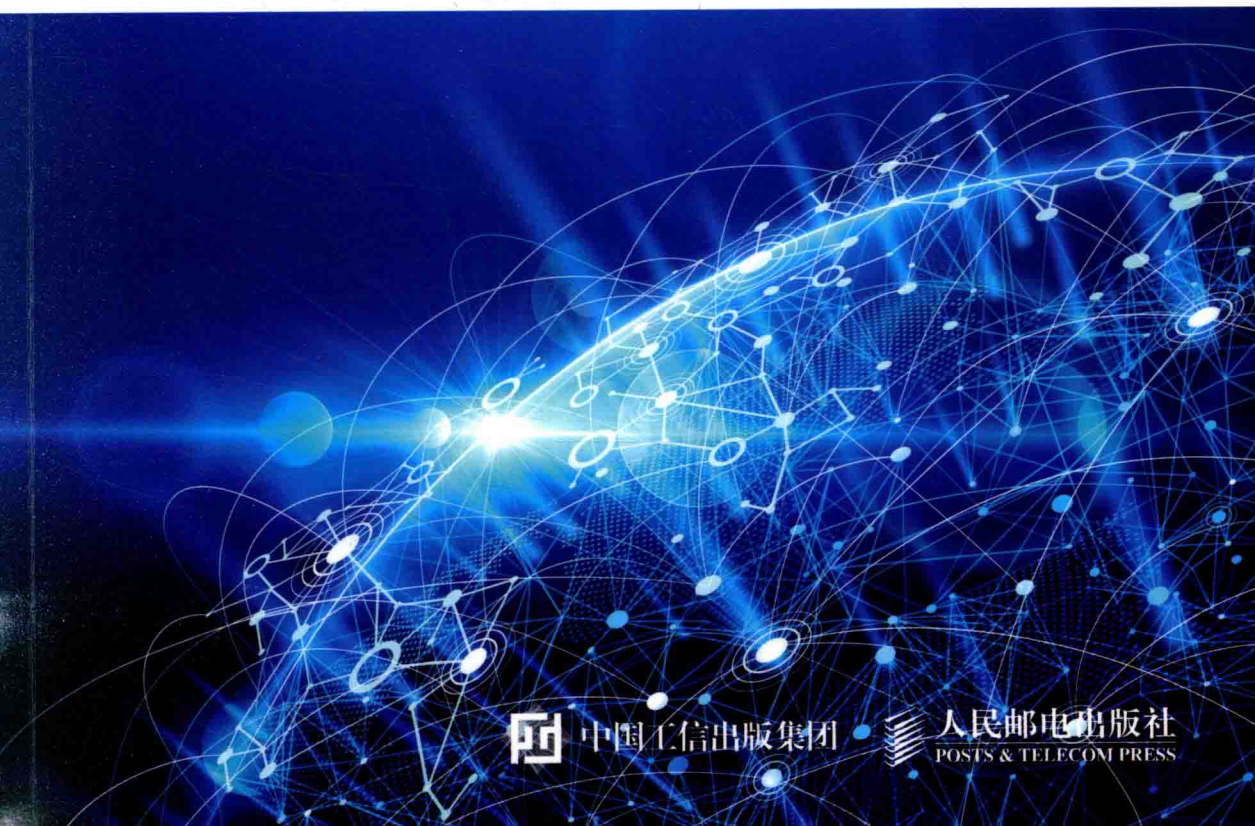
CNCERT/CC
国家互联网应急中心

# 2015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

CNCERT/CC
国家互联网应急中心

# 2015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**

2015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, 2016.6
ISBN 978-7-115-42291-0

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2015 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2016)第081451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（简称“国家互联网应急中心”，英文缩写为“CNCERT”或“CNCERT/CC”）发布的2015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2015年开展的网络安全威胁治理行动等重要活动或网络安全事件做专题分析。此外，本书对2015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，并预测了2016年网络安全热点问题。

本书的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。

**2015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：14　　2016年5月第1版
字数：150千字　　2016年5月北京第1次印刷

ISBN 978-7-115-42291-0

定价：79.00元

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

# 2015年网络安全大事记

◆ 2015年1月5日，机锋论坛的2300万用户数据在网上疯传，引发公众的广泛关注。360补天漏洞响应平台负责人赵武对此表示：“经调查，网上流传的2300万数据是机锋2013年的老数据。但机锋论坛还有多个高危漏洞没有完全修复，其2700万最新用户数据也暴露在黑客枪口下。”

