图说计算机病毒简史

现在的计算机用户似乎都有了些共识。当计算机运行不正常的时候，当显示器蓝屏、频繁死机、文件打不开的时候，大部分用户的第一反应就是：“我是不是中了病毒？”

往往是这样。在大概十年以前，曾经听说过“戴口罩防止被计算机病毒传染”的笑话。现在不会再有人把这个笑话当真了，因为计算机病毒已经成为了我们在使用计算机的过程中必然会接触到的东西。在接下来的部分里，我们将会带领读者，一起去看看这些在我们计算机中不受欢迎的小小程序。

一、早期的计算机病毒

在生物学领域中，病毒本来是指一类比较原始的、有生命特征的、能够自我复制和只能够在细胞内寄生的非细胞生物。但在计算机科学领域里，所谓病毒，“是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”（1994年2月18日颁布的《中华人民共和国计算机信息系统安全保护条例》第二十八条）

从这个定义可以看出，计算机病毒（Computer Virus）与其他计算机程序的重要区别在于自我复制性以及它的破坏性。

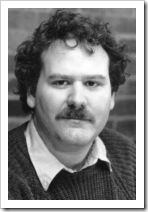
实际上早在电子计算机发明以前，[约翰·冯·诺依曼](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%BA%A6%E7%BF%B0%C2%B7%E5%86%AF%C2%B7%E8%AF%BA%E4%BE%9D%E6%9B%BC)（John Von Neumann）就在一篇名为《复杂自动装置的理论及组识的进行》的论文里提出了可自我复制的程序的概念。顺便提一句，现在几乎所有计算机都是按照冯·诺依曼提出的构想而设计的，都属于“冯·诺依曼机”，而冯·诺依曼本人也被称为“计算机之父”。



冯·诺依曼，帅哥

在20世纪60年代初，[美国电报电话公司](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%BE%8E%E5%9B%BD%E7%94%B5%E6%8A%A5%E7%94%B5%E8%AF%9D%E5%85%AC%E5%8F%B8)（AT&T）的[贝尔实验室](http://www.techcn.com.cn/index.php?doc-innerlink-%E8%B4%9D%E5%B0%94%E5%AE%9E%E9%AA%8C%E5%AE%A4)（Bell Lab）中的三个年轻人[维克多·A·维索特斯克](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%BB%B4%E5%85%8B%E5%A4%9A%C2%B7A%C2%B7%E7%BB%B4%E7%B4%A2%E7%89%B9%E6%96%AF%E5%85%8B)（Victor A Vysottsky）、[马尔科姆·道格拉斯·迈克尔罗伊](http://www.techcn.com.cn/index.php?doc-innerlink-%E9%A9%AC%E5%B0%94%E7%A7%91%E5%A7%86%C2%B7%E9%81%93%E6%A0%BC%E6%8B%89%E6%96%AF%C2%B7%E8%BF%88%E5%85%8B%E5%B0%94%E7%BD%97%E4%BC%8A)（Malcolm Douglas McIlroy）和[罗伯特·H·莫里斯](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%BD%97%E4%BC%AF%E7%89%B9%C2%B7H%C2%B7%E8%8E%AB%E9%87%8C%E6%96%AF)（Robert “Bob”H Morris）在忙于设计和开发UNIX操作系统之余，开发了一个叫做“达尔文”（Darwin）的游戏，在一台IBM 7090计算机上运行，以模拟生物的进化过程。他们这个游戏中，应用了冯·诺依曼曾经提到过的程序自我复制的理论。后来这个程序也被称为“磁芯大战”（Core War），参与者自己撰写程序来和别人的程序争夺地盘，并且争取消灭别的程序。当时他们使用的编程语言是“Redcode”。1983年A.K.Dewdney（Alexander Keewatin Dewdney）在《科学美国人》（Scientific American） 杂志上发表了一篇名为《计算机娱乐》（Computer Recreations）的文章，把这种游戏介绍给大众。因为这种游戏只能在指定的环境中运行，因此虽然其中的某些程序具备了自我复制的能力，但是还不能称之为病毒。实际上，在他发表这篇文章的时候，“计算机病毒”这个名词还没有被发明出来呢。这个名词是直到1983年11月才首次提出的。

1983年，[弗雷德·科恩](http://www.techcn.com.cn/index.php?doc-innerlink-%E5%BC%97%E9%9B%B7%E5%BE%B7%C2%B7%E7%A7%91%E6%81%A9)（Fred Cohen）正在南加州大学（University of Southern California）攻读他的博士学位，他写出了可自我复制及感染能力的程序。他发现，这个程序能够在一个小时内传遍他的整个电脑系统，快的话只需要五分钟。11月10日他在一个电脑安全研讨会上公布了自己的研究结果，并且指出：“这一类型的程序可在电脑网络中象在电脑之间一样传播，这将给许多系统带来广泛和迅速的威胁。”他的导师[艾德勒曼](http://www.techcn.com.cn/index.php?doc-innerlink-%E8%89%BE%E5%BE%B7%E5%8B%92%E6%9B%BC)（Len Adleman）将这一类型的程序命名为计算机病毒。（BTW，艾德勒曼也是牛人来的。[RSA加密算法](http://www.techcn.com.cn/index.php?doc-innerlink-RSA%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)中的A，就是他。）



