病毒防治

Virus

便携手册

Useful Computer VIRUS Preventive

陆金山 · 王岩增 编著

上海科学技术出版社

电脑操作快捷通

病毒防治便携手册

陆金山 · 王岩增 编著

上海科学技术出版社

电脑操作快捷通

图书在版编目(CIP)数据

病毒防治便携手册/陆金山等编著.—上海：上海科学技术出版社，2003.3

(电脑操作快捷通丛书)

ISBN 7-5323-6922-6

Ⅰ.病… Ⅱ.陆… Ⅲ.电脑病毒—防治—手册

Ⅳ.TP309.5-62

中国版本图书馆CIP数据核字(2003)第003029号

电脑操作快捷通丛书

病毒防治便携手册

陆金山·王岩增 编著　　杨燕 编辑

上海科学技术出版社出版、发行(上海瑞金二路450号　邮政编码200020)

东方印刷厂印刷　新华书店上海发行所经销

2003年5月第1版　2003年5月第2次印刷　印数：5 001—8 000

ISBN 7-5323-6922-6/TP·274

定价：12.00元

前言

＞常见病毒、特征危害与防治方法尽列
＞令电脑百毒不侵

随着电脑的普及，因特网的蓬勃发展，电脑病毒在世界各地泛滥成灾。数以千万计的电脑遭到破坏，用户的资料被吞噬，直接和间接的经济损失无法估量。

关于电脑病毒的书籍现在开始多了起来，这说明社会对于电脑病毒的重视程度正在提高。但是，电脑病毒的发展和电脑技术的发展几乎是同步的，因此更需要能及时反映电脑病毒防范技术最新动向和解决方法的实用技术书籍。本书的出版，正是顺应了电脑技术这一发展需要。

本书有几个特点，首先是内容新，许多新近出现的电脑病毒在书中都有比较详细的介绍；其次是实用性强，对电脑病毒防治中的许多常见问题都提供了具体的解决方案，凡具有初级电脑知识的读者都能按书中介绍自行解决有关问题；第三是提供了病毒信息来源以及部分杀毒软件公司联系信息，令读者能及时了解电脑病毒的发展动向以及防治措施。

希望本书的出版能帮助读者了解各种电脑病毒的特性，提高防范电脑病毒的意识，加强电脑病毒防范的力度，使大家能安全地使用电脑。这也是作者的一个心愿。

1.1 什么是电脑病毒

电脑病毒其实是一段很小的程序，它是一种会不断繁殖及感染的程序码。它拥有与生物学上病毒类似的自我复制和传染机制，因而得名。

根据中国法律的定义：电脑病毒，是指编制或者在电脑程序中插入的破坏电脑功能或者毁坏数据，影响电脑使用，并能自我复制的一组电脑指令或者程序码。

电脑病毒通常会寄存在可执行的文件之中，或者是软、硬盘的开机扇区启动部分，随着被感染程序由操作系统装入内存而同时执行，病毒因此获得系统控制权。它们一般通过磁盘、光盘、电脑网络、电邮(即电子邮件)附件等途径传播。影响包括：输出一段文本音响信息、占据磁盘空间、甚至删除文件、改变存储数据属性等，导致被感染的电脑部分或完全丧失正常工作的能力，速度降低，功能失常，死机。

随着因特网技术的发展，电脑病毒的含义也在逐步发生着变化，从广义的角度而言，与电脑病毒的特征和危害有类似之处的黑客程序、特洛伊木马和蠕虫，也可归为电脑病毒。

1.2 电脑病毒的分类

电脑病毒的分类方法有许多种，以下是按照通常方式，即根据其感染的途径以及采用的技术进行划分。

1. 引导型病毒（Boot Virus）

引导型电脑病毒会影响软盘或硬盘的引导扇区。引导扇区是磁盘中最重要的部分，包含了磁盘本身的信息以及用以启动电脑的一段程序。如果用带有引导型病毒的磁盘启动电脑，它们就会感染整个系统。

