高等学校信息安全系列教材

恶意代码防范

刘功申　张月国　孟魁　编著
李建华　主审

高等教育出版社
HIGHER EDUCATION PRESS

高等学校信息安全系列教材

恶意代码防范

Eyi Daima Fangfan

刘功申　张月国　孟　魁　编著
李建华　主审

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本书是在作者多年教学经验和信息安全社会培训工作的基础上编写而成的，力求反映作者近年来的最新科研成果。全书共分为13章，在简单介绍恶意代码的基本概念和类别的基础上，重点探讨了恶意代码防范的思路、技术、方法和策略，并给出了恶意代码的防治方案。

本书内容深入浅出，用通俗的语言和实例向读者展示恶意代码防范的知识。教材配套资源丰富，易学易教，包括PPT电子版课件、多种题型的题库、实验用软件和源代码等。

本书适合作为普通高等学校信息安全及相关专业本科生的教材，也可作为相关领域的工程技术人员的参考书。

图书在版编目(CIP)数据

恶意代码防范/刘功申，张月国，孟魁编著. —北京：
高等教育出版社，2010.7
ISBN 978-7-04-029055-4

Ⅰ.①恶… Ⅱ.①刘… ②张… ③孟… Ⅲ.① 电子计算机-安全技术-代码-高等学校-教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2010)第109303号

策划编辑 武林晓　**责任编辑** 武林晓　**封面设计** 于文燕　**责任绘图** 尹文军
版式设计 史新薇　**责任校对** 杨雪莲　**责任印制** 朱伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街4号	**咨询电话**	400-810-0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
			http://www.hep.com.cn
经　　销	蓝色畅想图书发行有限公司	**网上订购**	http://www.landraco.com
印　　刷	北京七色印务有限公司		http://www.landraco.com.cn
		畅想教育	http://www.widedu.com
开　　本	787　1092　1/16	**版　　次**	2010年7月第1版
印　　张	23.5	**印　　次**	2010年7月第1次印刷
字　　数	520 000	**定　　价**	36.00元

物料号　29055-00

前　言

信息安全是一个复杂的系统工程。在这个系统工程中，不能仅仅依靠技术或管理的任何一方来解决问题，而应该从技术和管理两方面进行统筹考虑。一套好的管理制度和策略应该是以单位实际情况为主要依据，能及时反映单位实际情况变化，具有良好的可操作性，由科学的管理条款组成。

随着信息技术的发展，信息资源管理将被作为国家战略来推进，企业竞争焦点也将落在对信息资源的开发利用上。“三分技术、七分管理、十二分数据”的说法成为现代企业信息化管理的标志性注释。信息资源已经成为继土地和资本之后最重要的财富来源。

对于恶意代码及其防范来说，曾经有一些简单的认识：计算机不可能因为仅仅读了一封电子邮件而感染恶意代码；恶意代码不可能损害计算机硬件设备；计算机不可能因为浏览一个图形文件而染毒；杀毒软件是防范恶意代码的一切；数据备份和恢复对防范恶意代码无关紧要；恶意代码防范策略是虚无缥缈的内容等等。但是，在恶意代码迅速发展的今天，这些说法都已经过时，我们必须更新关于恶意代码及其防范工作的知识。

本书是在作者多年教学经验和信息安全社会培训工作的基础上编写而成的，力求反映作者近年来的最新科研成果。全书共分为13章，在简单介绍恶意代码的基本概念和类别的基础上，重点探讨了恶意代码防范的思路、技术、方法和策略，并给出了恶意代码的防治方案。

本书各章内容简介如下。

第1章恶意代码概述。本章分析了引入恶意代码概念的原因，介绍了恶意代码的种类和特征，并在此基础上探讨了恶意代码的关键历史转折点、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

