知识工程在计算机反病毒技术中的应用

周锋 编
潘锦平 宙

上海科学技术文献出版社

知识工程在计算机反病毒技术中的应用

周　锋　编
潘锦平　审

上海科学技术文献出版社

(沪)新登字 301 号

知识工程在计算机反病毒技术中的应用

周 锋 编
潘锦平 审

上海科学技术文献出版社出版发行
(上海市武康路 2 号)
全国新华书店经销
上海科技文献出版社昆山联营厂印刷

开本 787×1092 1/32 印张 7.375 字数 178,000
1993 年 2 月第 1 版 1993 年 2 月第 1 次印刷
印数：1—2,500
ISBN 7-5439-0069-6/T·253
定价 4.70 元
《科技新书目》279-314

前　言

计算机病毒的流行引起了普遍的关注，研究与发展反病毒技术已经提到议事日程，计算机病毒的入侵与反入侵——这场信息对抗已经在智能化的高技术领域内展开，因此，研制与开发广谱的、自动化的抗病毒软件系统以至专家系统已是势在必行。本书在详细地剖析计算机病毒的设计思想、解剖特征及其工作原理的基础上，论述了应用知识工程的理论与方法指导反病毒技术的研究以及抗病毒系统的开发。书中第一、二章介绍了计算机病毒的概况、构成及其各组成部分的工作原理，第三章是计算机反病毒的解析基础，第四章详细地剖析了目前流行的典型的计算机病毒，第五章着重论述了计算机反病毒技术的方法论，第六章则对反病毒的策略以及病毒的治疗、预防与免疫技术作了深入的探讨，第七章介绍了知识工程的基本理论与方法，第八章则具体叙述了应用知识工程的思想开发智能化反病毒软件系统的技术，第九章专门介绍了反病毒专家系统的研制、开发与实现。

本书从反病毒技术方法论与知识工程理论的高度，深入浅出地叙述了反病毒软件与专家系统开发的具体方法，具有较强的实用性，适合于大专院校师生及广大计算机工作者的阅读与参考。

本书蒙上海交通大学潘锦平教授审阅，在编写过程中得到了潘教授的指导，也得到了华东师范大学李玉茜教授和上海第二工业大学何守才副教授的帮助，在此，对他们的指导和帮助表

示衷心的感谢。

由于作者水平有限，编写时间仓促，书中所述，如有不当之处，恳请各位专家与广大读者批评指正。

编者　1992年2月

目　录

第一章　计算机病毒的概述

§1.1　计算机病毒的起源与发展

70年代中叶，计算机病毒开始出现于美国的一些科幻小说之中，使生活在信息社会中的人们也颇感新奇。然而，曾几何时，这个人们臆想中的幽灵却活生生地出现在世界各地的计算机系统之中，并已泛滥成灾，对信息系统的安全构成了严重的威胁。

Fred Cohen博士于1983年正式指出了计算机病毒的客观存在，并于1984年在VAX-11/750机上以实验证明了他的科学论断。这种能够进攻计算机系统并能进行自我复制的指令序列可以对系统资源造成不同程度的损害，甚至构成当今社会国计民生中的严重灾难。

然而，计算机病毒究竟如何产生？又是如何发展起来的呢？关于"病毒"起源问题，目前仍是众说纷纭，各执其词，但从目前已经出现的计算机病毒的情况来看，病毒产生的原因，大致有以下几种类型：

(1) 软件生产公司为了保护自身的经济权益，防止非法拷贝而采取的防范措施。为报复非法复制者，破坏其计算机系统资源而设计的病毒程序。

(2) 雇员或软件工作者发泄不满情绪，偷置"特洛伊木马"于软件之中，伺机发作。对雇主或单位进行报复，以破坏企业计算机网络或系统。

(3) 软件人员的自我表现。大多数计算机病毒的制造者，至

少在某个方面具有较精深的计算机知识。有些软件人员制造的病毒程序无专门的破坏目的或明显的报复动机，仅仅是技巧的炫耀与卖弄。然而一旦"魔瓶"打开，则一发而不可收，贻害非浅，其严重后果或许对这类病毒作者本人来说也是始料所不及的。

