普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇
网络侦查与电子物证系列丛书主编：秦玉海

恶意代码调查技术

于晓聪 秦玉海 主编

http://www.tup.com.cn

Investigation
Malicious
Code

根据教育部高等学校信息安全类专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

恶意代码调查技术

于晓聪 秦玉海 主编

Information Security

http://www.tup.com.cn

清华大学出版社

北京

内 容 简 介

本书从恶意代码犯罪的角度出发，对计算机病毒、木马、网页恶意代码和僵尸网络等典型的恶意代码犯罪及其调查技术进行研究并介绍。通过本书可以了解各类恶意代码的特点、危害及传播方式，恶意代码犯罪及其调查取证方法等方面的内容。全书共5章，具体内容包括恶意代码调查技术概述、病毒案件调查技术、木马案件调查技术、网页恶意代码案件调查技术、计算机恶意代码防范及相关法律法规等。

本书可作为高等院校信息安全专业及网络安全与执法专业等相关专业本科生的教材，也可供公安专业的学生以及相关部门的办案人员参考阅读。

图书在版编目（CIP）数据

恶意代码调查技术/于晓聪，秦玉海主编. —北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-34932-7

Ⅰ. ①恶… Ⅱ. ①于… ②秦… Ⅲ. 电子计算机—安全技术—高等学校—教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第321454号

责任编辑：张　民　战晓雷
封面设计：常雪影
责任校对：梁　毅
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.5　　**字　　数**：360千字
版　　次：2014年2月第1版　　**印　　次**：2014年2月第1次印刷
印　　数：1～2000
定　　价：29.00元

产品编号：056305-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高〔2006〕9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前言

随着互联网技术的发展和普及，人们的生活与网络的联系越来越紧密，以网络方式获取和传播信息已经成为现代信息社会的重要特征之一，日益发达的网络产品越来越多，如网上商城、网上银行、网络游戏、移动办公和网络即时通信等，这些网络应用已经深入到人们生活的各个方面。网络上传输着各种重要的信息，如银行账号密码、电子邮件、私人照片等，同时网络上也到处充斥着盗号木马、僵尸网络、远程控制程序等各种恶意代码程序及工具，一些动机不纯的黑客想尽办法利用便捷的网络和黑客技术去破坏或盗取这些重要信息，如盗取网游账号、盗取 QQ 号码、盗取网银、发起 DDOS 攻击等，因此，网络安全问题已经成为越来越多的人们关注的焦点。

当前，网络信息安全技术已经影响到社会的政治、经济、文化和军事等各个领域。恶意代码犯罪已成为信息安全领域乃至全社会共同关注的焦点，它能够使人们的经济财产遭受损失，个人信息泄露，知识产权受到不法侵害，甚至威胁到国家政府机关等重要部门的信息安全，已给个人和社会带来严重的困扰。

近年来，网络案件侦查部门应运而生，应时代的需要发展也越来越快，从最初网监科室的几个办案人员发展到现在独具规模且实力不断壮大的网监队伍，对网络犯罪起到了一定的威慑和惩治作用。但随着恶意代码技术的高速发展，信息安全与防范技术往往落后于不断推陈出新、不断升级的网络犯罪手段与技术，网络犯罪侦查部门面临着前所未有的严峻挑战。

本书从恶意代码犯罪的角度出发，对典型的恶意代码、恶意代码犯罪及其调查技术进行研究并介绍，不仅适合作为高等院校信息安全专业及公安院校网络安全与执法专业等相关专业本科生的教材，对于公安专业的学生以及相关部门的办案人员也具有一定的参考价值。

本书由于晓聪、秦玉海编写。其中第 1 章、第 2 章由秦玉海编写，第 3 章至第 5 章由于晓聪编写。第 1 章为恶意代码调查技术概述，主要包括恶意代码概念、主要行为、主要类型及特征、恶意代码的发展、恶意代码案件的发展、典型恶意代码案件的审判等方面的内容。第 2 章介绍病毒案件的调查技术，主要包括计算机病毒概述、编制病毒的相关技术、典型病毒代码分析、病毒案件的调查与取证方法等内容。第 3 章介绍木马案件的调查技术，主要包括木马概念、木马相关技术、典型的木马代码、僵尸网络技术及其最新进展、木马案件的调查与取证方法、木马的防范等方面的内容。第 4 章介绍网页恶意代

