2012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

CNCERT/CC

人民邮电出版社
POSTS & TELECOM PRESS

2012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

CNCERT/CC

人民邮电出版社
北京

图书在版编目（CIP）数据

2012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, 2013.7
ISBN 978-7-115-32194-7

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2012 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2013)第124469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）发布的 2012 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结果和通信行业相关单位报送的大量数据，涵盖了互联网网络安全宏观形势判断、网络安全监测数据分析、网络安全工作专题分析、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。

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。

◆ 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
执行编辑　李鹏飞
责任印制　杨林杰
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷
◆ 开本：800 × 1000　1/16
印张：13.75　　2013 年 7 月第 1 版
字数：221 千字　　2013 年 7 月北京第 1 次印刷

定价：59.00 元

读者服务热线：(010)67119329　印装质量热线：(010)67129223
反盗版热线：(010)67171154

目录 CONTENT

2012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

CNCERT/CC

人民邮电出版社
北京

图书在版编目（CIP）数据

2012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, 2013.7
ISBN 978-7-115-32194-7

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2012 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2013)第124469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）发布的 2012 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结果和通信行业相关单位报送的大量数据，涵盖了互联网网络安全宏观形势判断、网络安全监测数据分析、网络安全工作专题分析、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。

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。

◆ 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
执行编辑　李鹏飞
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：800 × 1000　1/16
印张：13.75　　2013 年 7 月第 1 版
字数：221 千字　　2013 年 7 月北京第 1 次印刷

定价：59.00 元

读者服务热线：(010)67119329　印装质量热线：(010)67129223
反盗版热线：(010)67171154

《2012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	周勇林	王明华	
委　　员	纪玉春	徐　娜	王营康
	徐　原	李　佳	何世平
	温森浩	赵　慧	李志辉
	姚　力	张　洪	朱芸茜
	朱　天	高　胜	胡　俊
	王小群	张　腾	何能强

前言 PERFACE

当前，互联网在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用。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。

《2012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大量信息，具有鲜明的行业特色。报告涵盖互联网网络安全宏观形势判断、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。同时，报告对2012年开展的虚假源地址攻击流量整治、移动互联网恶意程序专项治理等工作进行专门介绍，并首次吸纳通信行业单位针对典型网络安全事件的深入分析报告。接下来，报告对2012年国内外网络安全监管动态、我国网络安全行业联盟和应急组织的发展、国内外网络安全工作的交流与合作等情况做了阶段性总结。最后，针对当前网络安全热点和难点问题，结合对2013年网络安全的威胁和形势判断，报告对下一步网络安全工作提出若干建议。

国家互联网应急中心

2013年5月

致 谢 THANKS

《2012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。国家互联网应急中心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《2012年中国互联网网络安全报告》撰写过程中，国家互联网应急中心向北京瑞星信息技术有限公司、北京网秦天下科技有限公司、北京网御星云信息技术有限公司、北京知道创宇信息技术有限公司、哈尔滨安天信息技术有限公司、恒安嘉新（北京）科技有限公司、金山网络技术有限公司、卡巴斯基技术开发（北京）有限公司、奇虎360软件（北京）有限公司、趋势科技（中国）有限公司、深圳市腾讯计算机系统有限公司、洋浦科技有限公司等单位征集了数据素材[1]，在此一并致谢。

由于编者水平有限，《2012年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，国家互联网应急中心诚挚地希望广大读者不吝赐教，多提意见，并继续关注和支持国家互联网应急中心的发展。国家互联网应急中心将更加努力地工作，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。

[1] 《2012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，国家互联网应急中心未做验证。

关于国家计算机网络应急技术处理协调中心

国家计算机网络应急技术处理协调中心（简称为国家互联网应急中心，英文缩写为CNCERT或CNCERT/CC），成立于1999年9月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全，保障基础信息网络和网上重要信息系统的安全运行。

2003年，国家互联网应急中心在全国31个省成立分中心，形成全国性的互联网网络安全信息共享、技术协同能力。目前，国家互联网应急中心作为国家公共互联网网络安全应急体系的核心技术协调机构，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，在协调骨干网络运营单位应急组织、域名服务机构应急组织等国内网络安全应急组织共同处理网络安全事件方面发挥着重要作用。

同时，国家互联网应急中心积极开展国际合作，是中国处理网络安全事件的对外窗口。国家互联网应急中心是国际著名网络安全合作组织FIRST的正式成员，也是APCERT的发起人之一，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。截至2012年年底，国家互联网应急中心已与51个国家和地区的91个组织建立“CNCERT/CC国际合作伙伴”关系。

国家互联网应急中心的主要业务能力如下。

事件发现。通过多种渠道发现网络攻击威胁和网络安全事件，包括网络安全事件自主发现，国内外合作伙伴的数据和信息共享，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。

预警通报。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事件报告，筛选危害较大的事件进行及时响应和协调处置，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。

联系方式

网址：http://www.cert.org.cn/

电子邮件：cncert@cert.org.cn

热线电话：+8610 82990999（中文），82991000（English）

传真：+8610 82990399

PGP Key：http://www.cert.org.cn/cncert.asc

目录 CONTENT