弗雷德·科恩

这下子人们终于知道该怎么称呼去年的一个恶作剧了。1982年初，就读于Mt.Lebanon高中的九年级学生理查德·斯克伦塔（Richard“Rich” Skrenta）在苹果II型（Apple II）计算机上写出了一个叫做“Elk Cloner”的程序，并且把它拷贝到游戏软盘中去。当时人们对于软件的版权问题还不太在乎，盗版情况十分严重，相互复制软件是十分平常的事。当写入了“Elk Cloner”的软盘运行或启动时，它就会把自己复制一份放在计算机内存里，一旦有人将一张没有这个程序的软盘插进被感染计算机并输入指令来查看文件列表时，“Elk Cloner”就会再复制一次并且把副本写入那张未被感染的软盘中。于是，这个程序就开始传播开来。当第50次启动被感染的软盘时，将会出现斯克伦塔写的一首短诗：

Elk Cloner: The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes it’s Cloner!

It will stick to you like glue

It will modify ram too

Send in the Cloner!

它会传染你的磁盘；

它会渗进你的芯片；

它在克隆哪。

它会和你如影随形；

还会修改你的内存；

继续传染吧。

这首诗写得倒像是使用说明。

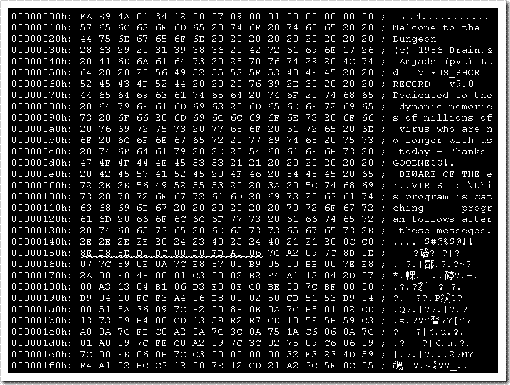


理查德·斯克伦塔，资深帅哥

这个恶作剧的影响超出了斯克伦塔的想象。直到10年后，一个水兵在海湾战争期间还曾遭遇过它。而这个时候，斯克伦塔已经从西北大学毕业好几年了。

无论如何，斯克伦塔的“Elk Cloner”的破坏性还不很突出。1986年初，在巴基斯坦的拉合尔（Lahore），巴锡特（Basit Farooq Alvi）和阿贾德（Amjad Farooq Alvi） 两兄弟编写了“巴基斯坦”（Pakistan）病毒，也被称为“(C)Brain”病毒。这是一种具有破坏性的病毒，在DOS操作系统下运行，会把自己复制到磁盘的引导区里，并且把磁盘上一些存储空间标记成不可用。对于DOS来说，计算机启动的最后一个步骤是读取并执行磁盘上的主引导记录。主引导记录读取并执行磁盘上第一个活动分区的分区引导记录，而分区引导记录将负责读取并执行IO.SYS，这是DOS最基本的系统文件。主引导记录和分区引导记录像是一本书上的目录，失去了它们，计算机这个机器脑袋就不会找到磁盘上存放的文件了。“巴基斯坦”病毒在一年之内就流传到了世界各地，并且很快衍生出了很多变种，其中有一些变种造成的损失比原始病毒造成的损失还大。这两兄弟在当地经营着一家销售IBM PC兼容机和软件的小商店，他们在接受时代周刊的采访时说，写出这个病毒的初衷只不过是为了保护自己写出的软件不被盗版而已。

有时候理想和现实之间的差距就是这么大。



被巴基斯坦病毒改变的引导区

又过了两年，罗伯特·T·莫里斯（Robert Tappan Morris）写出了世界上第一个通过网络传播的病毒。还记得我们刚才提到的“达尔文”游戏的三个发明者吗？其中有一个叫做罗伯特·H·莫里斯，正是这个莫里斯的父亲。那是1988年，小莫里斯正在康奈尔（Cornell）大学读研究生。他想统计一下当时连接在网络上的计算机的数目，所以就写了一个程序，并且在11月2日从麻省理工学院（Massachusetts Institute of Technology，MIT）的一台计算机上释放了出去。考虑到网络管理员们可能会删除掉他的程序，从而让他的的统计结果不够准确，所以他设置了一个自认为比较合理的方案：他让这个程序有一定的概率对自己进行复制，无论它所在的计算机有没有被感染都是这样。



