特洛伊木马的工作原理及清除

白 皓

（项城市气象局，河南 项城 466200）

摘 要：介绍了特洛伊木马程序的隐藏、加载及清除技术。

关键词：特洛伊木马；隐藏；隐藏；清除

中图分类号：**文献标识码**：B **文章编号**：1004－6372(2003)02－0042－01

计算机技术的飞速发展，使网络在气象部门广泛应用。但是网络技术的低门槛造就了一些恶意程序，特洛伊木马（以下简称“木马”）就是其中最常见的一种。如果计算机被植入了“木马”，就有可能被别人控制，从文件删除到硬盘格式化都轻而易举。“木马”传播的主要途径是捆绑在其他文件中，其中 EXE 格式最容易被捆绑，BMP、HTML、JPG、WAV、MP3 等格式也可能被捆绑，所以只要下载软件、浏览网页、收发邮件甚至听音乐，就有可能被植入“木马”。虽然有很多杀毒软件都声称可以清除“木马”，但它们并不能防范新出现的“木马”程序。只要知道“木马”的工作原理，就能及时发现并清除“木马”程序。

1 “木马”的隐藏

“木马”程序在运行的时候不会出现任何提示，也不会在任务栏和任务管理器中显示。它是如何隐藏的呢？“木马”把 Form 的 Visible 属性设为 False、ShowInTaskBar 设为 False，运行时就不会出现在任务栏中。另外，只要木马把自己设为“系统服务”，也不会出现在任务管理器中。

2 “木马”的加载

“木马”会在用户每次启动时自动装载服务端，Windows 系统启动时自动加载应用程序的方法 “木马”都会用上，主要有以下 3 种。

2.1 在 win. ini 文件中

在[WINDOWS]下面，“run = ”和“load = ”是可能加载“木马”程序的途径。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名为不熟悉的启动文件，计算机就可能中上“木马”了。另外，也得看清楚，因为好多“木马”，如“AOL Trojan 木马”，把自身伪装成 command. exe 文件，如果不注意可能不会发现它不是真正的系统启动文件。

2.2 在 system. ini 文件中

在[BOOT]下面有个“shell = 文件名”。正确的文件名应该是“explorer. exe”，如果是“shell = explorer. exe 程序名”，那么后面跟着的就是“木马”程序。

2.3 在注册表中

“HKEY－LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Run”目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为 EXE。切记有的“木马”程序生成的文件很像系统自身文件，想通过伪装蒙混过关。如“Acid Battery v1.0 木马”，它将注册表“HKEY－LOCALMACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”下的 Explorer 键值改为 Explorer = “C:\WINDOWS\expiorer. exe”，“木马”程序与真正的 Explorer 之间只有“i”与“l”的差别。在注册表中还有很多地方可以隐藏“木马”程序，如“HKEY－CURRENT－USER\Software\Microsoft\Windows\CurrentVersion\Run”、“HKEY－USERS\＊＊＊＊＊＊＊\Software\Microsoft\Windows\CurrentVersion\Run”目录下都有可能隐藏“木马”程序。

3 “木马”的清除

知道了“木马”的工作原理，清除“木马”就变得很容易。如果发现有“木马”存在，马上将计算机与网络断开，防止别人通过网络对你进行控制；然后编辑 win. ini 文件，将[WINDOWS]下面“run = ‘木马’程序”（或“load = ‘木马’程序”）更改为“run = ”（或“load = ”）；编辑 system. ini 文件，将[BOOT]下面的“shell = ‘木马’文件”更改为“shell = explorer. exe”；在注册表中，先在“HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”下找到“木马”程序的文件名，再在整个注册表中搜索并替换掉“木马”程序，还需注意的是：有的“木马”程序如 BladeRunner“木马”，并不是直接将“HKEY－LOCAL—MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”下的“木马”键值删除就行了，如果删除它，“木马”会立即自动加上，因此需要记下“木马”的名字与目录，然后退回到 MS－DOS 下，找到此“木马”文件并删除掉，重新启动计算机，再到注册表中将所有“木马”文件的键值删除，至此，木马就被成功地清除。

收稿日期：2002－12－16