经吉林省中小学教材审定委员会审查通过

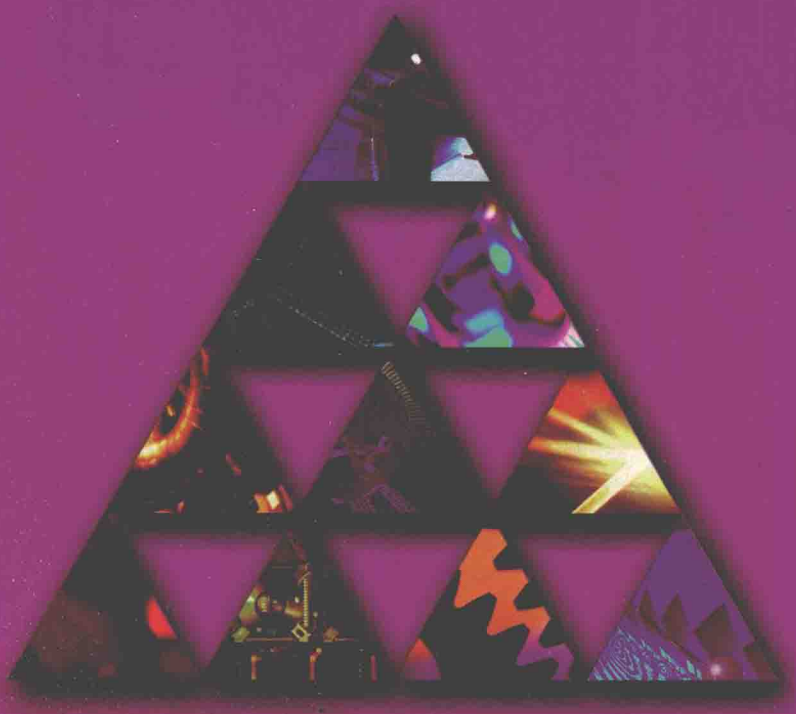
全国哲学社会科学"九五"重点课题
"面向21世纪中国基础教育课程教材改革研究"研究成果

初中版

信息技术

第三册

主编 / 董玉琦 解月光



吉林教育出版社

全国哲学社会科学“九五”规划国家重点课题
“面向21世纪中国基础教育课程教材改革研究”
研究成果

信息技术

初中版　第三册

主编　董玉琦　解月光

吉林教育出版社

信息技术　初中版　第三册　　董玉琦　解月光　主编

责任编辑　崔剑仑　　装帧设计　王　康

出版　吉林教育出版社（长春市同志街1991号　邮编　130021）
发行　吉林省新华书店发行集团有限公司
印刷　长春市时风彩印有限责任公司

开本　787毫米×1092毫米　1/16　8.5印张　　字数　210千字
版次　2003年6月第2版　2013年7月第12次印刷
定价　8.09元
书号　ISBN 978-7-5383-4229-1

前　言

2000年10月在北京召开了全国中小学信息技术教育工作会议。会上教育部决定，从2001年起，用5－10年的时间在全国中小学普及信息教育，全面实施“校校通”工程，以信息化带动教育的现代化，努力实现基础教育跨越式的发展。

全国哲学社会科学“九五”规化国家重点课题“面向21世纪中国基础教育课程教材改革研究”的子课题——“中小学信息教育的实证研究”立项以后，经过充分准备，开发了第一轮实验教材，并从1999年9月开始在东北三省的几十所实验学校使用；2000年9月，第二轮实验教材通过吉林省中小学教材审定委员会的审定，作为吉林省中小学信息技术实验教材在吉林省中小学使用。本套教材就是在第一轮、第二轮实验教材的基础上，经广泛征求使用该教材的教师、学生以及各界关注中小学信息教育研究的有关人士的意见和建议，组织本学科一线教师精心编写而成的。分为小学版、初中版。