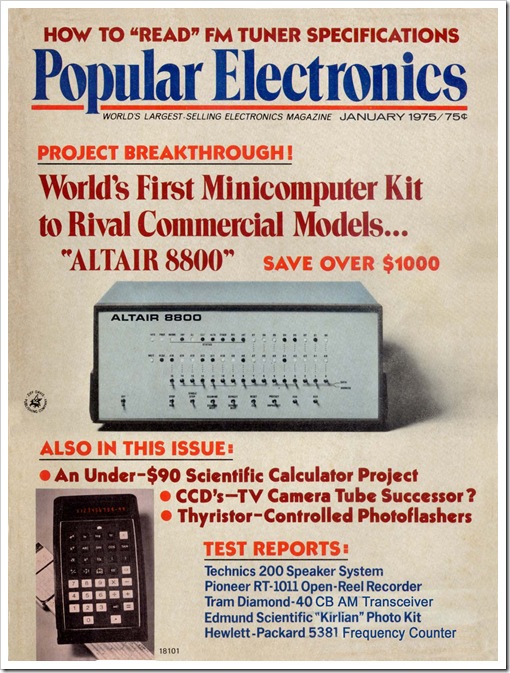
罗伯特·T·莫里斯，青涩帅哥

就像我们在有些科幻动作电影中看到的那样，整件事超出了他的控制。他的撰写的这个程序有点问题，开始无休止地复制自身，占据了大量磁盘空间、运算资源以及网络带宽，最终导致网络瘫痪和计算机死机。他的这个程序感染了大约6，000台计算机，而受到影响的则包括5个计算机中心和12个地区结点以及在政府、大学、研究所和企业中的超过250，000万台计算机。美国国防部马上成立了计算机应急行动小组，来削弱这次事件的影响并且减少损失。据估计，这个程序造成的经济损失大约在9，600万美元左右。人们从这时开始，才意识到病毒能够带来什么样的危害。

后来他被判处1万美元罚款和400小时的社区服务。由此看来，从事计算机科学的研究也是有风险的。他的这个小小实验给计算机病毒添加了一个全新的分类，叫做“[蠕虫](http://www.techcn.com.cn/index.php?doc-innerlink-%E8%A0%95%E8%99%AB)”（Worm）。

有趣的是，早在1977年出版的一本小说中就提到了类似的概念。加拿大作家托马斯·J·瑞安（Thomas.J.Ryan）写那本科幻小说叫做《P-1的青春期》（The Adolescence of P-1，一译《P-1的春天》），在那本小说里，一个叫做“P-1”的人工智能程序几乎传染了所有美国的计算机。后来，加拿大以此拍了一部叫做《捉迷藏》（Hide and Seek）的电视电影，获得了不错的评价，在IMDB上得分高达8.9分。

说到这里的时候，我们得大概谈一下计算机操作系统和互联网。虽然公认的电子计算机发明于1946年，但是此后很长时间都不是普通大众能够买得起的。那时候的计算机过于庞大，过于昂贵，并且过于复杂，只有一些政府机构和大型企业才能够购买和使用。一直到20世纪70年代初的时候，Intel才创造性地推出了8008芯片，把计算机的运算器部分全部做在了一个小小的硅芯片上。第二年，他们推出了8080，速度是8008的十倍。微软（Microsoft）公司的创始人比尔·盖茨（William “Bill” Henry Gates III）和保罗·艾伦（Paul Gardner Allen）在1975年1月份的《大众电子学》（popular electronics）杂志封面上看到了真正的微型计算机的广告，那是一台由MITS（Micro Instrumentation and Telemetry Systems）设计和制造的叫做牵牛星8800（Altair 8800）的方头方脑的家伙，以现在的眼光看起来简单得可怕。它没有我们现在看来司空见惯的屏幕，而是通过发光二极管的点亮或者熄灭来表示信息。就是这样一个方盒子促使比尔·盖茨和保罗·艾伦创建了传奇般的微软公司。在他们创建微软公司的时候，苹果公司（Apple Inc）要到第二年的愚人节才会成立，国际商用机器公司（International Business Machines Corporation，IBM）已经有了79年的历史，惠普（Hewlett-Packard Company，HP）也已经36岁了，而迈克尔·戴尔（Michael Dell）这个DELL公司的创始人才十岁，还没开始做他的邮票生意呢。

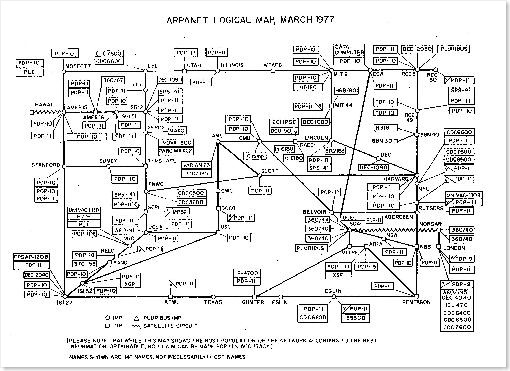


带有Altair 8800广告的《大众电子学》封面

七十年代是计算机发展的战国时期。每一个厂商都在试图与其他厂商采用不同的标准，以巩固自己的顾客群，使他们不会很容易就转到别的厂商的机器上。1980年，IBM提出了“兼容机”（Compatible Machine）概念，占据了大量的市场份额。微软公司推出了MS-DOS（Microsoft Disk Operating System），并且和IBM的PC捆绑销售，很快就流行了起来，进而慢慢奠定了软件业巨头的地位。随后其他计算机厂商也迅速跟进，纷纷生产能够和IBM PC兼容的硬件。而苹果公司，虽然推出了广受欢迎的苹果-II（Apple-II）型，但是因为坚持不开放硬件和软件标准的原因，市场份额开始快速地萎缩了。

