计算机病毒和反病毒对策

马希荣 (宁夏大学计算中心)

本文就计算机病毒的防范对策提出自己的见解。

一、计算机病毒、病毒表现形式及其破坏性

计算机病毒是一种在计算机系统运行过程中能把自身精确拷贝到其他程序体内的程序。根据美国著名计算机安全专家 Pred CoHen 说，感染性是判断病毒的必要条件。广义的计算机病毒则包括所有引起计算机故障、毁坏计算数据的破坏性程序。PC 机上的病毒大多符合狭义计算机病毒的定义。计算机病毒的主要特征有：

* 计算机病毒是人为制造的软件；
* 计算机病毒的运行是非授权入侵；
* 计算机病毒可隐藏在可执行程序和数据文件中；
* 具有再生机制，即可传播性；
* 具有依附其它媒体的寄生能力，即可潜伏性；
* 在一定条件制度下，使病毒程序活跃起来，即可激发性。

诸如磁盘引导扇区被破坏，目录区被修改，磁盘出现坏扇区，系统运行中出现死机，磁盘文件被修改或破坏，磁盘文件长度改变，磁盘上出现异常文件，屏幕上出现异常信息或图像，系统运行速度明显下降，内存空间显著减少等等都是计算机病毒的表现形式。

目前流行的计算机病毒，其破坏性主要表现在以下几个方面：

①破坏系统的程序和数据资源，造成系统动态运行中的运行错误，致使系统瘫痪；

②全部删除或部分破坏软盘、硬盘上的可执行程序和数据文件；

③破坏文件分配表 FAT；

④在磁盘上制造“坏”扇区，并隐藏病毒程序内容；

⑤破坏内存分配，减少系统可用的有效存储空间；

⑥破坏磁盘的文件目录；

⑦修改或破坏数据文件，可执行文件；

⑧增加无意义的回路，降低计算机系统的运行速度

⑨空挂系统，封锁键盘。

二、计算机病毒产生的必然性

当今计算机病毒是计算机发展到一定阶段的必然产物，它是计算机犯罪的一种新的衍化形式。在相当程序上受到社会环境的刺激，诸如计算机应用的普及和社会化，知识产权和环境保护，计算机法律不健全都会刺激计算机病毒的产生和发展。

计算机病毒产生的深层次原因是计算机系统自身的脆弱性造成的，其涉及硬件脆弱性和软件脆弱性。其脆弱性在 PC 机上表现得最彻底。在 MS-DOS 下，一切系统资源都是透明的、开放的，磁盘数据、文件系统、中断系统及 DOS 本身，毫不设防，用户可以随意修改，各层次都可能受到攻击。特别是微型计算机系统是通过软盘作为信息传输和交换载体，系统自身就缺少对用户非法侵入的防范能力。

软件是硬件的外层，软件为用户提供了使用系统的逻辑界面和手段。软件的脆弱性是由于：

. 软件的本质和特征；

. 软件是用户使用计算机的工具；

. 软件是信息传输和交流的工具；

. 软件可以非法侵入载体；

. 软件可以非法侵入计算机系统；

. 软件具有寄生性，可以潜伏在载体或计算机系统中，从而构成合法文件含义下的非授权文件；

. 软件具有进攻性，一个人为设计的特定软件可以破坏指定的程序或数据文件，可以造成计算机系统瘫痪；

. 软件的可激发性，是一定条件刺激下的逻辑炸弹；

人们应当注意软件的二重性，既软件巨大的创造性和潜在的破坏性力量。软件是工具、手段，在某种情况下又是一种知识武器。

三、反计算机病毒之对策

在计算机病毒泛滥的同时，反病毒对策的研究在与病毒对抗中发展起来。从诊断、治疗和预防三个方面抑制病毒的泛滥，研究成果斐然，已经出现许多反病毒产品。但是，反病毒对策是一个综合治理的问题，需要全社会计算机使用者的参与。应采取一系列科学管理方法和预防措施。

