HZ BOOKS 华章科技
Mc Graw Hill Education

信息安全技术丛书

恶意软件、Rootkit和僵尸网络

[美] Christopher C. Elisan 著 郭涛 章磊 张普含 张翀斌 译

Malware, Rootkits & Botnets
A Beginner's Guide

- Amazon五星畅销书，恶意软件、rootkit和僵尸网络领域入门经典，译著双馨，10余家安全机构联袂推荐
- 既从攻击者的角度详细介绍了恶意软件的技术原理和攻击方法，又从防御者的角度深入讲[illegible]以及应对各种威胁的解决方案和最佳实践

机械工业出版社
China Machine Press

信息安全
技术丛书

恶意软件、Rootkit和僵尸网络

Malware, Rootkits & Botnets
A Beginner's Guide

[美] Christopher C. Elisan 著 郭涛 章磊 张普含 张翀斌 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

恶意软件、Rootkit 和僵尸网络 /（美）埃里森（Elisan, C. C.）著；郭涛等译 . —北京：机械工业出版社，2013.9
（信息安全技术丛书）
书名原文：Malware，Rootkits & Botnets：A Beginner's Guide

ISBN 978-7-111-43695-9

I. 恶… II. ①埃… ②郭… III. 计算机网格—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2013）第 190948 号

本书是恶意软件、rootkit 和僵尸网络领域的经典入门书，也被誉为是该领域最好的一本书，10 余家安全机构联袂推荐，Amazon 五星畅销书。由国际知名的安全技术专家撰写，中国信息安全测评中心软件安全实验室主任领衔翻译，译著双馨。本书既从攻击者的角度详细介绍了恶意软件的技术原理、攻击流程和攻击方法，又从防御者的角度深入讲解了恶意软件的分析方法以及应对各种威胁的解决方案和最佳实践。书中包含大量案例，不仅实践性强，而且还颇有趣味。

本书共分为四部分。第一部分（第 1 ~ 4 章）迅速导入“基础知识”，介绍当前面临的威胁、主要网络攻击手段，使读者能充分了解什么是恶意软件、rootkit 和僵尸网络。第二部分（第 5 ~ 8 章），是本书核心部分，从更高的视角来讲解以下内容：攻击者的恶意软件操作形式；网络犯罪团体的组织形式；攻击者如何利用现有技术去创建、部署、管理可控的恶意软件和僵尸网络，涵盖整个威胁流程，使读者对恶意软件编写者的思维方式和操作方法有深入了解，极具参考价值。这部分还将阐明普通用户如何于不知不觉中成为网络犯罪组织的参与者，以及攻击者获益链条。第三部分（第 9 ~ 11 章），主要讲解“企业应对方案”，引导读者进一步了解威胁处理方法、提高系统安全性的秘技、了解现有系统安全性的实用性方法，以及识别和缓解潜在威胁的业界最佳实践。第四部分（第 12 章），此部分回顾本书所讲内容，并着重讨论了恶意软件、rootkit 和僵尸网络今后的发展态势，使读者了解目前反恶意软件领域的前沿研究工作。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：高婧雅
北京市荣盛彩色印刷有限公司印刷
2013 年 10 月第 1 版第 1 次印刷
186mm × 240mm · 16.75 印张
标准书号：ISBN 978-7-111-43695-9
定 价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

本书赞誉

本书对于面临网络攻击巨大压力的现今世界来说是一个极大的鼓舞，该书是所有信息技术人员理解当今网络威胁环境的指南。

——张伟钦，趋势科技公司首席开发官

如《孙子兵法》所说，“知己知彼，百战不殆”。Christopher Elisan 的这本书系统地揭示了恶意软件编写者和反恶意软件解决方案供应商的思维过程。Christopher 在书中非常慷慨地分享了他的安全知识和经验。他用自己的亲身经历解释了行业术语、常见的做法、恶意软件分析的各种方法，以及“好人”和“坏人”都会用到的工具和技术。阅读这本书能够帮助读者更好地了解自己和敌人。我认为，对于负责保护主机、应用、网络的安全，避免它们遭受已知和未知威胁的所有安全专家而言，这本书都是必读的材料。