(4) 计算机流氓的恶作剧。由于家庭电脑的普及，不少青少年乃至某些熟悉计算机的人，故意干扰计算机系统而编制的具传染能力的捣乱程序。

(5) 具有犯罪目的的计算机病毒程序。为了达到某个目的，以破坏企业计算机系统运行作为要挟敲诈手段而设计的病毒代码。

尽管计算机病毒研制者可以具有各种不同的动机，然而有一点可以肯定，即"病毒"的产生必定是具有特定目的的人故意泡制出来的，它既具有类似生物病毒的某些特征，也享有计算机程序的权利，并能对计算机系统造成不同程度的损害。

与其他计算机技术相比，"病毒"研制技术问世较晚，但其发展速度之迅猛，波及覆盖面之广，危害程度之烈却是令人吃惊的。从1975年科普作家臆想中的"计算机病毒"到1983年Fred Cohen博士正式指出，并用实验证明"计算机病毒"的客观存在仅花了几年的时间，从这以后的几年里，计算机病毒以令人瞠目的汹涌之势，迅速遍及全世界。受攻击的用户总数几乎是直线上升，其危害程度也越来越严重。1987～1989年，几乎是计算机病毒猖狂肆虐、泛滥成灾的年代。美国统计的受病毒攻击的用户总数，1988年2月为3000户，1989年7月则为50000户，实际上不同程度受染的计算机系统远远不止这些，许多病例只不过因未构成严重的损害而未列入统计之列。

计算机病毒的研制技术，也已经从一些简单的捣乱程序发展到作用于军事领域及高技术领域之中。人们已经发现，可以

通过无线电波将病毒程序植入攻击目标，这完全超出了一般病毒传播的技术范畴。至于目前病毒的种类、开发技术、传染方式、破坏程度等真可以说是日新月异、花样翻新，足以使人深感忧虑。

纵观计算机病毒的发展历史，我们不难得出这样一个结论：计算机病毒是一门精深的学问。就目前情况来看，它大多数被应用于破坏目的，而从发展趋势来看，病毒正在向高技术及军事领域渗透，对人类构成了更为巨大的潜在危险。但值得强调指出的是：计算机病毒并非必定有害，本来可以引导其沿着造福于人类的道路健康发展的。如震惊世界的蠕虫病毒虽造成了极其严重的后果，肇事者莫里斯(Robbet·T·Morris)也受到了法律的制裁。但"蠕虫"程序可以作为网络设备诊断工具，利用其重新自定位能力向网络中未占用的设备发送拷贝，从而检测网络中机器情况。因此，象细菌、生化甚至核动力那样，人类有必要在计算机病毒与反病毒技术的发展上制定正确的导向，致使这门技术应用于为人类造福的领域。

§1.2 计算机病毒的定义与特性

迄今为止，世界计算机学术界尚未对计算机病毒作出一个统一的确切定义，即使是计算机病毒学专家 Fred Cohen 博士及 B·W·Burnham 作出的计算机病毒之定义，也被认为具有一定的片面性。事实上，从计算机病毒的构成、寄生方式及其作用机理，可以将其定义为：能够侵入计算机系统并能够进行自我繁殖；能够攻击计算机系统并对其产生不同程度损害的指令序列。从这个定义出发，可以看出计算机病毒必然具备如下基本特性。

1. 程序特性

它必定是为完成某些特定功能而设计的一批指令代码的有序集合。尽管它可以不是一个完整的程序，但它具有明显的编制目的性，程序的逻辑性和有序性，并享有一切程序所共享的权利。

2. 寄生特性

作为计算机病毒，它必定要在计算机系统内寻找不同的宿主作为寄生与隐蔽的基地以保存自已，并伺机进行复制或进行破坏。(不同的计算机病毒具有不同的宿主对象，某些计算机学者就是根据计算机病毒的不同宿主对象，对其分类，实际上是据病毒的寄生方式将其分为内存寄生型、磁盘寄生型、文件寄生型等)显然，本特性也包含了计算机病毒程序的隐蔽性和潜伏性。

3. 进攻特性

计算机病毒的进攻特性事实上包括了引发、传染、破坏和表现四大特性。其中引发与传染是一切计算机病毒共有的必备特征，而计算机病毒的破坏和表现特性，则因计算机病毒的种类不同，在程度上或兼有性方面会有相当的差异，如有些计算机病毒就没有明显的表现部分。

