可能大家会有疑惑，为什么一个exe程序的“扩展名”会显示为txt呢？其实，说它是一个“txt病毒”并不准确，严格来讲，它是一种混淆视听的手段。因为对于一个exe程序来说，我们不单单可以把它伪装成txt格式，还可以伪装成诸如jpg、doc、ppt等格式。其实现原理就是采用了“反转字符串”的方法。

我们就拿“熊猫烧香”病毒样本为例：

图3

首先可以使用Resource Hacker将该程序的图标修改为文本文档的图标：

图4

然后我们将这个程序重命名为“readtxt.exe”，此时保持重命名的状态别确定，将光标移到“read”与“txt”的中间，单击鼠标右键，选择“插入Unicode控制字符”中的“RLO”：

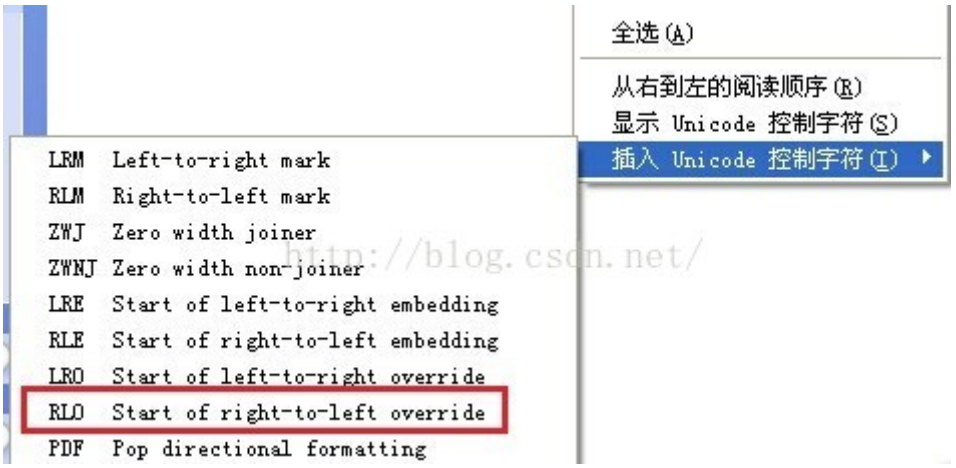

图5

这个“RLO”是一个转义字符，只要在一行字符前面加上它，就可以实现文本的反向排列。它是Unicode为了兼容某些文字的阅读习惯而设计的一个转义字符。当我们加入这个字符后，从而也就实现了图2中的效果。

那么利用这个原理，我们就能够实现非常多有创意的，并且颇具迷惑性的文件名称，再将文件的图标修改为对应的假的后缀名的图标，那么我相信，即便是资深反病毒爱好者，也很可能会落入陷阱的。