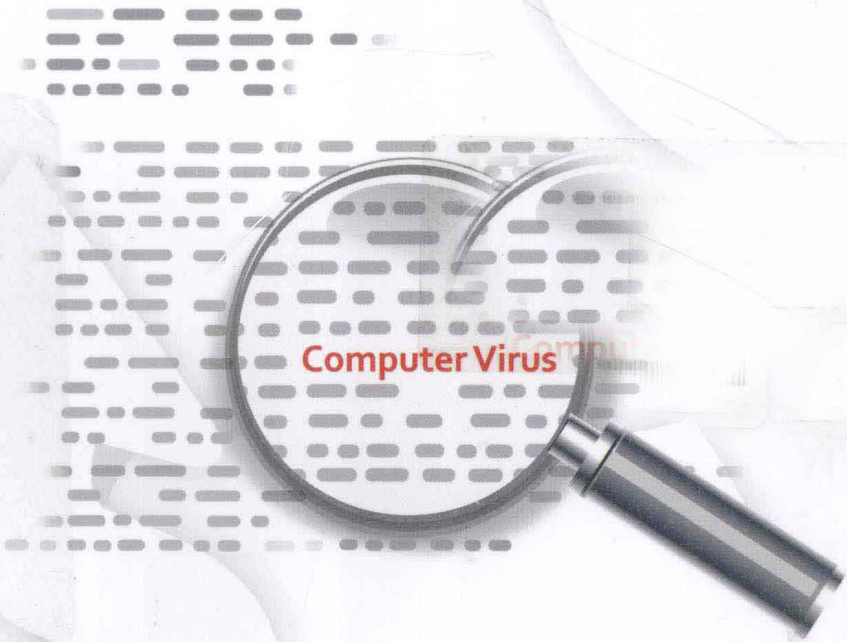
Broadview
www.broadview.com.cn

安全技术大系

计算机病毒揭秘与对抗

王倍昌 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

计算机病毒揭秘与对抗

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

随着计算机及其应用的发展，计算机病毒迅速泛滥，已极大地影响着广大的计算机用户，几乎所有的计算机用户都受到过计算机病毒的困扰。本书将深入揭秘计算机病毒完成各种功能（如：隐藏自身、隐蔽执行、自动运行、感染正常程序、自我保护等）所使用的病毒技术原理，并且介绍相应的对抗技术，同时也介绍了当今流行的反病毒技术。掌握这些技术后，就可以开发出自己的计算机病毒查杀工具、计算机病毒分析工具、反病毒扫描工具、系统恢复工具等实用性工具，从而帮助您成为专业的反病毒工程师。

本书适用于作为大专院校计算机相关专业师生参考用书，也适合于广大计算机爱好者阅读。

图书在版编目（CIP）数据

计算机病毒揭秘与对抗 / 王倍昌编著. —北京：电子工业出版社，2011.10
（安全技术大系）
ISBN 978-7-121-14605-3

Ⅰ. ①计… Ⅱ. ①王… Ⅲ. ①计算机病毒－防治 Ⅳ. ①TP390.5

中国版本图书馆 CIP 数据核字（2011）第 188393 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：徐津平
特约编辑：顾慧芳
印 刷：三河市鑫金马印装有限公司
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：34 字数：679 千字
印 次：2011 年 10 月第 1 次印刷
印 数：4000 册 定价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

本书背景

所谓计算机病毒，就是具有不良目的，对计算机具有一定破坏性、对用户具有一定危害性的特殊程序。计算机病毒具有一定的危害性，人们需要预防它。一旦计算机中毒就需要加以治疗。这样人们就不得不去研究分析计算机病毒。

近些年，计算机病毒对广大网民的危害越来越严重，人们也越来越重视对计算机病毒的防护。随之，书店中，网络上涌现出大量的计算机病毒相关的书籍和文章。在众多的学习资料中，大多都是介绍计算机病毒的概念、分类、发展、特性、危害及防护措施等内容，对计算机病毒原理进行揭秘剖析的文章少之又少。很多网络安全爱好者对计算机病毒的认识仅停留在理论概念和简单应用上。

