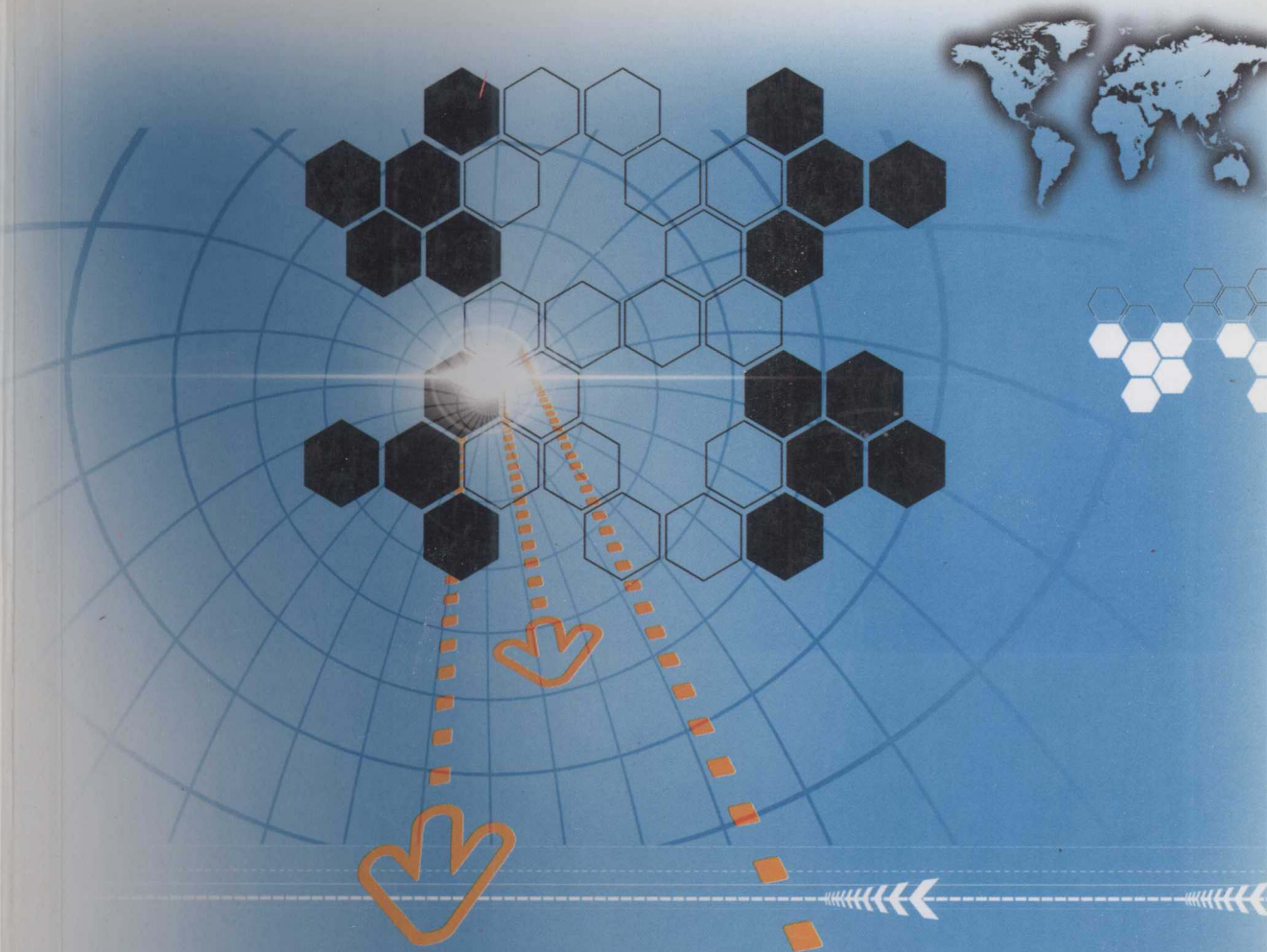
21世纪高职高专精品教材

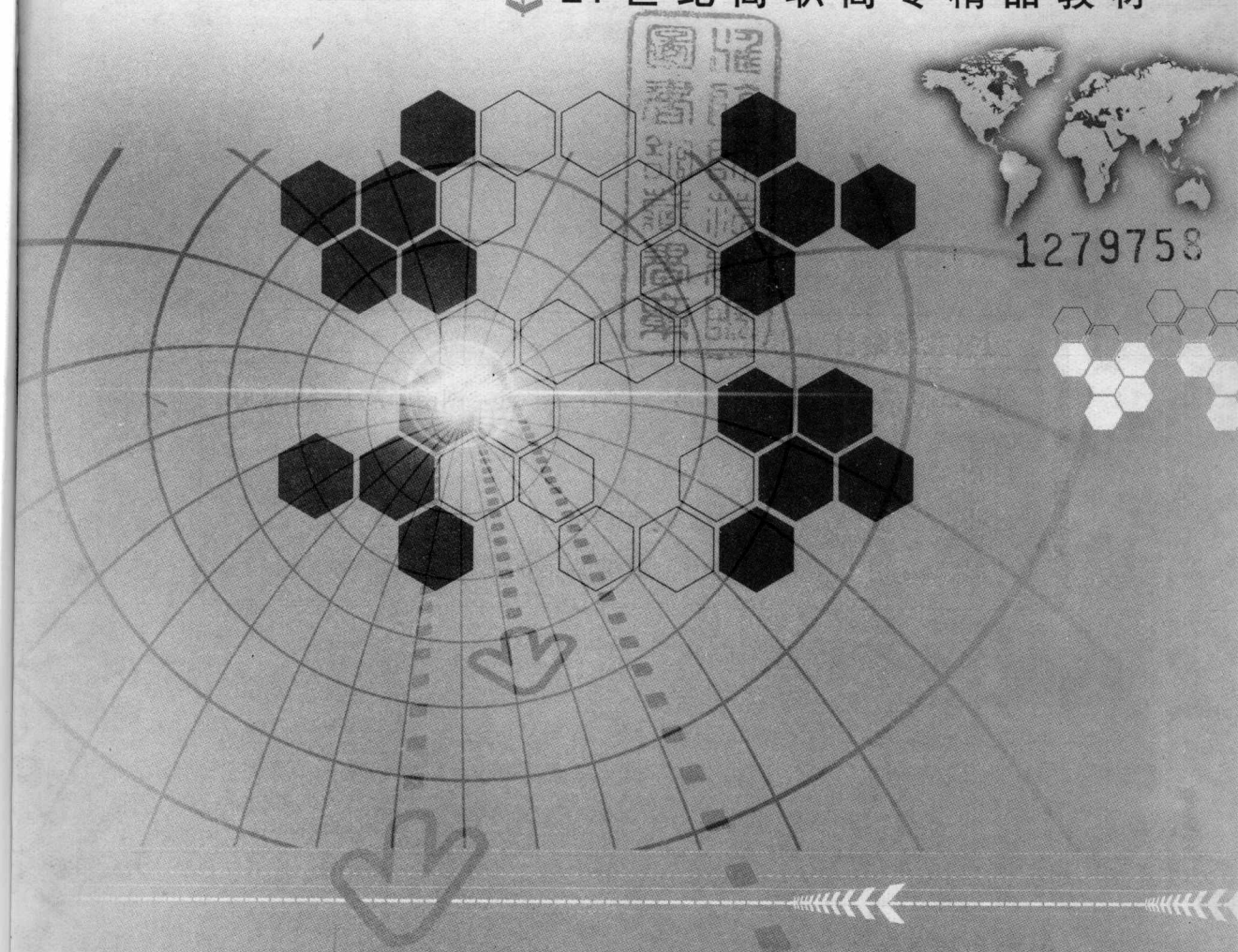


主　编　张波云
副主编　朱天相
　　蒋光和

计算机病毒原理与防范

湖南师范大学出版社

21世纪高职高专精品教材



主　编　张波云
副主编　朱天相
　　蒋光和

计算机病毒原理与防范

湖南师范大学出版社

图书在版编目（CIP）数据

计算机病毒原理与防范／张波云主编．—长沙：湖南师范大学出版社，2007.7

ISBN 978-7-81081-659-5

Ⅰ.计… Ⅱ.张… Ⅲ.计算机病毒—防治 Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字（2007）第 003250 号

