

计算机病毒的检测与防治

主 编:刘清波 刘振鹏 马 力
副主编:蔡淑珍 徐建民

计算机病毒的检测与防治

23.9.5

23/1

出版

警官教育出版社

TP309.5
LQE/1

计算机病毒的检测与防治

主 编: 刘清波 刘振鹏 马 力

副主编: 蔡淑珍 徐建民

警官教育出版社

(京)新登字 167 号

JS386/82

书 名：计算机病毒的检测与防治

著 者：刘清波等

责任编辑：李剑涛

封面设计：世 良

责任校对：魏济杰

出版发行：警官教育出版社

(北京西城木樨地北里 2 号 100038)

印 刷：河北大厂县胶印厂印刷

经 销：新华书店总店北京发行所

版 次：1995 年 10 月第 1 版

印 次：1995 年 10 月第 1 次印刷

印 张：13

开 本：16

字 数：280 千字

印 数：10000 册

ISBN 7-81027-667-0/G · 214

定 价：16.80 元

前 言

计算机是当代发展最为迅猛的科学技术,其应用几乎已深入到人类社会活动和生活的一切领域,大大提高了社会生产力,计算机在现代化建设中的战略地位和作用日益突出。但是进入 80 年代后期国际上陆续出现了大量的计算机病毒,并呈不断蔓延的趋势。计算机病毒对计算机的正常运转构成了严重的威胁,轻则影响计算机系统的运行性能,重则破坏系统中的数据和文件,以至于系统突然瘫痪。计算机系统的安全问题日益受到人们的重视和关切。

计算机病毒是一种程序,它通过修改其它程序,把自身拷贝“贴”在其它程序之内,从而完成对其它程序的传染。由于程序就是设计者的代言人,如果病毒程序设计者怀有恶意,那么他所设计的程序就可能对计算机系统构成严重的威胁。计算机病毒并不是一种利用操作系统缺陷的程序,而是通过正常的操作执行正常的用户程序,任何系统只要允许信息被分享、解释并再传送,病毒就能扩散到整个系统,因此不要期望取消这些系统功能来达到防护的目的。

我们编写这本书,试图从实用角度出发,尽量全面地介绍计算机病毒的特性、特征及防范和消除方法。本书第一章概述了计算机犯罪的概况及病毒的流行、蔓延情况,并介绍了关于计算机病毒起源的几种看法;第二章简要介绍了计算机病毒的本质及特点,目的是使读者对计算机病毒有形象地了解,充分认识计算机病毒的危害性;第四章阐述了防范计算机病毒的一些措施;第五章详细介绍了几种防病毒软件的使用方法,使一般读者可以利用现有防病毒软件有效地诊断、消除计算机病毒;第六章概述了防病毒卡的作用并介绍了国内几种常见的防病毒卡;最后一章全面介绍了计算机病毒所涉及到的有关 DOS 系统的基本知识和人工检测、防范各类计算机病毒的方法,以便读者能在现有防病毒产品无能为力时,能利用人工手段及时发现并消除新的计算机病毒。

本书第一、二章由蔡淑珍编写,第三章由刘清波编写,第四、六章由徐建民编写,第五章由马力编写,第七章由刘振鹏编写,最后由刘清波、刘振鹏统编定稿。在本书编写过程中,张会芹同志协助主编做了大量工作,在此表示感谢。

由于我们水平有限,错误和缺点在所难免,恳请读者批评指正。

编者

目 录

第一章 计算机病毒概况	1	一、 传染途径	23
§ 1 计算机系统的脆弱性	1	二、 传染步骤	23
§ 2 计算机犯罪概述	3	三、 传染方式	24
一、 概念	3	四、 传染过程	24
二、 手段	4	§ 6 计算机病毒的破坏性	24
三、 特点	6	一、 破坏现象	25
四、 社会危害性	7	二、 症状	25
§ 3 计算机病毒的产生	8	第三章 流行计算机病毒介绍	28
一、 科学幻想	8	§ 1 小球病毒	28
二、 核心大战	8	一、 表现形式	28
三、 恶作剧	9	二、 传染途径	29
四、 软件保护	9	三、 组成	29
五、 美国软件俱乐部	10	四、 诊断	30
§ 4 计算机病毒的蔓延情况及其危害	11	五、 消除	32
一、 计算机病毒在国外的情况	11	六、 变种	33
二、 计算机病毒在国内的情况	12	§ 2 巴基斯坦智囊病毒	34
三、 计算机病毒制造者面面观	13	一、 表现形式	35
第二章 计算机病毒原理	14	二、 传染途径	35
§ 1 什么是计算机病毒	14	三、 组成	35
§ 2 计算机病毒的特点	15	四、 诊断	36
一、 自身的特点	15	五、 消除	36
二、 攻击的特点	17	§ 3 大麻病毒	37
§ 3 计算机病毒的分类	18	一、 表现形式	38
一、 按照攻击的对象分类	18	二、 传染途径	38
二、 按照有无标识的特性分类	19	三、 对不同磁盘的破坏作用	39
三、 按照破坏程度分类	19	四、 与小球病毒的比较	40
四、 按照传染方式分类	19	五、 诊断	41
五、 按照入侵系统的途径分类	20	六、 消除	42
§ 4 计算机病毒的结构	21	七、 与小球病毒构成的复合病毒分	
§ 5 计算机病毒的传染性	23	析	44