——Chee Tan，Avira 公司业务发展总监

如果在没有牺牲有关数据和系统的关键知识点的情况下，就很难对安全知识进行简化。而 Christopher 能够针对安全中最为复杂的主题进行阐述，并且在没有牺牲关键知识点的情况下进行简化。这本书不仅是初学者必读的，同时也会受到高级用户的喜爱。

——Richard Kohn，赛门铁克公司高级产品经理

该书深入浅出地阐述了反恶意软件厂商的工作，以及他们在与恶意软件编写者之间永无止境的“猫捉老鼠”游戏中遇到的巨大挑战，宏观地展现了如今恶劣的恶意软件环境是多么普遍而又现实。

——David Monaco，Radialpoint 公司信息安全总监

在当今的信息驱动时代，计算机是我们日常使用的工具。智能手机、平板电脑或笔记本电脑能够提高我们的生活品质，我们的生活越来越依赖于这些设备的安全使用。如何确保我们的信息得到妥善保护？ Christopher 用通俗易懂的语言解释了 IT 领域中最令人激动的部分：反病毒世界。通过阅读这本书能够明白如何准备这场斗争。任何想要为自己的安全负责的人都必须阅读这本书。

——Vasco Duarte，Avira Operations 有限责任公司敏捷开发培训教练

这是如今关于恶意软件最好的图书之一。从攻击者和防护者两个角度，细致地阐述了恶意软件技术，并列举了大量的真实案例。如果你是一名初学者，该书可以帮你建立起坚实的知识基础；如果你是专业人士，它会让你相信，你之前实施的工作还不够好，还需要面对未来严峻的挑战；如果你是首席信息官或者 IT 安全经理，它让你更清楚地了解为什么恶意软件的战争很艰巨，为什么需要为它分配更多的预算。

——Lixin Lu，validEDGE 公司首席技术官

本书对于恶意软件以及如何保护你和你的组织免受恶意软件的侵害来说是一个非常好的引子。如果学习各种术语让你觉得疑惑或者担忧，剩余的部分会清晰地解释基础知识，帮助你从“好人”和“坏人”两个角度了解大局。之后，你将会准备评估你的安全状态，识别潜在的恶意软件威胁，并采取措施。

——Roger Harrison，Blue Coat Systems 公司 WebPulse 高级研发总监

如果你正在进入（或想要了解）计算机安全行业，本书是必读的，它能引导你快速地学习威胁环境的所有术语、概念和技术。它准确地阐述了恶意软件的发展历史，以及反恶意软件实验室为解决面临的计算机威胁所采取的努力。

——Jong Purisima，GFI-VIPRE 公司反病毒实验室经理

本书精彩地介绍了威胁智能感知和恶意代码分析的技术与科学。Chris Elisan 通过真实、务实的方法来为读者（无论经验或水平）提供详细的方法论和用于加强读者理解、丰富读者专业知识的例子。随着威胁活动越来越普遍和复杂（威胁着全球越来越多的组织），迅速理解威胁环境的能力将变得不可或缺。

——Will Gragido，RSA 公司威胁观察部门高级经理，《网络犯罪与间谍活动：破坏性多向量威胁的分析》[⊖]作者

这是一本新鲜而非常有见地的专著，概述了今天恶意软件分析过程的所有关键要素。必须拥有。

——Mario Vuksan，ReversingLabs 公司首席执行官

⊖ 英文名为《Cyber Crime and Espionage：An Analysis of Subversive Multi-Vector Threats》，2011 年 2 月 Syngress 出版社出版。——译者注

译 者 序

当今世界信息技术迅猛发展，人类社会正进入一个信息化的新纪元，社会、生活的方方面面对信息资源、信息技术和信息产业的依赖程度越来越大。与此同时，由信息技术发展而带来的网络安全问题，也正变得日益突出。网络安全已经成为关系国家安全的重大战略问题。

