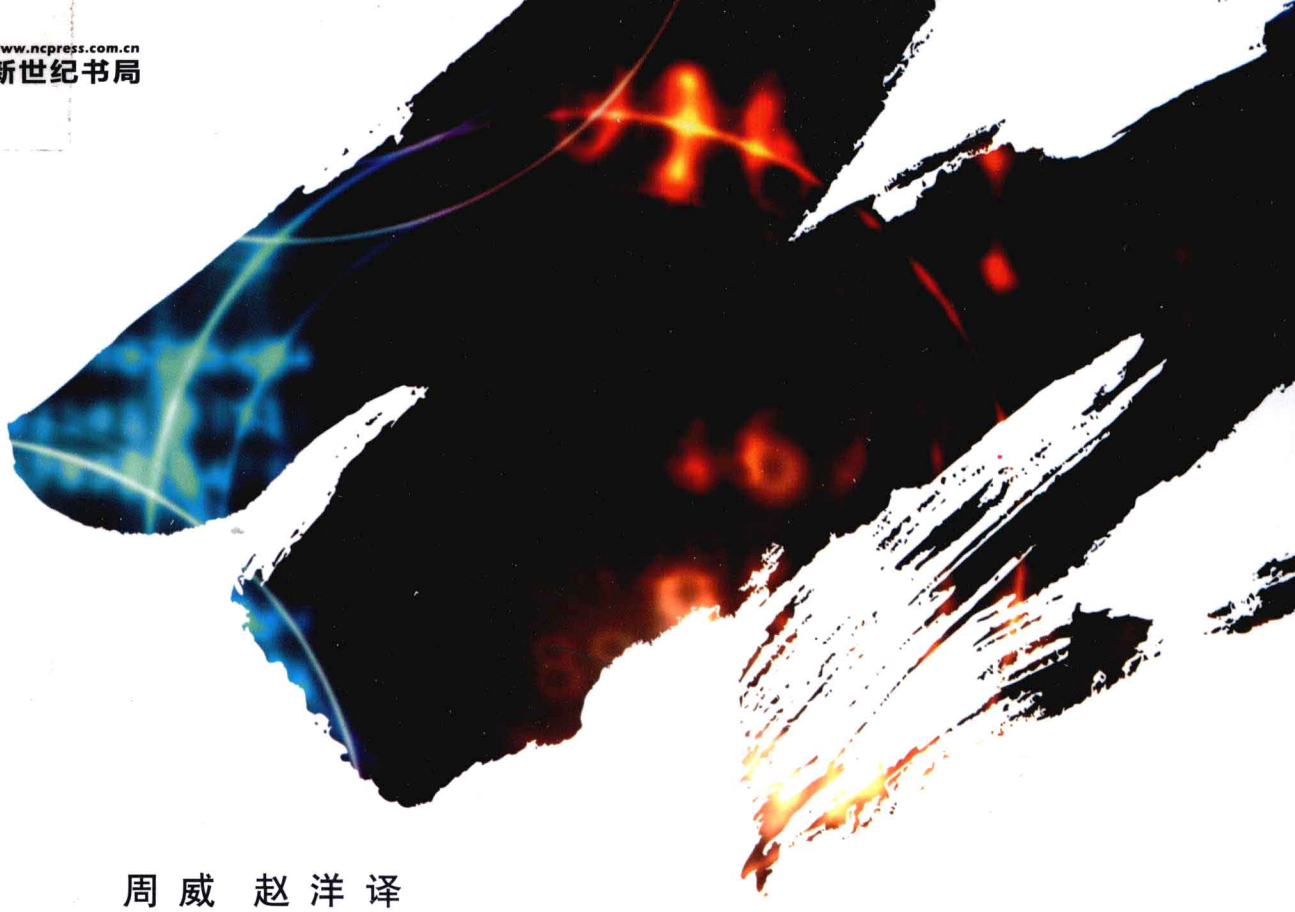
www.ncpress.com.cn
新世纪书局



周威 赵洋 译

移动恶意代码

攻击与防范

Mobile Malware Attacks and Defense

Ken Dunham, Saeed Abu-Nimeh, Michael Becher, Seth Fogie
Brian Hernacki, Jose Andre Morales, Craig Wright 著

