走近安全

网络世界的攻与防

360企业安全研究院◎著

读网络安全科普书 看网络安全新鲜事

洞悉无处不在的威胁 掌握保护自己的武器

让网络更安全 让世界更美好

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

走近安全

网络世界的攻与防

360企业安全研究院◎著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

网络安全与我们息息相关，如何更好地理解网络安全，看清国家以及社会各行各业、各企事业单位和个人面临的网络安全形势与问题，找到网络安全风险与隐患的应对之道，应是我们思考的重要命题。本书以解读网络安全为主线，从安全简史、威胁无处不在——个人篇、威胁无处不在——政企篇、现代网络安全技术导论、现代网络安全技术——个人篇、现代网络安全技术——政企篇、网络安全体系建设与制度建设、全球主要安全会议与安全赛事简介几部分深入浅出地介绍网络安全相关知识，结合大量研究数据和案例，探寻网络世界的攻与防。

本书可供政企机关管理人员、安全部门负责人，网络与信息安全相关科研机构研究人员，高等院校相关专业教师、学生，以及其他对网络空间安全感兴趣的读者学习参考。

图书在版编目（CIP）数据

走近安全：网络世界的攻与防 /360 企业安全研究院著. —北京：电子工业出版社，2018.7
ISBN 978-7-121-34270-7

Ⅰ. ①走… Ⅱ. ①3… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 109339 号

策划编辑：戴晨辰
责任编辑：戴晨辰　　文字编辑：郭　枫
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：720×1000　1/16　印张：18.25　　字数：296 千字
版　　次：2018 年 7 月第 1 版
印　　次：2018 年 7 月第 1 次印刷
定　　价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

序

Foreword

创新思路　把握安全

1946 年，世界上第一台电子计算机的诞生迎来了信息时代的晨曦；1969 年，互联网前身“阿帕网”的诞生开启了信息沟通的“地球村”时代。网络如同一把双刃剑，用得好，它是阿里巴巴的宝库，一声“芝麻开门”，有取之不尽的财富；用得不好，它是潘多拉的魔盒，装着灾难幽灵，不仅会影响人们的日常生活，而且会危及社会稳定与国家安全。网络安全问题从来没有像今天这样受到全社会的关注，不仅成为社会的热点，也是学术界、工业界、大众传媒等关心的焦点领域。

我国已有超过 7 亿的网民，正如习近平总书记指出的，这是一个了不起的数字，也是一个了不起的成就。2016 年，《国家网络空间安全战略》发布，2017 年，《中华人民共和国网络安全法》正式实施，网络安全建设成为各行业发展不可或缺的一环。

由于网络安全涉及学科众多，产业链错综复杂，技术与产品日新月异，不要说非专业人员，即便是信息领域的专家，想要准确应对网络安全威胁，拥有完备的安全防护理念，实现有效处置网络安全问题，仍面临巨大挑战。

做好网络安全工作，“人”的因素是第一位的。面对新挑战、新课题，一方面需要尽快提高各行业从业人员，尤其是高级管理人员、领导干部对网络安全的理解水平；另一方面，也需要教育部门尽快培养计算机与网络安全相关学科专业人

才，以适应、满足当前国家和社会对网络安全人才的迫切需要。

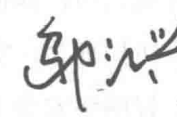
2015 年，“网络空间安全”正式列为一级学科；2016 年，包括战略支援部队信息工程大学在内的 29 所高校，成为我国首批拥有“网络空间安全”一级学科博士学位授权点的高校。2017 年 9 月，《一流网络安全学院建设示范项目管理办法》发布，正式提出我国在 2017—2027 年期间实施一流网络安全学院建设示范项目，形成 4~6 所世界一流网络安全学院。这些措施为新时代加强网络安全教育与人才培养，奠定了良好的基础。

然而，日益增长的社会人才需求仅靠相关院校体系化的教育培养是远远不够的，还需要推进产学合作、创新育人的培养模式。例如，高等院校、科研机构与行业企业，在课程设置、教材编写、实验室建设、实训演练等各个环节加强深度合作，发挥各自优势，强化协同效益，从而为国家和社会输送更多实战型网络安全人才。同时，也为培养重视网络安全、理解网络安全、践行网络安全责任的各行业管理人才、各领域从业人员，探索新模式、新路径。