《孙子兵法》有云“知己知彼，百战不殆”，如今这句话不仅仅适用于传统意义上的军事战争，在重要性日益凸显的网络信息战中亦是如此。能够掌握更多、更前沿的信息科技技术，就能在未来的信息化军事战争中夺取先机。本书从“己”和“彼”两个角度系统地揭示了恶意软件编写者和反恶意软件解决方案供应商的思维过程，不仅仅描述了恶意软件、rootkit 和僵尸网络的本质、复杂性和危害性，同时还根据作者的亲身体验提供了术语解释、最佳实践、预算建议和行动计划等。

本书首先展现给读者的是当前面临的网络威胁、常见的网络攻击手段，使得读者能够充分了解什么是恶意软件、rootkit 和僵尸网络。然后本书深入探讨了各种恶意软件是怎样被网络犯罪分子所利用，以及如何应对这些恶意软件的威胁。最后本书对恶意软件、rootkit 和僵尸网络的未来进行了展望。

为推动国内的漏洞分析和风险评估工作，提高国家信息安全保障能力和防御水平，中国信息安全测评中心长期跟踪和关注相关领域的理论进展和技术进步，有针对性地精选一些优秀书籍翻译成中文，供国内读者参考借鉴。

本书翻译工作还得到了邵帅、侯元伟、吴健雄、时志伟、董国伟、柳本金、王嘉捷、康凯、连一汉、王眉林等同志的支持和帮助，在此深表感谢。

本书得到了中国信息安全测评中心“漏洞分析与风险评估”专项工程、国家自然科学基金项目（61272493、61100047）的支持。

序

互联网上的虚拟世界与现实世界大不相同。在现实世界中，人们只需要担心周围的犯罪分子，而在网络世界，犯罪分子可能远在世界的另一端。由于互联网的无边界性，网络犯罪往往呈现国际化特征。

如今，计算机病毒和恶意软件开发者不再是那些为了在同行中获取名声和荣誉的业余黑客，而是一些用这种手段赚钱的职业罪犯。这些人想进入所有人的计算机系统，窃取他们的网银支付密码和信用卡账号。

我一生中很大一部分时间都在旅途上，因此也拜访过那些网络犯罪分子活动的聚集区。我到过莫斯科、圣保罗、塔尔图斯、维尔纳、圣彼得堡、北京和布加勒斯特。

我接触过一些地下黑客组织，也与很多警察打过交道，我认为事情并不像表面看起来那么简单。人们认为很多其他的事情需要优先处理（例如针对银行业的攻击），对吗？

对，但是进行深入的调查，会出现更复杂的局面。例如，我在巴西曾经和一个网络犯罪调查官交谈过，我们谈到巴西出现的问题以及圣保罗如何成为世界上最大的网银木马的发源地。

那位犯罪调查官看着我说："我知道这些问题，但是你也应该知道圣保罗是世界著名的谋杀之都，人们经常在街头进行枪战，因此我们应该将有限的精力放在哪里呢？打击网络犯罪，还是打击那些会死人的犯罪活动？"

所有事情都需要综合权衡，将网络犯罪的损失和人员伤亡损失进行权衡的话，就能看出哪一个更重要。

国家执法部门和法律体系很难应对日益增长的网络犯罪，因为他们的资源有限、专业人员有限。由于这些犯罪活动遍布全球，受害者、警察、检举者和法官很难发现所有的犯罪活动。执法部门通常对网络犯罪采取行动迟缓，很少有人因为网络犯罪被拘捕，相比于现实的犯罪活动而言，针对网络犯罪的处罚有时显得太轻。

因为网络犯罪检控的优先级比较低，对网络犯罪实施的处罚经常会拖延，所以就给了那些网络罪犯一个错误的信号。这就是网络犯罪迅速增加的原因。现在，对网络犯罪分子而言，他们被抓和受到处罚的机会微小，但利润却非常丰厚。

