计算机病毒的危害与防治

常春喜 (国防科技大学计算机系)

计算机病毒是一个越来越引起人们关注的课题,其重要性不仅表现在科学技术方面,还表现在国家安全的军事、政治斗争方面。近年来,计算机病毒像一阵恶浪,席卷各地,令全世界计算机界、军界惊惶失措。此文综述计算机病毒的研究情况。介绍了几起世界上较有影响的病毒案例及其恶果,并给出避免计算机遭受病毒侵害的几种常用措施,以及当前计算机病毒“疫苗”的研究进展。

目前,随着计算机工业突飞猛进的发展,计算机网络技术也日益发展壮大。随之出现的计算机安全问题,也愈来愈成为计算机专家们关注的焦点。众所周知,计算机的发展同计算机的安全是相辅相成的。影响计算机安全的因素多种多样,广义地概括起来不外乎两种:自然因素和人为因素。常见的有自然灾害、意外事故和人为破坏。近年来出现的计算机病毒问题,属于人为破坏的范畴,是计算机安全领域的一个比较突出的问题。本文将从计算机病毒的基本概念出发,结合几则国外计算机病毒案件的实例,系统地讨论计算机病毒的危害及防治。

一、什么是计算机病毒

计算机病毒的概念是弗莱德·科恩(Fred Cohen)于1987年11月3日在一次关于计算机安全的学术研讨会上首次提出的。

为了更好地了解计算机病毒,我们先来谈谈生物病毒。

众所周知,生物病毒是能够侵入人体和其它生物体内的病原体,在它潜入人或其它生物体内的细胞后,会大量繁殖与其本身相仿的复制品,这些复制品又去感染其它健康的细胞,被感染的细胞多半会因此死去。

计算机病毒和生物病毒一样,也是一种能够侵入计算机和计算机网络,危害其正常工作的“病原体”。所谓计算机病毒,是指进入计算机数据处理系统的错误信息,它可以

是一段计算机程序或一组计算机指令;当把它输入正常工作的计算机后,会把已储存的信息搞乱或破坏;它具有再生能力,会自动进入所有关联的程序中进行自我复制,冲乱其它正在运行的程序,破坏计算机的正常运转。正是由于这一现象与生物病毒在人体细胞中的扩散很相似,所以被称作计算机病毒。

弗莱德·科恩为计算机病毒所作的定义是:

计算机病毒是一个能够通过修改程序,并把自身的复制品包括在内去“传染”其它程序的程序。

病毒程序的关键性质是它具有传染性,即病毒的传递性。应该指出,病毒程序不一定都具有恶意攻击的目的,就是说有些病毒程序是“良性的”。例如,1988年11月2日致使美国国防部ARPANET网络瘫痪的病毒程序便属此类“良性病毒程序”。

与计算机病毒有相似性的概念还有:逻辑炸弹、蠕虫、特洛伊木马、核心战、后门等。

其它如数据欺骗、意大利香肠术、寄生术、陷井门、异步攻击、超级冲杀、数据泄漏、截获电磁辐射信息、线路窃听等,都是七十年代、八十年代威胁计算机安全的主要手段。

二、计算机病毒的案例

近几年来,世界上发生计算机病毒案例有很多起,下面介绍的仅是其中较有影响的一部分案例,从中我们可以对计算机病毒的危害有较深入的了解。

实例1 程序员利用计算机病毒报复

据报道,在美国的一家计算机公司,一位程序员被公司辞退后,回到家里越想越生气,决定来个“大反攻”,对公司进行报复,当晚即回公司输入一个程序,使计算机“发病”。结果这个程序五年后才发生作用,造成整个作业系统的混乱,计算机专家们费了九牛二虎之力,才把这个程序找了出来。另外有一个在银行工作的计算机工作人员,也输入一个“若我的名字在人事档案中消失,会计系统则会紊乱”这样一个程序。结果当他被辞退后,不仅银行的会计系统紊乱,而且所有与这家银行联网的部门也都出现了紊乱。