第2章典型恶意代码。在总结现有恶意代码类别的基础上，介绍了几款典型的恶意代码：普通计算机病毒、蠕虫、特洛伊木马、恶意脚本、流氓软件、逻辑炸弹、僵尸网络、网络钓鱼、Rootkit、智能移动终端恶意代码、垃圾信息、其他新型恶意代码等。

第3章恶意代码防范原理。恶意代码防范技术分为6个层次：检测、清除、预防、免疫、策略、数据备份及恢复。在此详细介绍了恶意代码的检测原理和方法、恶意代码清除的原理和方法、恶意代码的防范、恶意代码的免疫。

第4章数据备份与数据恢复。随着恶意代码清除难度的加大，数据备份和数据恢复技术走向前台。数据备份及恢复技术不仅是灾难备份和灾难恢复的核心技术，也是恶意代码领域的核心内容。

第5章商业安全软件的常用技术。本章主要介绍了商业软件采用的特殊防范技术，例如内存检测技术、广谱杀毒技术、虚拟机技术、驱动程序技术、云查杀技术等。

第6章 OAV 软件分析与使用。OAV(OpenAntiVirus)是由德国开源爱好者发起,并由众多爱好者合作开发的反病毒软件。本章详细分析了 OAV 的框架、主要函数以及使用方法。

第7章 ClamAV 软件分析与使用。ClamAV 是运行在 Linux 操作系统上的最好的病毒检测开源软件,应用非常广泛且升级及时。本章详细分析了 ClamAV 的框架、主要函数以及使用方法。

第8章恶意代码检测用匹配算法。介绍了恶意代码检测引擎的关键技术之一——扫描算法。可以用于商业软件的扫描算法包括单模式匹配算法、多模式匹配算法、HASH 算法等。

第9章常用杀毒软件及解决方案。介绍了企业网络的典型结构、典型应用、网络时代的恶意代码攻击和传播特征,最后得出企业网络恶意代码防范体系的技术和工具需求,从而给出一些典型的防治方案。

第10章 Linux 系统杀毒工具。主要介绍3款适用于 Linux 桌面用户使用的杀毒软件,它们具有良好的、面向用户的图形化操作界面和杀毒性能,且都有免费版本供读者选择。

第11章 Windows 系统防范工具。主要从病毒查杀、木马查杀、个人防火墙角度介绍一些国内外著名的杀毒软件、木马查杀工具和个人防火墙工具,还介绍了一些有特色的其他防范工具,例如,Regmon,Filemon,Process Explorer 等工具。

第12章智能手机安全防范工具。手机恶意代码的防范也越来越引起人们的重视,相关的防范软件相继推出。本章介绍了国内外手机恶意代码防范软件,并重点介绍了几款典型手机安全防护类工具的使用方法。

第13章恶意代码防治策略。通过描述防御性策略得到的不同建议,来避免所控制的计算机受到恶意代码的影响。本章侧重于全局策略和规章,还就如何制定一个防御计划,如何挑选一个快速反应小组,如何控制住恶意代码的发作,以及防范工具的选择等问题提出了一些建议。

本书的读者对象为普通高校本科生和相关领域的工程技术人员。

张月国负责第10章和第11章的编写工作,孟魁主要完成了第13章的编写工作,同时负责全书实验材料的整理,其他章节主要由刘功申完成。在本书完稿之际,作者要衷心感谢上海市经济与信息化委员会的资助;感谢曾经参加过作者培训课程的所有领导、同仁和学生,他(她)们为作者的讲义提出过很多宝贵建议;感谢我的研究生们,他们参与了书稿的校对工作;感谢各类参考资料的提供者,这些资料既丰富了教材的内容也开阔了作者的知识面;感谢我的夫人和孩子,该书稿的完成离不开家人的默默支持。

本书配套的教学资源请到“中国高校计算机课程网”下载,具体方法是:打开网址 http://computer.cncourse.com,登录后点击“教材中心”,在“教材搜索”栏利用书名、作者或书号搜索出《恶意代码防范》一书,在打开的教材页面点击“配套资源”,即可下载相关资源。