网络安全的普及教育离不开优秀教材，也离不开大众科普读物。360 公司作为国内网络安全企业的佼佼者，具备良好的互联网安全技术研发能力与创新实力，在大数据、云计算、网络技术攻防、反网络欺诈等关键领域拥有长期的经验和知识积累。

本书由 360 企业安全研究院撰写，是对网络安全复杂理论体系的一次全方位科普解读，内容涉及个人安全、企业机构安全、国家关键信息基础设施安全等众多方面，覆盖范围广，内涵丰富，讲述方式新颖，是网络安全领域值得一读的科普书。本书既可作为高等院校网络空间安全方向的参考教材，也可作为行业管理人员、科技人员，以及对网络空间安全感兴趣的读者的参考读物。

希望这本书的出版能使更多的人认识和了解网络安全，激发更多的有志者投身网络安全事业，在各自的岗位上为网络强国战略贡献力量！



中国工程院院士

前言

Preface

互联网应用的快速普及与政企机构信息化建设的不断深入，使得网络安全问题日益凸显，越来越多的人开始关注网络安全。

作为现代互联网技术的一个独特分支，网络安全技术的专业性、对抗性很强，普通大众往往难以理解其中的奥秘。但从科普的角度，从基本原理的层面理解网络安全威胁，理解网络安全技术，对于提高大众的安全防范意识，加强网络安全管理是十分必要的。

本书是一本面向领导干部、政企机构管理人员的网络安全科普读物。本书从安全简史、威胁无处不在——个人篇、威胁无处不在——政企篇、现代网络安全技术导论、现代网络安全技术——个人篇、现代网络安全技术——政企篇、网络安全体系建设与制度建设、全球主要安全会议与安全赛事简介几部分，系统、全面地介绍网络安全领域的基础知识，希望能够帮助读者初步了解网络安全工作的重要性及基本方法论。

本书通俗易懂，书中对所有安全问题、安全技术的介绍不涉及复杂的技术细节，重点介绍主要现象、基本原理和最终结果。作为一本科普读物，读者不需要具备通信、计算机或网络安全方面的专业知识，即可顺畅阅读本书的绝大部分内容。

本书主要编写思路如下。

在网络安全威胁与安全技术的介绍部分，由于普通个人面临的安全问题及解决办法与政企机构存在很大的区别，因此本书区分个人安全与政企安全两个方向分别进行介绍。

在个人安全威胁方面，本书主要介绍安全漏洞、病毒木马、恶意网页、网络诈骗和物联网威胁等；在政企安全威胁方面，本书主要介绍木马病毒、网站漏洞、信息泄露、DDoS 攻击、网络扫描、邮件攻击、工业互联网和高级网络威胁等。

在针对个人的现代网络安全技术方面，本书主要介绍云查杀、白名单、人工智能引擎和主动防御等关键技术；在针对政企机构的现代网络安全技术方面，本书主要介绍边界防御与控制、终端安全与管控、BYOD 问题的解决、虚拟化安全、认证与加密、邮件安全、漏洞扫描与防护、漏洞的人工挖掘、DDoS 监测与防御、威胁态势感知、网络安全靶场及工业互联网防护等方面的关键技术。

本书在介绍网络安全基础知识的同时，还专门用一章的篇幅介绍现代网络安全技术的基本思想和方法论，以帮助读者系统理解各种网络安全威胁和网络安全技术之间的联系。

此外，本书还针对网络安全方面的法律法规、网络安全等级保护等方面的知识进行简要介绍，并探讨现代政企安全建设与管理，网络主权与全球网络空间治理等方面的问题。这些内容可以帮助读者从更高的层面、更广的范围来理解网络安全的总体形势与方针政策。

本书的出版离不开电子工业出版社章海涛、戴晨辰编辑的大力支持，以及其他工作人员的辛勤付出，在此向他们一并表示感谢。由于作者水平所限，不妥之处在所难免，恳请网络安全业界专家、广大读者朋友批评指正，共同为我国网络空间安全科普与教育事业贡献力量！