早些年的我，经常会听到这样的词汇："我中毒了，病毒对我的系统进程进行注入了"；"我中了 LPK DLL 劫持型病毒了"；"计算机病毒通过 SPI 完成了网络劫持"；"这个病毒加壳了"等等。那时对计算机病毒也算是了解，也懂得一定的手工杀毒的方法，对于这样的词汇并不陌生，然而实质上并不完全理解。学习不是要知其然，更要知其所以然么？到底病毒是怎样注入的呢？为什么 LPK 病毒会在磁盘的每个目录中都释放一个 lpk.dll 动态链接库呢？病毒怎样通过 SPI 劫持网络呢？病毒所加的壳究竟是什么原理，怎么就使得病毒变小了，还难以分析了？带着这些疑问，我经常在网络上，图书馆去寻找答案。然而找到的往往更多是一些关于应用层面的内容，剖析原理的学习资料实为难寻。

之后，自己开始从事了反病毒工作，随之对先前的疑问逐渐了解，同时也发现计算机病毒所利用的各种技术手段确实很高，这些病毒技术其实也可以用在正常的程序设计中，往往能够达到出人意料的效果。计算机病毒所常用的技术本身并不是危害四方的罪魁祸首，而是滥用这些技术为非作歹的黑客们。我想，像我之前那样，想了解计算机病毒技术原理的爱好者们肯定也很多，为了帮助他们少走弯路，能够完全彻底的掌握计算机病毒原理，我越来越想写一本关于计算机病毒原理揭秘性的书籍，揭开神秘的病毒技术，让那些网络安全爱好者们能够从原理上对抗病毒，不再对计算机病毒感到神秘，在杀毒的道路上，不仅仅使用他人编写的工具，而且自己也能编写病毒查杀工具，修复被病毒破坏的系统。

希望这本书能够成为致力于网络安全事业人员的良师益友，让您在深入学习反病毒技术上有所获益。

本书内容

本书共分为六章：第 1 章讲解了计算机病毒的基础知识。第 2 章讲解反病毒相关的 Windows 系统知识并且概述了计算机病毒的奥秘。第 3 章讲解 Windows 系统开发相关知识以及计算机病毒相关的 Windows 编程技术。第 4 章讲解 PE 文件格式。第 5 章讲解计算机病毒常用的技术原理和使用 C/C++语言的实现细节，以及相关反病毒技术的实现。第 6 章讲解当今比较流行、比较高级的反病毒技术。

本书读者

本书以 C/C++语言作为开发语言，详细介绍计算机病毒惯用技术的原理和实现细节，并且讲解了相应反病毒技术的设计和实现。学习本书需要具有 C/C++语言的基础知识，熟悉一定的 Windows 编程技术。最好对计算机病毒常见行为及分析技术有所了解。

感谢

在编写本书过程中，特别感谢我的挚友 2 白在许多技术细节上不厌其烦的给予我帮助，感谢电子工业出版社策划编辑毕宁给予我文章结构安排上的指导。

联系方式

由于作者水平有限加之时间的仓促，书中难免存在一些不足或笔误，如果您在阅读过程中发现了，或者有任何难以理解的疑惑，欢迎与笔者进行交流，笔者愿与您一同分享学习进步、解决问题的快乐。联系邮箱 dnc2588@163.com。另书中涉及的代码或程序等读者可以到安全阁反病毒论坛 www.safe163.com 进行下载。同时也欢迎到这个论坛进行反病毒技术的学习和交流。

笔者

2011 年于长春

目　录

CHAPTER 1

第 1 章　计算机病毒概述

这一章将介绍计算机病毒的基本知识以及计算机病毒的防治，通过对本章的学习，您将对计算机病毒有初步了解。

1.1　计算机病毒基本知识

1.1.1　计算机病毒概念

自然界中的生物病毒是一类个体微小、无完整细胞结构、含单一核酸（DNA 或 RNA）、必须在活细胞内寄生并复制的非细胞型微生物。而本书所说的计算机病毒，并非是自然界中的生物病毒，而是人为的计算机代码。

“计算机病毒”一词最早是由美国计算机病毒研究专家 F.Cohen 博士提出的。世界上第一例被证实的计算机病毒是在 1983 年出现在计算机病毒传播的研究报告中，同时还有人提出了蠕虫病毒程序的设计思想。1984 年，美国人 Thompson 开发出了针对 UNIX 操作系统的病毒程序。1988 年 11 月 2 日晚，美国康尔大学研究生罗特·莫里斯将计算机病毒蠕虫投放到了网络中，该病毒程序迅速扩展，造成了大批计算机瘫痪，甚至欧洲联网的计算机也受到了影响，造成直接经济损失近亿美元。