刚才提过的“巴基斯坦”病毒就是感染DOS下磁盘引导区的病毒。一般来说，一种病毒只能在一种操作系统上运行，DOS的流行成了“巴基斯坦”病毒流行的先决条件。

再来看看造就了“蠕虫”的互联网。我们现在使用的互联网（Internet，也叫做因特网）脱胎于1968年末美国国防部国防先进技术研究署（Defense Advanced Research Projects Agency，DARPA）的一个计划。这个计划叫做“ARPANET”（Advanced Research Projects Agency Network，先进技术研究署网络），本意是连接各个厂商生产的不同计算机，从而保障在战争时期的通信和指挥依然通畅。项目进行得很顺利，1969年就开始实验，连接了美国本土的四所大学和研究机构。后来越来越多的大学和机构都加入了这个网络，并且企业和个人也开始尝试通过网络来传递信息，最终成为了我们现在所使用的互联网。附图是1977年APRANet的示意图，我们可以看到，当时麻省理工学院（MIT）就已经在连接在这个网络上了。



ARPANET，1977（点击可看大图）

1989年11月9日柏林墙塌了，1991年12月25日苏联解体了，持续了数十年的“冷战”时代终于终结了。互联网开始迅速发展，不仅仅应用于研究和军事领域，大量的商业信息也在互联网上传递起来。1994年年，互联网上的商业信息首次超过了科研信息，互联网作为一个商业平台的潜质开始慢慢地为人们所了解。我国在这年加入了互联网，同时打开了一条病毒进入国内的高速公路。

这个时候，在DOS上传播的病毒也已经发展了好几个阶段了。从最早的引导区病毒开始，发展到DOS可执行阶段、伴随及批次阶段、幽灵阶段和病毒制造机阶段。而我们现在广泛使用的Windows操作系统的始祖——Windows95还没上市呢。

最早的引导区病毒除了我们提到过的“巴基斯坦”病毒之外，比较知名的还有“小球”（Pingpang）、“石头”（Stone）以及“米开朗基罗”（Michelangelo）病毒。“小球”病毒是最早传入我国的计算机病毒，最早是在大连市统计局被发现的。当这个病毒发作时，计算机屏幕上会出现一个小球弹跳不休，在碰到屏幕边缘的时候就反弹，像乒乓球一样。这也是这个病毒名字的由来。感染了“石头”病毒的计算机屏幕上将会显示“Your PC is Now Stoned.”，并且可能导致某些硬盘和软盘无法再使用。“米开朗基罗”每年3月6号发作——这一天是米开朗基罗的生日——发作起来会删掉当前磁盘上的所有数据。

1989年，出现了可执行文件型的病毒。这类病毒把自己复制到可执行文件中，当用户运行这个可执行文件的时候，病毒就会在内存中复制一份，并且传染那些未被感染的可执行文件。一般来说，被可执行文件型病毒感染的文件，会比正常文件略大一些。例如“1575”、“1465”、“2062”、“4096”等病毒，就是用它们自身所占的字节数来命名的。这一类病毒中最出名的应该算是“黑色星期五”病毒和它的一个变种“耶路撒冷”（又名Stone3）。这种病毒每到既是十三号又是星期五的日子发作，一旦发作计算机里的数据基本上就保不住了。

大概是在1992年，出现了一种叫做“金蝉”（Golden Cicada）的病毒，给病毒分类又加了一种“伴随型病毒”。这种病毒会把原来的文件改名，如果原来文件的扩展名是“EXE”，那么就改成“COM”；如果是“COM”，就改成“EXE”，然后把自己改成文件本来的名字。扩展名是文件名的点后面的部分，例如“病毒简史.doc”这个文件的扩展名就是“doc”。扩展名是给操作系统看的，操作系统决定用什么程序或软件来打开当前的文件，例如“doc”类型的文件默认情况下是用Word这个软件来打开的，如果计算机上没有安装Word的话，就会用写字板来打开。在DOS和后来的Windows操作系统中，“EXE”扩展名表示这是一个可执行文件，“COM”扩展名表示这是一个命令型文件。一般来说，当同一个文件夹下存在同名的EXE文件和COM文件时，DOS将会先执行COM文件。“金蝉”病毒就是利用了DOS的这个特性，当用户认为自己是在运行一个可执行文件的时候，实际上已经运行了病毒。

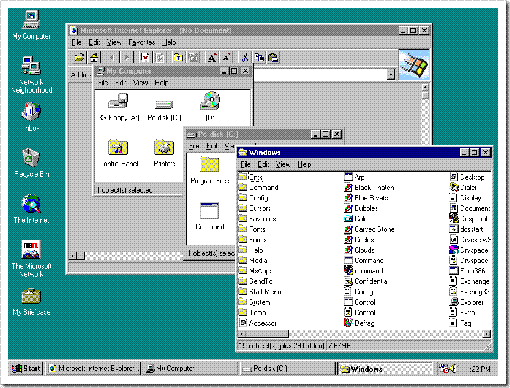
又过了两年，出现了幽灵病毒。这是一类新的病毒，在每次感染时都会产生出不同的代码，让过去依据“病毒特征码”来进行查杀的杀毒软件头疼不已。这是随着汇编语言的发展而出现的新技术，在反查杀的技术水平上比过去的病毒高出了一大截。随后病毒制造机也出现了，其中具有代表性的是VCL（Virus Creation Lab，病毒制造实验室），能够生成上千万种病毒，每一种的特征码都不同。病毒生产开始规模壮大了，并且出现了一些专门研究病毒制造技术的组织，例如VLAD、29A等等。其中位于澳大利亚的VLAD组织是世界上最早编写出能够传染Windows 95和Linux操作系统的病毒的组织，技术实力很强。