实例2 “特洛伊木马”的危害

自1987年春以来,美国一些不法的“计算机入侵者”们以个人计算机通讯为媒介,采用被称为“特洛伊木马”的计算机病毒程序,进行恶劣活动。

他们在电子显示板上显示带有诱人名称的程序,即破坏性程序。当使用者通过网络线路引入个人计算机时,使用者的软件即被破坏。该病毒的传染能力极强,每使用一次程序即自行增殖。由于它有自行增殖的能力,所以危害性极大,不仅在个人计算机用户之间,而且还侵入到商业网内。

实例3 IBM 公司遭受计算机病毒袭击

1987年12月,人们发现计算机病毒已侵入世界闻名的计算机公司IBM在坦帕的广播网内。计算机画面本应出现有关圣诞节内容的通信,却反复出现无意义的病毒程序。不但美国,连以色列的赫布来大学也遭到这种病毒程序的侵入,致使多年的研究资料报废。

实例4 蒙特利尔程序员的恶作剧*

实例5 计算机病毒“入侵”台北

在台湾台北市举行的1988年国际计算机围棋赛中,台湾大学资讯(注:即信息)工程研究所俞旭升参加比赛的Macintosh计算机被计算机病毒侵扰,完全瘫痪。他在比赛中发现计算机有不正常的重复动作,根本无法对奕。经过指导教授鉴定,确认计算机的硬磁盘机已被病毒侵入,比赛程序也被病毒“吞

* 见《计算机科学》1988年№5,“一种‘病毒’引起计算机行业恐慌”。

噬”。据推断,造成感染的原因,可能是赛前在学校教授如何操作计算机时,从有毒的软盘内将资料拷贝到硬磁盘机。在比赛时,选手将自己的程序磁盘放入磁盘机读取,硬磁盘机的病毒自动扩散到比赛程序,不断地自我复制,侵害正常程序。据说目前这是第一件“计算机病毒”入侵台湾的案例。由于该病毒来源有限,应不难查出病因。而且台湾的计算机并未连成网络,因此不像美国发生的计算机病毒那样,会通过网络快速蔓延扩散,根本无法防范。

实例6 美国高科技史上的“灾难”

1988年11月2日晚,美国国防部远景规划署(Defense Advanced Research Projects Agency) ARPANET网上的电子计算机突然停止工作,终端屏幕上显示出一系列乱七八糟的符号。ARPANET网连接全国三百个大学、私人公司、研究中心、军事基地和国防部研究机构的约六千台电子计算机。与该网络相连的全国军用、民用计算机网络——东起麻省理工学院、哈佛大学、马里兰海军研究实验室、马里兰大学,西到加利福尼亚大学伯克利、圣地亚哥分校,以及弗吉尼亚的太空总署研究中心、斯坦福大学国家研究所,甚至兰德公司研究中心的电子计算机网,都同时出现了故障,整个网络瘫痪了二十四个小时。

网络刚一瘫痪,正在进行国际科技研究工作的人员顿时陷入一片混乱之中,手忙脚乱而又无可奈何。与此同时,电子计算机却仍在紧张地运行——输入计算机的快速扩散性病毒程序大量复制与病毒程序相仿的信息,这些毫无意义的符号通过电子邮件方式提供给与自己相连的网络,致使它们也相继“罢工”。当天夜里,国防部成立了一个应急中心,处理这起病毒袭击案,着手调查并协同全国数千名电子计算机专家进行网络的“消毒”工作。

到11月3日下午为止,全国共有六千多台联网的电子计算机遭受病毒侵害,造成了瘫痪或半瘫痪的后果。据统计,这次病毒侵害造成的直接经济损失达数百万美元,对各大研究中心研究工作的影响则难以用美元来估算。由于ARPANET还与国际上联网,其“病毒感染”还波及了国外的一些研究机构。计算机专家们认为,这是美国有史以来,电子计算机系统遭受的一次最严重、规模最大的病毒侵袭。

