浅议高校机房病毒危害及其防范

刘莉琳
(西安财经学院 陕西西安 710061)

摘 要:高校计算机机房的设备非常容易受到病毒的感染,给计算机教学和带来了极大的不便和危害。本文是从计算机病毒的定义展开,针对高校计算机房常见病毒种类和危害,从加强管理、技术和网络三个方面进行防范提出的自己的见解和看法。
关键词:病毒 危害 防范 机房 高校
中图分类号:G647 文献标识码:A 文章编号:1672-3791(2013)01(a)-0019-01

随着科学技术的不断发展,计算机及其技术得到了更为广泛的应用,计算机课程已成为高校的必修课之一。高校计算机房由于计算机终端多,使用人员复杂,且与各种网络相连,容易遭到病毒破坏。

1 计算机病毒

计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。通俗来讲,计算机病毒就是一个程序或一段可执行代码,通过网络、U盘等蔓延影响计算机正常用。

2 机房常见计算机病毒

计算机病毒可分类有很多种,按照病毒属性可分为以下几大类。

(1)按存在媒体分。可分为网络病毒,文件病毒,引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件,文件病毒感染计算机中的文件(如:COM,EXE,DOC等),引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。

(2)按传染方法分。病毒可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,程序挂接系统调用并合并到操作系统中去。非驻留型病毒在得到机会激活时并不感染计算机内存。

(3)按破坏能力分。病毒可分为无害型、无危险型、危险型和非常危险型。无害型除了传染时减少磁盘的可用空间外,对系统没有其它影响;无危险型仅仅是减少内存、显示图像、发出声音及同类音响;危险型在计算机系统操作中造成严重的错误;非常危险型能删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

(4)按病毒算法分。病毒可分为伴随型、蠕虫型、寄生型、诡秘型和变型病毒,伴随型病毒并不改变文件本身,它们根据算法产生EXE文件的伴随体,当DOS加载文件时,伴随体优先被执行加载执行原来的EXE文件;蠕虫型病毒通过计算机网络传播,不改变文件和资料信息,利用网络从一台机器的内存传播到其它机器的内存,计算网络地址,将自身的病毒通过网络发送;寄生型病毒指伴随型和蠕虫型外的其他病毒都称为寄生型病毒;诡秘型病毒一般不直接修改DOS中断和扇区数据,而是通过设备技术和文件缓冲区等DOS内部修改,不易看到资源,使用比较高级的技术。利用DOS空闲的数据区进行工作;变型病毒(又称幽灵病毒)这一类病毒使用一个复杂的算法,使自己每传播一份都具有不同的内容和长度。

3 计算机病毒的主要危害

计算机病毒不但可能会对计算机单机硬件及软件系统造成破坏,可能也会对互联网产生灾难性的打击。随着信息网络技术的发展,计算机病毒的威胁日益严重。

(1)直接破坏数据信息。大部分病毒激发时直接破坏计算机的信息数据,包括格式化磁盘、改写文件分配表和目录区、删除重要文件等。被病毒破坏的硬盘,有些还可以进行数据修复,不要轻易放弃。

(2)占用磁盘空间。寄生在磁盘上的病毒总要非法占用一部分磁盘空间。一些文件型病毒传染速度很快,在短时间内感染大量文件,每个文件都不同程度地加长了,就造成磁盘空间的严重浪费。

(3)抢占系统资源。大多数病毒会抢占系统资源,抢占内存,还抢占中断,导致内存减少,导致一部分软件不能运行,从而干扰了系统的正常运行。

(4)影响运行速度。病毒影响计算机速度,主要表现:病毒判断传染激发条件时增加了对计算机的状态监视,病毒加密运行需额外执行指令,病毒进行传染时同样要插入非法的额外操作。

(5)不可预见危害。绝大部分病毒都存在不同程度的错误。错误病毒的另一个主要来源是变种病毒。计算机病毒错误所产生的后果往往是不可预见的,人们不可能花费大量时间去分析数万种病毒的错误所在。大量含有未知错误的病毒扩散传播,其后果是难以预料的。

(6)系统运行影响。兼容性是计算机软件的一项重要指标。病毒的编制者一般不会在各种计算机环境下对病毒进行测试,因此病毒的兼容性较差,常常导致死机。

(7)用户心理压力。实际上,计算机并没有病毒。当是出现诸如计算机死机、软件运行异常等现象时,普通用户去准确判断是否是病毒所为,给人们造成巨大的心理压力。

4 高校机房病毒防范

随着病毒的不断变种,网络病毒越来越多,而且因为网络的开放性,所以这种病毒的传染速度更快,破坏力更强。随着计算机应用的发展,人们深刻地认识到凡是病毒都可能对计算机信息系统造成严重的破坏。

(1)从管理上防范。从管理上加强预防,要做到不运用来历不明的软件,特别是盗版软件。机房应制止未经检测的移动盘插入计算机,严禁上机打游戏。由于游戏的运转环境较多,传染病毒的可能性较大;本单位运用的计算机应有严厉的运用权限;对一切的系统盘以及移动盘停止写维护,避免盘中的文件被感染;系统中的重要文件要停止备份,特别是数据要定期备份;规定合理的读写权限等。

(2)加强技术防范。从技术办法加强预防。采用内存常驻防病毒的程序;运转前对文件停止检测;改动文档的属性;改动文件扩展名等,可以使得大多数病毒会失去效能。

(3)加强网络防范。要建立一个整套网络软件及硬件的维护制度,定期对电脑进行维护。在维护前,要注意做好数据转移或者备份工作;同时,要采取必要的安全保护措施,防止操作系统被破坏。对计算机的网络软件文件,在维护时,可以隐藏、只读等措施,防止学生在使用时无意间删除等。同时,在教学课练习时,可以利用网络设置软件分别规定应防问共享区的存取权限、口令字等安全保密措施,从而避免共享区的文件和数据等被破坏。对一台电脑,都要设置上网口令,并记录下每天的网络运行日志,以便有针对性检查维护等。最后需要说明的是,对网络软件的维护,电脑故障的维修,一定要指定专人,严格按操作手册进行。

因使用人群多,高校计算机机受到病毒威胁概率更大,保证计算机安全,光靠软件是不行的,最重要的是要用户有良好的计算机使用习惯和病毒防范意识。

参考文献

[1] 方涛.学校机房计算机病毒的防范与解决方法[J].信息与电脑(理论版),2011(1).
[2] 齐春妮.基于网络中控环境下的高校多媒体教室管理——以闽江学院为例[J].福建电脑,2009(12).
[3] 裴虹,裴波.高校多媒体教室建设的研究与探讨[J].高等工程教育研究,2008(S1).
[4] 邵清.浅谈我校校园网络安全隐患及防护措施[J].电脑知识与技术,2011(20).