中小学信息技术课程的根本目标在于培养学生的信息素养。信息素养的基本内涵是“信息处理能力”，即恰当地选择信息工具，主动地利用信息资源，有效地采集信息、加工信息、发布信息等处理信息的基本能力；信息技术课程的内容不仅包括信息技术的学习，还包括信息科学的学习、信息伦理道德和法律法规的学习等；在信息技术课程的学习方法方面，应突出研究性学习、协作性学习、自主性学习等。

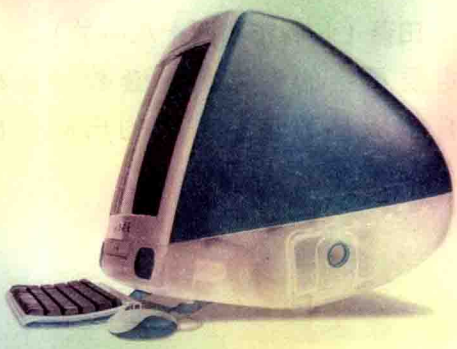
本套教材由董玉琦、解月光主编。本书是本套教材初中版的第三册（共五册，初中一、二年级每学期各一册，初中三年级全一册），分为五个单元，使用十八学时左右。参加本书编写的人员有董玉琦（东北师大）、解月光（东北师大）、王业宏（长春市第四十五中学）、于洋（长春市第九十八中学）、杨杰（长春市第四十七中学）、田薇（长春市第四十八中学）。

本教材审定委员会的专家为这套教材初稿提出了十分中肯的意见与建议，吉林教育出版社为这套教材的出版付出了诸多努力，在此一并谨致谢意。

编　者

2002年5月

目　　录



第一单元

计算机病毒的防治

在信息化高速发展的今天，计算机已经越来越被大多数人了解和使用，计算机软件也随着人们需求而飞速发展，但是这种可以代替人类脑力劳动的电子产品，也出现了它的“杀手”——计算机病毒。计算机病毒不但可以破坏计算机的软件，还可以破坏计算机的硬件系统，使计算机无法正常工作，给用户带来极大的不便。那么怎样解决这个问题，对付这个“杀手”呢？让我们进行以下知识的学习。

【学习目标】

1. 了解信息安全的重要性;
2. 认识到计算机病毒的危害、了解计算机病毒的种类、掌握计算机病毒的预防措施;
3. 会使用一些常用的杀毒软件。

【学习设备、设施】

计算机及一些常用的杀毒软件。

【学习活动】

1. 学习信息技术知识与技术一;
2. 学习信息技术知识与技术二;
3. 同学以组为单位给计算机杀毒;
4. 每组同学要完成一篇有关计算机病毒体会的报告。

【学习成果】

1. 会使用杀毒软件;
2. 写一篇关于计算机安全方面的小论文。

【基础知识与技能】

1. 计算机病毒简介;
2. 杀毒软件的使用方法。

信息技术知识与技能一：

计算机病毒简介

一、什么是计算机病毒

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，就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

1. 病毒的危害

计算机染上病毒发作后就很容易感觉出来，计算机病毒发作时一般会有较明显的现象，如有时计算机的工作会很不正常、程序运行不了、莫名其妙地死机、突然重新启动；有的病毒发作时一下子黑屏、蓝屏，病毒通常会破坏内存里的数据和硬盘上的文件，非常危险。

但也有一些病毒并不发作，只是占据硬盘空间。总之，只要计算机工作不正常，就有可能是染上了计算机病毒。

计算机病毒的危害是多方面的，在小的方面，它可以让计算机不能正常工作，把工作成果毁坏一空；在大的方面，它可以使银行、企业以及科研机构的计算机系统瘫痪，有时甚至无法用金钱来计算它所带来的损失。