计算机病毒原理与防范

◇主　　编：张波云

◇责任编辑：颜李朝

◇责任校对：胡晓军

◇出版发行：湖南师范大学出版社

地址/长沙市岳麓山　邮编/410081

电话/0731.8853867　8872751　传真/0731.8872636

网址/http：//press.hunnu.edu.cn

◇经销：湖南省新华书店

◇印刷：长沙银都印务有限公司

◇开本：787×1092　1/16

◇印张：19.25

◇字数：480 千字

◇版次：2007 年 8 月第 1 版　2008 年 8 月第 2 次印刷

◇印数：3001—4000 册

◇书号：ISBN 978-7-81081-659-5

◇定价：36.00 元

前 言

随着计算机应用的不断普及，计算机病毒的蔓延对计算机系统安全的威胁也日益严重，已成为计算机系统的大敌。它不仅对计算机操作人员、各个计算机应用单位，而且对整个社会包括经济、科技、国防和安全部门都构成一种现实的威胁。因此，剖析计算机病毒的基本原理及相应的防治技术，强化计算机系统的安全可靠性仍是计算机应用领域的重要课题。

本书比较全面地介绍了计算机病毒的基本原理和主要防治技术，通过实例详细地阐述了计算机病毒的产生机理、寄生特点、传播方式、危害表现以及病毒的预防方法和清除知识，特别是在计算机病毒的传播、变形病毒、手机病毒、病毒自动生产机以及计算机病毒理论等方面进行了比较深入的分析和探讨。最后本书指出了计算机病毒对抗进展情况以及以后的发展趋势。本书还对虚拟病毒实验工具 Virlab 做了介绍，通过该模拟器的使用可以加深对病毒特性的感性认识。

本书通俗易懂，注重可操作性和实用性，希望能帮助读者了解计算机病毒的共性及个性特征，学会病毒的检测、辨识和防治方法，从而提高对计算机病毒的防治能力，以保证计算机系统的安全。

本书共十五章，各章内容如下：

第 1 章是计算机病毒概述，包括计算机病毒的危害、病毒的发展历史、病毒的产生原因和病毒引发的社会问题——计算机犯罪。

第 2 章介绍计算机病毒的基本概念，包括病毒的定义、病毒的特性、病毒的结构、病毒的分类、病毒的命名以及病毒的演化。

第 3 章介绍计算机病毒的作用机制，包括病毒的感染机制、触发机制以及病毒的破坏行为。

第 4 章介绍计算机病毒技术基础，包括计算机体系结构、磁盘结构、文件系统、操作系统基本知识。

第 5 章对典型 DOS 操作系统平台下的病毒作了详细的分析，分析对象包括引导型病毒和文件型病毒。

第 6 章分析了 Windows 平台下 PE 格式病毒的基本原理，如：病毒的重定位、获取 API 函数地址、文件搜索、内存映射文件、感染其他文件、病毒返回到 Host 程序等，详细分析了 W32. Netop. Worm 的源代码，并对典型 Win32 PE 病毒 CIH 做了详细剖析。

第 7 章对当今最为泛滥的脚本病毒做了详细的分析，介绍了脚本程序运行的基础，阐述了 VBS 脚本病毒和 Word 宏病毒的原理和特征，并对爱虫病毒和美丽杀病毒作了细致的分析。

第 8 章介绍了特洛伊木马的基本概念和特征，深入分析了木马的攻击技术，对典型木马“冰河”做了剖析，简要说明了木马的发展趋势。

第 9 章对网络蠕虫作了全面的介绍，包括蠕虫的发源、定义、结构、传播和攻击手段，对蠕

虫的传播策略和攻击方法做了详尽分析，并详细剖析了典型蠕虫“红色代码Ⅱ”。

第10章对新出现的手机病毒作了简介，介绍了手机病毒的概念、类型和基本攻击方式，对手机病毒与计算机病毒的联系、手机病毒的现状与发展趋势做了阐述，并对数款典型手机病毒作了简要剖析。

第11章介绍了反病毒技术，包括病毒的各种检测方法、各种流行病毒的清除方法、病毒的预防以及病毒检测实战和防毒软件的使用。

第12章介绍了病毒变形技术，包括变形病毒的定义、病毒变形的机理、密码技术在变形中的应用，并给出了实例演示，最后介绍了病毒自动生产技术。

第13章介绍了计算机病毒的传播。通过对计算机病毒疫情、计算机病毒的生命周期、病毒的传播途径的详细描述，进而总结出了病毒传播的数学模型，以指导反病毒技术的研究。

第14章对计算机病毒进行理论研究，包括病毒的伪代码描述、压缩病毒的定义、病毒的可检测性研究、计算机病毒的变体和病毒防治的可能性的研究。为有利于进一步深入理解计算机病毒的本质、研究计算机病毒的机制，特别介绍了基于图灵机的病毒计算模型，让读者了解如何用形式化的方法来刻画计算机病毒。

