JISUANJI EYI DAIMA FENXI

计算机恶意代码分析与防范技术

YU FANGFAN JISHU

李锦 / 编著

群 众 出 版 社

JISUANJI EYI DAIMA FENXI

计算机恶意代码分析与防范技术

YU FANGFAN JISHU

李锦 / 编著

群 众 出 版 社

图书在版编目（CIP）数据

计算机恶意代码分析与防范技术 / 李锦著；—北京：群众出版社，2009.6
ISBN 978-7-5014-4466-3

Ⅰ. 计… Ⅱ. 李… Ⅲ. 电子计算机-安全技术-代码 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2009）第 076941 号

计算机恶意代码分析与防范技术
李锦 编著
责 编 晓 潇
群众出版社出版、发行
地址：北京市丰台区方庄芳星园三区 15 号楼
邮编：100078 电话：（010）52173000 转
网址：www. qzcbs. com
电子信箱：exiaoxiaohong@hotmail. com
新华书店经销 北京通天印刷有限责任公司印刷
开本 787 × 1092 1/16 印张 17.75 字数 333 千字
2009 年 6 月第 1 版 2009 年 10 月第 2 次印刷
ISBN 978-7-5014-4466-3/ TP · 17 定价：38.00 元

前　言

自1946年第一台计算机问世以来，计算机给人们生活带来了前所未有的便利和效率。它改变了人们的交流方式、生活方式；改变了全球的经济结构、社会结构；整个世界真正变成了一个地球村，Internet已经成为人类社会最重要的组成部分。

随着计算机应用的不断普及，在给人类社会带来便捷的同时，计算机技术发展到一定阶段的产物——恶意代码也随之降临并泛滥，严重威胁人类生活的各个领域，已成为计算机系统的大敌。它不仅对计算机操作人员、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了现实威胁，其危害程度越来越受到关注。因此，剖析计算机恶意代码的基本原理及相应防治技术，增强人们的防范意识，强化计算机系统的安全可靠性，已成为摆在我们面前的重要课题。

恶意代码的分析是敏感话题。很多人认为，这项工作会引起病毒的泛滥，也有人质疑，到底有没有必要学习恶意代码的编程机理？恶意代码的泛滥是因为编写它的队伍庞大，还是源于了解它的人太少？这些问题确实值得人们深思。我们的态度是："知己知彼，百战不殆。"要想战胜对手，首先要了解你的对手。同样，要想在与恶意代码的战争中取得胜利，首先要消除恐惧心理，掌握它的开发机理，才可能最终达到防范与清除的目的。

本书从恶意代码的定义入手，全面介绍各类计算机恶意代码的开发机理和清除防范方法。章节安排尽量彼此独立。先后顺序的安排上基本遵循恶意代码发展的主线，由易到难，并兼顾知识的连续性。全书的内容具体安排如下：

第一章，计算机恶意代码概述。主要介绍计算机恶意代码的定义、发展历程、分类、特征、命名规则、危害等几方面的内容。

第二章，预备知识。主要介绍计算机硬盘结构、计算机文件系统、

中断、DLL 、API 函数、注册表、debug 的使用、winhex 的使用等方面的知识。通过本章的学习，读者可以更好地理解后面章节中介绍的各种恶意代码的开发机理，也为数据恢复技术的学习打下基础。

第三章，DOS 病毒。主要介绍 DOS 操作系统、简单的 DOS 批处理病毒、病毒的一般结构、DOS 引导型病毒——“大麻”病毒基本原理以及 DOS 引导型病毒的清除方法。了解 DOS 病毒开发的技术内幕，对更好理解 Windows 病毒等恶意代码开发机制有触类旁通的作用。

第四章，PE 文件病毒。主要介绍 PE 文件格式、病毒的重定位技术、获取 API 函数地址的方法、病毒搜索文件方法、内存映射文件、PE 病毒感染文件基本步骤、FUNLOVE 病毒分析与清除方法。

第五章，宏病毒。主要介绍 Word 宏与宏病毒知识、宏病毒开发技术、“美丽莎”宏病毒源代码分析、“美丽莎”病毒清除方法。最后向读者介绍宏病毒防范知识。

第六章，脚本病毒。重点介绍脚本语言、WHS 与脚本病毒、脚本病毒开发机理、“爱虫”病毒分析。最后介绍脚本病毒的防范知识。

第七章，网络蠕虫。主要包括蠕虫的定义、蠕虫的功能模块与工作流程、蠕虫的开发机理、蠕虫的检测与防范。最后对 2006 年著名的“熊猫烧香”蠕虫做了剖析，并给出了清除与防范方法。