另外，应用计算机病毒破坏军事对手的电脑网络和指挥系统也已经成为战争中的一种有效而实用的手段。

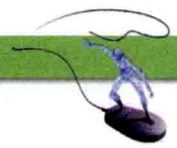
2. 病毒的分类

（1）按寄生方式分为引导型病毒、文件型病毒和复合型病毒

引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的特点，在引导系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。如1575/1591病毒、848病毒感染.COM和.EXE等可执行文件;Macro/Concept、Macro/Atoms 等宏病毒感染 .DOC 文件。

复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治，如果只发现该病毒的一个特性，把它只当做引导型或文件型病毒进行清除。虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。这种病毒有 Flip 病毒、新世纪病毒、One-half 病毒等。




(2) 按破坏性分为良性病毒和恶性病毒

良性病毒是指那些只是为了表现自身，并不彻底破坏系统和数据，但会大量占用CPU时间，增加系统开销，降低系统工作效率的一类计算机病毒。这种病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据,而是为了让使用染有病毒的计算机用户通过显示器或扬声器看到或听到病毒设计者的编程技术。这类病毒有小球病毒、1575/1591病毒、救护车病毒、扬基病毒、Dabi病毒等等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张。也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

恶性病毒是指那些一旦发作后，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。这类病毒有黑色星期五病毒、火炬病毒、米开朗基罗病毒等。这种病毒危害性极大，有些病毒发作后可以给用户造成不可挽回的损失。

二、病毒的特征代码

1. 非授权可执行性

用户通常调用执行一个程序时，把系统控制交给这个程序，并分配给它相应系统资源，如内存，从而使之能够运行完成用户的需求。因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序，而故意调用执行。但由于计算机病毒具有正常程序的一切特征性：可存储性、可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常程序。

2. 隐蔽性

计算机病毒是一种具有很高编程技巧、短小精悍的一段可执行程序。它通常粘附在正常程序之中或磁盘引导扇区中,或者磁盘上标为坏簇的扇区中,以及一些空闲概率较大的扇区中,这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

3. 传染性

传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质,然后通过自我复制迅速传播。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内，通过像 Internet 这样的网络传遍世界。

4. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力,这种媒体我们称之为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间越长，病毒传染的范围也越广，其危害性也越大。

5. 表现性或破坏性

无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源(如占用内存空间,占用磁盘存储空间以及系统运行时间等)。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序，删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无

可挽回的损失。因此，病毒程序的副作用轻者降低系统工作效率，重者导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，使之进行传染;或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件可以是敲入特定字符，使用特定文件，某个特定日期或特定时刻，或者是病毒内置的计数器达到一定次数等。

三、计算机病毒的主要来源

计算机病毒主要来源于：从事计算机工作的人员和业余爱好者的恶作剧、寻开心制造出的病毒；软件公司及用户为保护自己的软件被非法复制而采取的报复性惩罚措施；旨在攻击和摧毁计算机信息系统和计算机系统而制造的病毒，蓄意进行破坏；用于研究或有益目的而设计的程序，由于某种原因失去控制产生了意想不到的效果。

信息技术知识与技能二：

杀毒软件的使用方法

既然计算机病毒也是程序，也是由人编写出来的，那我们就会有办法来对付它，使用杀毒软件是消灭病毒最直接的方法。杀毒软件可以把病毒杀死，将它们从计算机中清除出去。

但是杀毒软件毕竟只是弥补的措施，一旦计算机中的资料已经被破坏，那么即使把病毒杀死，也是无法找回以前的资料了，这个损失可是相当大的。所以，预防病毒才是最重要的。比如“kvw3000”就是一种很好的杀毒软件，它不仅可以杀死病毒，而且在Windows下都具有自动检测防御病毒的能力，会在你的电脑接触到带毒的文件时立刻弹出警报并自动杀毒。

另一方面，杀毒软件是针对已经出现的病毒，可能会被新出现的病毒钻了空子。尤其是在Internet高速发展的今天，病毒传播得极为迅速。对此，好的杀毒软件一般隔很短的时间就有新的病毒库升级，我们一定要养成定期升级的习惯。