科学出版社

Mobile Malware Attacks and Defense

移动恶意代码攻击与防范

Ken Dunham
Saeed Abu-Nimeh, Michael Becher
Seth Fogie, Brian Hernacki
Jose Andre Morales, Craig Wright
著

周 威 赵 洋 译

科 学 出 版 社
北 京

图字：01-2010-2756 号

Mobile Malware Attacks and Defense
Ken Dunham，et al.
ISBN-13：9781597492980

ISBN：9789812727053

图书在版编目(CIP)数据

移动恶意代码攻击与防范 /（美）敦汉姆（Dunham，K.）等著；周威，赵洋译 .—北京：科学出版社，2012.6

书名原文：Mobile Malware Attacks and Defense

ISBN 978-7-03-034575-2

Ⅰ.①移… Ⅱ.①敦… ②周… ③赵… Ⅲ.①移动电话机－安全技术 Ⅳ.①TN929.53

中国版本图书馆 CIP 数据核字（2012）第 114839 号

责任编辑：田慎鹏 霍志国 / 责任校对：张 林
责任印制：华 程 / 封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京市鑫山源印刷有限公司
科学出版社发行 各地新华书店经销
*
2012 年 6 月第 一 版 开本：787×1092 1/16
2012 年 6 月第一次印刷 印张：23
字数：447 000

定价：59.00 元
（如有印装质量问题，我社负责调换）

技术作者

Ken Dunham（CISSP，GSEC，GREM，GCFA，GCIH 金奖荣誉获得者）具有超过十年的信息安全一线工作经验。作为提供安全风险分析和服务的 iSIGHT Partners 公司的全球响应中心主管，他负责监管所有全球网络威胁响应业务。Dunham 先生经常会就当前一些最新出现的安全风险向联邦政府和私营机构的网络安全部门高层做介绍，此外，他还与地缘政治和漏洞研究专家保持定期沟通，广泛汇总恶意代码情报并将重大的网络威胁通知新闻媒体。2006 年，某主流传媒公司评价其为“全球最受关注的恶意代码问题专家”。

Dunham 先生会经常发现一些新的恶意代码，他的日常工作还包括为麦金塔电脑（Macintosh）撰写反病毒软件，为 About. com、SecurityPortal、AtomicTangerine、Ubizen、iDEFENSE 和 VeriSign 编写恶意代码。他是互联网社区反病毒支持的先驱者之一，其网站被雅虎网络生活杂志、PC Week、美国在线等评为最好的全球资源。Dunham 先生还是 HTCIA（高科技犯罪调查协会）、GE TS. & WPS（政府应急通信和无线优先服务）、AVIEN、Virus Bulletin、InfraGard、RCG Information Security Think Tank、CME 和许多其他非官方信息领域的重要成员。2005 年和 2006 年，Dunham 先生分别参与了美国中央情报局“寂静地平线（Silent Horizon）”互联网军事演习（蓝军身份）和美国国土安全部“网络风暴（CyberStorm）”网络战演习（观察员身份）。

Dunham 先生是公认的逆向工程专家，他会对客户网络所面临的突发性漏洞利用和恶意代码风险及攻击进行常规分析。作为 Wildlist（病毒清单）组织的报告者，他每月都会向该组织提供病毒事件报道。Dunham 先生与人合著了多部著作，同时也是信息安全杂志专栏作家。此外，他还是 ISSA（信息系统安全协会）及 InfraGard（美国联邦调查局的附属机构）的爱达荷州分会创始人。

Ken Dunham 撰写了第 1，2，3 章和第 6 章。

撰 稿 人

Saeed Abu-Nimeh 是南方卫理公会大学（Southern Methodist University）的博士研究生。他的研究重点是互联网和电子邮件安全。他对网络钓鱼和网址嫁接攻击很感兴趣，并研究开发了阻止电子身份盗窃和防范各类针对移动用户攻击的解决方案。他是 IEEE、APWG（反网钓工作组）和 SMU HACNet（高可靠计算和网络）实验室的成员。