§ 4 黑色星期五病毒	45	四、组成	65
一、表现形式	46	五、诊断	65
二、传染途径	46	六、消除	66
三、组成	47	§ 10 2153(Omicron)病毒	66
四、诊断	48	一、特点	66
五、消除	48	二、引导方式	66
§ 5 杨基都德病毒	49	三、传染过程	67
一、表现形式	49	四、诊断	67
二、传染途径	50	五、消除	68
三、组成	50	第四章 计算机病毒诊治与	
四、诊断	51	防范	70
五、消除	52	§ 1 计算机病毒的检测	70
§ 6 磁盘杀手病毒	53	一、外观检查法	70
一、表现形式	53	二、特征串搜索法	70
二、传染途径	54	三、对比检查法	71
三、组成	54	四、中断向量检查法	72
四、破坏判别条件	55	§ 2 计算机病毒的防治	73
五、诊断	55	一、软件保护手段	74
六、消除	56	二、硬件保护手段	76
§ 7 快乐星期日病毒	57	§ 3 计算机病毒的预防措施	76
一、表现形式	58	§ 4 计算机病毒的综合治理	78
二、组成	58	一、对计算机病毒进行综合治理的	
三、诊断	59	情况	78
四、消除	59	二、技术措施	79
§ 8 DIR II 型病毒	60	三、法律	79
一、特点	61	四、国际合作	79
二、引导方式	61	第五章 常见防病毒软件的使用	80
三、传染过程	62	§ 1 防病毒软件简介	80
四、诊断	62	一、防病毒软件种类	80
五、消除	63	二、常用防病毒软件概览	81
§ 9 米开朗基罗病毒	63	§ 2 Central Point Anti-Virus 解毒	
一、特点	64	软件	82
二、引导方式	64		
三、传染过程	64		

一、CPAV 的安装	82	二、对病毒检测和消除产品的认识	134
二、CPAV 的使用	85	三、我国反病毒产品的市场现状及发展趋势	134
三、CPAV 软件的菜单	90	四、反病毒产品的评测原则	136
四、BOOTSAFE·EXE 程序的使用方法	108		
五、VSAFE·COM 程序的使用方法	111		
§ 3 McAfee Associates 消毒软件	116	第七章 人工诊治计算机病毒技巧	138
一、SCAN 的使用方法	116	§ 1 DOS 系统功能与磁盘参数	138
二、CLEAN 的使用方法	117	一、构成及启动机制	138
§ 4 公安部开发的消毒软件	119	二、文件的管理机制	141
一、SCAN 的使用方法	119	三、内存控制与文件加载	150
二、KILL 的使用方法	121	四、与病毒有关的中断与系统功能调用	155
第六章 防病毒卡介绍	124	§ 2 动态调试程序 DEBUG 的使用	160
§ 1 防病毒卡概况	124	一、初始化	161
一、对防病毒卡的认识	124	二、使用方法	161
二、防病毒卡的选择	125	三、常用命令一览表	167
§ 2 常见的防病毒卡	127	§ 3 系统引导型病毒的分析 and 防治	168
一、瑞星防病毒卡	127	一、引导过程	168
二、吉星防病毒加密卡	127	二、传染方式	169
三、华能防病毒卡	128	三、破坏或表现方式	169
四、华星病毒免疫卡	128	四、检测方法	170
五、优益病毒防治卡	129	五、病毒消除	171
六、卫佳防病毒卡	129	六、2708(香港)病毒的分析与防治	171
七、新创智能病毒防护卡	130	§ 4 文件型病毒的分析与防治	182
八、九强防病毒加密卡	130	一、引导过程	182
九、蓝十字防病毒卡	130	二、传染方式	183
十、惠远硬盘保护防毒卡	131	三、检测方法	184
十一、启扬防病毒产品	131	四、病毒消除	185
§ 3 反病毒产品综述	132	五、维也纳病毒的分析与防治	186
一、特征及分类	133		

第一章 计算机病毒概况

随着计算机的问世,计算机犯罪也随之出现,在70年代发案率迅速上升,到80年代已经构成发达国家和发展中国家日益严重的社会问题。人们预计,计算机犯罪将成为90年代恐怖分子进行的破坏活动。尤其到了计算机科学技术高速发展的80年代末,在计算机安全领域中又出现了计算机病毒。计算机病毒对计算机系统安全性的威胁大大超过了以往各种计算机犯罪手段。而且,这种犯罪手段更具有高技术性。