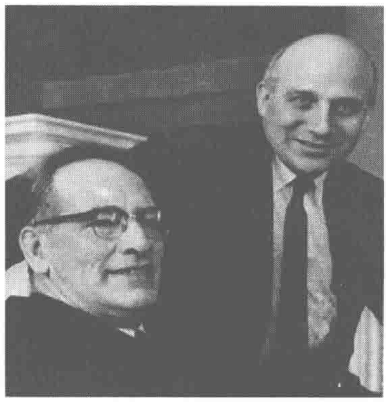
目录

Contents

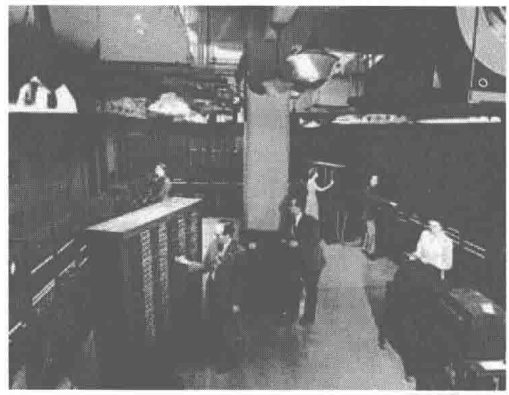
第一章 Chapter 1 安全简史

一、诞生，从计算机到互联网

1946 年 2 月 14 日，世界上第一台电子计算机在美国宾夕法尼亚大学诞生。这台名为“埃尼阿克(ENIAC)”的计算机占地面积为 150 平方米，总重量为 30 吨，使用了 18000 只电子管，6000 个开关，7000 只电阻，10000 只电容，50 万条导线，耗电量达 140 千瓦，每秒可进行 5000 次加法运算。当然，与今天相比，这个庞然大物的计算能力可能还不及一个手持计算器。



人类第一台计算机的研发小组领导莫奇来和爱克特



人类第一台计算机

在第一代电子管计算机之后，计算机技术又经历了三个重要的发展阶段：第二代晶体管计算机阶段，第三代中小规模集成电路计算机阶段和第四代超大规模集成电路计算机阶段。计算机技术的升级换代，不仅使计算能力呈指数级提高，同时也使计算机变得越来越小。今天，我们手中的一部小小的手机，甚至是一块手表，都是一台智慧的计算机。

互联网的出现要比计算机晚得多。20 世纪 60 年代，美国军方机构就已经开始尝试把计算机连接成网络。但直到 1983 年，美国 ARPA(高级研究计划署)和美国国防部通信局才联合研发出著名的 TCP/IP 协议，这标志着真正意义上的互联网诞生。

中国是全球互联网发展速度最快的国家之一。1994 年，中国正式接入

国际互联网。经过20余年的发展，截至2016年12月，中国网民数量已达到7.31亿，80%以上的网民会使用手机上网。中国早已成为全球互联网用户最多的国家。同时，以BAT3(百度Baidu、阿里巴巴Alibaba、腾讯Tencent和360的简称)为代表的一大批自主品牌的互联网企业，也已经走在了全球网络产业的最前沿。

2015年3月5日，在十二届全国人大三次会议上，李克强总理在政府工作报告中首次提出“互联网+”行动计划，“互联网+”的概念由此开始逐渐深入人心。同时，全球主要国家也已经普遍将网络空间视为继陆、海、空、天之后的“第五空间”。由于网络信息传播突破了时空限制，对传统安全防范体系造成巨大冲击，网络空间安全已成为国家综合安全建设的重要组成部分。

二、感染，从病毒到木马

恶意程序是计算机和互联网面临的最早的，也是最基本的网络威胁形式之一。其最常见的表现形式就是病毒和木马。那么，病毒和木马又是如何发展起来的呢？

(一)磁芯大战与病毒起源

计算机病毒(Computer Virus)一般是指能够对计算机软、硬件功能或数据代码进行破坏的计算机程序。除了破坏性，早期的病毒还普遍具有一定的传染性和自我复制性。

