CNCERT/CC
国家互联网应急中心

2016年
中国互联网网络安全报告

+ 国家计算机网络应急技术处理协调中心 著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

CN CERT CC
国家互联网应急中心

2016年
中国互联网网络安全报告

+ 国家计算机网络应急技术处理协调中心 著

人民邮电出版社
北京

图书在版编目（CIP）数据

2016年中国互联网网络安全报告 / 国家计算机网络应急技术处理协调中心著. -- 北京 : 人民邮电出版社, 2017.6
ISBN 978-7-115-45678-6

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2016 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2017)第078730号

内 容 提 要

本书是国家计算机网络应急技术处理协调中心发布的2016年中国互联网网络安全年报。本书汇总分析了国家互联网应急中心自有网络安全监测数据和通信行业相关单位报送的数据，具有鲜明的行业特色和重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，本书对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、安全漏洞预警与处置、网络安全事件接收与处理、网络安全信息通报等情况进行深入细致的分析，并对典型网络安全事件做专题分析。此外，本书对2016年国内外网络安全监管动态、国内网络安全组织发展情况和国内外网络安全重要活动等情况做了阶段性总结，并预测2017年网络安全热点问题。

本书内容依托国家互联网应急中心多年来从事网络安全监测、预警和应急处置等工作的实际情况，是对我国互联网网络安全状况的总体判断和趋势分析，可以为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，提高全社会、全民的网络安全意识。

2016年中国互联网网络安全报告

◆ 著　　国家计算机网络应急技术处理协调中心
责任编辑　牛晓敏

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京光之彩印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：16　　2017年5月第1版
字数：380千字　　2017年5月北京第1次印刷

ISBN 978-7-115-45678-6

定价：89.00元

读者服务热线：（010）81055488　**印装质量热线：**（010）81055316
反盗版热线：（010）81055315

目 录 CONTENTS

CN CERT CC
国家互联网应急中心

2016年
中国互联网网络安全报告

+ 国家计算机网络应急技术处理协调中心 著

人民邮电出版社
北京

图书在版编目（CIP）数据

2016年中国互联网网络安全报告 / 国家计算机网络应急技术处理协调中心著. -- 北京 : 人民邮电出版社, 2017.6
ISBN 978-7-115-45678-6

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2016 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2017)第078730号

内 容 提 要

本书是国家计算机网络应急技术处理协调中心发布的2016年中国互联网网络安全年报。本书汇总分析了国家互联网应急中心自有网络安全监测数据和通信行业相关单位报送的数据，具有鲜明的行业特色和重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，本书对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、安全漏洞预警与处置、网络安全事件接收与处理、网络安全信息通报等情况进行深入细致的分析，并对典型网络安全事件做专题分析。此外，本书对2016年国内外网络安全监管动态、国内网络安全组织发展情况和国内外网络安全重要活动等情况做了阶段性总结，并预测2017年网络安全热点问题。

本书内容依托国家互联网应急中心多年来从事网络安全监测、预警和应急处置等工作的实际情况，是对我国互联网网络安全状况的总体判断和趋势分析，可以为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，提高全社会、全民的网络安全意识。

2016年中国互联网网络安全报告

◆ 著　　国家计算机网络应急技术处理协调中心
责任编辑　牛晓敏

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京光之彩印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：16　　2017年5月第1版
字数：380千字　　2017年5月北京第1次印刷

ISBN 978-7-115-45678-6

定价：89.00元

读者服务热线：（010）81055488　**印装质量热线：**（010）81055316
反盗版热线：（010）81055315

《2016年中国互联网网络安全报告》
编委会

主任委员	黄澄清
副主任委员	云晓春　刘欣然
执行委员	严寒冰　丁　丽　李　佳
委　　员	狄少嘉　徐　原　何世平　温森浩
	李志辉　姚　力　张　洪　朱芸茜
	郭　晶　朱　天　高　胜　胡　俊
	王小群　张　腾　吕利锋　何能强
	李　挺　陈　阳　李世淙　徐　剑
	王适文　刘　婧　饶　毓　肖崇蕙
	贾子骁　张　帅　吕志泉　韩志辉
	马莉雅　徐丹丹　雷　君　邱乐晶
	王江波