4. 复制特性

这是指计算机病毒在计算机系统内可以进行自我复制或可在程序运行中作衍生复制。

§1.3 计算机病毒的寄生与分类

计算机病毒的分类学中，目前存在着许多不同的分类方法。按病毒的危害性分类，可把病毒分为良性与恶性两种。凡是破坏数据或文件的病毒，称为恶性计算机病毒，反之为良性计算机病毒。按寄生方式分类，又可分为 ① 操作系统型；② 外壳型；③ 入侵型；④ 源码病毒四大类型。按病毒解剖特点，又可

分为前插式、后插式、间隙插入式三类。笔者认为，上述各分类方法均存在划分界线不清，并对病毒诊治无益之弊，而可取的两种分类方法是：

1. 以操作系统为划分范围的分类法

可将病毒分为两大类型：

(1) 系统病毒：指存在于操作系统内部，随系统启动过程加载并产生作用的病毒，如：小球病毒(Ping Pang Virus)，大麻病毒(Stone Virus)等。

(2) 过程病毒：指存在于系统程序之外某个可执行体内的病毒，这类病毒的加载依赖于所在的过程。这里的过程是指在操作系统下可直接运行的程序文件，在DOS系统中，一般指exe文件与com文件，当然也可以是bat，ovl和obj文件。

2. 寄生方式分类法

按照计算机病毒依附寄生的介质进行划分，可将计算机病毒分为：

(1) 内存宿主型。

(2) 磁盘宿主型。磁盘宿主型病毒又可分为：

① 主引导区寄生型：一般是指侵占硬盘主引导扇区的病毒。

② 引导区寄生型：一般是指侵占操作系统中引导扇区的病毒。

③ 可执行文件寄生型：其范围基本上同第一种分类法中的过程病毒。

§1.4 计算机病毒的危害

下面列举一些事例，以窥计算机病毒危害之一斑。

1987年5月，美国《普罗威斯顿报》编辑部发现帕金斯公司

防止非法拷贝的计算机病毒，其时病毒已广泛侵入了报社计算机网络系统的各结点设备。

1987年12月IBM公司收到的圣诞祝贺程序系计算机病毒程序，最后导致因病毒程序大量占用网络及系统资源而被迫部分停机。

1987年11月18日，美国Iehigh大学，发现600个以上的机器设备及媒介受到Iehigh病毒的攻击。

1988年3月2日，潜伏已久并已广泛传播的Apple机病毒迫使大批受染的Apple机停机，以"庆祝苹果机的生日"。

1988年夏季，前苏联发现了三种入侵计算机系统的病毒，专家们经过三个多月刻苦努力地工作，才基本上排除了病毒的危害。

1988年台北举办国际围棋比赛时，首次发现了入侵台湾的计算机病毒，致使参加比赛的Macintosh计算机系统瘫痪，最后只得停赛。

1988年以来，全世界发现了100多种病毒（我国也先后发现了50多种病毒），据不完全统计约有40万台以上的计算机，11%以上的设备受到了计算机病毒的侵扰和破坏。

另外，诸如日本的窃取计算机口令进行犯罪活动的病毒程序以及利用银行金融系统计算机网络进行高技术非法活动的病毒程序等已属屡见不鲜，被称为高科技史上的"灾难"。由美国康奈尔大学23岁的研究生罗伯特·莫里斯(Robbet·T·Morris)编制的"蠕虫"病毒程序(Tapworm)则导致了一场震惊世界的病毒灾害：1988年11月2日，美国计算机网络INTERNET受到病毒的攻击，在不到24个小时内，病毒迅猛扩散并大量地耗费计算机的时空资源，使大批计算机专家及操作人员惊慌失措，成千台计算机迅速受"灾"，许许多多机器因过载而被迫停机，尽管美国

高等院校及专家们竭力采取紧急措施，控制疫情蔓延，但已经造成了约8000万美元以上的直接经济损失。此外，劣迹深重的"黑色星期五病毒"则于1989年11月13日星期五，在全世界数十万台计算机中发作，在世界范围内造成了难以估量的损失。这一切引起了计算机学术界的关注。如果在军事部门或尖端武器的控制系统中植入了病毒代码或要害部门受到病毒程序的入侵，其后果真是不堪设想，将会导致人类生命财产的惨重损失。