那些网络犯罪监管人员（例如圣保罗调查人员）所面临的现实是，必须平衡资源和资金的使用，不可能对每一种威胁都做出响应。对付网络犯罪，关键就是合作。好消息是计算机安全界在应对网络犯罪时已达成默契，竞争对手之间也会互相帮助，虽然这些情况并

不为外界所知，但是安全公司会长期保持互帮互助关系。

表面上，计算机安全厂商之间是一种直接的竞争关系，尤其在销售和市场方面。但是在技术方面，工程师之间都非常友好，相互了解，毕竟全世界范围内仅有几百个顶级的反病毒分析工程师。

这些分析人员在私人会晤、研讨会和安全会议上当面进行沟通；他们也通过加密的邮件、安全的聊天工具在线上进行联系，通过这些方式对发生的安全事件相互交换信息。

表面上，这样做毫无道理，为什么要和竞争对手在如此广泛的范围内进行合作呢？这是因为我们有一个共同的敌人。

我们知道，普通软件公司没有敌人，只有竞争者。但是信息安全领域不一样，竞争关系仍然存在，但这不是主要问题，我们的主要敌人是病毒、蠕虫、垃圾邮件、钓鱼网站的制作者。这些人非常讨厌信息安全人员，并且经常直接攻击我们。我们的工作就是阻止他们，保护用户不受攻击。

在这个领域，所有公司都有一个共同的目标，这就是他们互帮互助的原因。

面对日益变化的网络攻击方法，安全人员需要来自各方的帮助。

这就是互联网的现状，我们是互联网的第一代用户，我们应该尽力使得后代的互联网环境更加安全。

Mikko Hypponen

F-Secure 公司首席研究员

前　言

本书是关于恶意软件、rootkit 和僵尸网络的入门读物，书中讨论的概念深入浅出，容易阅读和理解。学习完本书以后，读者就可以和同事、本领域的专家就恶意软件、rootkit 和僵尸网络进行深入讨论。

本书适用的读者群

本书适合以下人员阅读：负责公司网络和系统安全的人员，需要提升自身的安全专业技术人员，学习相关课程的学生，对恶意软件、rootkit 和僵尸网络感兴趣的用户。

本书涉及的内容

本书将介绍一些关于恶意软件、rootkit 和僵尸网络的概念和主题。什么是威胁？是什么将它们变得如此危险？网络犯罪人员使用的是什么技术？本书还将着眼于使用这些技术对目标进行攻击的网络犯罪，他们是谁？他们在其中担任什么角色？他们怎样成功地窃取钱财？

本书不仅仅包含计算机安全的黑暗面，也讨论了保护组织网络的一些方法，提出了一些切实可行的步骤和规则，以提高组织的安全性。

怎样使用本书

读者可以从头到尾按照顺序仔细阅读本书，这将使读者有更加清晰的思路，因为本书的后续章节都是建立在前面章节的基础上的。但是这不是阅读本书的唯一方法。尽管章节之间是相互联系的，但是对每个章节而言，可以单独阅读以了解本章的主旨，而没有必要顾虑前后章节的顺序。每个章节在一定程度上也是相互独立的，因此如果读者熟悉某一章节的内容，可以直接跳过该章节。本书也可以作为参考书来使用。

本书架构

本书包含四个部分，共 12 章。

第一部分　基础知识

第一部分简单介绍当今我们面临的威胁，介绍网络攻击的手段，使读者充分了解什么是恶意软件、rootkit 和僵尸网络。第一部分包含四章。

第 1 章是背景知识，简单介绍了当前面临的威胁，讨论了恶意软件对人们日常生活的影响，使读者快速地进入恶意软件、rootkit 和僵尸网络的学习之中。

第 2 章展示了丰富的恶意软件世界，首先介绍了恶意软件技术的发展史，重点是最近几年的发展状况，恶意软件如何影响和改变数字世界的，以及我们对计算机信息处理技术的理解。根据恶意软件的行为和目的等不同特征，本章对其进行了不同的分类。