总之，为了预防病毒，我们一定要注意以下几点：

1. 安装可以自动防毒的杀毒软件；
2. 定期升级杀毒软件。
3. 不要随便拷贝来历不明的软件，不要使用未经授权的软件。
4. 网上下载的软件一定要先查毒再使用。
5. 收到来历不明的电子邮件时，千万不要随手打开附件！
6. 在电脑没有染毒时做好应急启动软盘。对重要的文件及时做备份。

图1-1 打开杀毒软件程序

下面我们具体来学习一下“kvw3000”杀毒软件的使用

1. “kvw3000”杀毒软件的启动和退出。

首先打开“开始”菜单找到“程序”菜单，再找到“kvw3000”菜单，单击“kvw3000”打开“kvw3000”杀毒软件如图1-1。

退出“kvw3000”程序时打开“文件”菜单找到“关闭”菜单，单击鼠标左键关闭“kvw3000”程序如图1-2。

2. “kvw3000”杀毒程序的应用。

进入“kvw3000”杀毒程序后在浏览中找到要杀毒的程序或文件夹，单击鼠标左键如图1-3。

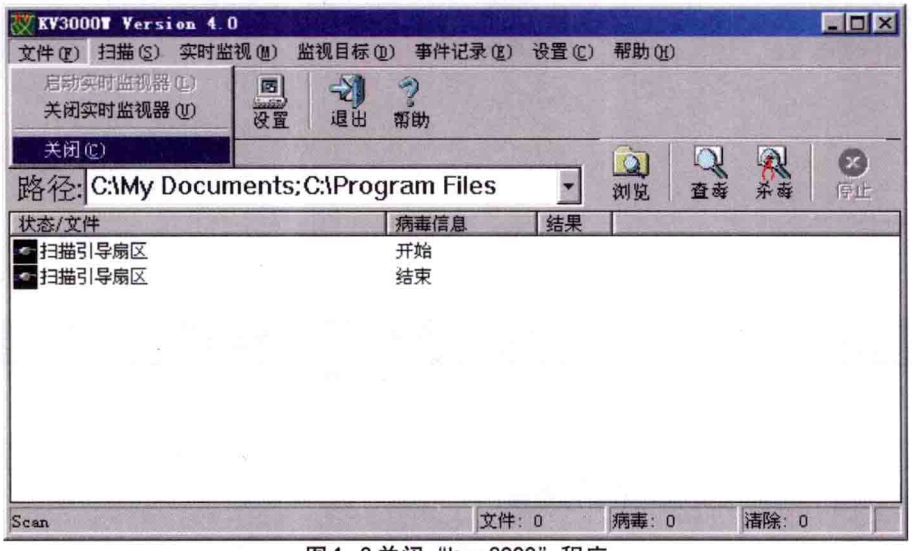


图1-2 关闭“kvw3000”程序

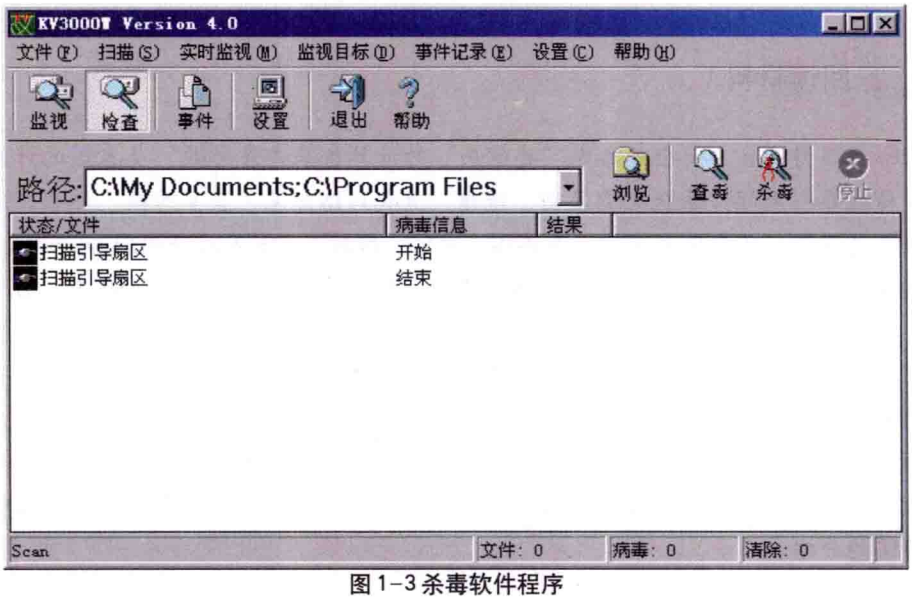


图1-3 杀毒软件程序

选择要杀毒的磁盘或文件后单击“确定”按钮后，计算机就会自动对我们所选择的磁盘或文件进行杀毒如图 1-4。

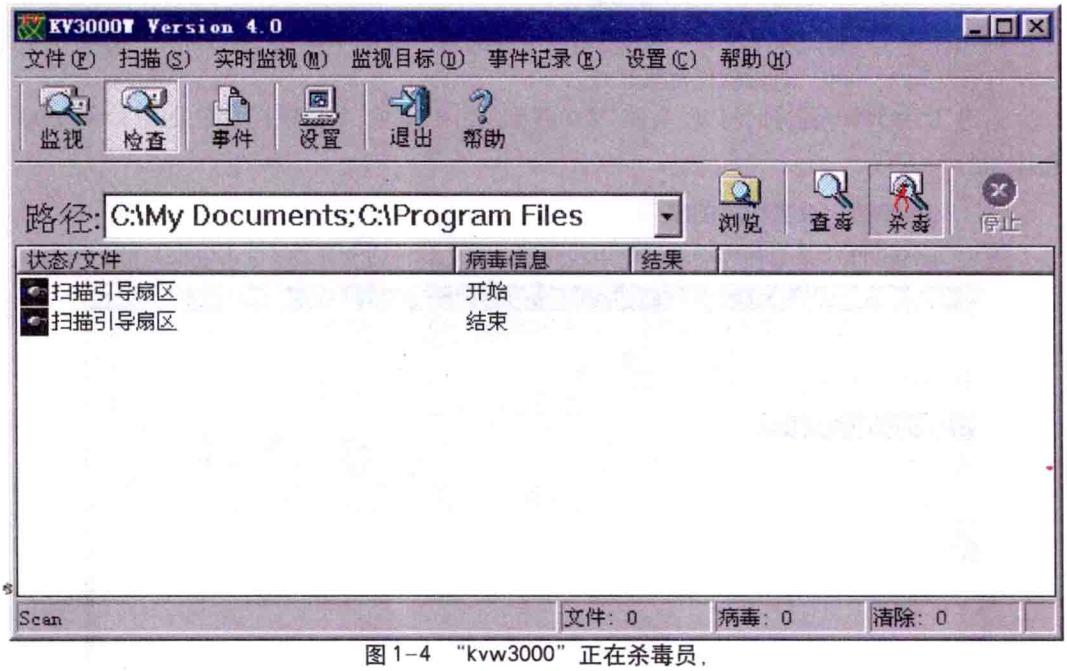


图 1-4 “kvw3000”正在杀毒员.

