浅析计算机病毒对气象业务网络的危害与防范*

龚贤创
(武汉气象中心,湖北 430074)

摘　要

简要地介绍了对气象业务网络危害极大的计算机病毒,分析了计算机病毒发展的趋势。介绍了武汉气象中心防病毒系统的设计及实践。表明"分组、分级"管理模式的计算机病毒防御系统能有效地抵御病毒对网络的进攻,保证气象业务正常运行。

关键词:计算机网络　计算机病毒　防毒系统

1　计算机病毒及发展的趋势

目前全世界已有超过 47000 多种计算机病毒,新的计算机病毒还在不断的产生。计算机病毒大致可分为:程序型病毒、引擎型病毒、宏病毒、蠕虫病毒、特洛伊木马型病毒,多态加密病毒等几种类型。

传统的计算机病毒传播主要是通过软盘、光盘等存储介质来实现的,其破坏对象主要是使用这些介质的单机系统,影响面有限。随着计算机网络的发展和 Internet 的普及,计算机病毒通过网络来传播,扩散途径有 1) 利用服务器漏洞植入后门程序的特洛伊木马;2) 通过电子邮件大肆传播,衍生出无数变种的计算机蠕虫,在近年破坏力较大的计算机病毒中,特洛伊木马、蠕虫型病毒占绝大部分;3) 通过浏览网页下载病毒[1,2]。

现代计算机病毒破坏和攻击对象已经不限于个人主机上的文件、内存资源、CPU 资源,出现了对网络的重要设备诸如 DNS、路由器、网络服务器进行攻击的病毒,具有很大的危害性。其次是计算机病毒结合传统病毒自动传播技术和黑客缓冲溢出技术的特点,一旦爆发就会具有规模效应。如 2001 年 7 月爆发的 nimda(尼姆达)计算机病毒,局域网内某台计算机感染上该病毒后,病毒迅速地在网内蔓延开来,形成连锁反应。武汉气象中心业务网络中有近百台计算机感染上了 nimda(尼姆达)病毒,险些造成整个业务系统的瘫痪。

随着计算机技术的不断发展,计算机病毒也变得越来越高级和复杂,有些病毒已经是多种类型计算机病毒的混合体,很难应用常规的方法对这类计算机病毒进行防范和清除。

2　计算机病毒防范的措施

传统的计算机病毒防范是采取"等待、发现、更新、杀除"的一种被动工作模式。它已

* 本文由湖北省气象局"湖北省气象局新型高速计算机网络改造"项目资助。
2002-03-25 收到,2002-09-18 收到修改稿。

经不能很好地遏制现代计算机病毒的传播与发展。针对计算机病毒发展的新特点应制定积极主动的计算机病毒防范措施。

计算机病毒防范的措施之一是及时作好系统的补漏工作[3]。计算机病毒通过系统软件设计中出现的漏洞进行传播是当前的计算机病毒扩散主要途径之一。计算机系统软件的设计商针对系统中存在的隐患和漏洞会定时发布系统补丁程序,而利用这些隐患和漏洞传播的计算机病毒程序往往滞后于补丁程序的出现。及时下载系统补丁程序,堵住系统的漏洞,是控制计算机病毒传播的一个很好的方法。

封住计算机病毒进入系统的通道是防范计算机病毒的另一项措施。应在网关、服务器、客户机等各个节点严密把守,才有可能避免计算机病毒的渗透。近年通过电子邮件和网络进行病毒传播的情况越来越严重,计算机网关是病毒进入网络的第一道入口。计算机网络的网关的防病毒显得尤为重要。计算机病毒一旦在网内传播开来,再对其逐一清除是件非常困难的事情。相对而言在网关处开始防计算机病毒,拒计算机病毒于网外则要容易得多。