当今信息系统在现代化建设中的重要作用和战略地位,充分显示了它的巨大生命力。同时,它自身的脆弱性和易于攻击的特点,使得信息系统的安全成为急待解决的重大课题。

第一节 计算机系统的脆弱性

现代计算机系统的实现是安全性、开放性及制造成本的一种折衷,任何一种计算机系统都存在着脆弱性,即由折衷所带来的系统不安全的问题。

1983年哥伦比亚发生了一件轰动一时的计算机盗窃案:1983年5月12日伦敦的大通银行接到哥伦比亚中央银行的计算机指令,把1350万美元过户到纽约大通银行的一个户头上。次日,这笔款项从纽约大通银行过户到纽约的摩根信托保险银行,然后转到苏黎世的以色列哈普林银行的一个美国人户头上。26日,这笔巨款又转移到巴拿马的一家银行。由于一个同案犯没有正确文件提取现金,这笔巨款再一次转移到欧洲。此案在1983年11月暴露,警方经过6个月调查,有12个人被捕,主要案犯普利伊托(哥伦比亚发展部前秘书长)被警方拘捕,但由于缺乏证据,又被释放。事后,哥伦比亚中央银行的一位告密者在一起交通事故中丧生。

1986年5月,前西德的4名罪犯利用计算机系统通过适当手段改变信用卡的磁带密码,欺骗计算机系统,获得了10万马克。后经严密侦察,4名案犯被捕。

1986年12月,法国银行发生了一起丢失几千万法郎的案件,这起利用计算机系统犯罪的案件,至今尚未侦破。

1988年,前西德汉诺威大学计算机系一个24岁的学生马蒂亚斯·斯佩尔,将自己的计算机系统同美国军方和军工承包商的30台计算机联网,在两年时间里收集了大量有关美国国防情报的机密。其中包括美国“星球大战”计划,北美防空司令部、核武器和通信卫星等方面的情报。此举曾震惊了美国国防部和联邦调查局。另据报道,由于美国国家航空航天局在全世界的数据网保密系统存在着缺陷,前西德的一些计算机爱好者利用这些缺陷钻了空子。这些计算机爱好者通过打入“航天飞机”、“挑战者号”和“机密”等关键字,进

入了美国航空航天局的数据网,便在屏幕上看到了有关“航天飞机 C 研究合同”、“系统的安全调查”和“助推火箭事故”等重要情报内容。这些计算机技术爱好者可以通过一些自己编制的程序接触美国国家航空航天局数据网用户的电子邮件窃取信息,甚至可通过适当的程序设计手段使整个数据网络陷于瘫痪。

1990 年 1 月 19 日,美国三名电子计算机工人被控利用政府的计算机取得军事机密情报。他们用个人计算机和偷窃的某电话公司的设备以及开关密码,取得了绝密的军事文件和联邦调查局关于菲律宾前总统马科斯密友的情报。

美国斯坦福研究所的研究表明,计算机犯罪的损失额每起案件为 45 万美元,是常规犯罪案件的几十倍到几百倍。据有关方面统计,目前美国每年由于计算机犯罪而遭受的损失超过百亿美元,前西德约为五十亿美元,英国为三十亿美元,法国为一百亿法郎。在美国硅谷,计算机犯罪每年正以 400% 的速度增长。近几年来,在日本、香港等国家和地区计算机犯罪案件也在迅速增长,已构成严重的社会问题。

在我国,计算机犯罪也已出现。深圳、大连等地就出现过计算机犯罪案件,在报刊上公开报道的计算机案件已达 10 起以上。

现实生活告诫人们,日益增长的计算机犯罪活动是计算机信息系统脆弱性的反映,它已构成了对国家安全和防御、政治、经济、科学技术、社会生活的严重破坏和威胁。计算机病毒的出现和蔓延,在很大程度上也反映了计算机系统的脆弱性。

计算机信息系统资源的脆弱因素包括:

数据输入部分:数据通过输入设备输入系统进行处理,数据易被篡改或输入假数据。

编程部分:用语言写成机器能处理的程序,这种程序可能会被篡改或盗窃。

软件部分:计算机系统离开软件就是一堆废铁。一旦软件被修改或破坏,就会损害系统功能,以至整个系统瘫痪。

数据库部分:数据库存有大量的各种数据,有的数据资料价值连城。若遭破坏,损失是难以估价的。

操作系统:操作系统是操纵系统运行、保证数据安全、协调处理业务和联机运行的关键部分,如被破坏就等于破坏了系统功能。

输出部分:经处理的数据要在这里译成人能阅读的文件,并通过各种输出设备输出,信息有可能被泄露或被窃取。

通信部分:信息或数据要通过它在机器间或主机与终端及网络之间传送,通信线路一般是电话线、专线、微波、光缆,前三种线路上的信息易被截取。

硬件部分:即除软件以外的所有硬设备,这些电子设备最容易被破坏或盗窃。

电磁波辐射:计算机设备本身就有电磁辐射问题,也怕外界电磁波的辐射和干扰,特别是自身辐射带有信息容易被别人接收造成信息泄漏。

辅助保障系统:水、电、空调中断或不正常会影响系统运行。

存取控制部分:安全存取控制功能还比较弱。

由于计算机的应用直接涉及到政治、经济和社会问题,因此,计算机安全问题必然会引起社会等重大问题。计算机信息系统的脆弱性也必然会导致计算机化社会或信息化社会的脆弱性。美国发生的 R·T·Morris 病毒事件使美国六千多台计算机受害就充分证明

了严重性。

第二节 计算机犯罪概述

一、计算机犯罪的概念

计算机犯罪与传统的犯罪活动有很大的不同。计算机犯罪是一种高技术手段的犯罪活动。从作案时间上来看,传统的犯罪活动是以分钟、小时、天、星期、年来计算的,而计算机犯罪通常是在短短的一瞬间发生并完成的。随着计算机网络的建立和发展,地理上的界限已不能阻挡这些犯罪活动的发生。对于军事系统或金融系统的计算机作案可以在一个国家内进行针对另外一个国家的破坏活动。

计算机犯罪的目标和作案方法及其表现形式多种多样,所以对于计算机犯罪的概念,到目前为止,国际上尚未形成一个统一的定义。这里简单介绍几种定义:

澳大利亚把计算机犯罪称为计算机滥用,并把计算机犯罪行为解释为与计算机有关的盗窃、贪污、诈骗、破坏等行为。

计算机滥用行为包括:

- (1) 未经批准修改、输入或输出数据;
- (2) 未经批准通过终端访问计算机系统;
- (3) 未经批准修改或使用应用程序;
- (4) 对电子数据处理设备实施犯罪:盗窃设备、文件或数据;
- (5) 破坏计算机设备;
- (6) 未经批准进行数据截收。

美国司法部对计算机犯罪给出了下面三个概念:

计算机滥用:任何与计算机技术相关的事件,在该事件中受害者遭受或可能已经遭受了损失,而犯罪者都有意获得或可能已经获得利益。

计算机犯罪:任何利用计算机技术知识作为基本手段的非法行为。

数据泄露:未经允许从计算机系统暗转移或取得数据拷贝。这里的数据泄露是指有计划的盗窃活动。

我国有关方面提出的计算机犯罪的定义是:以计算机为工具或以计算机资产为对象实施的犯罪行为。

计算机在犯罪方面的四个角色是:

- (1) 犯罪客体——计算机资产是犯罪分子攻击的对象或目标;
- (2) 犯罪主体——计算机为犯罪提供了犯罪场所和环境,替罪犯执行了犯罪活动;
- (3) 犯罪工具——计算机为罪犯的犯罪工具;
- (4) 犯罪象征——罪犯利用计算机进行诈骗或者进行恐怖活动。

当前,计算机犯罪主要有以下类型:

- 程序、数据、存储介质的物理性破坏;
- 窃取或转卖信息资源;
- 盗用计算机机时;
- 利用通讯线路进行非法活动;
- 非法进行程序修改活动;
- 信用卡方面的计算机犯罪。

二、计算机犯罪的手段

计算机犯罪手段主要分暴力和非暴力两种。暴力手段是指对计算机资产实施物理破坏,使用武器摧毁系统设备和设施,炸毁计算机中心等活动。而非暴力手段是指用计算机技术知识及其它技术进行犯罪活动。后者称为高技术犯罪或智能犯罪,而且这部分犯罪最为常见。根据对目前计算机犯罪案例分析,大多数计算机犯罪活动采用以下手段:

(1)数据欺骗

在计算机系统中,非法篡改输入/输出数据,其中包括在数据输入计算机前和输入过程中更改数据。有的采取假造或冒充的文件,利用软磁盘或计算机磁带来进行互换,篡改原始输入数据。

从信息流和传输界面的角度来看,在每一个已装备了计算机系统的企事业部门,都存在着用户可以接触或从事生成、记录、传送、编辑、检查、变更和转换送入系统中的数据,并能够在数据产生过程中进行修改。非法篡改输入/输出数据是最普通最常见的计算机犯罪活动。

(2)特洛伊木马

这种方法是程序中暗中存放秘密指令,使计算机在仍能完成原指定任务的情况下,执行非授权的功能。例如,当工厂一种新产品问世时,每当把顾客名单列入指定文件时,程序员便利用计算机把有关名单存入一个特殊的非授权文件,利用这种手段,程序员可以拿到一份具有潜在价值的名单。