Saeed 撰写了第 6 章（部分内容）。

Michael Becher 于 2006 年获得德国亚琛工业大学（RWTH Aachen University of Technology）计算机科学硕士学位。目前，他是德国曼海姆大学（University of Mannheim）的在读博士生，参与由移动网络运营商 T-Mobile 资助的移动设备安全性研究项目，移动恶意软件及通用软件的动态分析是其主要研究课题之一。Michael 曾致力于安全领域的其他若干课题，并撰写过一篇有关通过 FireWire 直接内存访问的论文和一本网络应用防火墙方面的书籍。

Michael 撰写了第 8 章。

Seth Fogie 是 Airscanner 公司副总裁，负责监管 Windows Mobile（Pocket PC）平台安全软件的开发。与他人合著了众多信息安全技术方面的书籍，其中包括由 Sams 出版社出版的畅销书《深度无线网络安全》（*Maximum Wireless Security*）和 *Windows Internet Security*：*Protecting Your Critical Data*（《Windows 互联网安全：保护您的关键数据》），O'Reilly 出版社出版的 *Security Warrior*（《防黑战士》），以及 Syngress 出版的 *Cross Site Scripting Attacks*：*XSS Exploits and Defense*（《跨站脚本攻击：XSS 攻击和防御》）。Seth Fogie 经常在各类 IT 和安全会议、研讨会上做报告，包括黑帽大会（Black Hat）、Defcon、CSI 和 Dallascon（达拉斯无线网络安全会议）等。此外，Seth 还参与了得克萨斯医学协会（Texas Medical Associate）HIPAA 医学教育课程的制定。他负责 InformIT. com 网站的安全，并在该网站上发表、评论、维护与安全相关的文章、书籍和信息。

Seth Fogie 撰写了第 7 章和第 10 章。

Brian Hernacki 是赛门铁克研究院（Symantec Research Lab）的产品架构师，在那里他与一支专业团队共同研发未来新技术。Hernacki 在计算机安全和企业软件开发领域有 10 年以上的经验。他曾在多个信息安全领域负责商业和非商业产品的研发，包括入侵检测与分析技术、蜜罐技术，以及无线和移动技术。Hernacki 以优异的成绩获得了密歇根大学计算机工程学士学位。

Brian Hernacki 撰写了第 11 章。

Jose Andre Morales 博士毕业于佛罗里达国际大学（Florida International University）计算机科学专业，主要研究基于自我复制的计算机病毒检测。他专注于移动设备的病毒检测并开发相应的反病毒解决方案。他是 Sigma Xi 科学研究会、Upsilon Phi Epsilon、ACM（美国计算机协会）和 IEEE 的会员。他也是 Computing Hispanic Ph. D. Mailing List（西班牙计算机博士邮件列表）的创始人之一。

Jose 撰写了第 3（部分内容），4，5 章。

Craig Wright 是 BDO Kendalls（NSW-VIC）Pty 有限公司风险咨询服务部门副主管。他撰写过大量 IT 安全方面的文章和书籍。他设计了世界上第一个网上娱乐场（Lasseter's Online）的架构。设计并维护了多个旨在保护澳大利亚证券交易所安全的系统。此外，他还为印度马辛德拉集团（Mahindra and Mahindra，印度最大的汽车制造商）制定了安全政策及流程。马辛德拉集团涉足汽车、拖拉机制造、IT 外包等多个商业领域，集团员工总数超过 50 000 人。Craig 是为数不多的通过了 GSE（GIAC Security Engineer）认证的专业人员，目前，他已经拥有 27 个 GIAC 认证证书，正在为第八个 GIAC Gold paper 而努力。

Craig Wright 撰写了第 9 章。

致谢/贡献者

作为本书的作者，我们由衷感谢来自计算机安全领域的众多同仁，感谢他们在移动恶意代码产品及服务的开发上持续不断的努力以及对我们的支持，感谢他们为本书提供的列表、资料和很多私人资源。下列人员在本书中贡献突出：