1.计算机系统的安全管理

计算机安全管理即从管理和使用上提出抵制病毒感染的有效措施。

. 设置系统特权，将用户程序和操作系统分离开来，保

护自身的重要部分；

. 建立用户特权，将各任务的信息区分开，控制用户之间的互访操作；

对于微型计算机应当注意：

. 对系统软件，可执行程序的写保护，尽可能不用软盘启动；

. 不使用未经检测的软磁盘；

. 坚持经常性备份；定期对微机程序进行比较测试和检查，以检测病毒有否侵入；

. 谨慎使用公用软件，防止病毒的传播和扩散；

. 不允许将各种游戏软件装入计算机系统。

2.加强软件保护，尊重知识产权

软件是人类智力的产品和知识的结晶，软件的开发往往要花费大量的人力、资金和时间。借助法律手段保护知识产权，防止他人复制或非授权使用计算机软件，可以加速软件的发展和知识产业的建立。

目前，我国计算机病毒的传播，在一定程度上反映了软件非法拷贝和侵犯知识产权的严重程度。另一方面，在一定程度和范围内，计算机病毒已作为违反知识产权的一种惩罚，对此人们应当提高警惕。

3.软件自我保护技术

传统的软件质量指标已不适应新的工作环境，除了易维护、易理解、可靠和效率高外，程序的健壮性必须成为一个重要的软件质量标准。以往的软件自我保护主要是防非法复制、非法使用。如何提高软件防修改防入侵的能力是新的课题。

加密技术是程序体防止计算机病毒入侵的一种手段，其原因是：一般情况下计算机病毒难以入侵加密的程序体；既使计算机病毒能够入侵加密的程序体，经过解密处理的病毒程序也失去了作用。

采取加密技术保护软件，一般情况下要求：被加密程序的解密密钥难以推算或难以搜索；生成的被加密程序具有不可复制性。确切的提法是采用一般方法复制的被加密程序，不能在计算机上直接运行。

以微型机为例，用户采用汇编语言编制的加密程序，其它用户或破译者可以利用反汇编工具将机器指令逐条加以解释，逐条理解指令的含义和加密程序的设计方法，DEBUG 程序本身就是一个破译程序的工具。因此，对于计算机系统上采用的加密技术，为了防止其它用户或破译者在计算机上动态解释解密程序，还需要考虑采取一定的反动态跟踪技术。

(1)反 DEBUG 跟踪

(2)键盘封锁

(3)设置各式各样的陷井(trap)

4.传统程序设计方法编制的反病毒软件过时，采用智能防治病毒专家系统传统程序设计方法编制的反病毒软件具有局限性，只能用于检测或消除固定模式的一种计算机病毒。这种反病毒软件不能用于计算机病毒变体，不能用于一类计算机病毒的检测或消除，不具有通用性。随着计算机病毒日益蔓延的情况下面临着以下问题：

(1)在病毒种类与病毒变体日趋增多的情况下，用户难以承担连续购买反病毒软件“系列产品”的开销。

(2)计算机病毒向病毒变体和智能病毒方向发展，使传统程序设计方法面临着一系列困难，不能适应客观形势发展的需要。

(3)防治计算机病毒需要占用大量的人力和物力。迫切需要防治病毒的人工智能系统(Arficial Intelligence)，在解决复杂的病毒程序问题，人工智能是以专家系统(Expert System)的形式得到应用的。专家系统具有以下特征：

它是一个智能程序系统；它内部具有大量专家水平的领域知识和经验；它能利用人类的知识和解决问题的方法来处理某一领域或方面的问题。

专家系统的知识库和推理机取代了普通程序设计中的数据和程序的概念。

专家系统的形成

计算机病毒的防范对策需要在实践过程中不断加以总结和摸索规律，以便形成一套行之有效的安全管理办法和措施。但是防范计算机病毒的根本问题在于防止计算机病毒对计算机系统非授权入侵，其中计算机物理界面的防范是基础，当今人们从逻辑界面来区分合法使用或非授权入侵，只能在一定条件下和一定范围内部分地解决问题，而无法从根本上解决问题。

参考文献：

[1]《计算机病毒大全》　刘　炯编译　湖北人民出版社　*1993* 年 *10* 月

[2]《计算机病毒剖析防治与免疫》　南方软件有限公司　文忠、水英 *1989* 年 *10* 月