第八章，“特洛伊木马”。主要包括“特洛伊木马”的定义、木马程序结构及工作原理、木马的开发技术、木马的检测与防范。最后详细剖析了“灰鸽子”木马技术原理，并给出查杀与防范方法。

本书着眼于当前计算机发展趋势和反病毒技术的最新成果，结构清晰，内容全面，通俗易懂，理论性与实用性并重，通过对典型恶意代码实例的分析，揭示了计算机恶意代码的本来面目，使读者能够举一反三，增加安全防范意识。

本书从各种专著、论文、书刊、期刊以及互联网引用了大量资料。在此，谨向各位作者表示衷心感谢。引用的资料有的在参考文献中列出，有的无法查证。对此，作者深表歉意。

衷心感谢公安部第三研究所国家反计算机入侵和防病毒研究中心的黄镇、张奎亭等几位专家的大力支持。他们在计算机病毒领域的出色工作给了我们很大的启示，在本书的创作过程中给予很多指导，为本书的创作提供了很多有益的意见和建议。同时也感谢在本书的创作

过程中给予大力支持的辽宁警官高等专科学校的领导和老师们。

本书在出版过程中得到了群众出版社晓潇等各位老师的支持和帮助，在此一并感谢。由于作者水平有限，疏漏之处在所难免，欢迎广大读者批评指正。

李锦

2009 年 4 月于大连

目　录

第一章　计算机恶意代码概述

本章要点：

- 计算机恶意代码定义
- 计算机恶意代码分类
- 计算机恶意代码发展历程
- 计算机恶意代码特征
- 计算机恶意代码命名规则

自 1946 年第一台计算机问世以来，计算机及互联技术飞速发展，改变了人们交流的方式，生活方式；改变了全球的经济结构，社会结构；整个世界即使远在天涯，却可以近在咫尺，真正变成一个地球村。Internet 已经成为人类社会最重要的组成部分。但福祸同降，在给人类带来便捷的同时，计算机技术发展到一定阶段的产物——恶意代码也随之降临并泛滥，严重威胁人类生活的各个领域，危害程度越来越受到人们的关注。

1.1　计算机恶意代码定义

提起“恶意代码”，绝大多数计算机用户都会深恶痛绝，因为没有“中过招”的人几乎凤毛麟角。谈虎色变之余，很多人会对“恶意代码”产生好奇，到底什么是“恶意代码”？它是如何编写的？使用了怎样的技术？会造成怎样的危害？危险来临之前，人们如何防患于未然？带着这些疑问，让我们在之后的叙述中慢慢揭开它的面纱。

“恶意”在汉语词典里的解释是：不良的居心，极坏的行为。“代码”在这里是指那些计算机可以识别并且运行的字符集合。通常情况下，人们把为达到某种特殊目的，未经授权便干扰或破坏计算机系统/网络的代码或程序称之为“恶

意代码”或“恶意程序”。关于“恶意代码”的定义，既没有国际标准，国内也无法律条文规定，这应该算业内比较流行、比较公认的一种解释。笔者认同这种解释，虽然它不具备法律性和权威性。

谈到“恶意代码”，人们很自然地会想到“计算机病毒”。关于二者的关系，业内还存在两种观点：

◆有人将“恶意代码”与“计算机病毒”混为一谈。笔者不认同这种看法。随着计算机技术的发展，“计算机病毒”已成为“恶意代码”的一个种类，是恶意代码的早期表现形式。

◆还有人将计算机病毒分为狭义和广义两种。狭义的计算机病毒可以使用下面颇具权威的定义。“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程序代码。”这是《中华人民共和国计算机信息系统安全保护条例》的解释，具有法律效应。广义上的计算机病毒是指不具有狭义计算机病毒的特征，但也破坏计算机系统的一些有争议的代码或程序，比如“蠕虫”或“木马”等“后计算机病毒”。这种观点认为，广义上的计算机病毒就等同于恶意代码。这一解释有一定道理，但笔者认为逻辑上容易混乱，而且绕口，容易引起人们的迷惑和误解。

