影响存储介质的病毒分析与防范对策

徐　杨

(中南民族大学　工商学院计算机科学与技术系,湖北　武汉　430223)

摘　要:双击磁盘驱动器时,有时出现无法打开驱动器的情况。这类情况多是由于计算机病毒引起。分类描述了这类病毒的症状表现、传播途径及解决方法,最后给出一些相关建议。

关键词:磁盘驱动器;计算机病毒;解决方法

中图分类号:TP309.2　　文献标识码:A　　文章编号:1672-7800(2006)12-0064-01

1　症状表现

当我们双击磁盘驱动器时,有时会出现无法打开驱动器的情况。这种情况通常发生在上网过后或者使用过移动储存设备后。最基本的特征是:双击磁盘驱动器不能直接将其打开,必须使用右键弹出式菜单的“打开”的命令来完成打开磁盘驱动器的任务。磁盘驱动器的弹出式菜单第一项由原来的“打开”变成“自动播放”,机器的操作响应明显变慢,硬盘灯频繁闪烁,有些甚至出现杀毒软件和防火墙无故关闭,单击任何应用程序都出现“打开方式”对话框的情况。

2　传播途径及其危害

以上现象都是由于机器中病毒而引起。总体分为两类:一类是rose病毒及其变体;一类是木马病毒。

Rose病毒及其变体主要通过U盘、移动硬盘等移动储存介质传播。当双击移动储存介质盘符时,病毒即被激活。病毒在系统中占用大量CPU资源,如果不进行处理,操作系统很有可能崩溃。具体表现为,开机后无法进入系统。

木马病毒通过网络传播,一般隐藏在网页里或者论坛中。当打开网页或者点击相关链接时,它会自动下载到本地计算机。此类木马病毒不仅修改操作系统的设置,还会记录相关网络应用程序的账号和密码,通过电子邮件发送到盗号者手中。这类病毒的典型案例有lsass,Copy和Desktop病毒。

3　解决方案

对于每一种导致磁盘驱动器双击打不开的病毒,处理方法各有不同,即使都为木马病毒,表现情况大体相同,其处理方法也存在差异。因此,当有此类病毒侵入计算机时,首先要保持平静,结合机器表现出的细微特点,找出真正的病毒起因。心情急躁,没有对症下药,将会适得其反。

3.1　Rose病毒

(1)特征。①使用移动储存介质以后出现双击打不开磁盘驱动器的情况。②在Windows任务管理器的进程页面中,出现一个或多个“rose.exe”进程。

(2)针对Rose病毒的杀毒方法。①在Windows任务管理器的“进程”页面中,结束掉所有名称为rose.exe的进程。②通过“运行”对话框进入注册表,查找所有“rose.exe”键值,并将其删除。③在“文件夹选项”的“查看”页面中,点选“显示所有文件和文件夹”,删除“隐藏受保护的操作系统文件”。④通过右键的“打开”菜单,进入各个磁盘驱动器,在根目录下删除所有的“rose.exe”和“autorun.inf”文件。⑤重新启动计算机。

3.2　Copy病毒

(1)特征。双击各驱动器都弹出“windows找不到copy.exe文件”的对话框。

(2)Copy病毒的杀毒方法。①开机进入安全模式。在任务管理器中结束“temp1.exe”进程和“temp2.exe”进程。②在“文件夹选项”的“查看”页面中,点选“显示所有文件和文件夹”,去勾“隐藏受保护的操作系统文件”。③删除C:\WINDOWS\目录下的“xcopy.exe”文件和“svshost.exe”文件,C:\WINDOWS\system32目录下的“temp1.exe”文件和“temp2.exe”文件。④删除各磁盘根目录下的“autorun.ini”文件,“copy.exe”文件和“host.exe”文件。⑤用优化工具清理注册表

3.3　lsass病毒

(1)特征。①双击鼠标打不开D盘,出现打开对话框。②在进程页面中显示有两个lsass.exe进程。

需要说明的是,用户名SYSTEM下的lsass.exe是正常系统进程。而对应本机用户名的大写LSASS.exe进程是病毒进程。如果只出现系统进程lsass.exe是正常情况,不必怀疑自己中了lsass病毒。

(2)lsass病毒的杀毒办法。①记录病毒LSASS.exe进程的PID值,“运行”“cmd”,输入“ntsd-c q-p PID值”,将进程结束。②在“文件夹选项”的“查看”页面中,点选“显示所有文件和文件夹”,去勾“隐藏受