特洛伊木马的关键是采用潜伏机制来执行非授权的功能。计算机病毒包括了特洛伊木马的功能。此外计算机病毒还具有很强的非授权的再生机制。

(3)意大利香肠战术

意大利香肠战术是迫使对方作出一连串的细小让步,最后达到原定目标的一种战术。这是从大宗财产中偷盗小额财产的一种计算机犯罪形式,形象的比喻为如同小偷取走一小片香肠,而人们并没有感到盘子中香肠数量的减少。

在法国的计算机犯罪中发生过类似的案件。工作人员处理客户定期存款时,每次扣下几个生丁(法国货币的名称,1法郎为100生丁),然后,将这点钱转到一个虚构的帐号上,日积月累,一年之后在这个帐号上神不知鬼不觉地弄到了一大笔款项。这种犯罪方法,在银行中同特洛伊木马方法结合,能随机地从几百个帐户中抽取零头,并把这笔钱转移到一个指定的帐户上,经一定时间间隔后,其数据相当可观。在我国银行已发现过类似的计算

机犯罪。

意大利香肠战术的关键是采用不易察觉的手段来进行非法活动。

(4) 超级冲杀

超级冲杀是由于大多数 IBM 计算机中心使用宏公用程序 Superzap 而取名的。这是一个当计算机停机、出现故障或其它需要人为干预的系统程序。它是一个有效的工具,相当于系统的一把总开关钥匙。如果被非授权用户使用,就构成了对系统的一种潜在威胁。例如,美国新泽西州一家银行的计算机操作人员曾利用干预程序修改了帐目,而没有通过普通的控制日报记录,从一个客户的帐目中盗走了 12.8 万美元。

超级冲杀的关键是非授权使用特殊情况下的计算机系统干预程序。

(5) 活动天窗

活动天窗通常是指故意设置的入口点,通过入口点可以进入大型应用程序或操作系统。在排错、修改和重新启动的时候,可以通过这些窗口访问有关程序。罪犯利用活动天窗,可以发现系统软件的一些薄弱环节,从而进行非法侵入活动。例如,美国底特律的几位汽车工程师发现了佛罗里达商用分时服务系统中的一个活动天窗,查到了公司总裁的口令,进而获得了具有重要商业价值的计算机文件。

活动天窗的关键是利用人为设置的窗口侵入系统。

(6) 逻辑炸弹

这是插入程序编码,这些编码仅在特定时刻或特定条件下执行,所以又称为定时炸弹或逻辑炸弹。逻辑炸弹是对系统的潜在威胁和隐患,可以造成严重危害。例如,过去曾发生过一起计算机犯罪案件,负责工资表的程序员在文件中放置了一个逻辑炸弹,当他本人被公司解雇或他的名字从工资表中去掉时,事先秘密放置的程序,在他本人离开 3 个月之后破坏系统的文件库。

逻辑炸弹的关键是特定条件下的程序激活。计算机病毒的可激发特征,实际上就是一个逻辑炸弹。

(7) 清理垃圾

这是从计算机系统或机器周围的废弃物中获取信息的一种方法。例如,系统没有清除临时输入或输出信息的缓冲存储器,或者没有清除磁盘或磁带上存储的信息,从而造成这些信息被人为窃取和利用。

例如,某一个用户从磁盘上获得了若干石油公司暂存的地震数据,并把这些具有商业价值的信息转卖给其它的石油公司。作为清理垃圾的一个具体例子,在北欧的一个国家,曾有人从丢弃的纸带中发现了法国共产党的整个年度的活动计划。

清理垃圾是有目的或有选择地进行工作现场或废弃物中的信息搜索。

(8) 浏览

在系统或终端设备上,利用合法手段在存储区搜索某些有兴趣或有潜在价值的东西,也有的利用合法访问系统某一指定部分文件的机会,趁机访问非授权文件,这些活动都是在正常操作掩护下的非法活动。

(9) 数据泄露

不管计算机犯罪的手段多么高明,直接从计算机系统中窃取数据是冒很大风险的。为

此,有的作案者将一些关键数据渗漏在一般性的报表之中,有的计算机间谍在计算机系统的中央处理机上安装了微型无线电发射机,将计算机处理的内容传送给几公里外的接收机。

数据泄露是有意转移或窃取信息的手段。

(10)顺手牵羊

在分时操作系统管理下的用户终端,当一个用户在使用自己的口令进入工作状态后,他可能临时有事短暂离开或去接电话,此时可能被他人利用,在没有得到授权的情况下,以人家的身份从中获取信息或数据。在数据处理中心,用户的程序和打印结果往往被人冒领或“代领”,有的发现磁带存放位置移动,有的软磁盘丢失,这是被人钻了管理上出现的漏洞。