最早提出计算机病毒概念的是计算机之父冯·诺依曼。作为计算机理论的奠基人，冯·诺依曼率先提出现代计算机的理论模型和技术框架，如今人们使用的绝大多数计算机系统仍然是冯·诺依曼结构。1949年，冯·诺依曼就在其论文《复杂自动装置的理论及组织的进行》中，首次提出一种会自我繁殖的程序的可能，这被后人公认为计算机病毒最早的理论原型。

不过，计算机病毒从理论到实践，也经历了漫长的过程。1966年，在

美国贝尔实验室里，工程师 Robert Morris（后为美国国家安全局首席科学家）和两位同事在业余时间共同开发了一个游戏：游戏双方各编写一段计算机代码，输入同一部计算机中，并让这两段代码在计算机系统中“互相追杀”。由于当时计算机采用磁芯作为内存储器，所以这个游戏又被称为磁芯大战。磁芯大战的原理与后来的病毒非常接近，因此也被普遍认为是计算机病毒的实验室原型。

（二）历史上的知名病毒

计算机病毒从实验室原型走进现实生活又经过了 20 年左右的时间。1986 年，第一款流行的计算机病毒“大脑病毒”诞生。此后的 20 多年时间里，先后出现了数十款颇具影响力的病毒。此处仅选择一些最具代表性和历史意义的知名病毒进行介绍。

1. 大脑病毒（1986 年）——公认的第一个流行计算机病毒

大脑病毒是世界上公认的第一个流行计算机病毒。它由一对巴基斯坦兄弟编写。因为他们公司出售的软件时常被任意非法复制，使得购买正版软件的人越来越少。于是，兄弟二人便编写了大脑病毒来追踪和攻击非法使用其公司软件的人。该病毒运行在 DOS 系统下，通过软盘传播，会在人们盗用软件时将盗用者硬盘的剩余空间“吃掉”。所以说，人类历史上的第一款病毒实际上是为了“正义”的目的而编写的“错误”的程序。

2. 莫里斯蠕虫（1988 年）——第一个通过互联网传播的病毒

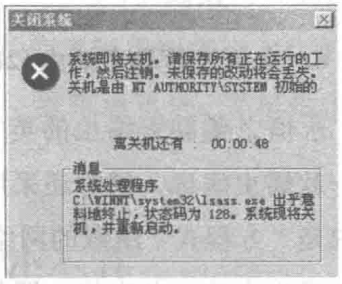
莫里斯蠕虫由康奈尔大学的罗特•莫里斯制作。1988 年美国国防部的军用计算机网络遭受莫里斯蠕虫袭击，致使网络中 6000 多台计算机感染，直接经济损失高达 9600 万美元。后来出现的各类蠕虫病毒都是模仿莫里斯病毒。罗特•莫里斯编写该病毒的初衷其实是为了向人们证明网络漏洞的存在，但病毒扩散的影响很快就超出了他的想象。为此，莫里斯被判有期徒刑 3 年、1 万美元罚金和 400 小时社区服务。

蠕虫是指利用网络进行复制和传播的一种病毒。其最初被命名为蠕虫的

原因是：在 DOS 环境下，该病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。

3. 冲击波病毒(2003 年)——历史上影响力最大的病毒

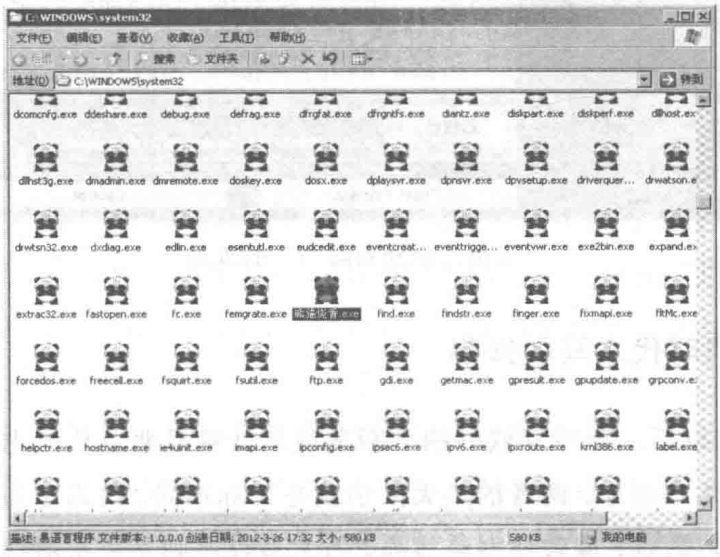
2003 年 8 月，冲击波病毒席卷全球，它利用微软网络接口 RPC 漏洞进行传播。该病毒感染速度极快，1 周内感染了全球约 80%的计算机，成为历史上影响力最大的病毒。该病毒再一次向人们展示了计算机不打补丁的危险性有多高。