在这一阶段，病毒的制造大都是一些计算机爱好者所为，出发点往往在于对技术的迷恋和好奇，而没有什么利益驱动。和杀毒软件设计者斗智，设计紧凑而精巧的代码，发现别人没有发现的漏洞并加以利用——这是这一阶段病毒发展的主题。

这些趴在键盘上彻夜不睡的年轻人只关心他们的技术。他们也许并不知道，这种好奇将会造就大约每年50亿美元的杀毒软件市场。

二、Windows和互联网时代的病毒和蠕虫

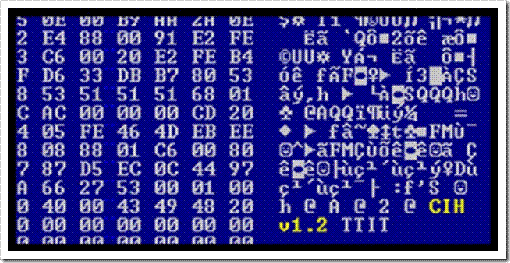
1995年8月24日，微软公司发布了划时代的操作系统——Windows 95（视窗95）。这是微软公司推出的第一套完全采用图形化用户界面（Graphical User Interface，GUI）的操作系统——在此之前的Windows系列版本只不过能算是在DOS上运行的一个软件而已。Windows 95迅速占据了大量的市场，其基于鼠标操作的直观的使用方式让计算机用户的学习成本大大降低。人们终于可以不再记忆那些复杂的命令和参数，只用动动鼠标就能完成自己的工作。这对于普通用户来说真是一大福音。



Windows 95，划时代的操作系统之一

但同时也是对病毒制造者的一大挑战。全世界的病毒制造者都在研究，怎样战胜声称“百毒不侵”的Windows 95。1996年，VLAD的Boza病毒首先做到了这一点。这个病毒会在每月的30号发作，受到感染的计算机将会显示一段文字说明，告诉用户这是VLAD组织的杰作。这是一个良性病毒，并不会造成什么损失，仅仅是表明自己的技术实力罢了。

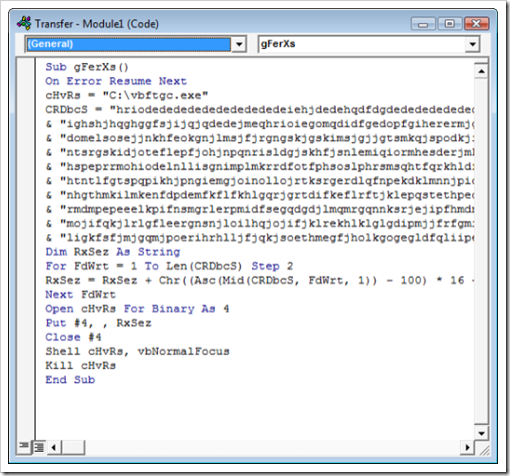
在这一时期，最出名的Windows病毒应该算是在1998年由台湾人[陈盈豪](http://www.techcn.com.cn/index.php?doc-innerlink-%E9%99%88%E7%9B%88%E8%B1%AA)编写的[“CIH”病毒](http://www.techcn.com.cn/index.php?doc-innerlink-%E2%80%9CCIH%E2%80%9D%E7%97%85%E6%AF%92)了。这个病毒一共有从V1.0到V1.4五个版本，其中造成最大损失的是V1.2版。在每年4月26日发作，改写磁盘引导区数据，并且可能会修改主板上的基本输入输出系统（Basic Input/Output System）芯片，甚至造成主板损坏。1999年4月26日，CIH V1.2首次大范围爆发，在全球有超过六千万台电脑被不同程度破坏，在2000年4月26日，又一次大范围爆发，估计在全球造成的损失超过十亿美元。这个病毒也被叫做“切尔诺贝利”（Chernobyl）病毒，因为4月26日是切尔诺贝利核电站发生核泄漏的日子。但是后来据陈盈豪自己供称，这个病毒和切尔诺贝利核电站一点关系都没有，26号只不过是他高中的学号而已。台湾警方很快逮捕了陈盈豪，随后发现，破坏力更大的CIH V2.0已经接近开发完成了。



CIH 1.2

在陈盈豪没有写出CIH之前，一类制作起来更容易但是传播速度更快的病毒就出现了。这就是“[宏病毒](http://www.techcn.com.cn/index.php?doc-innerlink-%E5%AE%8F%E7%97%85%E6%AF%92)”（Macro Virus）。宏是微软公司的Office软件包提供的一种工具，可以让用户避免重复工作。它就像是在DOS下的批处理，在用户发出指令后，完成预先定义好的一系列工作。在Office中，宏有两种定义方式，其一是用宏录制器录制用户操作，二是通过Visual Basic语言编辑器手工编辑。在默认情况下，Word将宏存贮在 Normal.dot这个模板文件中，当打开一个文档时，会首先加载这个模板文件，以便让所有的Word文档都能使用。

宏病毒就利用了这一特性。一般来说，宏病毒附在文档中，当在未被感染的计算机上打开的时候，这个宏就会改写模板文件，把自己添加进去。以后只要一执行Word，这个受感染的通用模板便会感染其后所编辑的所有文档中去。如果在其他计算机上打开了感染病毒的文档，宏病毒又会转移到这台计算机上。