计算机病毒实际上是一个程序，一段可执行代码。就像生物病毒一样，计算机病毒有独特的复制能力，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，它们就随同文件的使用一起蔓延开来。除了复制能力外，某些计算机病毒还有其他一些共同特性：一个被污染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字或图像上时，它们可能已毁坏了文件、再格式化了你的硬盘驱动器或引发了其他类型的灾害。即使病毒并不寄生于一个污染程序，但它仍然能通过占据存储空间给你带来麻烦，并降低你的计算机的全部性能。

“计算机病毒”有很多种定义，国外流行的定义是指一段附着在其他程序上的可以实现自我繁殖的程序代码。可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能“传染”其他程序的程序。另一种定义是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。还有一种定义是人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自身复制并传播，使计算机的资源受到不同程度的破坏等。这些说法在某种意义上都借用了生物学病毒的概念，计算机病毒同生物病毒所相似之处是能够侵入计算机系统和网络，危害正常工作的“病原体”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。所以，计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的，具有对计算机资源进行破坏作用的一组程序或指令集合。

在《中华人民共和国计算机信息系统安全保护条例》中明确定义，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破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

在这里我们要强调计算机病毒也是一个程序，或者是一段可执行的代码。而这个程序或者可执行代码对计算机功能或者数据具有破坏性，并且具有传播、隐蔽、偷窃等特性。

1.1.2 计算机病毒的特点

计算机病毒是人为编写的，具有自我复制能力，是未经用户允许而执行的代码。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务，其目的对用户是可见的、透明的。而计算机病毒具有正常程序的一切特性，但它隐藏在正常程序中，当用户调用正常程序时，它窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的并且未经用户允许的。它的主要特征如下。

1．破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。良性病毒可能只显示些画面或发出点音乐、无聊的语句，或根本没有任何破坏动作，只是会占用系统资源。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，有的甚至对数据造成不可挽回的破坏。

凡是由软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏，其表现：占用 CPU 时间和内存开销，从而造成进程堵塞；对数据或文件进行破坏；打乱屏幕的显示等。

2. 隐蔽性

病毒一般是短小精悍的一段程序，通常潜入到正常程序或磁盘中。病毒程序与正常程序不容易被区别开来，在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间内感染大量程序。而且计算机系统在受到感染后通常仍能正常运行，用户不会感到有任何异常。试想，如果病毒在传染到计算机上之后，机器会马上无法正常运行，那么它本身便无法继续进行传染了。正是由于其隐蔽性，计算机病毒才得以在用户没有察觉的情况下扩散到其他计算机中。大部分病毒的代码之所以设计得非常短小，也是为了隐藏。多数病毒一般只有几百或几千字节，而计算机对文件的存取速度是很快的，将这短短的几百字节加入到正常程序之中，一般不易察觉。甚至一些病毒程序大多夹在正常程序之中，因此很难被发现。

3. 潜伏性

大部分病毒在感染系统之后不会马上发作，它可以长时间隐藏在系统中，在满足其特定条件时才启动其表现（破坏）模块，只有这样它才可以进行广泛地传播。如“PETER-2”在每年 2 月 27 日会提 3 个问题，答错后将会把硬盘加密。著名的“黑色星期五”在逢 13 号恰好又是星期五时发作。国内的“上海一号”会在每年三、六、九月的 13 日发作。当然，最令人难忘的便是每年 4 月 26 日发作的 CIH 病毒。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

4. 传染性

对于绝大多数计算机病毒来讲，传染是它的一个重要特性。它通过修改别的程序，并把自身的副本包括进去，从而达到扩散的目的。正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的，而病毒却能够使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。另外，计算机病毒还可以通过各种可能的渠道，如 U 盘、光盘和计算机网络传染给其他计算机。当你在一台机器上发现了病毒时，往往曾经在这台计算机上使用过的 U 盘也已感染上了病毒，而与这台机器相联网的其他计算机或许也被该病毒感染了。因此，是否具有传染性是判别一段程序是否为计算机病毒的最重要条件。