作者简介:徐杨(1980-),女,湖北武汉人,中南民族大学工商学院计算机科学与技术系助教,华中科技大学硕士研究生,研究方向为计算机网络。

木马的防范与清除技术研究

吴进波[1,2]，段善荣[1]

（1.咸宁学院 计算机系，湖北 咸宁 437005；2.武汉理工大学 计算机学院，湖北 武汉 430070）

摘 要：特洛伊木马常被用作网络系统入侵的重要工具和手段，它已经涉及到了计算机系统及网络安全的各个方面。介绍了木马的基本原理、及其入侵的手段，提出了针对木马入侵的防范措施和清除方法。

关键词：木马；入侵；客户/服务器

中图分类号：TP309.2 文献标识码：A 文章编号：1672-7800(2006)12-0065-03

0 前言

木马，全称特洛伊木马（Trojan horse），这一词语来源于古希腊神话，在计算机领域是一种客户/服务器程序，是黑客最常用的基于远程控制的工具。目前，比较有名的国产木马有：“冰河”、“广外女生”、“黑洞”、“黑冰”等；国外有名的木马则有：“SubSeven”，“Bo2000（Back Ori——fice）”、

保护的操作系统文件”。③删除病毒文件。删除C:\Program Files\CommonFiles\目录下的INTEXPLORE(.pif)文件；C:\Program Files\Internet Explorer\目录下的INTEXPLORE.com文件；C:\WINDOWS\目录下的EXERT.exe文件，IO.SYS.BAK文件和LSASS.exe文件；C:\WINDOWS\Debug\目录下的DebugProgram.exe文件；C:\WINDOWS\system32\目录下的dxdiag.com文件，MSCONFIG.COM文件和regedit.com文件。通过右键的‘打开’菜单，进入D盘驱动器，删除根目录下的“Autorun.inf”和“command.com”文件。④用优化工具清理注册表。⑤利用注册表修复软件修复相关键值。

3.4 Desktop病毒

由木马病毒引起的Desktop病毒的发作有一个过程，首先是双击打不开一个或多个磁盘驱动器，然后出现杀毒软件防火墙自动关闭（以便盗取网络应用程序的账号和密码），杀毒软件加载出错。有甚者出现双击所有应用程序都出现‘打开’对话框。

这种病毒通过线程注入技术能够绕过防火墙的监视，连接到病毒作者指定的网站下载特定的木马及其他病毒。因此，如果上网期间发现硬盘灯无故频繁闪烁，应该及时执行断网操作。

如果遇见所有的应用程序都打不开的情况，建议用Ghost恢复系统盘。利用Ghost恢复系统盘不同于系统还原。系统还原只是把以前的还原点提出来，然后覆盖到系统上。这样只是修复系统但病毒并没有删除。而Ghost是在删除原先系统的基础上，按照Ghost文件备份恢复系统。因此，恢复后的系统和原系统没有关联。但使用这种方法的前提是：先利用Ghost备份过系统。

系统盘恢复后，其他磁盘驱动器可能还是双击打不开，这时只需将其根目录下的隐藏文件“Autorun.inf”删除即可解决。

4 建议

对于移动储存介质，预防Rose及其变体病毒的操作是：当插入计算机出现操作提示框时，不要选择任何操作，直接关掉。通过右键的弹出式菜单选择‘打开’进入。因为直接双击会激活病毒。建议在计算机上使用移动储存介质时，先杀毒，后使用。此外，在公共场所使用移动存储介质，将介质属性调为只读状态，能够避免病毒的写入。

lsass、Desktop等木马病毒，主要通过网上传播。因此，在浏览网页和论坛时，不要轻易点击链接。下载网络资源，先杀毒，再使用。

对于IE浏览器的设置，最好在‘安全’界面的‘自定义级别’中，禁用Java程序脚本。能够阻止木马程序的下载。

如果已经中了病毒，也要保持头脑冷静，不要盲目格机。毕竟有些重要资源丢了可惜。发现异常情况，及时用杀毒工具进行查毒处理，并借用网络共享资源分析异常原因。抓住问题的关键进行排查和解决。

参考文献：

[1] 徐超汉.计算机网络安全实用技术[M].北京：电子工业出版社，2005.

[2] 吴世忠.网络信息安全的真相[M].北京：机械工业出版社，2001.

[3] 张友生，米安然.计算机病毒与木马程序剖析[M].北京：北京科海电子出版社，2003.

（责任编辑：曙 光）

作者简介：吴进波（1972-），男，咸宁学院讲师，主要研究方向为演化计算、计算机免疫学；段善荣（1974-），女，硕士，讲师，主要研究方向为计算机免疫学、计算机安全。