码案件的调查技术，主要包括网页恶意代码概述、相关技术、典型的网页恶意代码分析、网页挂马案件的调查与取证方法、网页恶意代码的防范等方面的内容。第5章介绍计算机恶意代码的防范及相关法律法规，主要包括反计算机恶意代码的作用原理、恶意代码防范策略、反计算机恶意代码的软件技术、反计算机恶意代码的取证工具、计算机恶意代码相关法律法规等方面的内容。

由于时间和水平有限，书中错误和不足在所难免，恳请读者批评指正。

编著者

2014年1月

目录

第1章 恶意代码调查技术概述

1.1 恶意代码的定义和类型

1.1.1 恶意代码的定义

恶意代码的英文是 malware，也就是 malicious software 的混成词。恶意代码的定义描述如下：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，它包含了所有带有敌意、插入、干扰正常使用、令人讨厌的程序和源代码。一个程序被看做恶意代码的主要依据是创作者的意图，而不是恶意代码本身的特征。

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，恶意代码具有独特的传播和破坏能力。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性，例如，特洛伊木马具有窃取信息的特性，蠕虫主要利用漏洞传播来占用带宽、耗费资源等。

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中的数据，甚至破坏计算机硬件，给用户带来巨大的损失。

1.1.2 恶意代码类型

大多数恶意代码可以分为病毒、木马、蠕虫或复合型。一个恶意程序可能由汇编语

言、C++、Java 或者 VBA 写成，但是它们仍然可以归入上述主要几类中，除非该程序同时具备上述两种或者多种功能。

1. 病毒

病毒是一种专门修改其他宿主文件或硬盘引导区来复制自己的恶意程序。在多数情况下，目标宿主未按被修改并将病毒的恶意代码的副本包括进去。然后，被感染的宿主文件或者引导区的运行结果再去感染其他文件。

2. 木马

木马，又叫做特洛伊木马，是一种非自身复制程序。它假装成一种程序，但是其真正意图却不为用户所知。例如，用户从网上下载并运行了一个他特别喜欢的多用户游戏，这个游戏看起来很刺激。但它的真正目的可能是将木马装入系统中以便黑客控制用户的计算机。木马并不修改或者感染其他文件。

3. 蠕虫

蠕虫是一种复杂的自身复制代码，它完全依靠自己来传播。蠕虫典型的传播方式就是利用广泛使用的程序（如电子邮件、聊天室等）。蠕虫可以将自己附在一封要送出的邮件上，或者在两个相互信任的系统之间用一条简单的文件传输命令来传播。不像病毒，蠕虫很少寄生在其他文件或者引导区中。

蠕虫和木马有很多共同之处并且很难分辨。两者明显的区别是：木马总是假扮成别的程序，而蠕虫却是在后台暗中破坏；木马依靠信任它们的用户来激活它们，而蠕虫从一个系统传播到另一个系统不需要用户的任何干预；蠕虫大量地复制自身，而木马并不这样做。

4. 研究代码

仅仅用作研究的恶意代码程序最初是在实验室里写的，是用来证明一种特殊的理论或者是专门给反病毒研究者做研究用的，但它们并未流传出去。

1.2 恶意代码的行为

1.2.1 什么是恶意代码的行为

恶意代码的行为是指恶意代码本身的个体表现特征和整体表现特征。有些恶意代码行为不具有危害性，如单纯弹出一个对话框；有些恶意代码行为则具有危害性，如删除用户计算机上的资料信息。

1.2.2 恶意代码行为的主要类型

恶意代码的行为可以分为监视型、破坏型、利用型和窃取型等类型。监视型行为主要有按键监视和远程监视用户的屏幕、音频和视频等。破坏型行为主要有：删除配置文件，

致使计算机不可恢复；远程操作用户的系统；对 win.ini 文件夹特定项的修改；对 system.ini文件的特定项的修改；对注册表特定键值的修改；文件关联；修改注册表；文件打开；文件复制；文件修改等。利用型行为主要有：将用户的计算机作为跳板攻击他人或传播病毒 通过隐藏文件、进程和网络的使用隐藏攻击者的存在等。窃取型行为主要有获取文件资料和硬盘数据共享等。

1.3　恶意代码产生的原因

恶意代码产生的原因多种多样。例如，有的是计算机工作人员或业余爱好者纯粹为了兴趣而制造出来的，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。

总结恶意代码产生的原因，有如下 3 个方面。

1. 技术因素

操作系统漏洞为攻击者提供了落脚点，相当于为攻击者打开了门缝，使攻击者有机可乘。另外，数据与可执行指令的混合，如脚本和宏等，也经常成为恶意代码的攻击途径。

2. 硬件环境因素

硬件环境因素主要是同构计算机环境和计算机环境空前的连通性。当前，计算机的网络构成基本相同，且计算机与计算机之间、计算机与网络之间、网络与网络之间的连通性很发达，传播速度大幅提升，使得恶意代码在计算机与网络上的传播极为畅通，加之网络上的大量数据信息，使管理者很难第一时间发现恶意代码的传播。