顺手牵羊是被人利用管理上的漏洞,从而造成文件或信息的丢失。

(11)冒名顶替

当用户使用口令时,被他人发觉并随后利用,并趁机窃取重要信息。因此,用户的口令要注意更新和保密。使用银行信用卡的用户要注意口令的保密和安全。

(12)蠕虫

使用未定义过的处理器来执行运算,在一个分布式网络系统中,可以通过网络来传播错误,进而造成网络服务遭到拒绝并发生死锁。通常需要重新启动才得以排除蠕虫对系统的恶性作用。

(13)核心大战

两个互相破坏对方的程序,实际运行中有可能造成对系统的破坏。计算机系统中应严格禁止核心大战之类的程序体之间相互攻击。

(14)计算机病毒

将具有破坏系统功能和系统服务及破坏或抹除数据文件的犯罪程序自动装入系统某个功能程序中,让系统在运行期间,将犯罪程序自动拷贝给其它系统,这就好象传染性病毒一样四处蔓延。这种犯罪手段一般用于联网系统。

(15)伪造证件

如伪造他人的信用卡、磁卡、存折等。

三、计算机犯罪的特点

目前各国计算机犯罪主要集中在两个方面:机密信息系统和金融系统。机密信息系统主要涉及具有重要政治、军事、经济价值的信息系统,也包括类似产品研制、销售和具有商业价值的非公开的信息系统。金融系统主要涉及通过计算机管理的金融市场和电子货币。

计算机犯罪与传统的犯罪活动有很大的不同。计算机犯罪是高技术犯罪活动,是瞬间可以发生的随机事件,并且已成为可以跨越国界的犯罪活动。计算机犯罪总是与计算机和信息紧密联系在一起。其特点是:

(1)罪犯趋向年轻化。在已发现的计算机罪犯中年龄范围为18~46岁,其平均年龄为25岁。

(2)罪犯往往是熟练的计算机技术人员,罪犯往往是掌握核心机密的人,其犯罪的破坏性就更大。特别是由于领导者用人不当,会产生严重的影响和后果。

(3)在计算机犯罪中共谋作案远比其它类型的案件更为多见。通常在已发现的计算机案件中有计算机专家,负责有关案件中的技术角色,还有外围组织成员,负责把技术活动转化为经济收益。

(4)计算机犯罪采用的手法和一般情况下的正常性活动只有很小的差别。计算机专家进行未授权的活动,往往不被制止,进而导致成为严重的犯罪活动。甚至有的计算机罪犯,把从事的欺骗和盗窃活动,辩解成为在机器上进行的某种游戏或智力训练。

(5)计算机犯罪是可在瞬间发生的高技术犯罪,往往不留任何痕迹,在法律中难以拿到证据,这也是在各个国家计算机犯罪日趋严重的重要因素。

(6)计算机犯罪活动趋向国际化,有的计算机犯罪是罪犯跑到其它国家进行的。

总之,计算机法律不健全或不完美,计算机安全技术与现实需要存在相当大的差距,特别是对计算机犯罪活动难以拿到罪犯的证据,这些因素都造成了各国计算机犯罪活动的日趋增加和严重。

四、计算机犯罪的社会危害性

在计算机应用普及较广的国家,如美国等国家,计算机犯罪已经形成了一定的气候,成为一种严重的社会问题,威胁着经济发展、社会安定和国家安全。我们只要看一下几个初步的统计数字,就能认识到计算机犯罪的社会危害性的严重程度。据国外资料统计,美国计算机犯罪活动造成的损失已达上百亿美元。前西德每年损失五十亿美元。英国为三十亿美元。现在在英国每40秒钟就有一起计算机诈骗案发生。据说这些数字只是很初步的,实际数据可能要大的多,因为有许多案件并不被人所知,也没有向警方报案,目的是为保住公司的信誉。亚洲国家和地区计算机犯罪问题也很严重。如日本、新加坡、香港等。我国在报刊上公开报导的计算机犯罪案件已达十起以上,据了解尚未被发现和发现了而未报告的案件远不止这些,这此案件中金额最小的有数千元,最大的87万元。

计算机犯罪的社会危害性的大小,在于计算机信息系统的社会作用的大小,在于社会资产计算机化的程度和计算机应用普及的广度。作用越大,程度越高,应用面越广,发生犯罪案件的机率就越高,社会危害性也就越大。这一点是国际计算机安全专家们的一致观点。斯坦福安全研究所计算机安全与犯罪专家帕克说,美国目前除用于国防和政府部门的阿帕网外,还有四大电子转帐系统,并与全国电话网融为一体,连接国内外八百五十多个银行。国内日转帐四千亿美元,跨国日转帐为六千亿美元。如果被计算机犯罪分子或集团从中窃取1%,就相当于联邦储蓄银行的总资产,如果被窃取10%,美国经济就会发生灾难,并将波及世界其他国家。而对从事计算机犯罪的人来讲,窃取一百万与窃取一亿在技术上实在没有什么差别。此外,还有发生计算机战争的可能性。计算机战争的威胁和危害远比核武器大。核武器是一种毁灭性武器,但是在你毁灭一个国家时,别国也在毁灭你,战争的真正目的不是为了毁灭一个国家,而是为了占领和掠夺。有专家认为,敌对国只要用高科技或雇佣一名或几名高级计算机技术人员,破坏或扰乱他国的主要的或大型计算机