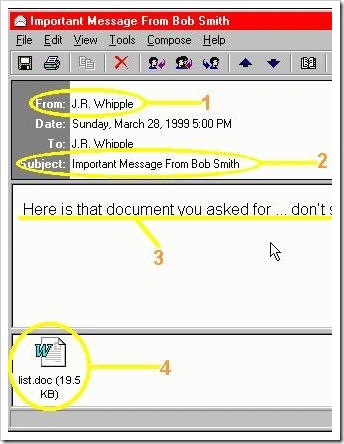
一段宏病毒代码

Visual Basic语言学习起来比较容易，宏病毒的门槛比传统病毒低得多，但是传染性惊人，破坏力也不容小觑。后来微软在Office里加入了宏扫描功能，当遇到带有不正常宏的文档的时候，会首先让用户选择是否要运行文档中的宏。杀毒软件也迅速跟进，现在宏病毒已经比较少见了。

但是通过互联网工具传播的病毒终于开始泛滥起来，病毒中的“蠕虫”这一分支越来越人丁兴旺了。

莫里斯撰写的“蠕虫”的特征是在网络上疯狂搜寻，寻找一切没有被传染的计算机。这一类病毒在发作时会大量占据计算机的运算资源和内存，并且造成网络拥堵。只要连接互联网，它就会传播，令人防不胜防。后来的大量病毒借鉴了这一做法，“梅丽莎”（Melissa）、“爱虫”（ILOVEYOU）、“红色代码”（Code Red）、“SQL监狱”（SQL Slammer）、“冲击波”（Blaster）、“震荡波”（Sasser）等是其中的最为知名的，并且都衍生出了数十种至数百种其他的变种。

“[梅丽莎](http://www.techcn.com.cn/index.php?doc-innerlink-%E6%A2%85%E4%B8%BD%E8%8E%8E)”（Melissa）蠕虫最早是在1999年3月26日被发现的，当时它导致了一台电子邮件服务器死机。被这个蠕虫感染的计算机会自动向微软电子邮件管理软件Outlook的联系人名单中前五十个邮件地址发送带毒的电子邮件，每份邮件都带着一个Word文档作为附件。当收到邮件的用户打开这个Word文档的时候，他的计算机就会感染这个病毒，并且进行新一轮的邮件发送。这种传染方式快得惊人，并且会占据了过多的网络带宽以及导致电子邮件服务器崩溃。据统计，这个蠕虫最终导致的损失可能超过8，000万美元。“梅丽莎”蠕虫的制造者是当时31岁的戴维·L·史密斯（David L. Smith），他说“梅丽莎”这个名字来自于他认识的佛罗里达州的一位舞女。在FBI和新泽西州警察的合作下，戴维·史密斯很快就被抓获了，并且被判处20个月的监禁以及5，000美元罚款。这是美国历史上第一次对病毒撰写者判处如此严厉。



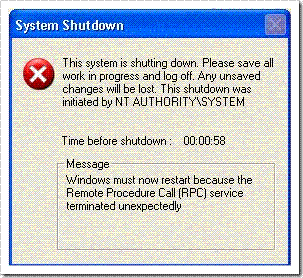
一封带有梅丽莎病毒的邮件

仅仅就在“梅丽莎”发作一年之后的2000年五月四日，在香港首次发现了“爱虫”蠕虫。“爱虫”和“梅丽莎”的传播方式类似，但是要凶狠得多。用户可能会接到一封电子邮件，主题是“ILOVEYOU”，还带有一个名为“LOVE-LETTER-FOR-YOU.TXT.vbs”的附件。当用户打开这个附件的时候，将会把同样的邮件发给用户地址簿里所有的地址。它还能查找本地磁盘和网络驱动器，并在所有目录和子目录中搜索可以感染的目标，能够感染超过十种类型的文件，甚至连MP3文件都不放过。“爱虫”在不到二十四小时的时间里传遍了全世界，仅仅一天就造成了大约55亿美元的损失。当然，这可能和它的名字也有一定关系。受到袭击的包括一些重要机构，美国国防部和CIA也在其中。在没有合适的杀毒程序的情况下，许多机构不得不关闭了电子邮件服务器。计算机安全专家大声呼吁用户在接到邮件时不要轻易打开附件，但是这种蠕虫还是持续蔓延开来，并且通过修改Windows操作系统中最重要的数据库之一——注册表，来保证它自己开机后就能自动运行。

2001年7月13日，红色代码从网络服务器上传播开来。它专门针对运行微软互联网信息服务器（Internet Information Server，IIS）软件的网络服务器来进行攻击，并且主动寻找其他易受攻击的主机进行感染。这个行为持续大约20-27天，之后它就开始对某些特定IP地址发起拒绝服务（Denial of Service，DoS）攻击，让目标计算机不能被访问。在短短不到一周的时间内，这个病毒感染了近40万台服务器，据估计多达100万台计算机受到感染。实际上，在六月中旬，微软曾经发布了一个叫做“MS01-033”的补丁来修补这个漏洞，但是大多数网管都没有安装这个补丁。