第15章介绍了病毒技术的新动向，包括病毒的发展趋势、病毒制作技术的新动向和计算机病毒对抗新进展以及计算机病毒研究的开放问题。

附录A介绍了虚拟病毒实验室VirLab1.5的基本使用方法，在该环境中可以仿真530多种病毒的行为。

附录B介绍了与计算机病毒相关的信息安全法律法规。

本书另附配套光盘，供相关人员使用，内容有：实验指导、国内外病毒研究论文、病毒研究工具、防杀病毒工具软件、病毒研究样本、病毒模拟器、病毒演示等，光盘中还包括网络安全有关法律法规。如需要者请与编者联系。

本书的研究和编写工作得到湖南省自然科学基金项目（编号：04JJ6032）和湖南省教育厅优秀青年项目（编号：05B072）资助。

本书从各种论文、书刊、期刊以及互联网中引用了大量的资料，在此谨向其作者表示衷心感谢。对于所引资料，我们尽量在参考文献中予以列出，如有遗漏，深致歉意。

衷心感谢中国人民解放军国防科学技术大学殷建平教授在研究过程中给予我们的指导，特别感谢祝恩、蔡志平博士和蒿敬波、刘运、程杰仁、张玲、龙军博士生，他们在计算机病毒领域的出色工作给予了我们极大的启示。感谢在写作过程中曾给予我们大力支持的计算机系的领导和老师们。

由于计算机病毒技术的不断发展，书稿涉及许多新的内容，尽管笔者已经尽了最大的努力，但仍感错误难免，恳请读者批评指正，使其不断完善。如有建议，请与编者联系（E-mail：hnjxzby@hotmail.com）。

作　者

2007年6月

目 录

第1章 绪 论

1.1 计算机病毒的危害

Internet 改变了人们的生活方式和工作方式，改变了全球的经济结构、社会结构，Internet 越来越成为人类物质社会的最重要组成部分，成为 20 世纪最杰出的研究成果。开放性和灵活丰富的应用是 Internet 的特色，但它们也带来了潜在的安全问题。越来越多的组织开始利用 Internet 处理和传输敏感数据，同时在 Internet 上也到处传播和蔓延着攻击方法和恶意代码，使得连入 Internet 的任何系统都处于将被攻击的风险之中。从 1988 年 CERT(Computer Emergency Response Team, CERT)由于 Morris 蠕虫事件成立以来，Internet 安全威胁事件逐年上升，近年来的增长态势变得尤为迅猛，从 1998 年到 2003 年，平均年增长幅度达 50% 左右，见图 1-1。导致这些安全事件的主要因素是系统和网络安全脆弱性(Vulnerability)层出不穷，从 1995 年到 2003 年 CERT 各年度接到的脆弱性报告数如图 1-2。这些安全威胁事件给 Internet 带来了巨大的经济损失。以美国为例，其每年因为安全事件造成的经济损失超过 170 亿美元。

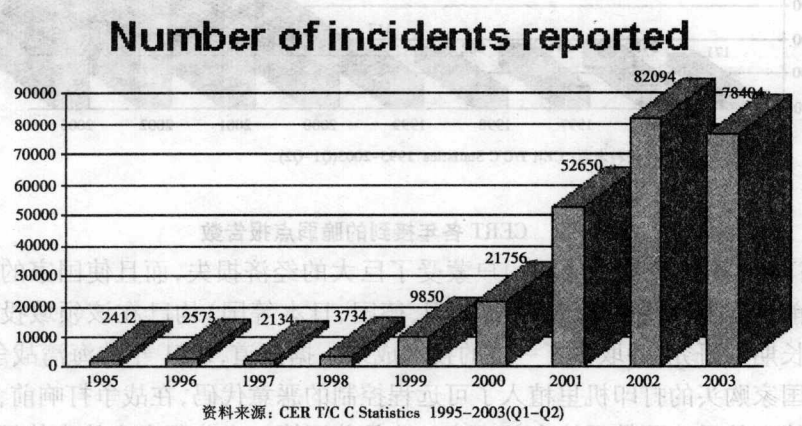


图 1-1 CERT 各年接到的安全事件数

在 Internet 安全事件中，病毒造成的经济损失占有最高的比例。与此同时，病毒还成为信息战、网络战的重要手段。日益严重的病毒问题，不仅使企业及用户蒙受了巨大经济损失，而且使国家的安全面临着严重威胁。