结束后会回到图 1-3 所示，我们再选择要杀毒的磁盘或文件，反复几次我们的计算机就会被全部杀毒。全部结束后关闭杀毒程序。

阅读材料 1

1999 年 3 月 6 日，一个种名为“美丽杀”的计算机病毒席卷欧、美各国的计算机网络。这种病毒利用邮件系统大量复制、传播，造成网络阻塞，甚至瘫痪。并且，这种病毒在传播过程中，还会造成泄密。在美国，白宫、微软和 Intel 等政府部门和一些大公司，为了避免更大的损失，紧急关闭了网络服务器，检查、清除“美丽杀”病毒。由于“美丽杀”病毒危害美国政府和大型企业的利益，美国联邦调查局（FBI）迅速行动。经过四五天的技术侦查，将病毒制造者史密斯抓获。但是“美丽杀”病毒已致使 300 多家大型公司的服务器瘫痪，这些公司的业务依赖于计算机网络，服务器瘫痪后造成公司正常业务停顿，损失巨大。并且，随后“美丽杀”病毒的源代码在互联网上公布，功能类似于“美丽杀”的其他病毒或蠕虫接连出台。如：PaPa.copycat 等。然而，这仅仅是计算机病毒肆虐网络的序曲。

一、世界主要流行的计算机病毒

根据国外统计资料，今年世界流行计算机病毒的前十位，主要有以下几种：

1. VBS_KAKWORM.A
2. TROJ_PRETTY_PARK
3. TROJ_SKA
4. VBS_LOVELETTER
5. PE_CIH
6. W97M_MELISSA
7. TROJ_MTX.A
8. TROJ_QAZ.A
9. W97M_ETHAN.A
10. O97M_TRISTATE

在这十种病毒中，通过网络主动传播的病毒占了七种，另外两种宏病毒可以感染人们编辑的文档，然后通过收发邮件进行传播，PE_CIH可以通过介质、网络下载进行传播。下面我们着重分析一下七种主动通过网络传播的计算机病毒。

1. VBS_KAKWORM.A

该蠕虫是在1999年10月份发现的。它由三部分组成：HTA 文件（HTML 应用程序），REG 文件和BAT 文件（MS_DOS批处理文件）。该蠕虫使用MS Outlook Express，通过邮件进行传播。

这种蠕虫首先将原有的AUTOEXEC.BAT复制为 AE.KAK，然后AUTOEXEC.BAT被修改并覆盖了KAK.HTA文件。系统的注册表也将被修改为：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

cAgOu = "C:\WINDOWS\SYSTEM\(name).hta"

其中，(name)是随机生成的八个字母的文件名。这样，可以保证蠕虫在每次Windows启动时能够得以运行。它在每月一日下午6点时显示这样一条信息："Kagou_Anti_Kro$oft says not today!"

2. TROJ_PRETTY_PARK

这种蠕虫病毒最早在1999年6月，在欧洲中部广泛流行，在今年三月，又再次爆发。它会每隔30分钟，将自身命名为'Pretty Park. Exe'，然后作为邮件的附件发送给邮件地址薄中的所有人。文件的图标使用著名的名为"南方公园"中的卡通形象。

另外，该蠕虫病毒还具有后门程序的功能，它会将感染此蠕虫病毒的系统的信息发送给一些IRC服务器，如：系统配置信息、登录密码和用户名、电话号码以及ICQ 号码等。这些IRC服务器列表如下：

irc.twiny.net	irc.stealth.net
irc.grolier.net	irc.club_internet.fr
ircnet.irc.aol.com	irc.anet.com
irc.insat.com	irc.ncal.verio.net

irc.anet.com	irc.insat.com
irc.ncal.verio.net	irc.cifnet.com
irc.skybel.net	irc.eurecom.fr
irc.easynet.co.uk	

同时，它还可以远程控制被感染的系统，如：创建／删除目录、上载／下载文件和删除或执行文件。

3. TROJ_SKA

这也是一个蠕虫病毒，它也称做“Happy99”。当“Happy99.EXE”被运行时，它将在Windows\System目录下生成一个名为SKA.EXE.的文件。同时，它会修改注册表。

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\

Ska.exe = Ska.exe

这样可以保证每次Windows启动时，该蠕虫可以被激活。当蠕虫运行时，将显示“Happy New Year 1999!!”并显示放焰火。该蠕虫将Happy99.EXE作为邮件附件进行传播。