原来,这起事件是康奈尔大学二十三岁的罗伯特·莫里斯(Robert Morris)干的。他是该校计算机科学专业的一年级研究生,其父老莫里斯是政府

安全部门的一位颇有名望的计算机安全专家。

老莫里斯设计的保护电子计算机UNIX操作系统安全的软件，成了小莫里斯“病毒程序”袭击的目标，小莫里斯声称自己的病毒程序只是一种“实验”。由于一个小小的疏忽，这个病毒程序自我复制失控，顷刻间广泛扩散。据他自己讲，造成这么严重的后果并非他的本意。“扫毒”专家们认为，小莫里斯技巧绝伦，他是看准了ARPANET网络在安全方面的三项小缺点守下的手。

11月4日，美国国防部宣布，经过日夜奋战，已经消除了2日在ARPANET网中作案的“病毒”源。经过清洗，受感染的计算机网络已恢复正常。所幸本次“病毒”属“良性软件”程序，只是造成障碍，致使停机瘫痪，而没有销毁计算机档案文件，而且侵害也未殃及核武器管理系统和储存重要军事机密的计算机网络。

三、危害及对策

从上一节的实例研究我们可以看出，由于计算机病毒自我复制能力极强，一旦染上，就会“传染”整个计算机网络。它所能造成的危害主要有以下几种：

(1) 病毒程序通过“自我复制”传染其它正在运行的程序，或与存储器中储存的程序争夺有限的存储空间；

(2) 病毒程序可冲毁存储器中的大量数据，致使计算机其它用户的数据蒙受损失；

(3) 病毒程序不仅侵害所使用的计算机系统，而且侵害与该系统联网的其它计算机系统；

(4) 病毒程序可导致计算机控制的空中交通指挥系统失灵，金融系统瘫痪，工厂生产停滞，卫星、导弹发射失败，政府机构、事业部门秩序紊乱等。

综上所述，尽管计算机病毒危害力极强，但也并不是说不能够预防。在美国的这次计算机病毒大规模侵袭中，AT & T公司就未受任何影响，原因是该公司早已采取了积极的预防措施；美国国家宇航局也是由于三月份发生“病毒”侵犯后采取了措施，此次才未受大的影响。

那么应该如何防范计算机病毒呢？我们知道，能够编制病毒程序、制造计算机病毒的，一般是计算机专业人员或对计算机技术相当精通的人。所以，在防范计算机病毒、

探讨计算机安全问题时，人的因素应该是重点考虑的。总之，我们应该从管理和技术两个方面来解决这个问题。

在管理上，我们应该：

(1) 加强对计算机工作人员的思想教育，树立高度的职业道德和法律观念，提高他们的觉悟；

(2) 制定计算机安全法律，在社会上大力普及该法律的教育。如擅自连接政府部门的计算机网或妨碍其正常工作，可判刑、罚金，甚至监禁；

(3) 要对国防科技机密管理系统、作战指挥系统、武器操纵方面的电子计算机提供特殊的安全保护措施；

(4) 研究一切影响计算机安全的因素和保障计算机安全的措施；

(5) 促进保障计算机安全产品的生产和应用，加强计算机安全技术的开发和研究。

在技术上，计算机病毒防范所采取的手段主要有基本限制、分割模型、流模型、限制解释等四种^{*}。由于计算机病毒的高传染性和高渗透性，加强对计算机病毒的防范无疑对系统的安全是有益的。

计算机安全专家们都很清楚，安全保护措施只是相对的，并非百分之百地保险。只要存在着计算机的共享，就有着病毒侵入和传染的可能。安全保护措施再严密，也难免有漏洞，“道高一尺，魔高一丈”。绝对地防止病毒传染，只有要求系统绝对地隔离才能办到，但这是不现实的。对此，弗莱德·科恩曾作出了这样的结论：

要使通用的系统共享与病毒防范共存在实际上是不可能的，只有综合起来加以权衡才能解决。

四、病毒“疫苗”的研究

前面我们说过，计算机病毒侵害计算机和生物病毒侵害生物的机理是一样的。只要生物受了病毒的感染，就要找出病毒产生的根源，并采取消灭这种病毒的措施，使生物具备抵抗病毒的“免疫力”。从计算机病毒出