1988 年 11 月泛滥的 Morris 蠕虫，顷刻之间使得 6000 多台计算机(占当时 Internet 上计算机总数的 10% 以上)瘫痪，造成严重的后果，引起世界范围内的信息安全专家的关注。

1998 年 CIH 病毒造成数十万台计算机受到破坏。

1999 年 Happy 99、Melissa 病毒大爆发。Melissa 病毒通过 E-mail 附件快速传播而使 E-

mail 服务器和网络负载过重,它还将敏感的文档在用户不知情的情况下按地址簿中的地址发出,利用了微软产品中如宏病毒等已知脆弱点。

2000 年 5 月爆发的“爱虫”病毒及其以后出现的 50 多个变种病毒,是近年来让计算机信息界付出极大代价的病毒,仅一年时间共感染了 4000 多万台计算机,造成大约 87 亿美元的经济损失。

2001 年,我国国家信息化领导小组计算机网络与信息安全管理工作办公室与公安部共同主办了我国首次计算机病毒疫情网上调查工作。调查结果显示感染过计算机病毒的用户高达 73 %,其中,感染三次以上的用户又占 59% 以上,网络安全依然存在大量隐患。

2001 年 8 月,“红色代码”蠕虫利用微软 Web 服务器 IIS 4.0 或 5.0 中 Index 服务的安全漏洞,攻破目标机器,并通过自动扫描方式传播蠕虫,在互联网上大规模泛滥。

2003 年,SLammer 蠕虫在 10 分钟内导致互联网 90% 脆弱主机受到感染。同年 8 月,“冲击波”蠕虫爆发,8 天内导致全球电脑用户损失高达 20 亿美元之多……

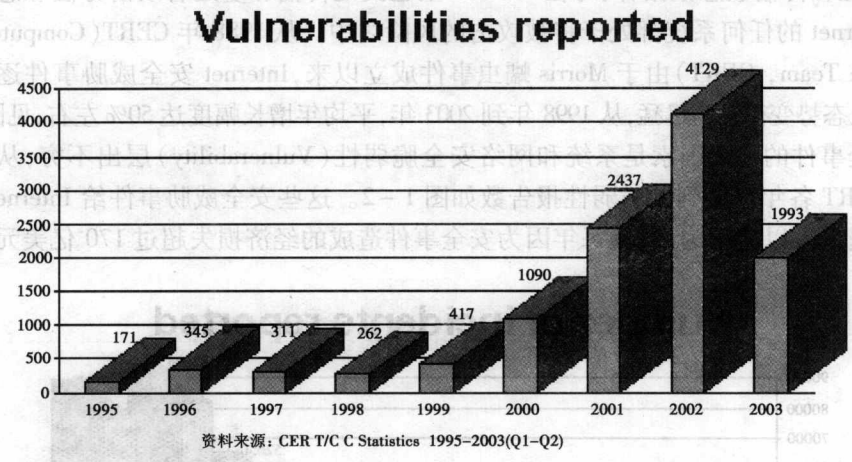


图 1-2 CERT 各年接到的脆弱点报告数

计算机病毒问题,不仅使企业和用户蒙受了巨大的经济损失,而且使国家的安全面临着严重威胁。目前世界上一些发达国家(如美国、德国、日本等国)均已在该领域投入大量资金和人力进行了长期的研究,并取得了一定的技术成果。据报道,1991 年的海湾战争,美国在伊拉克从第三方国家购买的打印机里植入了可远程控制的恶意代码,在战争打响前,使伊拉克整个计算机网络管理的雷达预警系统全部瘫痪。这是美国第一次公开在实战中使用恶意代码攻击技术取得的重大军事利益。病毒攻击成为信息战、网络战最重要的入侵手段之一。病毒问题无论从政治上、经济上,还是军事上,都成为信息安全面临的首要问题。计算机病毒的机理研究成为解决病毒问题的必需途径,只有掌握当前病毒的实现机理,加强对未来计算机病毒趋势的研究,才能在病毒问题上取得先决之机。病毒问题已成为信息安全需要解决的、迫在眉睫的安全问题。