1.2 计算机恶意代码的分类

分类学创始人 Carolus Linnaeus 说，“对事物的研究，首先从认识事物开始。认识事物，需要根据不同特性或属性区分事物，并对事物进行系统分类。分类是科学研究的基础。”对事物进行系统分类研究的作用和意义，集中体现在：①描述：描述研究对象，将其转化为易于理解、分析和管理的对象；②理解：好的分类方法有助于人们更清晰、更系统地理解所研究的对象；③预测：通过对已知领域或已知事物系统分类研究，可进一步预测未知领域，或为进一步研究提供指导。

对计算机恶意代码进行分类研究，目的在于更好地描述、分析、理解它的特性、原理、危害及防治技术。分类的主要问题在于选择哪些属性作为分类依据。依据不同，分类自然不同。可按恶意代码破坏能力、攻击的操作系统、特有的算法、寄生对象和驻留方式、是否依赖宿主程序分类。

本书按恶意代码是否依赖宿主程序进行分类。这种分类方法不一定很完整，但简单明了。按照此一分类方法，恶意代码可分为两大类（如图 1.1）。一类是依赖于主机程序的恶意代码，不能独立于应用程序或系统程序，即存在宿主程序。这一类别包括病毒、后门、逻辑炸弹、“特洛伊木马”。另一类是独立于主机程序的恶意代码，能在操作系统上运行的独立程序。这一类别包括拒绝服务程序、蠕

虫、细菌。下面对各种恶意代码概要介绍。

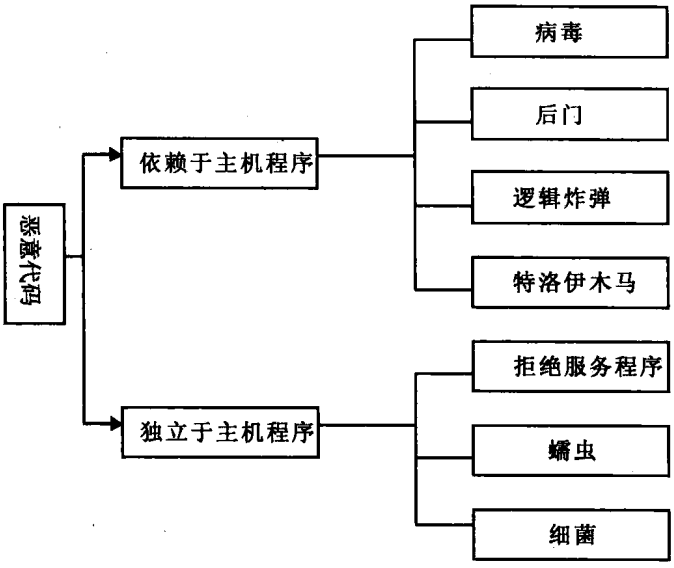

图 1.1　恶意代码分类

1.2.1　计算机病毒

生物界的病毒——“virus”源于拉丁文，原指一种动物来源的毒素，能增殖、遗传和演化，因而具有生命最基本的特征。生物病毒区分于其他生物的特征是：①含有单一核酸（DNA 或 RNA）的基因组和蛋白质外壳，没有细胞结构；②在感染细胞的同时或稍后释放核酸，然后以核酸复制的方式增殖，而不是以二分裂方式增殖；③严格的细胞内寄生性，缺乏独立的代谢能力，只能在活的宿主细胞中，利用细胞的生物合成机器来复制核酸，并合成由核酸编码的蛋白，最后装配成完整的、有感染性的病毒单位，即病毒粒。病毒粒是病毒从细胞到细胞，或从宿主到宿主传播的主要形式。它能侵入人体或其他生物体内的病原体，潜入细胞后，会大量繁殖生成复制品。这些复制品又去感染其他健康细胞。大部分被感染的细胞会因此而死亡或失去原来的功能。它是具有传染性和杀伤性的非人为有机体。我们熟悉的生物病毒有天花病毒、狂犬病毒、禽流感病毒、艾滋病毒、2003 年肆虐全球的非典型肺炎（SARS）病毒等。

“计算机病毒（Computer Virus）”实际上是因为与生物病毒有惊人的相似之处，才引申而来的。它的本质是为达到某种目的而制作和传播的计算机代码或程序。和生物病毒相比，它们都具有寄生性、传染性和破坏性。有些计算机病毒会像生物病毒那样寄生在计算机用户的文件中，而且会伺机机发作，并大量地复制病毒体，感染本机的其他文件和网络中的计算机，给人类社会生活造成不利影