由于时间和水平有限,内容难免疏漏,恳请读者批评指正,使本书得以进一步改进和完善。作者联系方式:lgshen@sjtu.edu.cn,博客:http://blog.csdn.net/samshmily。

作者 刘功申

2010年5月于上海交通大学

目　录

第 1 章　恶意代码概述

随着信息技术、互联网技术，特别是信息安全技术的发展，计算机病毒的概念越来越不能全面反映其内涵了，恶意代码的概念被适时地提出，并逐渐为人们接受和使用。随着恶意代码技术的发展，恶意代码的数量也在迅速增加。卡巴斯基实验室声称，至 2008 年底，全球大约有 1 400 000 种不同形式的恶意代码。究竟有多少恶意代码存在于世，这是个不可解问题！

为什么会提出恶意代码的概念？恶意代码和计算机病毒究竟有怎样的关系？恶意代码究竟包含哪些内容？恶意代码是怎样一步一步从无到有发展壮大的？

本章主要介绍恶意代码的基本概念，并在此基础上介绍恶意代码的发展历史、分类、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

本章学习目标

- 明确恶意代码的基本概念
- 了解恶意代码的发展历史
- 熟悉恶意代码的种类
- 熟悉恶意代码的命名规则
- 了解恶意代码的未来发展趋势

1.1　恶意代码概念的产生

国务院颁布的《中华人民共和国计算机信息系统安全保护条例》，以及公安部出台的《计算机病毒防治管理办法》将计算机病毒均定义为：计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并且能够自我复制的一组计算机指令或者程序代码。

我国刑法规定，故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照破坏计算机信息系统罪定刑处罚。而在互联网中流行的蠕虫、木马是否属于刑法上的计算机病毒等破坏性程序，目前还没有立法或者司法解释。根据上述有关计算机病毒的定义，感染文件的普通病毒属于计算机病毒，但是蠕虫（部分）、木马（绝大部分）并不进行自我复制，因此不符合病毒的特征，不属于计算机病毒，而它的危害性却是巨大的，因为它包含能够在触发时导致数据丢失甚至被窃的恶意代码。

有关专家认为,如果根据相关部门发布的条例来理解,将蠕虫和木马解释为计算机病毒是不符合刑法定罪原则的,而蠕虫和木马是否属于“计算机病毒等破坏性程序”,我国法律没有对此作出解释。蠕虫和木马的大量出现对刑法的部分规定提出了挑战,对刑法规定的破坏性程序必须作出明确的界定。由此可见,网络恶意代码技术的发展,导致刑法在这方面的规定显现滞后。因此,必须通过立法将木马、蠕虫等恶意代码纳入破坏性程序范围。

在美国,有些州(例如,加利福尼亚、西弗吉尼亚等)的地方法规中,把恶意代码解释成计算机系统的污染物。显然,他们的法律适用面更加宽泛。

在信息安全技术领域,重新审视目前流行的破坏性程序,有很多已经不能用“计算机病毒”这个概念来解释了。以下从两个方面进一步说明:就恶意代码的类型而言,这些破坏性程序除了木马之外,还有僵尸网络、流氓软件、逻辑炸弹、网络钓鱼、恶意脚本等。就感染平台而言,传统的计算机病毒的定义仅仅局限于计算机平台,而今后必将流行的智能手机恶意代码则运行于手机平台。关于手机上的恶意代码就不能简单地归类于传统的计算机病毒概念了。

在法律领域,专家们努力的方向是扩大法律解释范围,把新型的破坏性程序及时补充到法律条文中。在技术领域,专家们的责任更是责无旁贷,因此,需要一个新的概念来概括这些破坏性程序。这个新的概念就是“恶意代码”。