1.2 病毒长期存在的原因

计算机技术飞速发展的同时并未使系统的安全性得到增强。技术进步带来的安全增强能

力最多只能弥补由应用环境的复杂性带来的安全威胁的增长程度。不但如此,计算机新技术的出现还很有可能使计算机系统的安全性变得比以往更加脆弱。

AT&T 实验室的 S. Bellovin 曾经对美国 CERT 提供的安全报告进行过分析,分析结果表明,大约 50% 的计算机网络安全问题是由软件工程中产生的安全缺陷引起的,其中,很多问题的根源都来自于操作系统的安全脆弱性。

病毒的一个主要特征是其针对性(针对特定的脆弱点),这种针对性充分说明了病毒正是利用软件的脆弱性实现其恶意目的的。造成广泛影响的 1988 年 Morris 蠕虫事件,就是利用邮件系统的脆弱性作为其入侵的最初突破点的。

互联网的飞速发展为恶意代码的广泛传播提供了有利的环境。互联网具有开放性的特点,缺乏中心控制和全局视图能力,无法保证网络主机都处于统一的保护之中。而且计算机和网络系统存在设计上的缺陷,这些缺陷会导致安全隐患。

尽管人们为保证系统和网络基础设施的安全做了诸多努力,但遗憾的是,系统的脆弱性终究不可避免。各种安全措施只能减小但不能杜绝系统的脆弱性;而测试手段也只能证明系统存在脆弱性,却无法证明系统不存在脆弱性。而且,为满足实际需求,信息系统的规模越来越大,安全脆弱性的问题会越来越突出。随着这些脆弱性逐渐被发现,不断会有针对这些脆弱性的新的病毒代码出现。

总而言之,在信息系统的层次结构中,包括从底层的操作系统到上层的网络应用在内的各个层次都存在着许多不可避免的安全问题和安全脆弱性。而这些安全脆弱性的不可避免,直接导致了恶意代码的必然存在。

1.3 计算机病毒的传播与发作

在当前的信息社会,信息共享是不可阻挡的发展趋势,而信息共享引起的信息流动正是病毒入侵最常见的途径。病毒的入侵途径很多,如:从 Internet 上下载的程序本身就可能含有病毒代码;接收已经感染病毒的电子邮件;从光盘或者软盘上往系统上安装携带恶意代码的软件;黑客或者攻击者故意将病毒代码植入系统等。

病毒感染就是通过用户执行该病毒代码或已经感染病毒代码的可执行代码,从而使得病毒得以执行,进而将自身或者是自身的变体植入其他可执行程序。被执行的病毒代码在完成自身传播的同时,若满足一定的条件,且具有足够的权限时,就发作并进行破坏活动,造成信息丢失或者泄密等严重后果。

病毒的入侵和发作都必须盗用系统或应用进程的合法权限才能完成自身的非法目的。

随着 Internet 的开放性以及信息共享的方便性和交流能力的进一步增强,病毒编写者的水平也越来越高,病毒代码可以利用的系统和网络的脆弱性也越来越多,从而病毒的欺骗性和隐蔽性也越来越强。

计算机病毒的检测技术总是落后于新的恶意代码的出现,“病毒之父”Cohen 博士和他的老师 Adelman 教授提出了“计算机病毒通用检测方法的不可判定性”的著名论断。一方面是我们很难区别正常代码和恶意代码,另一方面,很多信息系统缺少必要的保护措施。因此,人们常常被病毒欺骗,而无意地执行病毒代码,据 CERT 统计,因被欺骗或者误用而引起的恶意代码事件超过所有事件的 90%。一旦条件满足,病毒代码就会传播或者发作。所以,计算机病毒被引入系统并执行是不可避免的。这是我们在研究如何解决病毒问题时首先必须面对的

事实。

1.4 计算机病毒的发展历程

尽管最近 Internet 发生了越来越多的计算机病毒安全事件，但是病毒并不是新生事物。近年来，攻击者一直在努力研究攻击能力和生存能力更强的病毒代码。下面讨论病毒的发展过程，希望能够进一步预测病毒将来的发展。图 1-3 显示了过去 20 年左右的主要病毒事件。