防止计算机病毒的破坏,保证网络安全需要整个网络安全体系来支撑[4]。单纯的防病毒或防黑客都很难保证系统的安全,应该进行综合考虑。建立起"防毒注重堵漏"和"防毒与防黑并重"的意识。在系统服务器的软件安装时,应该最大限度地增加安全性能高的选件。对重要服务器使用防火墙技术,进行访问控制保护。在不影响业务的情况下,应经常对网络服务器的内容进行备份。

3 武汉气象中心业务网络计算机病毒防范体系

武汉气象中心网络系统(见图 1)包含四个部分:网关、邮件服务器、文件服务器、桌面机。这里,网关是使用代理服务器为共享上网提供服务;邮件服务器使用 Notes Server 作为邮件代理服务;文件服务器使用 NT Server 作为业务系统的共享文件服务器;桌面计算机多数使用 Win98/2000。由于气象信息具有相当高的时效性和共享性,使得气象业务网络的计算机防病毒工作增加了难度。计算机病毒的生存机率与传播能力成正比,当计算机病毒感染那些共享的气象信息和数据后,就可能传播到使用这些数据的计算机系统,并迅速地蔓延开来。信息共享程度越高,计算机病毒传播速度也就越快。如果限制气象信息的共享,则会降低它们的使用时效,而失去应有的价值。

来自系统外部(Internet 或外网)的病毒入侵,这是目前计算机病毒进入气象业务网络的主要途径。因此在与外部连接的网关处进行计算机病毒拦截,则是效率最高耗资最少的措施。可以使进入内部的病毒数量大为减少。

气象业务网络内部采用邮件 Notes Server 系统实施办公和信息自动化,每天在内部进行大量交换政务信息和电子邮件的工作。如果不进行计算机病毒防范,网络邮件 Notes Server 就可能成为计算机病毒集散地之一。一旦有某个用户感染了病毒,通过电子邮件方式该病毒将以几何级数的增长模式在网络内迅速传播,并且很容易导致邮件系统负荷过大从而瘫痪。

文件资源共享是网络提供的基本功能。文件服务器大大提高资源的重复利用率,并

且能对信息进行长期有效的存储和保护。气象预报业务系统 MICAPS 主要是通过共享文件服务器 NT Server 进行工作的。然而,一旦服务器感染了计算机病毒,就会对所有访问者构成威胁。计算机病毒入侵的另外一个途径就是桌面用户。由于网络的共享性,某个感染病毒的桌面计算机可能随时感染到其他机器,因此在网络内对所有的客户机进行防毒控制是很有必要的。

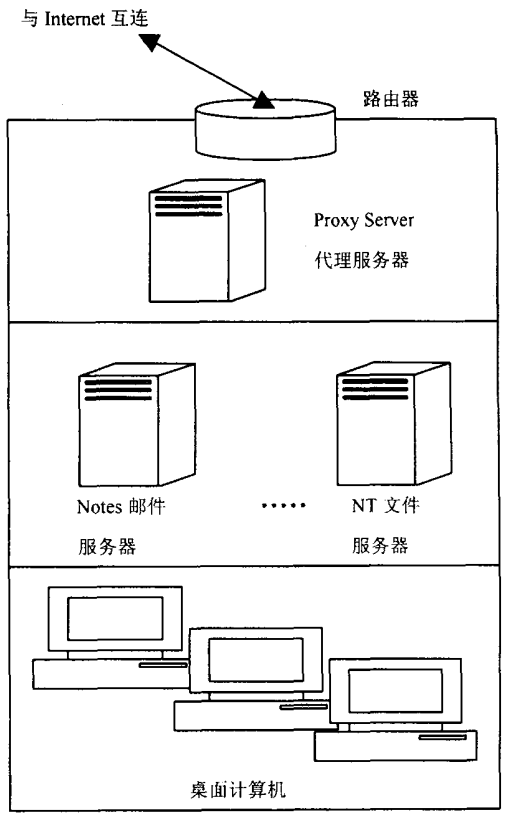

图 1　武汉气象中心网络构成示意图

武汉气象中心防计算机病毒系统主要是针对网关、邮件系统、文件服务器和桌面计算机四方面进行计算机病毒的防范。(1) 网关防毒,主要是对流经网关的 SMTP、HTIP 和 FTP 信息进行病毒扫描和查杀,该软件部署在网关处的代理服务器上;(2) 邮件系统防毒,定时地扫描并清除邮件邮箱和公共文件中附带的病毒以及其他功能;(3) 文件 NT 服务器的防毒,实现对计算机病毒监控,病毒码自动更新功能以及病毒活动日志、多种报警通知等功能;(4) 桌面客户机的病毒防护,实现通过服务器自动分发和更新客户端工作站的防计算机病毒软件。