诚然，由于我国尚未大规模使用大型计算机网络及广泛采用大型的计算机系统，因此计算机病毒尚未形成大的"灾情"。然而随着大中型企业中C·I·M·S(Computer Integrated Manufacturing System) 及M·R·P (Material Requires Planning)系统的普遍推行，计算机反病毒技术将被提上重要的议事日程。从而，对反病毒技术也将提出更高的要求。在本书各章节中，将详细地介绍对各类计算机病毒的防治方法，尤其是如何以知识工程的理论来指导反病毒技术发展的基本机理。在这里，还要强调指出，计算机反病毒技术必须首先着眼于"以防为主"的"反入侵"原则，大力宣传教育，提高计算机工作人员的职业道德水准，制订并执行计算机软件法规，这对防止计算机病毒的流行将起到事半功倍的效果。

第二章　计算机病毒的构成

§2.1　计算机病毒的一般构成

计算机病毒一般由引导部分、标志部分、引发部分、传染部分、表现部分与破坏部分组成。但需要指出的是：上述这几个组成部分并不是每种计算机病毒都必然具有的，每个组成部分也不一定构成独立的程序模块。例如：从"小球"病毒的存储结构来看，长度为1024个字节的病毒代码占两个扇区，第一扇区中存放了引导程序和一部分传染程序，另一扇区中存放着表现程序与一部分的传染程序。从程序的结构分析来看，"小球"病毒具有引导模块、传染模块与表现模块，没有明显的破坏程序，有病毒特征标志部分，但不是独立的程序模块。此外，大多数病毒之引发部分的程序，一般都分别写入传染、表现与破坏模块之中，很少将引发部分设计成一个独立的程序模块，它只是作为其它模块的辅助部分，其功能是监视系统运行的状态，判别是否满足病毒的传染条件、表现条件或破坏条件，从而触发对应的病毒程序，以执行某种特定的操作。

然而，既然称之谓计算机病毒，则一般来说，应包括引导部分、传染部分及表现部分这三个基本构成，恶性病毒还具有破坏部分。不同种类的计算机病毒在程序结构上会有很大的差异。如："巴基斯坦智囊"病毒就没有明显的表现模块与破坏模块，只有引导模块与传染模块。又如："维也纳"病毒，则只作为一种瞬时病毒不驻留内存，也没有引导模块，仅仅只有传染模块与破坏模块。本章以下各节将对计算机病毒的这几个基本构成，作进

一步的介绍与说明。

§2.2 引导部分

计算机病毒的引导部分，一般都作为一个独立的程序模块出现，并且大多数计算机病毒都拥有引导模块。它作为计算机病毒的"先导部队"，完成对计算机系统的进攻。绝大部分病毒往往采用各种不同的方式，将自身的引导程序首先"攻入"计算机系统，继而完成其它一系列的操作。如操作系统型病毒("小球"病毒、"大麻"病毒、"巴基斯坦智囊"病毒等)都是在系统启动时，将病毒的引导程序读入内存，并获得系统控制权，使之得到优先执行。引导程序的执行结果大多是完成病毒其余部分的读入和安装，占领内存或磁盘的某个区域。通常，引导程序选择不易被发现或不易被覆盖的区域作为病毒的寄生基地，以保证病毒的隐蔽性与潜伏性。引导程序还能制造某些假象(如制造伪坏簇，重新设置内存大小等)对病毒本身进行保护。此外，引导程序还将完成一系列中断向量的修改，为病毒的传染、表现和破坏部分创造运行条件。在"小球"病毒内，这一系列复杂的操作都是由只占一个扇区—512个字节的引导程序来完成的，其编程相当精炼，利用系统的弱点又恰到好处，确实可称得上设计精妙，匠心独具。

§2.3 标志部分

计算机病毒的标志部分是设计者在病毒程序中某个特定位置上设置的一串字符，标志部分的内容与设置的位置均为某个病毒所固有，因此，它往往是某个计算机病毒的标志符，称作病毒的特征串。从目前已经发现的病毒来看，有用标志符来表示病毒制造者的地点、国籍、人名或病毒攻击之目标的，也有用标志