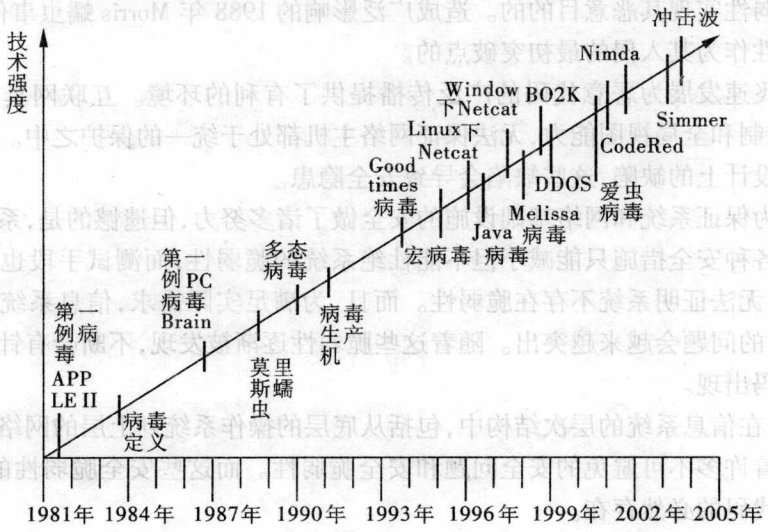


图 1-3 恶意代码发展历程

从图 1-3 我们可以总结出恶意代码从 20 世纪 80 年代发展至今体现出来的几个主要特征：

①恶意代码日趋复杂和完善。从非常简单的、感染游戏的 Apple II 病毒发展到复杂的操作系统内核病毒和今天主动式传播和破坏性极强的蠕虫，病毒在加快传播速度和提高生存能力等方面取得了很大的成功。

②病毒编制方法及发布速度更快。病毒刚出现时发展较慢，但是随着网络飞速发展，Internet 成为病毒发布并快速蔓延的平台。特别是最近几年，不断涌现的恶意代码，证实了这一点。

③从病毒到电子邮件蠕虫，再到利用系统漏洞主动攻击的恶意代码。病毒的早期，大多数攻击行为是由病毒和受感染的可执行文件引起的。然而，在最近几年，利用系统和网络的脆弱性进行传播和感染开创了恶意代码的新纪元。

表 1-1 列举了二十年来病毒发展史上的里程碑事件，我们从中能够体会到上述的几个特征。

表 1-1 病毒发展史上的里程碑事件

时间	事件	描 述
1981—1982 年	首次发现计算机病毒	运行在 Apple II 计算机系统上的游戏中至少发现了三种不同的病毒，其中包括 Elk Cloner 等。
1983 年	正式定义计算机病毒	Cohen 把计算机病毒定义为“一段程序，它可以通过修改其他的程序以包含其自身，或者自身的一个变种，来感染这些程序”。

续表

时间	事件	描 述
1986 年	第一个 PC 病毒	Brain 病毒感染 MS-DOS 操作系统，是恶意代码时代到来的一个重要标志。
1988 年 11 月	Morris	Robert Tappan Morris 编写，这个初级蠕虫使早期的 Internet 网上的大部分主机瘫痪了，当时成了全球新闻的头条。
1990 年	第一次出现多态病毒 Tequtla	为了避免被反病毒系统发现，这些病毒每次运行时的形式都不同，从而开辟了多态病毒的先例。
1991 年	出现了病毒生产机（VCS）	它攻击了 BBS 系统，为病毒编写者们提供了一个可以创建他们自己定制的病毒代码的工具包。
1994 年	Good Times Virus Hoax	这个病毒并不感染计算机，它完全是虚构的。计算机用户被警告这个即将到来的、完全虚构的恶意代码将会造成巨大的破坏，引起用户心理上的恐惧。
1995 年	第一次出现宏病毒	这类恶意病毒出现在 Microsoft Word 宏语言中，感染文档文件。这一技术很快传播到了其他程序中的其他宏语言。
1996 年	Unix 系统上的 Netcat	这一由 Hobbit 编写的病毒仍然为今天的 UNIX 系统留下了最著名的后门。尽管人们大量合法地和非法地使用 Netcat，它仍常被误用做后门。
1998 年	第一个 Java 病毒	StrangeBrew 病毒感染其他的 Jave 程序，把病毒带入了基于 Web 的应用领域。
1998 年	Windows 上出现 Netcat	Windows Netcat 是由 Weld Pond 编写的，同时它也被用作为 Windows 系统的一个著名后门。
1998 年 7 月	Back Orifice	黑客组织 Cult of the Dead Cow（CDC）编写的，考虑了通过网络远程控制 Windows 系统。
1999 年 3 月	Melissa 病毒/蠕虫	这个 Word 宏病毒通过 E-mail 传播，感染了成千上万个计算机系统。它既是病毒，也是蠕虫，因为它感染文档文件，同时也通过网络传播。
1999 年 7 月	Back Orifice 2000（BO2K）	CDC 完全重写了远程控制 Windows 系统的 Back Orifice，新版本比旧版本具有更好的操作界面，开放的 API 函数接口，能够远程控制鼠标、键盘和屏幕。
1999 年 10 月	分布式拒绝服务攻击代理	TFN（Tribe Flood Network）和 Trin00 拒绝服务攻击代理出现，这些工具让攻击者通过一台客户机控制成百上千的攻击代理，通过统一控制、协作的方式对被攻击主机发起洪泛攻击。
1999 年 11 月	Knark 核心级 RootKit	一个自称 Creed 的人发行了一个基于 Linux 内核操作的工具，Knark 创建了一套完整的嵌入 Linux 内核的工具包，攻击者能够有效地隐藏文件、进程和网络行为。