对于气象业务网络来说,部署防计算机病毒系统是比较复杂的,尤其是各业务系统分布在不同的建筑物中,需要通过一套管理模式来实现对整个系统内的防毒工作。武汉气象中心建立了防治计算机病毒的"分组、分级"管理模式;既将信息安全的管理权限分为多个级别,首先建立业务网络的防计算机病毒超级管理员,然后依据业务系统类型的不同创建若干普通管理员,将同类业务的若干客户端分派给他,成为一个管理分组;普通管理员可以对自己管理的客户端进一步分组,加以管理。在这种管理模式下,超级管理员和普通管理员的权限和分工是相当明确的。防计算机病毒超级管理员主要具备添加、删除普通管理员的帐号以及对全网的计算机进行查杀计算机病毒等职能;普通管理员则主要负责对所辖的计算机进行分组和查杀计算机病毒。这种分级管理模式使得计算机病毒的查杀工作管理起来更加明确和有效。

当气象网络局部范围内业务系统感染了某种计算机病毒时,可由普通管理员完成局部范围内的计算机病毒的查杀工作。如果某种计算机病毒大范围侵入气象业务网络时,局部范围内查杀计算机病毒的工作则是难以奏效的,需要进行全网同步杀毒工作。如 2001 年武汉气象中心业务网络内计算机感染了 nimda(尼姆达)病毒,表现的特征是感染系统内部 dll 文件,并且产生大量复制的垃圾邮件,造成系统响应速度明显下降,严重地影

响了气象业务系统的正常工作。超级网络管理员根据该病毒发作的特性,向全网客户端发出查杀 dll 文件的命令。全网的计算机在不影响气象业务正常工作的情况下,在后台完成查杀计算机病毒的工作。通过实践来看,这种管理办法是成功的,它有效地遏止了计算机病毒在气象中心业务网络中的蔓延,保障气象业务网络的安全。同时降低维护工作人员的数量和维护成本,缩短了升级、维护系统的响应时间。

4 结束语

计算机病毒的防范工作除了上述的技术措施外,还要加强管理措施工作。气象业务部门应该尽快地建立和完善相应地规章制度,并严格执行。同时对工作人员进行计算机病毒及其危害性的教育,增强广大工作人员对计算机病毒的防范意识。

参 考 文 献

1 李海泉,李建. 计算机网络安全与加密技术. 北京:科学出版社,2000. 399 ~ 504.
2 刘荫铭,李金海. 计算机安全技术. 北京:清华大学出版社,2000. 227 ~ 241.
3 胡昌振,李贵涛. 面向 21 世纪网络安全与保护. 北京:北京希望电子出版社,1999.
4 宁 章. 计算机及网络安全与保护基础. 北京:北京航天大学出版社,1999.

BRIEF ANALYSES OF VIRUS DAMAGE TO METEOROLOGICAL OPERATIONAL NETWORK AND ANTI-VIRUS METHODS

Gong Xianchuang
(*Wuhan Meteorological Center, Wuhan* 430074)

Abstract

The computer virus damage to the meteorological operational network and the computer virus's variation tendency are analyzed. The design and application of the anti-virus system of the Wuhan Meteorological Center, Hubei Province, are introduced. It is shown that the anti-virus system using the group and rank management model is effective against computer virus for the meteorological operational network and can insure the normal operation of meteorological service.

Key words: Meteorological operational network Computer virus Anti-virus system