1.2 恶意代码的概念

《Malware: Fighting Malicious Code》中给出的恶意代码定义为:运行在目标计算机上,使系统按照攻击者意愿执行任务的一组指令。

在维基百科中,恶意代码的英文对照词是 Malware,也就是 Malicious Software 的混成词。恶意代码的定义描述为:恶意代码是在未被授权的情况下,以破坏软硬件设备、窃取用户信息、扰乱用户心理、干扰用户正常使用为目的而编制的软件或代码片段。这个定义涵盖的范围非常广泛,它包含了所有敌意、插入、干扰、讨厌的程序和源代码。一个软件被看做是恶意代码主要是依据创作者的意图,而不是恶意代码本身的特征。

依据这个定义,恶意代码将包括计算机病毒(Computer Virus)、蠕虫(Worm)、特洛伊木马(Trojan Horse)、Rootkit、间谍软件(Spyware)、恶意广告(Dishonest Adware)、流氓软件(Crimeware)、逻辑炸弹(Logic Bomb)、后门(Back Door)、僵尸网络(Botnet)、网络钓鱼(Phishing)、恶意脚本(Malice Script)、垃圾信息(Spam)、智能移动终端恶意代码(Malware In intelligent Terminal Device)等恶意的或讨厌的软件及代码片段。国际上目前新出现了一种以“扰乱用户心理”为目的的软件,也应该属于恶意代码范畴。由于这类软件的使用范围非常小,因此,不为人们熟知。在这个定义范围内,恶意代码不是有缺陷的软件,也就是说,包含有害漏洞但其目的是合法的软件不是恶意代码。例如,微软的 Windows 操作系统,尽管也包含很多有害漏洞,但因为其目的是合法的,因此,Windows 不是恶意代码。

恶意代码是一个具有特殊功能的程序或代码片段,就像生物病毒一样,恶意代码具有独特地传播和破坏能力。恶意代码可以很快地蔓延,又常常难以根除。它们能把自身附着在各种类型的对象上,当寄生了恶意代码的对象从一个用户到达另一个用户时,它们就随同该对象一起蔓延开来。除传播和复制能力外,某些恶意代码还有其他一些特殊特性,例如,特洛伊木马具有窃取信息的特性,流氓软件具有干扰用户的特性,而蠕虫则主要具有利用漏洞传播来占用带宽耗费资源等特性。

迄今为止,各种恶意代码表现出不同的特征,但总结起来,恶意代码具有以下 3 个明显的共同特征。

1. 目的性

目的性是恶意代码的基本特征,是判别一个程序或代码片段是否为恶意代码的最重要的特征,也是法律上判断恶意代码的标准。

2. 传播性

传播性是恶意代码体现其生命力的重要手段。恶意代码总是通过各种手段把自己传播出去,到达尽可能多的软硬件环境。

3. 破坏性

破坏性是恶意代码的表现手段。任何恶意代码传播到了新的软硬件系统后,都会对系统产生不同程度的影响。它们发作时轻则占用系统资源,影响计算机运行速度,降低计算机工作效率,使用户不能正常使用计算机,重则破坏用户计算机的数据,甚至破坏计算机硬件,给用户带来巨大的损失。

1.3 恶意代码的发展历史

恶意代码的产生原因多种多样,有的是计算机工作人员或业余爱好者纯粹为了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复制而制造的,这些情况助长了恶意代码的制作和传播。还有一种情况就是蓄意破坏,它分为个人行为和政府行为两种。个人行为多为雇员对雇主的报复行为,而政府行为则是有组织的战略战术手段。在“海湾战争”中,美国国防部的某个机构曾对伊拉克的通信系统进行了有计划的恶意代码攻击,一度使伊拉克的国防通信系统陷于瘫痪。另外还有些恶意代码是用于研究或实验而设计的“有用”程序,由于某种原因失去控制而扩散出去,成为危害四方的恶意代码。但是,无论是基于什么目的而产生的恶意代码,都给用户带来了非常大的危害。