第 3 章介绍了 rootkit 控制目标主机并且隐藏自身的几种常见技术。

第 4 章定义了什么是僵尸网络以及其主要的组件，僵尸网络与攻击者通信的不同方法，僵尸网络利用怎样的网络逃避技术来避免执法部门的检测或查处。

第二部分　恶劣的现状

通过阅读第一部分，读者具有了一定的基础知识，并对相关威胁有了一定了解。第二部分是本书的核心，读者将会从更高的视角来了解以下内容：攻击者怎样操作；网络犯罪团体的组织形式；用现有的技术去创建、部署、管理受其控制的恶意软件和僵尸网络。读者将会了解整个威胁的流程：从恶意软件的产生，攻击目标的选择，通过不同的感染载体进行部署，感染系统，到最终执行恶意软件。第二部分也将阐明普通用户怎样不知不觉地成为网络犯罪组织的参与者，以及攻击者如何从恶意行为中获益。第二部分包括四章。

第 5 章介绍了威胁生态系统的概念及其构成，不仅讨论了高级可持续威胁的组成元素，而且包括了其幕后的犯罪分子。该章还深入阐述了这些犯罪分子怎样利用受控主机赚钱，怎样出售窃取的数据，怎样利用普通人作为“洗钱者”来洗钱。

第 6 章深入讨论了日益增加的恶意软件幕后到底隐藏着什么，恶意软件的数量从前些年的屈指可数到今天的五位数规模。该章讨论了能创造大量的恶意软件，并使它们具备免杀能力的各种工具和方法。为了更好地理解上述工具和方法如何逃过反病毒软件的检测，该章还揭示了反病毒软件常用的特征检测技术。该章还带领读者走进恶意软件工厂，了解大规模生产恶意软件的方法。

第 7 章描述了恶意软件是如何侵入系统内部的。该章列举并剖析了恶意软件攻击目标系统所采用的不同方法和技术，也就是感染载体。

第 8 章讨论了恶意软件成功入侵目标系统后所会做的一些事情，主要讨论恶意软件如何感染系统和系统一旦感染后恶意软件的一些行为。

第三部分　企业的应对

通过前两部分内容，读者对犯罪集团如何利用恶意软件、rootkit 或僵尸网络来攻击目标系统应该有了一定的了解，第三部分将引导读者进一步了解应该如何处理这些威胁，以及如何提高系统的安全性。该部分还介绍了理解现有系统安全性的实用方法，以及如何使用产业界的最佳实践方法来识别和缓解系统面临的潜在威胁。第三部分包含三章。

第 9 章介绍了以下基本概念：通过分析系统资产的价值以及它成为攻击者的重要目标的原因，来阐述应该如何保护组织的计算机系统；通过引入基于系统资产的价值和组织当前的网络安全状况等参数来度量系统安全性的“事故响应机制”，阐述如何处理和解决可能存在的威胁。

第 10 章通过网络和主机中的异常现象来检测和识别可能存在的威胁，并基于攻击的指令对这些威胁进行分类，因此使得受威胁的系统受到保护，并且采取合适的缓解技术。

第 11 章是关于威胁的缓解。组织可以通过快速响应来缓解遭受的威胁，也可以通过更具有防御性的方法来缓解威胁，例如定期进行安全审计和用户安全意识培训等。

第四部分　结束语

第四部分讨论威胁的未来发展趋势。该部分基于目前的趋势，近期和长期的技术发展，以及恶意软件技术的发展，讨论了恶意软件、rootkit 和僵尸网络今后的发展态势。该部分也使得读者了解目前反恶意软件领域的前沿研究工作，并明白这是在“好人”与攻击者之间永不停歇的战斗。第四部分包括以下内容。