前 言 FOREWORD

互联网在我国政治、经济、文化以及社会生活中发挥着举足轻重的作用。国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文缩写为“CNCERT”或“CNCERT/CC”）作为我国非政府层面网络安全应急体系核心技术协调机构，在社会网络安全防范机构、公司、大学、科研院所的支撑和支援下，在网络安全监测、预警、处置等方面积极开展工作，历经十余年的实践，形成多种渠道的网络攻击威胁和安全事件发现能力，与国内外数百个机构和部门建立了网络安全信息通报和事件处置协作机制，依托所掌握的丰富数据资源和信息实现对网络安全威胁和宏观态势的分析预警，在维护我国公共互联网环境安全、保障基础信息网络和网上重要信息系统安全运行、保护互联网用户上网安全、宣传网络安全防护意识和知识等方面起到重要作用。

自2004年起，国家互联网应急中心根据工作中受理、监测和处置的网络攻击事件和安全威胁信息，每年撰写和发布《CNCERT/CC网络安全工作报告》，为相关部门和社会公众了解国家网络安全状况和发展趋势提供参考。2008年，在收录、统计通信行业相关部门网络安全工作情况和数据基础上，《CNCERT/CC网络安全工作报告》正式更名为《中国互联网网络安全报告》。自2010年起，在工业和信息化部通

信保障局的指导以及互联网网络安全应急专家组的帮助下，国家互联网应急中心精心编制并公开发布年度互联网网络安全态势报告，受到社会各界的广泛关注。

《2016年中国互联网网络安全报告》汇总分析国家互联网应急中心自有网络安全监测数据和通信行业相关单位报送的数据，具有鲜明的行业特色和重要的参考价值。报告涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面的内容。其中，报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、安全漏洞预警与处置、网络安全事件接收与处理、网络安全信息通报等情况进行深入细致的分析，并对2016年典型网络安全事件进行专题介绍。此外，报告对2016年国内外网络安全监管动态、国内网络安全组织发展情况和国内外网络安全重要活动等做了阶段性总结。最后，报告对2017年网络安全热点问题进行预测。

本书电子版可从CNCERT/CC官方网站（http://www.cert.org.cn）下载。

国家计算机网络应急技术处理协调中心

2017年5月

致 谢 THANKS

《2016年中国互联网网络安全报告》的写作素材均来自于国家互联网应急中心网络安全工作实践。CNCERT/CC网络安全工作离不开政府主管部门长期以来的关心和指导，也离不开各互联网运营企业、网络安全厂商、安全研究机构以及相关合作单位的大力支持。在《2016年中国互联网网络安全报告》撰写过程中，CNCERT/CC向北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、哈尔滨安天科技股份有限公司、北京神州绿盟科技有限公司、深信服科技有限公司、恒安嘉新（北京）科技有限公司、任子行网络技术股份有限公司征集了数据和专题分析素材[1]，特此致谢。

2016年，为维护公共互联网安全，净化公共互联网网络环境，CNCERT/CC联合有关单位，在网络安全监测、预警、处置等方面积极开展工作。其中，阿里云计算有限公司、北京新网数码信息技术有限公司、上海美橙科技信息发展有限公司、厦门商中在线科技有限公司、成都西维数码科技有限公司、厦门纳网科技有限公司、成都飞数科技有限公司、厦门市中资源网络服务有限公司等单位对CNCERT/CC事件处置要求及时响应，积极配合。北京天融信网络安全技术有限公司、成都卫士通信息产业股份有限公司（北京）、哈尔滨安天科技股份有限公司、北京神州绿盟信息安全科技股份有限公司、恒安嘉新（北京）科技有限公司等单位向CNCERT/CC进行了大量有价值的信息通报，为网络安全预警通报工作提供了良好的支撑。中国移动MM、OPPO软件商店、木蚂蚁、百度手机助手、小米应用商店、360手机助手、PP助手、腾讯应用宝、华为应用市场、安智市场积极配合开展移动互联网恶