Collin Mulliner 是一名程序员、白帽黑客和专职安全研究人员。移动设备（特别是智能手机）及移动网络的安全性是他的重点研究领域。近年来，Collin 在蓝牙安全方面做了很多研究和开发工作，他创造了第一个蓝牙端口扫描器。从 1997 年至今，Collin 参与完成的项目已涉及绝大多数现有的移动设备平台。2006 年，Collin 获得了美国加州大学圣巴巴拉分校（University of California at Santa Barbara）计算机科学硕士学位。

第 7 章的 Palm 和 J2ME 相关内容由 Collin Mulliner 撰写。

Ralf Hund 是德国曼海姆大学数学和计算机科学专业的在读硕士。作为曼海姆大学“可靠分布式系统实验室（Laboratory for Dependable Distributed Systems）”的一名学生助理，他参与并开发了针对 Windows Mobile 平台的沙盒方案等多项工作。他对 IT 安全（例如软件安全、恶意软件静态分析和恶意软件动态分析）的实践尤为感兴趣。

Ralf 在 Windows 和 Linux 系统的逆向工程及编程方面有 10 年以上的经验，特别是对底层技术细节很有研究。

第 8 章针对移动恶意代码行为分析的技术部分由 Ralf Hund 撰写。

此外，我们还要感谢 Mikko H. Hypponen、Fred Doyle、Joep Gommers 和 Josh Murray 在对本书的技术审查方面所提供的帮助。

目　录

第 1 章
移动恶意代码介绍

本章解决：

- 移动恶意代码问题日趋重要
- 移动恶意代码威胁介绍
- 移动安全领域专业术语

☑ 小结
☑ 快速解决方案
☑ 常见问题

引言

进入新世纪，智能手机、PDA 以及其他手持嵌入式设备如 iPhone 等不断推陈出新、增速惊人。伴随着移动设备、移动用户以及移动市场的蓬勃发展，移动恶意代码也找到了生根、发芽的土壤，移动领域中的数字犯罪、网络诈骗等活动日趋成熟、不断蔓延。

早在新世纪伊始的 2000 年甚至更早些时候，就有一些专家对移动设备的安全前景表示过深深的担忧，他们曾预言将会很快爆发针对智能手机和其他移动设备的大规模攻击。一晃数年过去，现在再回头看，我们发现这些专家的预言在很大程度上都错了。事实证明，组织一次大规模的移动攻击仅靠发现、利用技术上的漏洞是远远不够的，它所需要的各种条件、因素远远超出了人们当初的理解。其实，这一点在传统计算机安全领域也曾被屡次证实。时光荏苒，随着近年来移动解决方案、移动服务提供商的快速成长，移动用户的迅速增长，全球移动市场资金规模的日益扩大，网络犯罪分子们也纷纷逐利而来。依据之前的经验教训，我们有理由相信，对于移动安全这一新兴领域，在它完全成熟之前，一定会经历更严重的阵痛、面临更严峻的考验。

本书是业界第一本定位于移动设备安全的书籍。当前，已经开始有一些国际会议议题关注、探讨相应的移动安全解决方案。随着移动技术的快速演进、技术人员（包括黑客）能力的不断提高以及全球网络犯罪黑市的日益成熟，普通用户也是时候该采取行动了。本书将带领读者了解一些基本的移动安全和移动恶意代码知识，并且提供了相应的防范策略和建议，希望这些内容能够帮助读者成功减少移动安全方面的威胁和风险。

警 告

本书包含漏洞利用和恶意攻击的讨论内容。请谨慎处理书中与此相关的代码和数据，并请依据道德和法律准则使用它们。同时，我们也已尽了最大的努力消除和弱化这些代码、数据的攻击性，以降低它们被非法和不道德滥用的可能性。

章节内容按照由易至难、循序渐进的方式安排。前 5 章不需要过多的专业基础，适合普通读者阅读。第 6 章，我们介绍了用于鉴别和防范网络钓鱼的数