“SQL监狱”也被称为“蓝宝石”（Sapphire），2003年1月25日首次出现。这个蠕虫需要满足较为苛刻的条件才会发作：它只感染服务器；它随机产生IP地址，并向这些IP地址发送自身的副本；如果当前的计算机刚好运行着未打补丁的微软SQL服务器桌面引擎（SQL Server Desktop Engine）软件，那么马上就会变成下一个传染源。然而，互联网上没有安装补丁的服务器为数可不少。这个蠕虫在十分钟之内感染了7.5万台计算机，甚至导致了大量的网络设备被迫关闭。

好容易到了夏天，“[冲击波](http://www.techcn.com.cn/index.php?doc-innerlink-%E5%86%B2%E5%87%BB%E6%B3%A2)”又袭来了。这个蠕虫最早于8月11日被检测出来，短短两天之内就达到了攻击顶峰。被传染的计算机当连接上互联网时就会弹出一个对话框，告诉用户这台计算机将在1分钟内关闭。对于这种会反复传染的病毒，人们实在不厌其烦，不得不发明了一些简单的土方法。其中最常见的一种是在提示关机后的一分钟内，把计算机的系统时间向前调一天。除此之外，这个病毒的作者似乎还想表达些别的什么。在病毒的可执行文件MSBLAST.EXE代码中隐藏着这样的信息：“桑，我只想说爱你！”（I just want to say LOVE YOU SAN!!）以及“比尔·盖茨，你为什么让这种事情发生？别再敛财了，修补你的软件吧！”（billy gates why do you make this possible? Stop making money and fix your software!!）和“红色代码”类似，在“冲击波”蠕虫发作前一个月，微软其实已经推出了相应的补丁“MS03-026”和“MS03-039”，但是却没有得到用户的重视。



冲击波病毒感染后，提示一分钟内关机

一年以后，“[震荡波](http://www.techcn.com.cn/index.php?doc-innerlink-%E9%9C%87%E8%8D%A1%E6%B3%A2)”发作了。这个蠕虫是德国一名17岁的高中生编写的，他在18岁生日那天释放了它。“震荡波”从2004年8月30日起开始传播，其破坏能力之大令法国一些新闻机构不得不关闭了卫星通讯。它还导致德尔塔航空公司（Delta）取消了数个航班，全球范围内的许多公司不得不关闭了网络。与先前多数病毒不同的是，“震荡波”的传播并非通过电子邮件，也不需要像“梅丽莎”或者“爱虫”那样需要用户的交互动作，完全自己一手包办了。它利用了未升级的Windows 2000/XP系统的一个安全漏洞，一旦传染到计算机上，它便主动扫描其他未受保护的系统并将自身传播过去。后来德国警方逮捕了这个孩子，但是由于编写这些代码的时候他还是个未成年人，虽然被法庭认定从事计算机破坏活动，但还是仅判了缓刑。

在这一个阶段，病毒制造者似乎还没有和经济利益有任何关系，看起来，他们只是往往为了宣扬自己的名声或者对现实生活不满。但是接下来，情况却奇怪地扭曲了。

三、商业利益驱动下的病毒产业链

在“爱虫”蠕虫里，包含了一个“[特洛伊木马](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A9%AC)”（Trojan Horse）。木马是一类特殊的程序，它会首先安装一个软件在计算机上，这样木马的主人就可以用来远程这台计算机，就像我们在使用Windows XP里自带的“远程协助”时的样子。严格地说，木马并不能算是病毒的一种，因为它一般不具有自我复制的特性。然而，大量的病毒和蠕虫结合了木马的功能，让病毒开始朝着一个怪异的方向前进了。

早在1983年，计算机科学的先驱[肯·汤普森](http://www.techcn.com.cn/index.php?doc-innerlink-%E8%82%AF%C2%B7%E6%B1%A4%E6%99%AE%E6%A3%AE)（Ken Thompson）就提出了木马的概念。他提到在UNIX上运行的一个小程序，这个小程序可以用来记录用户登录时使用的用户名和密码。它会把收集到的信息藏在一个不起眼的小角落里，直到它的主人来把这些信息取走。后来在DOS上和在Windows操作系统上也出现了木马，并且很快就被应用在获得计算机用户的帐号和密码上。

2004年1月18日，“Bagle”蠕虫被发现了。它的传染方式类似“爱虫”，同样是当用户点击邮件中的附件之后就会感染并且向联系人发送，但也有些不同之处。其中最为人们注意的是它会收集用户的电子邮件地址，并且把这些邮件地址发送到一个指定位置。反病毒专家推测，也许这个蠕虫的作者打算把收集到的邮件地址卖给那些通过电子邮件来推销的商家。几天后，这个蠕虫的作者放出了源代码，让任何具有一定编程能力的人都可以制造出自己的蠕虫变种。“Bagle”蠕虫被设定为到了1月28日就停止传播，但是在那之后，依然有许多变种肆虐在互联网上。

这可以算是一个转折点。在此之前，病毒和蠕虫的作者似乎并没有什么经济利益而言，因为通过技术危害他人计算机安全及隐私而获利的行为和“黑客精神”背道而驰。但是“Bagle”蠕虫的出现，标志着“通过恶意软件获利运动”的开始。这时开始，一条黑色的地下产业链开始慢慢建立起来。