2008 年 12 月 5 日,在卡巴斯基实验室举办的病毒分析师峰会上,卡巴斯基实验室的高级区域研究师 David Emm 发表了关于恶意代码市场分析的主题演讲。David 在主题演讲中指出,恶意代码的数量每秒钟都在增长,到 2008 年底为止,全球大约存在恶意代码 1 400 000 种,如图 1-1 所示。

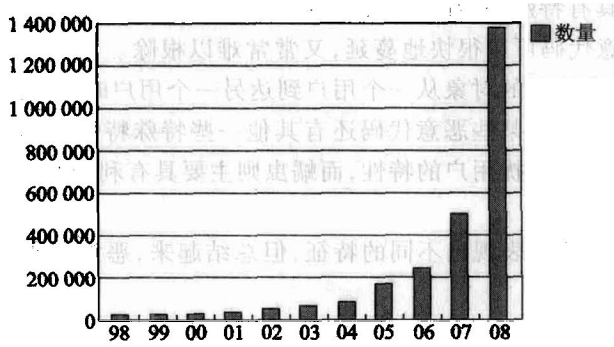

图1-1 全球恶意代码数量增长图示(卡巴斯基实验室)

以下回顾恶意代码从出现到蓬勃发展的历史过程中的一些关键环节。

自从1946年第一台电子计算机ENIAC问世以来,计算机与人们的生活已经越来越息息相关,人们甚至已经无法在没有计算机的世界里生活。但是人们发现就如同人会生病一样,计算机的世界里也存在病毒,计算机也会染病。那么,恶意代码是如何一步一步地从无到有、从小到大发展到今天的呢?

其实,恶意代码的初始阶段都集中体现为计算机病毒这一典型的恶意代码。在第一台商用计算机出现之前,伟大的计算机技术先驱——冯·诺依曼(John Von Neumann)在他的一篇论文《复杂自动装置的理论及组织的进行》里,就已经勾勒出了病毒的蓝图。

"计算机病毒"这个词汇最早是出现在科幻小说里的。1977年夏天,托马斯·瑞安(Thomas. J. Ryan)的科幻小说《P-1的春天》(The Adolescence of P-1)成为美国的畅销书。作者在这本书中描写了一种可以在计算机中互相传染的病毒,病毒最后控制了7 000台计算机,造成了一场灾难。不过,这在当时并没有引起人们的注意。

磁芯大战(Core War)是在冯·诺依曼病毒程序蓝图的基础上提出的概念。起初绝大部分的计算机专家都无法想象会存在这种能自我繁殖的程序,可是少数几个科学家默默地研究着这个问题。直到10年之后,在美国电话电报公司(AT&T)的贝尔(Bell)实验室中,这些概念在一种很奇怪的电子游戏中成形了,这种电子游戏称为磁芯大战。

磁芯大战玩法如下:双方各写一套程序并输入同一部计算机中,这两套程序在计算机系统内互相追杀,有时它们会放置一些关卡,甚至有时会停下来修复被对方破坏的几行指令。当被困时,它们可以将自己复制一次从而逃离险境,因为它们都在计算机的记忆磁芯中游走,因此被取名为磁芯大战。这个游戏的特点在于双方的程序进入计算机之后,玩游戏的人只能看着屏幕上显示的战况,而不能做任何更改,直到某一方的程序被另一方的程序完全"吃掉"为止。

1983年11月3日,弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序。伦·艾德勒曼(Len Adleman)将这种破坏性程序命名为计算机病毒(Computer Viruses),并在每周一次的计算机安全讨论会上正式提出,8小时后专家们在VAX 11/750计算机

系统上成功运行该程序。就这样,第一个恶意代码实验成功。这是人们第一次真正意识到计算机病毒的存在。

1986 年初,巴锡特(Basit)和阿姆杰德(Amjad)两兄弟编写了 Pakistan 病毒,即 Brain。Brain 是第一个感染 PC 的恶意代码。随着 PC 的蓬勃发展,恶意代码迅速发展壮大起来。