4. VBS_LOVELETTER

当该病毒运行后，它自动给邮件地址列表中所有的地址发送邮件，并将自身作为邮件的附件。同时，该病毒感染力极强，可寻找本地驱动器和映射驱动器，并在所有的目录和子目录中搜索可以感染的目标。该病毒感染扩展名为“vbs”，“vbe”，“js”，“jse”，“css”，“wsh”，“sct”，“hta”，“jpg”，“jpeg”，“mp3”和“mp2”等十二种类型文件。当病毒找到有扩展名为“js”，“jse”，“css”，“wsh”，“sct”，“hta”文件时，病毒将覆盖原文件，并将文件后缀改为“vbs”；当感染扩展名为“vbs”，“vbe”的文件时，原文件将被病毒代码覆盖；当感染扩展名为“jpg”，“jpeg”的文件时，用病毒代码覆盖文件原来的内容，并将后缀加上.vbs后缀，随后毁掉宿主文件，破坏了这些数据文件原始内容。扩展名为“mp3”和“mp2”的文件，其属性被改为隐含文件，然后创建病毒文件，其文件名为以原始文件名添加后缀.vbs作为新的文件名，例如：原始文件为jianyan.mp3，该文件被感染后，jianyan.mp3的文件属性改为隐含文件，然后生成病毒文件jianyan.mp3.vbs。但是，这十二种后缀的文件如果在磁盘的根目录下，则不会遭受破坏。

5. W97M_MELISSA

当打开染有该病毒的Word文档时，它首先感染模版文件Normal.dot。此后，新创建的文档和修改编辑的文档都会感染此病毒。该病毒将把自身作为附件自动发给邮件地址列表中前五十个地址。

6. TROJ_MTX.A

这是同时具有病毒、蠕虫和后门程序特点的程序。它把自己作为邮件附件，附件的名称通常为：I_am_sorry_doc.pif，或是zipped_files.exe，然后通过邮件传播，它还可以传染windows目录下的32位EXE文件和DLL文件。

7. TROJ_QAZ.A

TROJ_QAZ.A具有蠕虫和后门程序的特点。它是在今年七八月份发现的。当它运行时，将修改注册表：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

startIE = "Notepad.exe qazwsx.hsq"

这样，可以保证每次随Windows 启动，然后可以通过网络共享进行传播。它将欲传染的系统中的Notepad.exe改为note.com然后将自身拷贝为Notepad.exe。当用户使用记事本程序时，该蠕虫将被激活。它可以允许远程用户控制感染此蠕虫的系统。并可以向某一特定地址发送信息。

二、网络时代计算机病毒的特点

1. 主动通过网络和邮件系统传播

从当前流行的前十位计算机病毒来看，其中七个病毒都可以利用邮件系统和网络进行传播。W97M_ETHAN.A和 097M_TRISTATE是宏病毒，它们虽然不能主动通过网络传播，但是，我们很多人使用Office系统创建和编辑文档，然后通过电子邮件交换信息。因此，宏病毒也是通过邮件进行传播的。所以，前十种病毒中，有九种是可以通过网络传播的。

2. 传播速度极快

由于病毒主要通过网络传播，因此，一种新病毒出现后，可以迅速通过国际互联网传播到世界各地。如"爱虫"病毒在一、两天内迅速传播到世界的主要计算机网络，并造成欧、美国家的计算机网络瘫痪。

3. 危害性极大

"爱虫"、"美丽杀"以及CIH等病毒都给世界计算机信息系统和网络带来灾难性的破坏。有的造成网络拥塞，甚至瘫痪；有的造成重要数据丢失；还有的造成计算机内储存的机密信息被窃取；甚至还有的计算机信息系统和网络被人控制。