信息系统,如国家决策、指挥控制、经济系统等,就足以使该国的经济崩溃、指挥失灵、决策错误。或者掌握了攻击你的重要系统的方法,或者掌握你的重要信息,就可以迫使你屈服,从而就可以达到发动战争的目的。许多国家的政府首脑和计算机安全专家们担心,计算机安全问题处理不当会对国家和整个社会造成大规模的毁坏。

近年来一些国家发生的电脑病毒等事件,已经充分证实这种担心不是多余的,而是各国所面临的现实问题。

第三节 计算机病毒的产生

当今,世界各国计算机界一提起计算机病毒,其恐惧程度不亚于“谈虎色变”。计算机病毒给科学事业和工程技术的发展带来了严重危害。可悲的是,目前还看不到结束这种现实的尽头。

计算机病毒的起源,到现在还没有一个为大家公认的确切说法。似乎所有计算机专家、计算机用户都在不同程度上或不同立场上进行分析和判断。下面介绍有关计算机病毒起源的几种说法。

一、科学幻想

并非只有研究人员和学校里的师生认识到计算机病毒的问题,科学幻想通常是超前科学。

1975年,托马斯·布伦纳(Thomas Brunner)在他所著的《震波骑士》(“Shock Wave Rider”)一书中,以“寄生虫”和“病毒”作主人公,第一次描写了在信息社会中,计算机作为正义和邪恶双方斗争的工具的故事,令人耳目一新。

1977年,托马斯·捷·瑞安(Thomas J·Ryan)出版了一本幻想小说《P-1的青春》(“Adolescence of P-1”),作者描写了一个十分聪明、寻找信息的病毒。这种病毒能从一台计算机到另一台计算机传染流行,能控制7000多台计算机的操作系统。

威廉·吉布森(William Gibson)1984年写了一本小说《神经瘤》(“Neuromancer”),小说里首次出现了一个新概念“自动化流氓”(Cyberpunk)。它的出版发行与计算机安全专家弗雷德·科恩(Fred Cohen)通过实验证明计算机病毒实现的现实性(1983年)时间不相上下。从那时以来,吉布森的观点不仅出现在作家邪恶的幻想幽灵之中,而且也出现在计算机现实世界之中。

二、“核心大战”——贝尔实验室游戏程序

早在60年代初期,美国电报电话公司贝尔实验室里有三个年轻的研究人员,常常做完工作后留在实验室里饶有兴趣地玩他们自己创造的计算机游戏。这三个聪明的年轻人是:道格拉斯·麦基尔罗伊(Douglas Mcilroy)、维克多·维索特斯克(Victor Vysotsky)和罗

伯特·莫里斯(Robert Morris)。他们对计算机内部的工作原理了解得十分透彻。这种被称为“核心大战”(Core Wars)的游戏很有刺激性。“核心”存储器里存放着数据和指令集,这个对别人的数据虎视眈眈的程序,经过奋力拼搏,就把别人的程序“吃掉”。“核心大战”是两个程序员编码之间一对一策略上的战斗,每一方都要编制一组再生程序。号令枪一响,双方将自己的再生程序送入计算机内存,相互展开攻击,设法毁灭对方的程序。这种程序就是一种计算机病毒的雏形,然而当时人们并没有意识到这一点。这种游戏的构想很快发展到高科技部门,比如象著名的麻省理工学院。

两个人在一台计算机上进行的“核心大战”游戏并没有多大的危险,一旦一个程序开始横冲直撞,机器就很容易垮台。但是,时隔不久,计算机网络的实施实现了计算机间的通讯,一个闹着玩的魔鬼程序抬起了头,在多个联网在一起的计算机之间到处复制。

三、恶作剧

有人认为,计算机病毒起源于搞恶作剧的人。这些人为了显示自己在计算机程序设计方面高超的技艺,或是要报复别人或学校(公司)而制造了计算机病毒。前者是无恶意的,所编写的病毒程序也大多不是恶意的,只是和对方开个玩笑,显示一下自己的才能以达到炫耀的目的。而后者则大多是恶意的报复,想从受损失一方的痛苦中取得乐趣,以泄私愤。例如在《计算机犯罪》一书中记录了这样一桩事实:某银行职员在计算机管理程序中插入了一小段程序,检查他的名字是否还在该银行系统的人事档案里,如果不在则破坏系统。结果,在他被解雇后,该程序便对银行数据进行了破坏,从而达到了他个人的报复目的。