“后门”（BackDoor）程序在木马之后紧接着就登场了。在过去，“后门”往往指的是程序员在撰写某个软件的过程中给自己留的一个方便通道，往往是为了调整和维护软件的需要。但是“后门”这个词很快也开始变得臭名昭著起来。现在我们提到的“后门”，大多数情况下指的是通过进入某台计算机后所设置的隐藏的帐户或者端口，可以通过这些端口来获得计算机的某些数据。病毒往往具备了在感染的计算机上开后门的功能，这样，病毒的制造者将会从传染的机器上获得源源不断的收益。

国内杀毒软件厂商瑞星近期发布了《中国大陆2007年电脑疫情和互联网安全报告》（http://www.rising.com.cn/2007/annual/index.htm），在这份报告中提到，2007年全年发现的病毒种类上升到了71万种，而仅仅在2004年，这个数字还只不过是6万而已。当前流行的病毒中巨大部分是木马病毒和后门病毒，居然占了病毒总数的84%。在2007年全国流行的十大病毒中，盗取用户帐号和密码的病毒居然占了四种，“网游盗号木马”、“QQ通行证”、“魔兽世界木马”、“传奇终结者”这几种病毒分别名列这个榜单的第一、第二、第四和第九位。

有些文章称，现在已经形成了一条明晰的病毒产业链。比较常见的盈利方式包括把从被感染的计算机机上获得的帐号和密码再次出售——在《魔兽世界》这款游戏中常见的“打金工作室”往往会大量购买这类帐号，比较好的QQ号码也能卖个不错的价钱。除此之外，还包括把被控制的计算机的控制权出售的盈利途径，购买者可以使用这些计算机发起分布式拒绝服务（Distributed Denial of Service，DDoS）攻击，从而使被攻击的网站或者服务器陷入瘫痪。

2006年11月，我国大量计算机遭受“尼姆亚”（Nimaya）病毒侵袭。这个病毒还有一个更为常见的名字，就是“[熊猫烧香](http://www.techcn.com.cn/index.php?doc-innerlink-%E7%86%8A%E7%8C%AB%E7%83%A7%E9%A6%99)”。这是国内编写的蠕虫病毒，通过多种方式传染，被感染的计算机上所有的可执行文件的图标都会变成一只熊猫手捧三支香的图标，因而得名。这种病毒会导致系统蓝屏、频繁重启、硬盘数据被破坏等，破坏力和传染力都十分惊人。然而，被人们所关注的，是这一病毒制造者被抓获后而引出的病毒产业链。警方曾经披露，少数地方甚至形成了计算机病毒产业群。



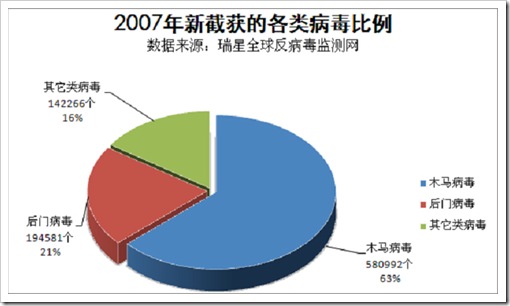
熊猫烧香

“熊猫烧香”病毒案告破后，其中一名被告曾经感叹：“这是个比房地产来钱还快的暴利产业！”

有需求，就有了供给。我国大多数计算机用户并没有很高的计算机应用水平，对于计算机安全方面更是谈不上了解。相当多用户认为安装杀毒软件就能够防止自己的计算机被病毒侵袭，但是却没有意识到仅仅有杀毒软件并不足够。现在我国已经成了恶意网站、恶意软件以及病毒和木马的重灾区。Google在今年2月4日公布了一项关于互联网上包含流氓软件网站的研究报告，在这份报告中提到，目前全世界大约有超过18万个网站、3百万个网页试图对访问者安装恶意程序，占网页总比例从2007年4月份上升到2008年1月份的1.3%。这份报告中提到的恶意程序包括但是不仅限于我们提到的病毒和木马程序。而更可怕的是，这类网站中，有65%以上位于中国。



瑞星发布的2004-2007年新增病毒样本数



瑞星发布的2007年截获的各类病毒比例

随着病毒产业链的完善，对病毒的需求也和以前不同了。现在的病毒更像是我们日常使用的软件，会在连接到互联网时升级，并且时时更新，反杀毒技术也在一日千里地发展着。“熊猫烧香”在出现半个月以后，就出现了50种以上的变种，这样的更新速度让杀毒软件和计算机用户防不胜防。

四、病毒还将继续

用户每天的使用计算机的过程已经变成了一场战争。在这场战争中，用户唯一可以依靠的只是杀毒软件。然而，杀毒软件仅仅像是盾牌一样只能防御，并且总会比病毒更慢一步。那些沉迷于计算机技术的“黑客”曾经的光荣一去不返，我们谈到病毒制造者时也不再会赞叹他们的聪明才智。

互联网的普及让越来越多的人可以不受限制地阅读和研究与计算机病毒有关的资料，并且可以轻松地把自己的实验品传递给他人。而隐藏在后的那只叫做“经济利益”的幕后黑手，会让病毒制造者更加乐此不疲。

我们现在使用的操作系统和应用软件功能越来越强大，代码也越来越复杂，而越复杂的东西必然会有越多的破绽。这些破绽永远都不可能被全部修复，从而永远会让病毒和木马找到突破口。

计算机软件和计算机病毒的关系就像是光明和黑暗，像善与恶，像美与丑。它必然会存在，并且将会永远存在下去。

（全文完）