1987 年世界各地的计算机用户几乎同时发现了形形色色的计算机病毒,例如,大麻、IBM 圣诞树、黑色星期五等。面对计算机病毒的突然袭击,众多计算机用户甚至专业人员都惊慌失措。

1988 年 3 月 2 日,一种苹果机的恶意代码发作。这天受感染的苹果机停止工作,只显示"向所有苹果电脑的使用者宣布和平的信息",以庆祝苹果机生日。这是第一个感染窗口系统的恶意代码。

1988 年冬天,正在康奈尔大学攻读的莫里斯,把一个被称为"蠕虫"的计算机病毒送进了美国最大的计算机网络——互联网。1988 年 11 月 2 日下午 5 点,互联网的管理人员首次发现网络有不明入侵者。当晚,从美国东海岸到西海岸,互联网用户陷入一片恐慌。由于当时的网络非常有限,其破坏力没有得到充分发挥。其实,蠕虫的概念起源更早,在 1982 年,Shock 和 Hupp 根据《The Shockwave Rider》一书中的概念提出了一种"蠕虫(Worm)"程序的思想。蠕虫的真正爆发却在十多年后,20 世纪初,蠕虫在互联网中大爆发,其原理正是来自于莫里斯的蠕虫。

1989 年全世界的计算机病毒攻击十分猖獗,我国也未幸免。其中"米开朗基罗"病毒给许多计算机用户造成了极大的损失。这个病毒比较著名的原因,除了它拥有一代艺术大师米开朗基罗的名字之外,更重要的是它的杀伤力非常强大。

1991 年在"海湾战争"中,美军第一次将计算机病毒用于实战,在空袭巴格达的战斗前,成功地破坏了对方的指挥系统,使之瘫痪,保证了战斗的顺利进行,直至最后胜利。

1992 年出现了针对杀毒软件的"幽灵"病毒,例如,One-half。该病毒直接挑战简单的特征码扫描技术,随后,各个安全厂商推出了启发式扫描、含有通配符的特征码等技术来应对幽灵型病毒。

1996 年首次出现针对微软公司 Office 的"宏病毒"。宏病毒的出现使病毒编制工作不再局限于晦涩难懂的汇编语言,由于书写简单,越来越多的恶意代码出现了。1997 年被公认为信息安全界的"宏病毒年"。宏病毒主要感染 Word、Excel 等文件。如 Word 宏病毒,早期是用一种专门的 Basic 语言即 Word Basic 所编写的程序,后来使用 Visual Basic。与其他计算机病毒一样,它能对用户系统中的可执行文件和数据文本类文件造成破坏。常见的宏病毒有 Taiwan NO.1(台湾一号)、Setmd、Consept、Mdma 等。

1998 年出现针对 Windows 95/98 系统的 CIH 病毒(1999 年被公认为计算机反病毒界的 CIH 病毒年)。CIH 病毒是继 DOS 病毒、Windows 病毒、宏病毒后的第四类新型病毒。这种病毒与 DOS 下的传统病毒有很大区别,它是使用面向 Windows 的 VXD(虚拟设备驱动程序)技术编制的。1998 年 8 月从台湾传入大陆的 CIH 病毒,共有 3 个版本:1.2 版、1.3 版、1.4 版。它们的发作时间分别是 4 月 26 日、6 月 26 日、每月 26 日。该病毒是第一个直接攻击、破坏硬件的计算机病毒,是破坏最为严重的病毒之一。它主要感染 Windows 95/98 的可执行程序,发作时破坏计算