第 12 章回顾本书所讨论的内容，并对恶意软件、rootkit 和僵尸网络的未来进行展望。

附录 A 描述了基于 BIOS（Basic Input Output System，基本输入 / 输出系统）和基于 EFI（Extensible Firmware Interface，可扩展固件接口）的启动过程。

附录 B 包含了恶意软件、rootkit 和僵尸网络的相关网络链接。

词汇表包含了与安全相关的定义和读者阅读本书过程中用到的术语。

关于标识

本书中有一些特殊的标识，希望能够帮助读者更好地阅读本书。

术语

“术语”帮助读者熟悉常见的信息安全领域的词汇，避免那些不熟悉的词汇或者表达影响阅读。

目　录

本书赞誉
译者序
序
前言

第一部分　基础知识

第 1 章　背景知识……1
1.1　一次恶意软件遭遇……1
1.2　目前所面临的威胁概述……2
1.3　对国家安全构成的威胁……3
1.4　开启旅程……4
1.5　本章小结……5
参考文献……5

第 2 章　恶意软件简史……6
2.1　计算机病毒……6
2.1.1　计算机病毒的分类……7
2.1.2　早期挑战……11
2.2　恶意软件……12
2.2.1　恶意软件分类……12
2.2.2　恶意软件的发展……21
2.3　风险软件……24
2.4　恶意软件开发套件……25
2.5　恶意软件的影响……26
2.6　本章小结……26

第 3 章　rootkit 的隐藏……28
3.1　什么是 rootkit……28
3.2　环境的结构……29
3.2.1　操作系统内核……29
3.2.2　用户态和内核态……29
3.2.3　ring……30
3.2.4　从用户态转换到内核态……30
3.3　rootkit 的类型……33
3.3.1　用户态 rootkit……33
3.3.2　内核态 rootkit……34
3.4　rootkit 技术……34
3.4.1　hooking……34
3.4.2　DLL 注入……37
3.4.3　直接内核对象操纵……38
3.5　应对 rootkit……38
3.6　本章小结……39

第 4 章　僵尸网络的兴起……41
4.1　什么是僵尸网络……41
4.1.1　主要特点……42
4.1.2　关键组件……43
4.1.3　C&C 结构……44
4.2　僵尸网络的使用……48
4.2.1　分布式拒绝服务攻击……49
4.2.2　点击欺诈……49
4.2.3　垃圾邮件转发……50
4.2.4　单次安装付费代理……51

4.2.5 大规模信息获取……52
4.2.6 信息处理……52
4.3 僵尸网络的保护机制……53
4.3.1 防弹主机……53
4.3.2 动态 DNS……54
4.3.3 Fast-Fluxing 技术……54
4.3.4 域名变化地址……57
4.4 对抗僵尸网络……59
4.4.1 技术战线……60
4.4.2 法律战线……61
4.5 本章小结……63
4.6 参考文献……64

第二部分 恶劣的现状

第 5 章 威胁生态系统……65

5.1 威胁生态系统组成……65
5.1.1 技术因素……66
5.1.2 人为因素……74
5.1.3 威胁生态系统的演进……78
5.2 高级持续性威胁……79
5.2.1 攻击方法……79
5.2.2 攻击的收益……82
5.3 恶意软件经济……84
5.4 本章小结……86

第 6 章 恶意软件工厂……89

6.1 逃避反病毒检测的必要性……90
6.1.1 恶意软件事件处理过程……91
6.1.2 恶意软件检测……98
6.1.3 反病毒产品绕过技术……101
6.2 建立恶意软件军队的必要性……111
6.2.1 下一代恶意软件工具套件……111
6.2.2 独立的防护工具……112
6.2.3 恶意软件装甲军队的作用……114
6.3 恶意软件工厂……115
6.3.1 恶意软件流水线……115
6.3.2 攻击者工具的获得……119
6.3.3 恶意软件日益泛滥……120
6.4 本章小结……121