恶作剧者是信息社会高度发展的产物。他们对给人类以自动化和信息处理高效率的计算机技术有着浓厚的兴趣,并且特别热衷于那些别人认为不可能做成的事情。他们也完全可能对计算机系统的安全造成攻击。现在,关于计算机病毒的起源问题还没有定论,但可以肯定,世界上流行的许多计算机病毒都是恶作剧者的产物。“星期天病毒”(Sunday,在美国西雅图发现)每周星期天发作,在显示“今天是星期天,何必这么辛苦工作呢?”之后,捣毁 FAT 表,使磁盘数据完全破坏;“荷兰女孩病毒”(Holland Girl,在荷兰发现)在其病毒程序中提供了一个名为“Sylvia”的荷兰女孩的征婚广告,据查,广告联系地址确有一个女孩。……。恶作剧的形式各异,花样不断翻新。被这些病毒侵扰后,常常被搞得哭笑不得。

四、软件保护

计算机软件是一种知识密集的高科技产品,计算机软件技术发展到一定程度,人们对于软件资源的保护并不尽合理。这样使得许多合法软件的非法复制现象极为平常,从而使得软件制造商和销售商的利益受到了严重的侵害。于是当计算机病毒出现之后有人认为这是软件制造商为了保护自己的软件不致被非法复制而导致的最终结果。软件制造商为了处罚那些非法拷贝者而在软件产品之中加入病毒程序并由一定条件触发传染。巴基斯坦智囊病毒在一定程度上是对软件保护起源说的一种证实。有人认为,巴基斯坦智囊病毒

是巴基斯坦的拉合尔的巴锡特(Basit)和阿姆杰德(Amjad)两兄弟为了追踪非法复制其软件产品的用户而编制的,它最初的“毒性”并不大,只是修改磁盘的卷标,将卷标改为“(C) Brain”。1987年5月,美国罗德岛《普罗威斯顿日报》编辑部发现存储在计算机中的文件变成了如下字符串:“欢迎进入土牢,请小心病毒,如需疫苗,请与我们联系。×××与×××敬上,帕金斯坦尼电脑公司”。当专家进一步追查时,发现这个病毒程序早已广泛传播,遍布于该报社计算机系统的各个结点。事后了解到,该程序是帕金斯公司防止非法复制的自卫性病毒。

五、美国软件俱乐部

美国计算机软件使用者俱乐部是由那些志同道合的计算机技术爱好者组成的一个团体。这些计算机爱好者通过这一组织,利用计算机网络分享彼此的设计心得。也有的人在公告板上展示自己发明的程序并注明欢迎大家通过网络来选用,但在一定时间内必须邮寄使用费用。通常这种公告板上的程序“暗藏杀机”,如果有人使用了这项程序却不付费用的话,在特定的时间内,暗藏在程序中的计算机病毒就象定时炸弹一样开始爆发,藉以警告那些“占便宜”的使用者。如果使用者乖乖地寄上费用的话,设计者会寄上解毒的程序。如果不知内情的“盗用者”把这种带着病毒的程序分享给其他朋友或亲友,于是一传十、十传百,计算机病毒就广泛传染开来。这样,美国的软件俱乐部就成了计算机病毒的起源,他们无心插柳柳成荫,而成了计算机病毒的催生者。这种说法似乎也有些道理。

计算机病毒的罪魁祸首到底是谁?到目前为止,依然众说纷纭。计算机界真正认识到计算机病毒的存在是在1983年。在80年代初,弗雷德·科恩(Fred Cohen)想试验一下计算机程序能否自我繁殖,结果他成功了,并以此撰写了博士论文。在1983年11月3日的计算机安全学技术讨论会上,弗雷德·科恩博士正式提出一种在运行过程中可以复制本身的破坏性程序,伦·艾德勒曼(Len Adleman)将它命名为计算机病毒(Computer Viruses)。随后获准进行实验演示。当天,专家们首先在运行UNIX操作系统的VAX 11/750机上实验,成功地验证了第一个计算机病毒。一周后,又演示了另外五个实验。在5次实验中,计算机病毒使计算机系统瘫痪所需的时间平均为30分钟,最短为5分钟。由此证实了计算机病毒的存在,并证明计算机病毒可以在短时间内实现其对计算机系统的破坏,且可以迅速地向外传播。实际上,计算机病毒的广泛传染始于1987年,在1988年才开始得到人们的重视,尤其是在1988年11月3日以后,计算机病毒几乎为计算机界人士所周知。

可以相信,计算机病毒的产生并广泛传染至全世界的很重要的原因在于那些对于计算机系统有深入了解的恶作剧者,他们在很大程度上起着推波助澜的作用。不过,正象计算机病毒的种类多种多样一样,计算机病毒的产生原因也肯定并非一种。无论如何,计算机病毒已在社会上广泛传播,现在摆在我们面前的问题是怎样预防和消除计算机病毒。