响，造成的经济损失数以亿计。影响较大的计算机病毒有著名的 CIH、“小球”病毒、“女鬼”病毒、“黑色星期五”等等。计算机病毒与生物病毒比较如表 1.1 所示。

表 1.1 计算机病毒与生物病毒比较

行为	计算机病毒	生物病毒
攻击目标	计算机软硬件	生物细胞
破坏目的	干扰计算机系统正常运行	改变细胞成分
复制特性	被感染的文件感染另一正常文件	病毒在被感染的细胞里繁殖
重复感染	带毒文件一般不再被感染	不再感染染毒细胞
潜伏性	带毒文件一段时期能正常工作	感染病毒后生物体可能没有症状
人为特性	人为编制的恶意程序	天然存在的
其他特性	病毒程序会出现变异；病毒程序能对抗杀毒软件的查杀；	生物体可能会出现对病毒的免疫姓性；生物体感染的病毒可能会变异；可能出现抗药性；

1.2.2 特洛伊木马

先来了解故事《木马屠城记》。这是一个古希腊神话故事。众神之王宙斯住在奥林波斯山上，妻子是神后赫拉。有一次，赫拉安排了一场盛宴，只有不和女神埃里斯没被邀请。宴会进行中，埃里斯突然出现，向众神投掷了一个金苹果。上面刻写着“给最美丽的人”。神后赫拉、智慧女神雅典娜和爱与美的女神维纳斯都认为自己是最美丽的，应该得到那个苹果。为了解决这个棘手的难题，宙斯叫三位女神去找特洛伊国王的小儿子帕里斯，他以英俊漂亮而知名。三位女神都试图以自己的魅力影响帕里斯的裁判。维纳斯答应让他得到最美貌的女人为妻，帕里斯就把金苹果判给了维纳斯，也因此得罪了赫拉和雅典娜。

当时希腊各部族也很强大，分成若干王国，总称阿凯亚人。斯巴达王的妻子海伦非常漂亮。帕里斯在维纳斯的帮助下把海伦骗到手，私奔到了特洛伊国的王城伊利昂城。一场战争不可避免地爆发了。希腊人开始远征特洛伊（现在的土耳其首都）。这场战争打了十年，伊利昂城还是久攻不下。后来，足智多谋的英雄奥德修斯想出了一个主意，制造一匹巨大的木马，奥德修斯和他挑选的三十名勇士隐藏在中空的马腹中，希腊人把这匹木马放到伊利昂城前面的海滩上，同时装作撤退，但没有走远。奥德修斯的堂兄西农扮成乞丐留了下来。他使特洛伊人相信，木马是众神送给伊利昂城的礼物，劝说他们把木马运进城去。特洛伊人欢喜若狂，大开城门，把木马拉进城去。那天夜里，西农给希腊大军发了信号。藏匿

于木马中的将士开秘门游绳而下，开启城门，四处纵火。城外伏兵涌入，部队里应外合，伊利昂城被烧毁，并被夷为平地。斯巴达王也夺回了漂亮的妻子海伦。

后世称木马为“特洛伊木马”（Trojan horse）。如今黑客程序借用其名，有“一经潜入，后患无穷”之意。现在网络中流行的“特洛伊木马”是指那些表面有用的软件、实际目的却是危害计算机安全，并导致严重破坏的计算机程序。完整的木马程序一般由两部分组成：一个是服务器程序，一个是控制器程序。“中了木马”就是指安装了木马的服务器程序。若你的电脑被安装了服务器程序，则拥有控制器程序的人就可以通过网络控制你的电脑、为所欲为。这时，你电脑上的各种文件、程序，以及在你电脑上使用的账号、密码就无安全可言了。

“特洛伊木马”与病毒的重大区别是“特洛伊木马”不具传染性，并不像病毒那样复制自身，也并不刻意感染其他文件。它主要通过将自身伪装起来，吸引用户下载执行。“特洛伊木马”中包含能够在触发时导致数据丢失甚至被窃的恶意代码。要使“特洛伊木马”传播，必须在计算机上有效地启用这些程序，例如打开电子邮件附件，或者将“木马”捆绑在软件中放到网络，吸引人下载执行等。相对而言，病毒主要是破坏你的信息，而“木马”窃取你的信息。典型的“特洛伊木马”有“灰鸽子”、“冰河”、“网银大盗”、“代理木马”、“AV 终结者”、“QQ 木马”等。不过，如今“木马”和其他种类的恶意代码都呈交叉性，如著名的“熊猫烧香”。它会破坏数据，也可以传播自己，更重要的是要盗取账号等信息。