[1] 《2016年中国互联网网络安全报告》中其他单位所提供数据的真实性和准确性由报送单位负责，CNCERT/CC未做验证。

意程序下架、移动互联网应用自律白名单等工作。北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、恒安嘉新（北京）科技有限公司、杭州安恒信息技术有限公司、哈尔滨安天科技股份有限公司、蓝盾信息安全技术股份有限公司、杭州华三通信技术有限公司、沈阳东软系统集成工程有限公司、北京奇虎科技有限公司（补天平台）、漏洞盒子以及腾讯玄武实验室、广西鑫瀚科技有限公司、西安四叶草信息技术有限公司、深信服科技股份有限公司、中国电信集团系统集成有限责任公司、华为技术有限公司等在漏洞信息报送方面表现突出。北京市政务信息安全应急处置中心、中国教育和科研计算机网、中国科技网、中国电信集团公司网络运行维护事业部、中国移动通信集团公司信息安全管理与运行中心、中国联合网络通信集团有限公司信息安全部、上海交通大学网络信息中心、北京安赛创想科技有限公司、西门子（中国）有限公司、拓尔思信息技术股份有限公司、腾讯安全响应中心（TSRC）、百度安全响应中心（BSRC）等单位在漏洞处置及技术能力协作方面表现突出。北京知道创宇信息技术有限公司、哈尔滨安天科技股份有限公司、河北翎贺计算机信息技术有限公司、北京神州绿盟科技有限公司、杭州安恒信息技术有限公司、恒安嘉新（北京）科技有限公司在网络安全威胁治理工作中起到了重要支撑作用。此外，本报告的完成离不开各单位在日常工作中给予的配合和支持，在此一并感谢。

由于编者水平有限，《2016年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，CNCERT/CC诚挚地希望广大读者不吝赐教，多提意见，并继续关注和支持我中心的发展。CNCERT/CC将更加努力地工作，不断提高技术和业务能力，为我国以及全球互联网的安全保障贡献力量。

关于国家计算机网络应急技术处理协调中心 ABOUT CNCERT/CC

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是“CNCERT”或“CNCERT/CC”），成立于2002年9月，为非政府非营利性的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT/CC的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

国家互联网应急中心的主要业务能力如下。

事件发现。CNCERT/CC依托“公共互联网网络安全监测平台”开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报。CNCERT/CC依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等，为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置。对于自主发现和接收到的危害较大的事件报告，CNCERT/CC及时响应并积极协调处置，重点处置的事

件包括：影响互联网运行安全的事件，波及较大范围互联网用户的事件，涉及重要政府部门和重要信息系统的事件，用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估。作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT/CC 还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

同时，作为我国非政府层面开展网络安全事件跨境处置协助的重要窗口，CNCERT/CC 积极开展国际合作，致力于构建跨境网络安全事件的快速响应和协调处置机制。CNCERT/CC 为著名网络安全合作组织 FIRST 的正式成员以及亚太应急组织 APCERT 的发起人之一。截至 2016 年，CNCERT/CC 与 69 个国家和地区的 185 个组织建立了“CNCERT/CC 国际合作伙伴”关系。

联系方式

CNCERT/CC 建立了 7×24 小时的网络安全事件投诉机制，国内外用户可通过网站、电子邮件、热线电话、传真 4 种主要渠道向 CNCERT/CC 投诉网络安全事件。

网　　址：http://www.cert.org.cn/

电子邮件：cncert@cert.org.cn

热线电话：+86 10 82990999（中文）

+86 10 82991000（English）

传　　真：+86 10 82990399

目 录 CONTENTS