**机锋论坛存在高危漏洞或导致2700万最新用户数据泄露**

**50家单位入选第六届CNCERT/CC网络安全应急服务支撑单位**

◆ 2015年5月25日，国家互联网应急中心在湖北省武汉市举行第六届CNCERT/CC网络安全应急服务支撑单位评选会议，评选产生了8家国家级应急服务支撑单位和42家省级应急服务支撑单位。

**2015中国网络安全技术对抗赛和中国计算机网络安全大会成功举办**

◆ 2015年5月26日，在工业和信息化部指导下，国家互联网应急中心（CNCERT/CC）在湖北省武汉市举办了2015中国网络安全技术对抗赛。2015年5月27-28日，以“智能网络·安全护航”为主题的2015中国计算机网络安全大会（第12届）在湖北省武汉市召开，来自政府和重要信息系统、企业、行业协会、科研院所等单位以及来自CNCERT/CC国际合作伙伴的代表共七百余人参加了本次大会。

**社保系统漏洞曝光涉及30余省数千万用户数据**

◆ 2015年4月，“补天漏洞响应平台”发布信息称：30余个省市的社保、户籍查询、疾控中心等系统存在高危漏洞；仅社保类信息安全漏洞涉及数据就达到5279.4万条，包括身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

◆ 2015年6月19日，国内32家单位在北京共同签署了《中国互联网协会漏洞信息披露和处置自律公约》，这是首次以行业自律的方式共同规范漏洞信息的接收、处置和发布方面的行为。

**《中国互联网协会漏洞信息披露和处置自律公约》在京签署**

◆ 网络安全法草案7月6日起在中国人大网上全文公布，并向社会公开征求意见一个月。2015年6月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。

**网络安全法草案全文公布并征求社会意见**

**“海莲花”APT组织被曝光长期攻击我国海事机构等重要部门**

◆ 2015年5月29日，360“天眼实验室”发布的报告，首次披露一起针对中国的国家级黑客攻击细节。该境外黑客组织被命名为“海莲花(OceanLotus)”。自2012年4月起，“海莲花”针对中国的海事机构、海域建设部门、科研院所和航运企业，使用木马病毒攻陷和控制政府人员、外包商、行业专家等目标人群的电脑，甚至操纵电脑自动发送相关情报，很明显是一次有国外政府支持的APT行动。

**《国家安全法》公布施行**

◆ 2015年7月1日，十二届全国人大常委会第十五次会议表决通过了新的国家安全法。国家主席习近平签署第29号主席令予以公布。法律对政治安全、国土安全、军事安全、文化安全、科技安全等11个领域的国家安全任务进行了明确，首次以法律形式提出“维护国家网络空间主权”。

## 三家企业通过中国反网络病毒联盟的移动互联网应用自律白名单认证

◆ 2015年8月19日，中国移动、炫彩互动网络科技有限公司、广州酷狗计算机科技有限公司3家移动互联网企业的4款数字证书和4款APP通过了白名单认证，其中包括“中国移动MM”、“中国电信爱游戏”、“酷狗音乐”等应用程序。此前，2015年“3·15”期间，中国反网络病毒联盟组织国内主流的14家手机应用商店建立“3·15白名单APP专题”，为网民铺设可信应用下载入口。

## 互联网网络安全威胁治理行动效果显著

◆ 2015年7月31日，CNCERT/CC会同中国互联网协会网络与信息安全工作委会发起了互联网网络安全威胁治理专项行动，重点打击以DDoS攻击、网页篡改为代表的制造、销售、传播网络攻击工具以及实施网络攻击行为的地下黑色产业链，效果显著。

## 习近平主席访美，达成中美网络空间的六点共识

◆ 2015年9月，习近平主席访美，与美方在网络议题相关的领域达成了六点共识，包括网络安全审查、商业领域加强信息通讯技术网络安全的一般措施、恶意网络活动提供信息及协助、反对网络窃取知识产权、制定和推动国际社会网络空间国家行为准则，以及建立两国打击网络犯罪及相关事项高级别联合对话机制。