冲击波病毒感染症状

4. 熊猫烧香(2007 年)——国内知名度最高的病毒

熊猫烧香是历史上知名度最高的一个“国产”病毒。该病毒从 2007 年 1 月开始肆虐网络，感染计算机数量达百万台。该病毒的主要特点是：将计算机上所有的可执行程序的图标改成熊猫举着三根香样子的图片，并可导致计算机系统，甚至整个局域网瘫痪。此后不久，免费安全软件和第三方打补丁的工具快速普及，这种单款病毒大规模传播的事件逐渐消失。



中毒后的计算机

5. 震网病毒(2010 年)——第一个针对工业系统的病毒

震网病毒是第一个针对工业系统的计算机病毒，也被认为是世界上首个“网络超级武器”。2010 年，伊朗核设施遭受震网病毒攻击，大量生产核燃料的离心机被破坏。

6. 永恒之蓝勒索蠕虫(2017 年)——全球影响最大的勒索病毒

永恒之蓝勒索蠕虫的英文名称为 WannaCry，其既是一款勒索软件，又是一款蠕虫病毒，同时还采用了军用攻击武器“永恒之蓝”(网络上流出的，据说是“方程式”组织的网络漏洞攻击武器代码)。其感染计算机设备后，会将计算机中的办公文档、照片、视频等文件加密，并向用户勒索比特币。

“永恒之蓝勒索蠕虫”的攻击

(三)互联网时代木马的兴起

2000 年以后，随着互联网的不断发展，计算机恶意代码也由病毒程序逐步转变为木马程序，两者的最大区别就是目标不同。病毒是为了破坏计算机中某些资料数据，或致使网络瘫痪。而木马程序则是秘密潜伏在被控设备

中，主要目的是盗窃被控用户的数据或个人隐私信息，从而获取一定的经济利益。

近年来木马程序的种类越来越多，破坏性也越来越大。目前，木马产业链越来越完善，从木马程序的开发、传播到销售，形成了一条分工明确的操作流程。黑客利用木马窃取的资料，从个人隐私信息到虚拟资产，包括QQ账号和密码、网游密码、信用卡账号、游戏装备、手机通讯录、手机短信等，这些都可以直接或间接转换为金钱。

三、扩散，威胁无处不在

2008年以后，在免费安全软件不断普及的大背景下，单纯的病毒、木马攻击越来越难以奏效。于是，以挂马和钓鱼技术为代表的网络攻击技术开始兴起。同时，随着物联网和可穿戴设备的快速普及，新型网络威胁不断涌现。在今天的“互联网+”时代，我们甚至可以说：威胁，无处不在。

(一)网页挂马与钓鱼

挂马技术是2005年开始逐渐流行的一种网络攻击技术，在2008—2010年活跃程度达到顶峰。这个时期网上每天最多可能出现数千至上万个挂马网页，很多网民深受其害。

所谓挂马，是指在网页中写入一段恶意代码，当用户使用有漏洞的浏览器浏览挂马网页时，计算机就会感染病毒，用户对感染病毒的过程没有感觉。由于挂马攻击是利用浏览器或系统漏洞进行的，所以，单纯使用杀毒软件往往难以有效防御。2010年以后，随着安全浏览器的普及，挂马攻击在国内的流行得到遏制。

钓鱼网站是另外一种恶意网页攻击方式，指那些页面上存在虚假欺诈信息的网站。常见的钓鱼网站包括：虚假购物网站、仿冒银行网站、虚假中奖网站、虚假QQ空间等。钓鱼网站是网络诈骗活动的重要辅助工具，其可帮