第 7 章 感染载体……123

7.1 感染载体概述……123
7.1.1 物理媒介……125
7.1.2 电子邮件……127
7.1.3 即时通信和聊天软件……130
7.1.4 社交网络……132
7.1.5 URL 链接……134
7.1.6 文件共享……140
7.1.7 软件漏洞……141
7.2 变成感染载体的可能性……143
7.3 本章小结……144

第 8 章 受感染系统……146

8.1 恶意软件感染过程……146
8.1.1 安装恶意软件文件……150
8.1.2 设置恶意软件的持久性……154
8.1.3 移除恶意软件安装证据……155
8.1.4 向恶意软件传递控制权……156
8.2 活跃的恶意软件……157
8.2.1 在系统中长期潜伏……158
8.2.2 和攻击者通信……161
8.2.3 执行有效载荷……163
8.3 本章小结……164

第三部分　企业的应对

第 9 章　组织保护……167

9.1　威胁事件响应者……168
9.2　理解系统的价值……169
9.2.1　系统对于组织的价值……169
9.2.2　系统对于攻击者的价值……173
9.3　理解系统的特征……175
9.3.1　系统类型……176
9.3.2　运营影响……177
9.3.3　主机数据的敏感度……178
9.3.4　系统用户……179
9.3.5　网络位置……179
9.3.6　资产的可访问性……179
9.3.7　资产访问权限……180
9.3.8　系统恢复……180
9.3.9　系统状态……180
9.4　设置系统优先级……180
9.5　企业安全态势……181
9.6　了解遭受攻击的代价……181
9.6.1　直接损失……182
9.6.2　间接损失……182
9.7　系统保护……183
9.7.1　威胁建模……183
9.7.2　识别合适的解决方案……184
9.7.3　前置式威胁检测……188
9.8　建立事件响应计划……190
9.8.1　识别不同的受害场景……191
9.8.2　识别解决方案模式……191
9.8.3　定义角色和职责……192
9.8.4　建立草案……193
9.8.5　定期演习……195
9.8.6　评审和改进……195
9.9　把一切付诸行动……196
9.10　保护之外……197
9.11　本章小结……197

第 10 章　检测威胁……199

10.1　建立基准……199
10.1.1　建立网络基准……199
10.1.2　建立主机基准……200
10.2　检测异常……200
10.2.1　检测网络异常……202
10.2.2　检测主机异常……202
10.3　隔离异常源……203
10.4　深入分析受感染资产……203
10.4.1　精确定位恶意软件……203
10.4.2　基于攻击意图对恶意软件进行分类……210
10.5　本章小结……211

第 11 章　缓解威胁……212

11.1　威胁缓解……212
11.2　立即式响应……213
11.2.1　隔离……214
11.2.2　验证……214
11.2.3　威胁的检测和分类……214
11.2.4　修复和恢复……215
11.3　先应式响应……216
11.3.1　预防措施……216
11.3.2　定期进行安全审计……224
11.4　内部威胁……224
11.4.1　什么是内部威胁……224
11.4.2　缓解内部威胁……225
11.5　保持警惕……227
11.6　本章小结……227

第四部分　结束语

第 12 章　永不停歇的战斗……229

12.1　本书回顾……229
12.2　未来展望……230
12.2.1　恶意软件的未来……231
12.2.2　rootkit 展望……234
12.2.3　僵尸网络的未来……234
12.3　好人们也很忙……235
12.4　冒险才刚刚开始……235
12.5　本章小结……236

附录 A　系统启动过程……237

附录 B　有用的网络链接……240

词汇表……242

第一部分

基 础 知 识

第1章 背景知识

本章主要内容

- 目前所面临的威胁概述
- 恶意软件对国家安全的威胁

本章首先简要介绍恶意软件、rootkit和僵尸网络，使读者对其有初步了解。作为一名逆向分析工程师和恶意软件研究者，我首先将介绍第一次遇到恶意软件的情形，那次经历激起了我的好奇心，并且这种好奇一直贯穿我的整个职业生涯。本章最后简要阐述人们面临的威胁，以及恶意软件对国家安全的威胁。