4. 变种多

目前，很多病毒使用高级语言编写，如"爱虫"是脚本语言病毒，"美丽杀"是宏病毒。因此，它们容易编写，并且很容易被修改，生成很多病毒变种。"爱虫"病毒在十几天中，出现三十多种变种。"美丽杀"病毒也生成三、四种变种，并且此后很多宏病毒都是"美丽杀"的传染机理。这些变种的主要传染和破坏的机理与母本病毒一致。只是某些代码作了改变。

5. 难于控制

利用网络传播、破坏的计算机病毒，一旦在网络中传播、蔓延，很难控制。往往准备采取防护措施时候，可能已经遭受病毒的侵袭。除非关闭网络服务，但是这样做很难被人接受，同时关闭网络服务可能会蒙受更大的损失。

6. 难于根治、容易引起多次疫情

“美丽杀”病毒最早在1999年3月份爆发，人们花了很多精力和财力控制住了它。但是，今年在美国它又死灰复燃，再一次形成疫情，造成破坏。之所以出现这种情况，一是由于人们放松了警惕性，新投入使用系统未安装防病毒系统；再者是使用了保存旧的染病毒文档，激活了病毒再次流行。

7. 具有病毒、蠕虫和后门（黑客）程序的功能

计算机病毒的编制技术随着网络技术的普及和发展也在不断提高和变化。过去病毒最大的特点是能够复制自身给其他的程序。现在，计算机病毒具有了蠕虫的特点，可以利用网络进行传播，如：利用E-mail。同时，有些病毒还具有了黑客程序的功能，一旦侵入计算机系统后，病毒控制者可以从入侵的系统中窃取信息，远程控制这些系统。呈现出计算机病毒功能的多样化、因而，更具有危害性。

三、网络时代计算机病毒的防治策略

1. 依法治毒

我国在1994年颁布实施了《中华人民共和国信息系统安全保护条例》和1997年出台的新《刑法》中增加了有关对制作、传播计算机病毒进行处罚的条款。2000年5月，公安部颁布实施了《计算机病毒防治管理办法》，进一步加强了我国对计算机的预防和控制工作。同时，为了保证计算机病毒防治产品的质量，保护计算机用户的安全，公安部建立了计算机病毒防治产品检验中心，在96年颁布执行了中华人民共和国公共安全行业标准GA 135_1996《DOS环境下计算机病毒的检测方法》和GA 243-2000《计算机病毒防治产品评级准则》。我们开展病毒防治工作要严格遵循这些标准和法规，这样才能有效地保障我国的计算机病毒防治水平。

2. 建立一套行之有效的病毒防治体系

根据计算机病毒的特点和多年病毒防治工作的经验，从根本上完全杜绝和预防计算机病毒的产生和发展是不可能的。我们目前面临的计算机病毒的攻击事件不但没有减少，而是日益增多，并且，病毒的种类越来越多，破坏方式日趋多样化。每出现一种新病毒，就要有一些用户成为病毒的受害者。在这种形势下，我们应该寻求一种有效的预防措施，力争将计算机病毒的危害降至最低。因此，急需建立一种快速的预警机制，能够在最短的时间内发现并捕获病毒，向计算机用户发出警报，提供计算机病毒的防治方案。为遭受计算机病毒攻击、破坏的计算机信息系统提供数据恢复方案，保障我国计算机信息系统和网络的安全。为此，公安部和国家计算机网络与安全管理中心在今年8月份决定，在建立天津的计算机病毒防治产品检验中心的基础之上，建立国家计算机病毒应急处理中心。该中心是我国计算机应急体系（CERT）中的一部分。国内从事病毒研究的机构和病毒防治产品的开发厂家，以及各省市公共信息网络安全监察部门都是应急体系的成员，CERT遵循的工作原则是“积极预防、及时发现、快速反应、确保恢复”。他们一旦发现计算机病毒，就及时向应急中心报告，对在我国发现的计算机病毒事件进行快速反应和处置，对重大计算机病毒疫情将报告公安部，向社会发布病毒疫情，减少计算机病毒对我国计算机信息系统和网络的破坏。