## 苹果XcodeGhost恶意程序出现为应用供应链安全问题敲响警钟

◆ 2015年9月13日，CNCERT/CC接到报告称，使用非苹果公司官方渠道的Xcode开发工具开发APP时，非官方Xcode会向正常的APP中植入恶意代码“XcodeGhost”，且被植入恶意程序的苹果APP可以在App Store正常下载并安装使用，感染国内用户达2140万。CNCERT/CC已在9月14日发布预警通报，提醒开发者切勿使用非苹果官方渠道的Xcode工具，以维护广大用户的个人信息安全。

## 第二届世界互联网大会召开

◆ 2015年12月16日，第二届世界互联网大会在浙江省桐乡市乌镇举行。本届大会的主题是“互联互通·共享共治——共建网络空间命运共同体”。开幕式上，中共中央总书记、国家主席、中央军委主席习近平发表主旨演讲。

## Java反序列化漏洞

◆ 2015年12月，CNCERT/CC通报Java反序列化漏洞情况，该漏洞影响多款应用广泛的Web容器软件。远程攻击者利用漏洞可在目标系统上执行任意代码，危害较大的可以取得网站服务器控制权。CNCERT/CC对相关Web应用的分布情况和受漏洞影响进行了探测，发现境内主机IP中Jboss、Weblogic、Jenkins受到漏洞影响的未修复比例分别是13.9%、50.4%、33.4%。

# CONTENTS 目 录

CNCERT/CC
国家互联网应急中心

# 2015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**

2015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, 2016.6
ISBN 978-7-115-42291-0

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2015 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2016)第081451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（简称“国家互联网应急中心”，英文缩写为“CNCERT”或“CNCERT/CC”）发布的2015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2015年开展的网络安全威胁治理行动等重要活动或网络安全事件做专题分析。此外，本书对2015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，并预测了2016年网络安全热点问题。

本书的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。

**2015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：14　　2016年5月第1版
字数：150千字　　2016年5月北京第1次印刷

ISBN 978-7-115-42291-0

定价：79.00元

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

# 《2015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　纪玉春 |
| 委　　员 | 狄少嘉　徐　娜　徐　原　何世平 |
| | 温森浩　赵　慧　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　王适文　刘　婧　饶　毓 |
| | 肖崇蕙　贾子骁　张　帅　吕志泉 |
| | 韩志辉　马莉雅 |

# FOREWORD 前 言

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10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网络安全环境、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的基础上，《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，在工业和信息化部网络安全管理局（原通信

保障局）的指导和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。

《2015 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 2015 年开展的网络安全威胁治理行动等重要活动或发生的典型网络安全事件做专题分析。此外，报告对 2015 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。最后，报告预测了 2016 年网络安全热点问题。

国家计算机网络应急技术处理协调中心

2016 年 4 月

# THANKS 致 谢

《2015 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（以下简称“CNCERT/CC”）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《2015 年中国互联网网络安全报告》撰写过程中，CNCERT/CC 向恒安嘉新（北京）科技有限公司、北京网秦天下科技有限公司、哈尔滨安天科技股份有限公司、北京奇虎科技有限公司、微软公司、腾讯公司、卡巴斯基技术开发（中国）有限公司、深信服科技有限公司、北京猎豹移动科技有限公司等单位征集并采用了网络安全数据和专题文章素材[1]，特此致谢。

2015 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。北京新网数信息技术有限公司、阿里云计算有限公司、厦门商中在线科技有限公司、上海美橙科技信息发展有限公司、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，配合积极；恒安嘉新（北京）科技有限公司、北京神州绿盟信息安全科技股份有限公司、哈尔滨安天科技股份有限

[1] 《2015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。

公司、北京奇虎科技有限公司、北京猎豹移动科技有限公司、北京瑞星信息技术有限公司等单位向 CNCERT/CC 报送了大量有价值的信息通报，起到了很好的预警效果；中国移动 MM、木蚂蚁、OPPO 软件商店、百度手机助手、小米应用商店、91 助手、应用汇、360 手机助手、安智市场、安卓市场积极配合开展移动互联网恶意程序下架等工作；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、北京奇虎科技有限公司（补天平台）、恒安嘉新（北京）科技有限公司、哈尔滨安天科技股份有限公司、乌云平台、漏洞盒子，在漏洞信息报送方面表现突出；中国教育和科研计算机网、上海交通大学网络信息中心、北京信息安全测评中心、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运行维护部、中国科技网、北京知道创宇信息技术有限公司等单位在漏洞处置和全局响应方面表现突出。此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，《2015 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 CNCERT/CC 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。