计算机木马病毒检测与防范

杨小刚
（湖南电子科技职业学院，湖南 长沙 410000）

摘 要 随着网络的发展和普及，计算机网络系统的安全问题也变得日益突出和复杂。木马病毒作为最常见计算机病毒之一，具有传播快、危害大等特征，给网络安全带了巨大的威胁。本文通过分析了木马原理和常见的木马分类，给出了木马检测和清除办法及木马防范。

关键词 木马；检测；防范

1 前言

木马（Torjan Horse），其名称取自古希腊的特洛伊木马记，它们悄悄地在寄宿主机上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限，在黑客进行的各种攻击行为中，木马都起到了先锋的作用。

2 木马概述

木马是一种基于远程控制的黑客工具，它通常寄生于用户的计算机系统中。 木马也是种病毒，它并不像普通计算机病毒那样感染计算机文件，木马一般以寻找后门、窃取密码和重要文件为主，还可以对计算机进行跟踪监视、控制、查看、修改资料等操作，并具有很强的隐蔽性、突发性和攻击性。

木马的传播方式主要有三种。一种通过 E-mail，攻击者将木马程序以邮件附件的形式发送出去，收件人只要打开附件就会感染木马；第二种是软件下载，一些非正式的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，下载完后只要运行程序，木马就会自动安装；第三种是通过会话软件的“传送文件”（如 QQ）进行传播，不知情的网友一旦打开带有木马的文件就会感染。

木马采用客户端（Client）/服务器（Server）工作模式。木马程序一般包含了客户端和服务端，客户端放在木马攻击者的计算机中，服务端放置在受害者的计算机中，木马攻击者通过客户端与受害者的计算机的服务端建立远程连接，一旦连接建立，攻击者可以随心所欲的控制受害者的计算机，如删除文件、更改密码等。

3 木马的分类

根据木马的特点及危害范围，木马可以分为针对网络游戏的木马、针对网上银行的木马、针对即时通信工具的木马、给计算机开后门的木马和推广广告的木马等五大类。

3.1 网游木马

随着网络游戏超高速发展，网上虚拟交易比较火爆，一些别有用心的病毒作者把目光盯在了这一安全性比较薄弱的环节上。2004 年，大量的网络游戏木马涌现。如果受害者计算机感染了网络游戏木马，用户账户就会被盗取，并把游戏装备转移，再由木马使用者卖出这些被盗取的游戏装备而获利。

3.2 网银木马

网络银行木马专门针对网上银行进行攻击，采用键盘记录的方法盗取网银的账号和密码，导致用户经济损失。

3.3 即时通信木马

该类木马利用及时通信工具（如 QQ、MSN）进行传播。受害者感染后会自动下载指定的病毒程序，造成恶作剧，比如“MSN 我要结婚的病毒”，受害者会向联系人自动发送大量的“我今天要结婚”的恶作剧信息。

3.4 后门程序

该类木马在网络中大量的传播。该类木马采用反弹端口技术绕过防火墙，对被感染的计算机进行远程文件管理和注册表等操作，并可以捕获被控制的计算机屏幕，可远程控制计算机。

3.5 广告程序

广告程序木马采用修改 IE 网页浏览器的默认主页，禁止多种系统功能，收集系统信息发送给传播广告木马的网站，更恶毒的是修改网页定向，导致一些网站不能登陆。

4 木马的检测和清除

计算机用户可以通过查看系统端口开放的情况、系统服务情况、系统任务运行情况、网卡的工作情况、系统日志及

运行速度有误异常等方法对木马进行检测。检测到计算机感染木马后，就要根据木马的特征进行清除。

4.1 查看开放端口

目前最为常见的木马通常是基于 TCP/IP 协议进行客户端与服务端之间的通信。因此可以通过查看本机的开放的端口、检查是否有可疑的程序打开了某个可疑的端口，如“冰河”木马使用的监听端口是 7626，“Back Orifice2000”使用的监听端口是 54320，“灰鸽子”使用的监听端口是 1027 等等。在 Windows 系统中可以使用本身自带的 Netstat 命令进行查看。