机 Flash BIOS 芯片中的系统程序,导致主板损坏,同时破坏硬盘中的数据。病毒发作时,硬盘驱动器不停旋转,硬盘上所有数据(包括分区表)被破坏,必须对硬盘重新分区才有可能挽救硬盘。同时,对于部分厂牌的主板(如技嘉和微星等),会将 Flash BIOS 中的系统程序破坏,造成开机后系统无反应。1999 年 4 月 26 日,CIH 病毒在全球范围大规模爆发,造成近 6 000 万台计算机瘫痪,经济损失约 100 亿美元。

1999 年 Happy99 等完全通过因特网(Internet)传播的蠕虫的出现,标志着网络恶意代码将成为新的挑战。其特点就是利用 Internet 的优势,快速进行大规模的传播,从而使蠕虫在极短的时间内遍布全球。

2001 年 7 月中旬,一种名为"红色代码"的恶意代码在美国大面积蔓延,这个专门攻击服务器的恶意代码攻击了白宫网站,造成了全世界恐慌。8 月初,其变种"红色代码 2"针对中文系统作了修改,增强了对中文网站的攻击能力,开始在中国蔓延。"红色代码"通过黑客攻击手段利用服务器软件的漏洞来传播,它造成了全球 100 万个以上的系统被攻陷而导致瘫痪。这是恶意代码与网络黑客首次结合,可以说对后来的恶意代码产生了很大的影响。

2003 年"2003 蠕虫王"在亚洲、美洲、澳大利亚等地迅速传播,造成了全球性的网络灾害。其中受害最严重的无疑是美国和韩国这两个 Internet 发达的国家。其中韩国 70% 的网络服务器处于瘫痪状态,网络连接的成功率低于 10%,整个网络速度极慢。美国不仅公众网络受到了破坏性攻击,甚至连银行网络系统也遭到了破坏,全国 1.3 万台自动取款机处于瘫痪状态。

2004 年是蠕虫泛滥的一年,根据中国计算机病毒应急中心的调查显示,2004 年 10 大流行恶意代码都是蠕虫,它们包括:

- 网络天空(Worm. Netsky)
- 高波(Worm. Agobot)
- 爱情后门(Worm. Lovgate)
- 震荡波(Worm. Sasser)
- SCO 炸弹(Worm. Novarg)
- 冲击波(Worm. Blaster)
- 恶鹰(Worm. Bbeagle)
- 小邮差(Worm. Mimail)
- 求职信(Worm. Klez)
- 大无极(Worm. SoBig)

2005 年是特洛伊木马流行的一年。在经历了操作系统漏洞升级、杀毒软件技术改进后,蠕虫的防范效果已经大大提高,真正有破坏作用的蠕虫已经销声匿迹。然而,病毒制作者(Vxer)永远不甘寂寞,他们又开辟了新的高地——特洛伊木马。2005 年的木马即包括安全领域耳熟能详的经典木马,例如,BO2K、冰河、灰鸽子等,也包括很多新鲜的木马,简单举例如下。

(1) 闪盘窃密者(Trojan. UdiskThief)

该木马会判断计算机上移动设备的类型,自动把 U 盘里所有的资料都复制到计算机 C 盘的

TEST 文件夹下，这样可能造成某些公用计算机用户的资料丢失。

（2）证券大盗（Trojan/PSW. Soufan）

该木马可盗取包括南方证券、国泰君安在内多家证券交易系统的交易账户和密码，被盗号的股民账户存在被人恶意操纵的可能。

（3）外挂陷阱（Trojan. Lineage. hp）

此木马可以盗取多个网络游戏的用户信息，如果用户通过登录某个网站，下载安装所需外挂程序后，便会发现外挂程序实际上是经过伪装的恶意代码，这个时候恶意代码便会自动安装到用户计算机中。