一个被病毒感染的程序能够传送病毒载体，如同感冒，能被传染。当你看到病毒载体似乎仅仅表现在文字和图像上时，它可能已毁坏了文件、再格式化了你硬盘，删除了驱动或造成了其他各种类型的灾害。即使病毒不寄生于单独一个被感染的程序，它还能通过占据存储空间给你带来麻烦，并降低你的计算机的全部性能。这些都和生物病毒在传播上相似，所以也就有“计算机病毒”名称的由来。

5. 不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，其代码千差万别，有些操作是共有的，如驻留内存，改中断。有些人利用病毒的这种共性，制作了声称可以查找所有病毒的程序。这种程序的确可以查出一些新病毒，但由于目前的软件种类极其丰富，而且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会产生许多误报，而且病毒的制作技术也在不断地提高，所以病毒对反病毒软件永远是超前的。

1.1.3 计算机病毒的产生与发展

冯·诺伊曼是20世纪最杰出的数学家之一，在他的一篇论文《复杂自动装置的理论及组织的进行》中，早已勾勒出病毒程序的蓝图。不过，在当时大多数的计算机专家都无法想象会有这种能自我繁殖的程序。1975年，美国科普作家约翰·布鲁勒尔（John Brunner）写了一本名为《震荡波骑士》（Shock Wave Rider）的书，该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事，成为当年最佳畅销书之一。1977 年，托马斯·捷·瑞安在其科幻小说《P-1 的春天》（也是当年的美国的畅销书）中就描写了一种可以在计算机中互相传染的病毒，病毒最后控制了 7000 台计算机，造成了一场灾难。而几乎在同一时间，美国著名的 AT&T 贝尔实验室中，3 个年轻人在工作之余，很无聊地玩起了一种游戏：彼此编写出能够吃掉别人程序的程序来互相作战。这个叫做“磁芯大战”的游戏，进一步将计算机病毒的概念体现了出来。

1983 年 11 月 3 日，弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼（Len Adleman）将它命名为计算机病毒（computer viruses），并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行了它，第一个病毒实验成功，一周后又获准进行 5 个实验的演示，从而在实验上验证了计算机病毒的存在。1986 年初，在巴基斯坦的拉合尔（Lahore），巴锡特（Basit）和阿姆杰德（Amjad）两兄弟编写了 Pakistan 病毒，即 C-BRAIN，该病毒在一年内便流传到了世界各地。由于当地盗拷软件的风气非常盛行，因此他们的目的主要是为了防止他们的软件被任意盗拷。只要有人盗拷他们的软件，C-BRAIN 就会发作，将盗拷者的硬盘剩余空间给吃掉。业界认为，这是真正具备完整特征的计算机病毒的始祖。

1988 年 3 月 2 日，一种苹果机的病毒发作，这天受感染的苹果机停止了工作，显示器只显示“向所有苹果电脑的使用者宣布和平”的信息，以庆祝苹果机生日。1988 年 11 月 2 日，美国 6000 多台计算机被病毒感染，导致 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，该事件迫使美国政府立即作出反应，国防部成立了计

算机应急行动小组。这次事件中遭受攻击的涉及 5 个计算机中心和 12 个地区结点，连接着政府、大学、研究所和拥有政府合同的 250000 台计算机。在这次病毒事件中，计算机系统直接经济损失达 9600 万美元。这个病毒程序的设计者罗伯特·莫里斯（Robert T.Morris），当年 23 岁，是在康乃尔（Cornell）大学攻读学位的研究生，其设计的病毒程序便利用了系统存在的弱点。由于罗伯特·莫里斯是入侵 ARPANET 网的最大的电子入侵者，而获准参加康乃尔大学的毕业设计，并获得哈佛大学 Aiken 中心超级用户的特权，但他也因此被判 3 年缓刑，罚款 1 万美元，还被勒令进行 400 小时的社区服务。