2. 文件型病毒

这类电脑病毒会感染可执行文件(包括*.exe和*.com文件)。一旦直接或间接地执行了这些受电脑病毒感染的程序，电脑病毒就会按照编制者的意图对系统进行破坏。

3. 混合型病毒

混合型病毒集引导型和文件型病毒特性于一体，可以通过这两种方式交叉混合进行感染，增加了病毒的传染性以及存活率。只要中毒就会经开机或执行程序而感染其他的磁盘或文件。

4. 宏病毒（Marco Virus）

宏病毒会感染某些程序建立的文档、数据库、表格等文件，例如MS Word或MS Excel的文件。打开受感染的文档，应用程序会启动宏病毒，宏病毒就可以按照病毒程序所设计的意图执行破坏及传播。

5. 特洛依木马型病毒（Trojan horse）

它是一个隐藏在正常程序中的非法Server/Client（服务器/客户机）程序，令电脑门户大开，任由黑客进入。当电脑系统启动时，它也同时自动启动，黑客可从网上远程控制用户电脑，或窃取用户的密码和数据。

6. 蠕虫（Worm）

电脑蠕虫是一种沿着网络扩散传播特定信息的小程序，原意是用作测试网络的连线是否接通，但很快被用作网络拒绝服务攻击（DoS攻击）。

7. Script病毒

Script语言（如VBScript 以及JavaScript）传送的时候，其实是纯文本程序，只要用相应的应用程序打开该文件，才会执行病毒程序，感染其他文件。例如VBScript以及 JavaScript 病毒必须通过 Microsoft 的 Windows Scripting Host（WSH）才能够启动。只要在 Windows 资源管理器双击 *.vbs 或 *.js文档便可以启动病毒。有些Script病毒会内嵌在HTML文档中，当使用者从具备 Script功能的浏览器（如IE）打开HTML网页时，内嵌Script病毒便会自动执行。

电脑病毒的种类虽多，但对病毒代码进行分析、比较可看出，它们的主要结构是类似的，有其共同特点。整个病毒代码虽短小但都包含三个部分：引导部分、传染部分和表现（破坏）部分。

1.3 电脑病毒的基本特征是什么

隐蔽性

大部分的病毒代码都设计得非常短小，这是为了便于隐藏。病毒一般只有几百或几千个字节，所以附在正常程序之中，不易被察觉。

潜伏期

大部分的电脑病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其破坏模式。如著名的【黑色星期五】病毒会在逢13日的星期五发作；CIH病毒会在26日发作等。

破坏性

破坏性视不同病毒而言，轻者会降低电脑工作效率，占用系统资源，重者可导致系统崩溃，损失数据。按其破坏度，可分为良性与恶性。良性病毒可能只显示某些画面或播放音乐、显示无聊的话语，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，如GENP、小球、W-BOOT等。恶性病毒则有明确的目的，或破坏数据、删除文件或加密磁盘、格式化磁盘，对数据造成不可挽回的破坏。

1.4 电脑病毒发作有哪些现象

病毒发作前

- [ ] 系统无故死机；
- [ ] 电脑无法启动；
- [ ] Windows运行不正常或无法正常启动；
- [ ] 运行速度明显变慢；
- [ ] 曾经正常运行的软件报内存不足、发生死机或者非法故障；
- [ ] 打印和通信发生异常；
- [ ] 系统文件的时间、长度发生变化；
- [ ] 运行Word，打开文档另存时无法以正常的文档格式保存；
- [ ] 无意中要求对软盘进行写操作；
- [ ] 磁盘空间迅速减少；
- [ ] 网络文件夹无法调用；
- [ ] 基本内存发生变化；
- [ ] 收到标题很诱人且夹带附件的电子邮件；
- [ ] 自动链接到一些陌生的网站；
- [ ] 上网速度突然变慢。

病毒发作时

- [ ] 提示一段不相干的话；

- ☐ 发出一段音乐；
- ☐ 产生特定的图像；
- ☐ 硬盘灯不断闪烁或长亮；
- ☐ 强制进行游戏；
- ☐ Windows桌面图标发生变化；
- ☐ 屏幕上突然全黑没有显示；
- ☐ 鼠标、键盘失去反应；
- ☐ 电脑突然重启或死机；
- ☐ 自动发送电子邮件或自动打开网页；
- ☐ 鼠标指针自己在动。