（4）我的照片（Trojan. PSW. MyPhoto）

该木马试图窃取热血江湖、传奇、天堂 2、工商银行、中国农业银行等数十种网络游戏及网络银行的账号和密码。该木马发作时，会显示一张照片使用户对其放松警惕。

2006 年木马仍然是恶意代码的主流，其变种层出不穷。2006 年的上半年，江民反病毒中心共截获新恶意代码 33 358 种。据江民病毒预警中心监测的数据显示，1 月至 6 月全国共有 7 322 453 台计算机感染了病毒，其中感染木马的计算机 2 384 868 台，占病毒感染计算机总数的 32.56%，感染广告软件的计算机 1 253 918 台，占病毒感染计算机总数的 17.12%，感染后门程序的计算机 664 589 台，占病毒感染计算机总数的 9.03%，感染蠕虫病毒计算机 216 228 台，占病毒感染计算机总数的 2.95%，监测发现漏洞攻击代码的计算机 181 769 台，占病毒感染计算机总数的 2.48%，感染恶意脚本的计算机 15 152 台，占病毒感染计算机总数的 2.06%。由此可见，木马将是未来几年恶意代码的主流。

随着 Internet 的进一步发展，依赖互联网作为传播途径的恶意代码成了当前最具威胁的破坏者。像冲击波、震荡波、灰鸽子等网络型恶意代码带来的损失都是不可估量的。表 1－1 显示了近年来几个经典恶意代码带来的巨大危害。

表 1－1 重大恶意代码危害列表①

年 份	攻击行为发起者	受害 PC 数目（万台）	损失金额（美元）
2007	熊猫烧香	超过 200	
2006	木马和恶意软件		
2005	木马		
2004	Worm Sasser		
2003	Worm MSBLAST	超过 140	
2003	SQL Slammer	超过 20	9.5 亿—12 亿

① 部分没有准确来源的数据没有列出。由于木马的特点在于窃取，因此，其破坏程度不可估计。

续表

年 份	攻击行为发起者	受害 PC 数目(万台)	损失金额(美元)
2002	Klez	超过 600	90 亿
2001	RedCode	超过 100	26 亿
2001	Nimda	超过 800	60 亿
2000	Love Letter		88 亿
1999	CIH	超过 6 000	近 100 亿

1.4 恶意代码的种类

在恶意代码技术的发展过程中,其特征不断变化,恶意代码的种类也不断增加。根据国内外多年来对恶意代码的研究成果可知,恶意代码主要包括普通计算机病毒、蠕虫、特洛伊木马、Rootkits 工具、流氓软件、间谍软件、恶意广告、逻辑炸弹、后门、僵尸网络、网络钓鱼、恶意脚本、垃圾信息、智能移动终端恶意代码等。

1. 普通计算机病毒

普通计算机病毒是指:编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。也就是传统意义上的计算机病毒,主要包括引导区型病毒、文件型病毒以及混合型病毒。感染引导区的病毒是较老的一种病毒,主要是感染 DOS 操作系统的引导过程。文件型病毒分为感染可执行文件的病毒和感染数据文件的病毒。前者主要指感染 COM 文件或 EXE 文件的病毒,例如,CIH 病毒。后者主要指感染 Word、PDF 等数据文件的病毒,例如,宏病毒等。混合型病毒主要指那些既能感染引导区又能够感染文件的病毒。

尽管有些文献把特洛伊木马、蠕虫等都划归到计算机病毒概念下,但这种分类法并不符合计算机病毒的定义。因此,本书所指的计算机病毒仅仅包括引导区型病毒、文件型病毒以及混合型病毒。

2. 蠕虫

提起蠕虫,影响最深的就是冲击波、震荡波、红色代码、尼姆达等名称。这些蠕虫在 2003 年至 2004 年达到高发期,并给整个信息安全领域留下了不可磨灭的印记。

尽管蠕虫的爆发期是从 2000 年后才开始的,但蠕虫这个名词的由来已久。在 1982 年,Shock 和 Hupp 根据《The Shockwave Rider》一书中的概念提出了“蠕虫”(Worm)程序的思想。1988 年,莫里斯把一个被称为“蠕虫”的恶意代码送进了美国的计算机网络,正式宣告了蠕虫的存在。