计算机病毒并不是来源于突发或偶然的原因。一次突发的停电或偶然的错误，会在计算机磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。而计算机病毒是一种比较完美的，精巧严谨的代码。这些代码按照严格的秩序组织起来，与所在的系统网络环境相适应，病毒不会通过偶然形成，并且需要有一定的长度，这个基本的长度从概率上来讲是不可能通过随机代码产生的。因此实际上计算机病毒是人为的特制程序。现在流行的病毒都是为了达到一定目的而由人为故意编写的。多数病毒可以找到作者信息和产地信息。通过大量的资料统计分析来看，病毒作者主要目的一般是：一些天才的程序员为了表现自己和证明自己的能力，而特制的一些恶作剧程序，从中寻找整蛊的快感。而另一些则为了达到一定目的，如对上司的不满、为了好奇、为了报复，或者为了谋取非法利益而编写具有隐藏，偷窃等行为的病毒。当然也有因政治、军事、宗教、民族、专利等方面需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。其产生的过程为：程序设计、传播、潜伏、触发、运行、实行攻击。究其产生的原因不外乎以下几种。

（1）一些程序设计者出于好奇或兴趣，也有的是为了满足自己的表现欲或者一些搞计算机的人员和业余爱好者的恶作剧、寻开心故意编制出一些特殊的计算机程序。这些程序让别人的计算机出现一些动画，或播放声音，或别的恶作剧，以显示自己的才干。而这种程序流传出去就演变成了计算机病毒，此类病毒破坏性一般不大。例如，像圆点一类的良性病毒。

（2）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。因为他们发现对软件上锁，不如在其中藏有病毒对非法复制的打击大。于是就运用加密技术编写一些特殊程序附着在正版软件上，如遇到非法使用，则此类程序自动被激活，于是又会产生一些新病毒，如巴基斯坦病毒。这更加助长了各种病毒的传播。

（3）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——就是蓄意进行破坏。例如，1987 年底出现在以色列耶路撒冷西伯莱大学的犹太人病毒，就是雇员在工作中受挫或被辞退时故意制造的。它针对性强，破坏性大，产生于内部，防不胜防。

（4）用于研究或有益目的而设计的程序，由于某种原因，失去控制或产生了意想不到的效果。

（5）产生于游戏。编程人员在无聊时互相编制一些程序输入计算机，让程序去销毁对方的程序，如最早的“磁芯大战”。这样，新的病毒又产生了。

（6）产生于个别人的报复心理，如台湾地区的学生陈盈豪，就是属于这种情况。他以前曾购买了一些杀毒软件，但是，拿回家使用时发现，并不像厂家所说的那么厉害，杀不了什么病毒，于是他就想亲自编写一个能避过各种杀毒软件的病毒，这样，CIH 就诞生了。这种病毒对计算机用户曾造成一度的灾难。

（7）由于政治、商业和军事等特殊目的。一些组织或个人也会编制一些程序用于进攻对方系统，给对方造成灾难或直接性的经济损失。

计算机病毒发展是伴随着计算机硬件、软件技术，尤其操作系统的发展而发展的。笔者简要列举一下计算机病毒如下的主要发展过程。

- 1977 年由美国著名科普作家——雷恩，在一部科幻小说《P1 的青春》中，首次提出了“计算机病毒”这一概念。
- 1983 年美国计算机安全专家——考因，首次通过实验证明了病毒的可实现性。
- 1987 年世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM 圣诞树、黑色星期五等，面对计算机病毒的突然袭击，众多计算机用户甚至专业人员都惊慌失措。
- 1988 年爆发了针对苹果机的计算机病毒，这是由美国康奈大学的研究生——罗特·莫里斯制作的蠕虫病毒导致网络上 6000 多台计算机受到感染。同年，我国也出现了能够感染硬盘和软盘引导区的 Stoned 病毒。
- 1989 年全世界的计算机病毒攻击十分猖獗，我国也未幸免。其中“米开朗基罗”病毒给许多计算机用户造成了极大损失。
- 1991 年在“海湾战争”中，美军第一次将计算机病毒用于实战，在空袭巴格达的战斗中，成功地破坏了对方的指挥系统，使之瘫痪，保证了战斗的顺利进行，直至最后胜利。
- 1992 年出现针对杀毒软件的“幽灵”病毒，如 One-half。
- 1996 年首次出现针对微软公司 Office 的“宏病毒”。
- 1997 年该年被公认为是计算机反病毒界的“宏病毒”年，“宏病毒”主要感染 Word、

