序就会首先加载该恶意dylib，



为了清晰的看到Thunder启动过程中，按照什么顺序搜索路径，设置环境变量export DYLD\_PRINT\_RPATHS="1"，输出LC\_LOAD\_DYLIB命令加载dylib库的详细信息。通过上述命令，可以看到环境变量已经被修改。



运行应用Thunder，