1.1 一次恶意软件遭遇

不知道从哪一天开始，我们的生活开始受到恶意软件的影响。我们中的每个人可能都记得第一次遭遇恶意软件时的场景。当时我有一台IBM兼容机，配置是80386SX架构、256MB硬盘和4MB内存，并且有两个5.25英寸和一个3.5英寸软盘驱动器，一台14英寸的黑白VGA显示器，一台爱普生点阵打印机。操作系统是DOS 6.22，在其上运行着Windows 3.11。这台机器对我来说很有用，我经常在这台机器上写一些Pascal、C和汇编语言程序。

偶尔，我会和一些被病毒感染的软盘不期而遇，例如STONED、Jerusalem和Brain病毒。但是McAfee反病毒软件能够处理这些病毒，因此我的电脑还是可以正常工作，并且还能使用WordPerfect编辑文件和玩一些带有MIDI声效的游戏。但是有一天，当我使用

Windows 3.11 时，计算机突然死机，完全没了反应。我看到的是一系列软件错误信息，我重启了机器并用 McAfee 进行杀毒，但是没有检测到任何病毒信息。我接着运行了 WIN.COM 试图启动 Windows 3.11，但是过了一分钟左右还是显示同样的错误信息。我用大约 10 张 3.5 英寸软盘又重新安装了 Windows 3.11，但是问题仍然存在。我完全不知道下面该怎么办。第二天我将计算机带到一个朋友那里，他开了一家计算机商店。他使用升级过 SCAN.DAT 的 McAfee 杀毒软件扫描了整个系统，找到了一种名为 DIE-HARD 2 的病毒。它感染了 Windows 3.11 的可执行文件和相关组件。因为 DIE-HARD 2 是一种 DOS 病毒，它的格式与 Windows 3.11 的不同，该病毒实际上破坏的是 Windows 3.11 的相关组件，因此，系统会显示软件错误信息。

术语 SCAN.DAT 是 McAfee 的病毒特征文件，也就是第一代 DAT 文件。

此次经历使我对病毒、病毒的本质以及病毒的工作原理产生了强烈的好奇心和浓厚兴趣。我以前修改 DOS 的 COMMAND.COM 文件使它显示一些有趣的错误信息、倒腾 Norton 组件的爱好逐渐被对病毒的好奇心所代替，直到它最终变成我的职业。在计算机工程系拿到学士学位后，由于具有汇编语言方面的专长，我进入了趋势科技公司，从此站在了与恶意软件斗争的第一线。

加入趋势科技公司以后，我了解到病毒和恶意软件技术的发展和巨大影响，这使我大开眼界。它使我清醒地认识到病毒对个人、商业以及执法部门所带来的严重威胁。在这家公司我和一个专家组一起工作，致力于解决当前世界所面临的恶意软件问题，这是一件非常有意思的事情。我们面临的威胁发展得如此迅速，唯一解决的途径就是不断学习和适应，否则，终将会被淘汰。不断学习是必需的，熟悉这种威胁的发展趋势也是有必要的。

1.2 目前所面临的威胁概述

恶意软件仍然是一种不容小觑的力量，并且计算机技术的发展并没有使其消亡。相反，恶意软件不断充分利用各种新技术，不断发展壮大。例如，电子邮件彻底颠覆了人们在全世界范围内发送信息的方式，它被用来在全球范围内快速传播恶意软件。社交网络站点发布的某些信息会将用户导向一些恶意的网址，而这些网址会自动在用户不知情的情况下，在系统上安装恶意软件。在以前的会议演讲中，我曾经展示过利用 Twitter 来控制那些驻留在目标系统中的恶意软件。除此以外，恶意软件也在不断增强自身的保护能力。技术的发展使得恶意软件能够逃避检测和分析，并且使得它们在渗透进入高价值目标时变得几乎不可阻挡。我在以前的会议演讲中还谈到，一些新的自保护技术使得检测恶意软件越来越困