3. 人员因素

人员因素主要是缺乏安全意识的用户群和恶意的用户。恶意代码泛滥很大的一个原因是人。有能力的人编写出恶意代码，可能是为了炫耀，也可能是为了赚钱。恶意代码在网络上的流传离不开那些附和者，恶意的网络用户或许是为了恶作剧而大肆传播扩散恶意代码，最终导致了严重的后果。用户的安全意识缺乏也是一个重要的原因。计算机本身区分不出一段代码是正常的还是恶意的，它只执行用户允许的程序代码。具有良好的安全意识是保障计算机免遭恶意代码攻击的一个有效手段。下面是一些基本的安全建议：

(1) 用干净的系统安装盘安装系统，并及时升级漏洞补丁到最新状态。

(2) 用确保干净的应用软件安装程序来安装应用软件，并升级应用软件的各类漏洞补丁。

(3) 第一时间安装好反病毒软件、防火墙和木马专杀工具等各类安全防护软件，开启各类安全保护功能，并升级安全库到最新状态。

(4) 做好操作系统的安全配置和审核策略，譬如合理使用软件限制策略，限制非法软件的运行。

(5) 在系统、应用软件及安全软件安装升级完毕之后，建议使用 Ghost 软件对系统进行备份，以便今后在系统出现安全故障时可以及时地将系统恢复到安全状态。

(6) 使用低权限账户登录系统，遵守"最小权限原则"进行各类日常操作。

(7) 对于疑似威胁操作(如访问可疑的网站和打开可疑的程序)，使用虚拟机或沙箱类软件进行隔离访问。

(8) 相信一切外来数据都是危险的，尽量不要打开来历不明的外来数据文件或程序。

(9) 使用安全的方式打开可移动存储设备，避免来自可移动存储设备的病毒。

(10) 系统出现安全故障之后，及时恢复系统到安全状态(使用 Ghost 类软件或者使用系统还原类软件)。

1.4 恶意代码的类型及特征

1.4.1 病毒

计算机病毒(Virus)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，并能自我复制的一组计算机指令或者程序代码。计算机病毒常宿主于文件或引导区，传播方式主要是通过用户打开文件、读取邮件或执行其宿主文件。计算机病毒具有如下主要特征。

1. 可执行性

计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，因此它享有一切程序所能得到的权力。病毒在运行时与合法程序争夺系统的控制权。计算机病毒只有当它在计算机内得以运行时才具有传染性和破坏性等活性。也就是说，计算机 CPU 的控制权是关键问题。若计算机在正常程序控制下运行，而不运行带病毒的程序，则这台计算机总是可靠的。在这台计算机上可以查看病毒文件的名字，查看计算机病毒的代码，打印病毒的代码，甚至复制病毒程序，都不会感染上病毒。反病毒技术人员整天就是在这样的环境下工作。他们的计算机虽也存有各种计算机病毒的代码，但已置这些病毒于控制之下，计算机不会运行病毒程序，整个系统是安全的。相反，计算机病毒一经在计算机上运行，在同一台计算机内，病毒程序与正常系统程序，或某种病毒与其他病毒程序争夺系统控制权时往往会造成系统崩溃，导致计算机瘫痪。

2. 传染性

传染性是生物病毒的基本特征。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么

病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他计算机进行数据交换或通过网络接触，病毒会继续进行传染。

3. 破坏性

所有的计算机病毒都是一种可执行程序，而这一可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，其具体情况取决于入侵系统的病毒程序。同时计算机病毒的破坏性主要取决于计算机病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

4. 潜伏性

一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周、几个月甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。潜伏性的第一种表现是指，病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘里待上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏；触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

5. 隐蔽性

病毒一般是具有很高编程技巧、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常，好像不曾在计算机内发生过什么。正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散并游荡于世界上百万台计算机中。大部分病毒的代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百或一千字节，而 PC 对 DOS 文件的存取速度可达每秒几百 KB 以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中，使人非常不易察觉。

6. 针对性

计算机病毒一般都是针对特定的操作系统，例如微软公司的 Windows 98、Windows 2000 和 Windows XP。还有针对特定的应用程序的病毒，比较典型的是针对微软公司的 Outlook、IE、服务器的病毒，称为 CQ 蠕虫，通过感染数据库服务器进行传播的，具有非常