续表

时间	事件	描　述
2000 年 5 月	爱虫病毒	VBScript 蠕虫通过 Microsoft Outlook 的漏洞进行传播，短时间内关闭了世界上万台计算机系统。
2001 年 7 月	红色代码	该蠕虫通过对 IIS 的缓冲区溢出攻击，在 9 小时内感染了世界范围 250000 台以上的计算机系统。
2001 年 7 月	内核入侵系统	通过包含易于使用的图形化用户接口和极其有效的隐藏机制，这个由 Optyx 开发的工具彻底改变了 Linux 内核的操作。
2001 年 9 月	Nimda Worm	这个极其有害的蠕虫采用了许多感染 Windows 系统的方法，包括 Web 服务器缓冲区溢出、Web 浏览器漏洞利用、Outlook E-mail 攻击和文件共享。
2002 年	Setiri Backdoor	尽管从未正式发布，但是通过指派一个不可见浏览器，这个特洛伊木马有能力绕过 PC 机防火墙、网络防火墙和网络地址解析设备。
2003 年 1 月	SQL Slammer Worm	这个蠕虫快速地传播使韩国几个网络服务提供商瘫痪了，短期内给整个世界造成了麻烦。
2003 年 2 月	Hydan Executable Steganography Tool	这个工具使得其用户可以在使用多态编码技术的 LinuxBSD 和 Windows 可执行文件内部隐藏数据。这些概念同样可扩展到防病毒和躲避入侵检测系统方面。
2003 年 7 月	Msblast. W32 蠕虫	波兰黑客组织 LSD 发现 Microsoft RPC 接口远程任意代码可执行漏洞，这是 Windows 操作系统历史以来最大的高风险漏洞，同年 8 月，Msblast. W32 蠕虫出现，8 天内导致全球电脑用户损失高达 20 亿美元之多。

然而，病毒的研究并没有停止，病毒代码编写者继续挖掘他们的技术和潜力，不时地发布更新的、破坏性更强的计算机病毒。

1.5　病毒起因

计算机病毒的起因多种多样，有的是计算机工作人员或业余爱好者为了纯粹寻开心而制造出来的，有的则是软件公司为防止自己的产品被非法拷贝而制造的报复性惩罚，等等。一般可归于以下几种情况：

1. 恶作剧

这种观点认为计算机病毒源于一些爱好计算机的青少年的恶作剧。美国康奈尔大学的莫里斯，编写蠕虫程序肇事后，被称为软件奇才，一些公司出高薪争相聘用他。莫里斯的父亲曾在 1983 年强调指出："一些懂技术的聪敏的孩子们的恶作剧在与公司或军方安全专家的智斗中可能取胜。"

几年后，小莫里斯用蠕虫证实了老莫里斯的预言。一个由著名专家组成的委员会在蠕虫事件调查报告中认为：莫里斯释放蠕虫是一种"忽视了明显的潜在后果的青少年行为"，"莫里