Excel 等文件。如 Word 宏病毒，早期是用一种专门的 Basic 语言即 WordBasic 所编写的程序，后来使用 Visual Basic 语言。与其他计算机病毒一样，它能对用户系统中的可执行文件和数据文本类文件造成破坏。常见的如 Twno.1（台湾一号）、Setmd、Consept、Mdma 等。

- 1998 年出现针对 Windows 95/98 系统的病毒，如 CIH（1998 年被公认为是计算机反病毒界的 CIH 病毒年）。CIH 病毒是继 DOS 病毒、Windows 病毒、宏病毒后的第四类新型病毒。这种病毒与 DOS 下的传统病毒有很大不同，它使用面向 Windows 的 VXD 技术编制。1998 年 8 月份从台湾地区传入内地，共有三个版本：1.2 版/1.3 版/1.4 版，发作时间分别是 4 月 26 日/6 月 26 日/每月 26 日。该病毒是第一个直接攻击、破坏硬件的计算机病毒，是迄今为止破坏最为严重的病毒。它主要感染 Windows 95/98 的可执行程序，病毒发作时，硬盘驱动器不停地旋转，硬盘上所有数据（包括分区表）被破坏，必须重新分区方有可能挽救硬盘；同时，对于部分厂家的主板（如技嘉和微星等），会将 Flash BIOS 中的系统程序破坏，造成开机后系统无反应。
- 1999 年 Happy99 等完全通过 Internet 传播的病毒的出现标志着 Internet 病毒将成为病毒新的增长点。其特点就是利用 Internet 的优势，快速进行大规模的传播，从而使病毒在极短的时间内遍布全球。梅莉莎为首种混合型的巨集病毒——它通过袭击 MS Word 作台阶，再利用 MS Outlook 及 Outlook Express 内的地址簿，将病毒往电子邮件广泛传播。同年四月，CIH 病毒爆发，全球超过 6000 万台电脑被破坏。
- 2000 年拒绝服务（Denial of Service）和恋爱邮件（Love Letters）“I Love You”拒绝服务袭击，威力很大，致使雅虎、亚马逊书店等主要网站服务瘫痪。同年，附着“I Love You”电邮传播的 Visual Basic 脚本病毒，更被广泛传播，终令不少计算机用户明白了小心处理可疑电邮的重要性。同年八月，也出现了首个只运行于 Palm 作业系统的木马（Trojan）程序——“自由破解（Liberty Crack）”。这个木马程序以破解 Liberty （一个运行于 Palm 作业系统的 Game boy 模拟器）作为诱饵，致使用户在无意中把这病毒通过红外线资料交换或以电邮的形式在无线网中广泛传播。
- 2001 年 9 月 18 日“尼姆达”病毒在全球蔓延，侵袭了 830 万部电脑，造成近 6 亿美元的损失。对于个人用户的电脑，“尼姆达”可以通过邮件、网上即时通信工具和 FTP 程序同时进行传染；对于服务器，“尼姆达”则采用和“红色代码”病毒相似的途径，即攻击微软服务器程序的漏洞进行传播。由于该病毒在自身传染的过程中占用大量的网络带宽和计算机的内部资源，因此许多企业的网络受到了很大的影响，有的甚至瘫痪。

- 2002 年 强劲多变的混合式病毒：求职信（Klez）及 FunLove 爆发。“求职信”是典型的混合式病毒，它除了会像传统病毒般感染电脑文案外，同时亦拥有蠕虫（worm）及木马程序的特征。它利用微软邮件系统自动运行附件的安全漏洞，耗费大量的系统资源，造成电脑运行缓慢直至瘫痪。该病毒除了以电子邮件作传播途径外，也可通过网络传输和电脑硬碟共享把病毒散播。

自 1999 年以来，Funlove 病毒已为服务器及个人电脑带来了很大的烦恼，受害者中不乏著名企业。一旦被其感染，计算机便处于带毒运行状态，它会再创建一个背景工作线程，搜索所有本地驱动器和可写入的网络资源，继而在网络中完全共享的文件中迅速地传播。