1.2.3 后门程序

说起“后门程序”，熟悉计算机的用户一定都听说过。早期的电脑黑客，在成功获得远程系统的控制权后，希望能有一种技术使得他们在任意时间都可以再次进入远程系统，于是，后门程序就出现了。

后门程序一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序，以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么，它就成了安全风险，容易被黑客当成漏洞进行攻击。传统意义上的后门程序往往只是能够让黑客获得一个 SHELL，通过这个 SHELL 进而进行一些远程控制操作。

有人将后门程序归为“特洛依木马”一类。其用途在于潜伏在电脑中，从事搜集信息或便于黑客进入。另一个原因在于后门程序不一定有自我复制的动作，不一定会“感染”电脑。都是隐藏在用户系统中向外发送信息，而且本身具有一定权限，以便远程机器对本机的控制。“后门”与“木马”的区别是：“木马”是一个完整的软件，而“后门”则体积较小且功能都很单一。在病毒命名中，

“后门”一般带有 backdoor 字样，而“木马”一般则是“Trojan”字样。

最著名的后门程序该是微软的 Windows Update。它的动作不外乎三个。开机时自动连上微软网站，将电脑现况报告给网站。网站通过 Windows Update 程序通知使用者，是否有必须更新的文件以及如何更新。稍加分析便知，“开机时自动连上微软网站”的动作就是后门程序特性中的“潜伏”，“将电脑现况报告”的动作是“搜集信息”。

全球著名黑客米特尼克在 15 岁的时候，闯入了“北美空中防御指挥系统”的计算机主机内，和另外一些朋友翻遍了美国指向前苏联及其盟国的所有核弹头的数据资料，然后又悄无声息地溜了出来。这就是黑客历史上利用“后门”进行入侵的一次经典之作。在破解密码的过程中，米特尼克一开始就碰到了极为棘手的问题。毕竟事关整个北美的战略安全，这套系统的密码设置非常复杂。但经过不断努力，在两个月时间里升级他的跟踪解码程序后，终于找到了北美空中防务指挥部的“后门”。这正是整套系统的薄弱环节，也是软件设计者留下来以便自己进入系统的地方。这样，米特尼克就顺顺当当、大摇大摆地进入了这个系统。

“后门”防范相对“木马”来说，更加困难，因为系统本身就包括远程桌面、远程协助这些可以进行远程维护的后门，所以对用户来讲，技术难度更大。

1.2.4 逻辑炸弹

要了解“逻辑炸弹”，最好先让我们回忆一下计算机发展史上著名“KV300L + +”事件。1996 年 9 月，著名的杀毒软件制造商江民公司 KV300 正式推出该产品，12 月就出现了假冒产品。1997 年 4 月 24 号，Internet 网上还出现了专门攻击 KV300 的“毒岛论坛”。它一方面在舆论上攻击 KV300，另一方面专门解密 KV300，提供制作 KV300 盗版盘的工具 MK300V。王江民，北京江民新技术有限公司董事长兼总裁，著名的反病毒专家，为维护消费者合法权益，打击盗版，随即和“毒岛”斗了起来。“毒岛”出 MK300V1，王江民把它反了，让用 MK300V1 做出的假冒盘不能升级。“毒岛”接着出 MK300V2 和 MK300V3，王江民先后也都把它们反了。就这样，他们从 4 月斗到了 6 月。1997 年 6 月 24 日，王江民在其网站主页上发布了 KV300L + + 版，内含主动逻辑锁，凡是在 MK300V4 制作的仿真盘（盗版盘）上执行 KV300L + + 的用户，硬盘数据均被破坏，同时硬盘被锁，软硬盘皆不能启动。从网上的求救信息可以看到，包括在校大学生的毕业论文被破坏，KV300 的代理商的电脑遭到破坏，求救的人不计其数（网上的求救信息并不能作为证据，因为不能排除有人误判断及有假消息）。从常规上可做推断：KV300 当时至少有几十万正版用户，盗版用户可能远远大于这一