^{*}见《计算机科学》，1988，N6，“关于计算机病毒的讨论”。

现之日起,人们就一直在努力寻找着能够消除这种病毒的“疫苗”,但目前进展幅度不大,尚未找出可以完全“解毒”的“灵丹妙药”。

现在国外市场上有一些商业性的,预防“病毒”的“疫苗”,但无一能确保整个计算机网络完全“免疫”。计算机一经连网,就很难保证无漏洞,只要有漏洞就有可乘之机。

在瑞典,有一家计算机公司已经研制出一种可以抵抗计算机病毒的“疫苗”。这种抵抗计算机病毒的“疫苗”,是一个计算机的标准型软件磁盘。当它被放置在计算机中后,就象一个“巡逻卫士”那样不断地对数据存储器进行抽样检查。它可以在每一个数据存储器的电子隔离层中发现故障并及时发出警告,从而使整个数据处理系统网络免遭“病毒”的“感染”。

在台湾,为了防止计算机病毒的蔓延,台湾交通大学最近研制成功一种称为“ANTIBUG”的解毒程序。1988年11月,该校曾发现有些计算机的磁盘受到“病毒”感染。经过多次研究,他们研制出一种简易程序,它可用于检测磁盘是否“中毒”,并进一步予以“解毒”,该程序被命名为“ANTIBUG”。

在日本,有一位十八岁的高中生小一正香,最近研制出一种专门对付计算机病毒程序的“疫苗”,这种抗病毒程序适用于大多数计算机系统。目前已有约二十种计算机病毒侵入日本。1988年9月,日本发生一次重大的“病毒”程序侵入事件。一种病毒侵入日本最大的计算机网络,内存数据被他人任意调用,造成很大损失。事件发生后,许多计算机专家竞相开始“疫苗”的研制。小一正香是日本第一位研制出“疫苗”程序的人。他设计的“疫苗”程序定名为“HOSPITAL”,该程序可以通过计算机操作员的操作来监视病毒的传染。如遇病毒侵袭,屏幕上即显示警报信号。为验证该程序的可靠性,他曾对八种“病毒”进行了试验,结果是令人满意的。

由于对计算机病毒的研究刚刚起步,各种病毒“疫苗”的研制机构刚刚建立,我们相

信,随着时间的推移,会有更多更有效的计算机病毒“疫苗”问世。

我们正处于信息时代,计算机安全问题已成为高技术领域的重要研究课题。由于国外计算机工业相当发达,网络连接面广,所以发生病毒感染的可能性极大。从我国的具体情况来看,计算机还未大量普及,计算机网络的规模还小——目前主要是小规模的局部网,所以计算机病毒感染的可能性较小。但是应该看到,在不远的将来,计算机安全问题将随着我国计算机的迅速发展而变得愈来愈重要,特别是在军事上将起着举足轻重的作用。鉴于国际上计算机安全的局势,希望我国对这个问题更加重视,大力开展这一方面的研究,扩大与外国同行的交流,以期将来更好地解决可能出现的问题,防患于未然。

本文得到了陈火旺教授、金士尧教授、陈慧清副教授的指导和帮助,在此表示感谢!

参考文献

- [1] Fred Cohen, Computer Viruses, Theory and Experiments, COMPUTER & SECURITY, Vol. 6, No. 1, Feb. 1987
- [2] Harold Joseph Highland, Computer Viruses and Sudden Death, COMPUTER & SECURITY, Vol. 6 No. 1, Feb. 1987
- [3] Karen Guilo, Security IS Loosely Practiced at Young Supercomputer Firms, DATAMATION, Vol. 34, No. 1, 1988
- [4] John Markoff, A 'Virus' Gives Business a Chill, THE NEW YORK TIMES, Mar. 17, 1988(中译文见本刊1988, No. 5)
- [5] 吴亮,“计算机病毒”,《计算机世界》, No. 203, Aug. 24, 1988
- [6] “美国军事计算机系统告急”,《参考消息》, Nov. 7, 1988
- [7] “侦测磁盘是否中毒”有妙方,《计算机信息报》, Mar. 7, 1989
- [8] 张德民,“向计算机病毒挑战的人”,《今晚报》, Apr. 2, 1989
- [9] Lehmann, F. Computer break-ins, Commun. ACM 30, 7 (July 1987) 584—585