- 2003 年冲击波（Blaster）and 大无极（SOBIG）蔓延。“冲击波”病毒于当年 8 月开始爆发，它利用了微软操作系统 Windows 2000 及 Windows XP 的安全、漏洞，取得完整的使用者权限，在目标计算机上执行任何的程序代码，并通过因特网，继续攻击网络上仍存有此漏洞的计算机。由于防毒软件也不能过滤这种病毒，病毒迅速蔓延至多个国家，造成大批电脑瘫痪和网络连接速度减慢。继“冲击波”病毒之后，又发生了第六代的“大无极”计算机病毒（SOBIG.F）肆虐，并通过电子邮件扩散。该“大无极”病毒不但会伪造寄件人身份，还会根据计算机通信录内的资料，发出大量以‘Thank you!’、‘Re: Approved’等为主旨的电邮，此外，它也可以驱使染毒的计算机自动下载某些网页，使编写病毒的作者有机会窃取计算机用户的个人及商业资料。
- 2004 年 1 月下旬出现悲惨命运（MyDoom），它利用电子邮件作传播媒介，以“Mail Transaction Failed”、“Mail Delivery System”、“Server Report”等字眼作电邮主旨，诱使用户开启带有病毒的附件文档。受感染的计算机除会自动转发病毒电邮外，还会令电脑系统开启一道后门，供黑客用作攻击网络的中介。它还会对一些著名网站（如 SCO 及微软）作分散式拒绝服务攻击（Distributed Denial of Service，DDoS），其变种更阻止染毒电脑访问一些著名的防毒软件厂商网站。由于它可在三十秒内发出多达一百封电子邮件，令许多大型企业的电子邮件服务被迫中断，在电脑病毒史上，其传播速度创下了新纪录。
- 2005 年的灰鸽子病毒是国内一款著名的后门，早在 2001 年便崭露头角。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。当在合法情况下使用时，灰鸽子是一款优秀的远程控制软件，但如果拿它做一些非法的事，灰鸽子就成为很强大的黑客工具。它以服务的形式启动使得难以调试分析，它通过拦截 API 调用隐藏自身文件及注册表项，并注入所有进程，造成查杀困难。
- 2006 年我国爆发了大规模的“熊猫烧香”病毒，它是一种蠕虫病毒的变种，而且是经过多次变种演化而来的。尼姆亚变种 W(Worm.Nimaya.w)之所以被称为“熊猫烧

香”病毒，是由于被它中毒电脑的可执行文件会出现“熊猫烧香”图案。用户电脑中毒后可能会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象。同时，该病毒的某些变种还可以通过局域网进行传播，进而感染局域网内所有的计算机系统，最终导致企业局域网瘫痪，无法正常使用。它能感染系统中的 exe、com、pif、src、html、asp 等文件，被感染的用户系统中所有.exe 可执行文件全部被改成熊猫举着三根香的模样。它还能中止大量的反病毒软件进程，并且会删除扩展名为 gho 的文件（该文件是一系统备份工具 GHOST 的备份文件），使用户的系统备份文件丢失。

- 2007 年出现的 AV 终结者（帕虫/U 盘寄生虫）是一系列主动攻击杀毒软件的病毒，感染用户近十万。该病毒可感染移动存储设备并修改所有磁盘分区的打开方式，运行后会产生一个由数字和字母随机组成的 8 位名称的病毒进程，关闭多款杀毒软件、防火墙和安全工具进程，并利用 IFEO 劫持技术禁用多种安全工具、强行关闭带有“病毒”及各杀毒软件和安全工具名称字样的网页，破坏系统的安全模式，禁用系统自动更新和监控注册表防止被删，还会下载数百种木马病毒。
- 2008 年造成较大危害并广泛流传的有机器狗、磁碟机等病毒。机器狗是一个木马下载器，通过网页、第三方软件漏洞传播，感染后会自动从网络上下载木马、病毒，危及用户账号的安全。机器狗运行后会释放一个驱动文件，与原系统中还原软件驱动进行硬盘控制权的争夺，可穿透目前技术条件下的任何软件硬件还原，并通过替换 userinit.exe 等系统文件，实现开机启动，新变种还可利用 IFEO 劫持技术禁用杀毒软件并破坏杀毒软件的 API hook。