4.2 查看和恢复 win.ini 和 system.ini 系统配置文件

查看和恢复 Win.ini 和 system.ini 文件是否被修改。有些木马通过修改 win.ini 文件中 windows 节的“load=file.exe，run=file.exe”语句进行自动加载，还可能修改 system.ini 中的 boot 节，实现木马加载，例如“shell=explorer.exe”修改成“shell=yzw.exe”。计算机用户只需恢复 win.ini 和 system.ini 原始数据，再删除木马文件。

4.3 查看启动程序并删除可疑的启动程序

如果木马自动加载的文件是直接通过 window 菜单上自定义添加的，一般都会放在主菜单的“开始—程序—启动”处。

4.4 查看系统进程并停止可疑的系统进程

木马再狡猾，也只是一个应用程序，需要在进程中执行，因此可以通过查看系统进程来推断木马是否存在，在 WindowsNT/XP 系统下，按下 Ctrl+Alt+Del 进入任务管理器，就可以查看系统正在运行的所有进程，如果对系统非常熟悉，对每个系统运行的进程知道它的作用，那么在木马运行时，就很容易发现哪个是木马程序的活动进程。在对木马清除时，首先要结束木马程序的系统进程，并进行下一步操作，修改注册表和清除木马文件。

4.5 查看和还原注册表

有些木马一旦被加载，会对注册表进行修改，通常，木马在注册表实现加载文件在以下几处：

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runonce

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservices

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservicesonce

HKEY_CURRENT_USER\software\microsoft\windows\currentversion\ runonce

HKEY_CURRENT_USER\software\microsoft\windows\currentversion\ runservices

此处，在注册表中的 HKEY_CLASSES_ROOT\exefile\shell\open\command= "" %1 " %* " 处，如果其中的 " %1 " 被修改为木马，那么每启动一次该可执行文件时木马就会自动启动一次。

查看注册表，将注册表中木马修改的部分还原。如，Hack.Rbot 病毒对注册表有关目录中添加键值 MicrosoftUpdata=Wuamgrd.exe，以便木马可随机启动，这时需要先进入注册表，将键值 MicrosoftUpdata=Wuamgrd.exe 删除掉。

4.6 使用杀毒软件和木马查杀工具检测和清除木马

最简单的检测和删除木马的方法是安装木马查杀软件，如卡巴斯基、瑞星、金山毒霸等。

5 木马的防范

目前木马已对计算机用户信息安全构成了极大隐患，做好对木马的防范工作已经刻不容缓。以下是最简单实用的木马预防方法和措施。

（1）不随意打开来历不明的邮件，阻塞可疑邮件。

（2）不随意下载来历不明的软件。

（3）及时修补漏洞和关闭可疑的端口。

（4）尽量少用共享文件夹。

（5）运行实时监控系统。

（6）经常升级系统和更新杀毒软件。

（7）限制不必要的具有传输能力的文件。

（8）关闭不常使用端口。

6 结束语

对于网络中比较流行的木马程序，传播速度快，危害比较严重，因此我们掌握了许多木马检测和清除方法的同时增强我们对木马的预防意识和措施，才能有效地防治木马的攻击。

参考文献

[1] 李涛.网络安全概述.北京：电子工业出版社，2004

[2] 刘远生.计算机网络安全.北京：电子工业出版社，2006

[3] Eric Maiwald 著，李庆荣等译.网络安全实用教程.北京：清华大学出版社，2003

[4] 林海等.计算机网络安全.北京：高等教育出版社，2002

收稿日期：4 月 27 日 修改日期：5 月 4 日

作者简介：杨小刚（1982-）男，汉族，湖南宁乡人，本科，湖南电子科技职业学院助教，研究方向：网络安全。