病毒发作后

- ☐ 系统无法启动；
- ☐ 硬盘无法访问；
- ☐ 系统文件丢失；
- ☐ 文件目录发生混乱；
- ☐ 数据和文档丢失；
- ☐ 部分文档自动加密码，丢失被病毒加密的有关数据；
- ☐ 硬盘被格式化；
- ☐ 破坏电脑硬件；
- ☐ 网络通信受阻，无法上网。

2.1 杀毒软件

电脑病毒的检测和清除是一件需要很高技术和经验积累的事情，手动杀毒风险很高，对一般用户往往不易掌握。所以我们防毒或杀毒，一般都会使用杀毒软件。

常见的杀毒软件

F-Secure	http://www.f-secure.com
McAfee VirusScan	http://download.mcafee.com
Norman Virus Control	http://www.norman.com
赛门铁克	http://www.symantec.com
Pc-cillin	http://www.antivirus.com/pc-cillin/
Sophos AntiVirus	http://www.sophos.com
北信源	http://www.vrv.com.cn
瑞星	http://www.rising.com.cn
金山	http://www.iduba.net
熊猫卫士	http://www.pandaguard.com
江民KV3000	http://www.jiangmin.com
趋势	http://www.trend.com
创源	http://www.e-secustar.com.cn
冠群金辰	http://www.kill.com.cn

病毒实时监控

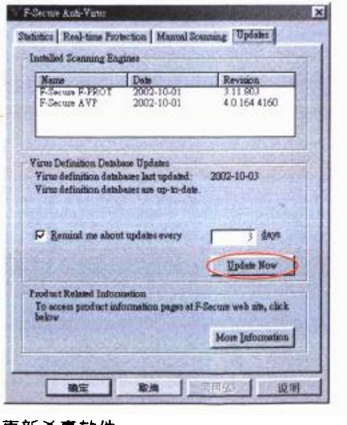
现时的杀毒软件都包含【病毒实时监控】功能(也称为病毒防火墙)，可以实时监控电脑系统，保障系统不受电脑病毒的感染，使得用户能够放心地使用电脑。安装杀毒软件时，记得开启【实时监控】功能。

用杀毒软盘启动系统进行杀毒

当Windows系统文件如Explorer.exe等感染了电脑病毒之后，往往无法在Windows运行状态下彻底杀除。这时，就需要使用DOS模式下的杀毒软件启动系统进行杀毒。安装好杀毒软件后，请制作一片【杀毒开机软盘】。本书中所提及的【用杀毒软盘启动系统进行杀毒】，即指此操作。

更新杀毒软件

一般来说，至少每周更新一次杀毒软件才能够较好地防治电脑病毒，有些杀毒软件甚至有每日更新的服务。杀毒软件商大多会在他们自己的网站上提供升级程序和更新病毒码软件，用户可以自行下载升级，也可以使用其自动联网更新。



更新杀毒软件

2.2 预防病毒措施

检测新购置的电脑软硬件系统

用户可以使用电脑杀毒软件对新购置的电脑硬盘进行检测来确保没有电脑病毒存在。因为有些软件厂商发售的软件，可能无意中已被电脑病毒感染，就算是正版软件也难保证没有携带电脑病毒的可能性，更不要说盗版软件了。

用硬盘启动电脑系统

在保证硬盘无电脑病毒的情况下，尽量使用硬盘启动系统，可以通过设置CMOS参数，使启动时直接从硬盘启动，而根本不去读软盘。很多人认为，软盘上如果没有Command.com等系统文件，就不会带电脑病毒，其实引导型电脑病毒根本不需要这些系统文件就能进行传染。

单部电脑系统的安全使用

使用外来的软盘、光盘前应先进行检查。在别人电脑上使用过自己的已打开了写保护的软盘，再在自己的电脑上使用前，也应进行电脑病毒检测。不要随便直接运行或直接打开电子邮件中夹带的附件文件，不要随意运行下载的软件，尤其是可执行文件和Office文档，都要先用最新的电脑杀毒软件进行检查。