“磁碟机”（磁盘精灵）是一个感染型下载者蠕虫，最早出现在 2007 年 2 月，起初威胁并不大，后来病毒作者参照其他病毒长处、不断改进，使得对该病毒的查杀越来越困难。该病毒可通过移动存储设备、网页、ARP 欺骗传播，运行后首先会在 C 盘根目录下释放驱动以恢复 SSDT，破坏杀毒软件的主动防御功能，然后释放并运行病毒文件，修改所有磁盘分区的打开方式，感染非系统分区的可执行程序及网页文件（包括压缩包内），挂全局钩子注入所有进程，破坏显示受系统保护文件，破坏安全模式，下载其他木马，并且在关机时会将自身写入启动项。与其他病毒不同的是，它通过向窗口发送大量垃圾消息的方式使多种杀毒软件、安全工具打开即崩溃，无法使用。

- 2009 年出现了 Conficker，也被称为 Downup、Downadup 或 Kido 的蠕虫。该病毒是 2008 年 11 月 20 日被发现的，是一款以微软的 Windows 操作系统为攻击目标的计算机蠕虫病毒，迄今为止已出现了 A、B、C、E 四个版本，目前全球已有超过 1500 万台电脑受到感染。Conficker 主要利用 Windows 操作系统 MS08-067 漏洞来传播，

同时也能借助任何有 USB 接口的硬件设备来感染。2009 年 2 月 12 日，微软公司悬赏 25 万美元，征集有关 Conficker 网络病毒制造者的信息。微软官方表示，之所以重金悬赏，是为了能够重奖之下出勇夫，但目前还没被发现 Conficker 的制造者，该病毒制造者把病毒程序发送到世界各地，只要有人试图破解它，它就会自动更新。面对这样一种病毒，网络安全专家都为此抓狂。美国 ABC 新闻网在广泛征求赛门铁克、美国司法部、全美白领犯罪中心（the National White Collar Crime Center）以及其他几家著名的科技咨询机构意见的基础上，在综合考虑 Conficker 蠕虫的影响范围、经济损失、影响力等因素。据统计 Conficker 蠕虫自 2008 年 11 月 20 日被发现以来，目前全球已有超过 1500 万台电脑受到感染。如果其制造者身份得以弄清楚，其制造者将跻身全球最著名 5 大黑客之列。

- 2010 年的极虎病毒是由是金山毒霸云安全实验室首家发现的，它是一款集磁碟机、AV 终结者、中华吸血鬼、猫癣下载器为一体的混合病毒。由于该病毒可利用 IE 极光 ODAY 漏洞进行传播，又是虎年的第一个重大恶性病毒，因此得名“极虎”。它的危害超越熊猫烧香，对杀毒软件的破坏力相当于 AV 终结者、磁碟机，对系统的破坏力更是史无前例，会下载各种盗号木马、流氓软件，盗账号，弹广告，刷流量，可谓无恶不作。极虎病毒拥有以下传播方式：

① 网页挂马传播，会利用极光 0day 等系统漏洞传播；

② 局域网共享传播，通过弱口令在局域网内渗透；

③ 通过 U 盘、数码存储卡、手机卡、移动硬盘等移动设备传播；

④ 软件捆绑，欺骗下载，在盗版电影下载站、游戏外挂下载站捆绑下载；

⑤ 感染网页格式的文件进行二次传播，如果不幸某网页中招，就可能造成网站的来访者中毒；

⑥ 感染可执行 exe 文件（很多人计算机中毒，没办法就会用 GHOST 镜像恢复系统，或格盘重装，但一般不是全部格式化，这样重装后，肯定会再次中毒）；

⑦ 感染 rar 压缩包内的可执行程序（这一招会令电脑运行变慢，进程中发现多个 rar.exe 在运行，并且无法结束，或结束后重新生成）；

⑧ 部分变种在系统文件夹创建 usp10.dll 和 lpk.dll（与猫癣病毒的传播手法一致）。

- 2010 年还出现了一种利用微软 Lnk 漏洞（快捷方式漏洞）的病毒，它是影响范围最大的一次微软漏洞事件，可以让黑客实现“看一眼就中毒”的传播感染方式，是最需要紧急防御的安全漏洞。漏洞存在于“Windows Shell”组件中，当受影响系统用户点击或者 Windows Shell 试图加载经过精心构造的恶意快捷方式图标时，由于 Windows Shell 没有正确地验证指定的参数，可导致恶意代码在本地运行。