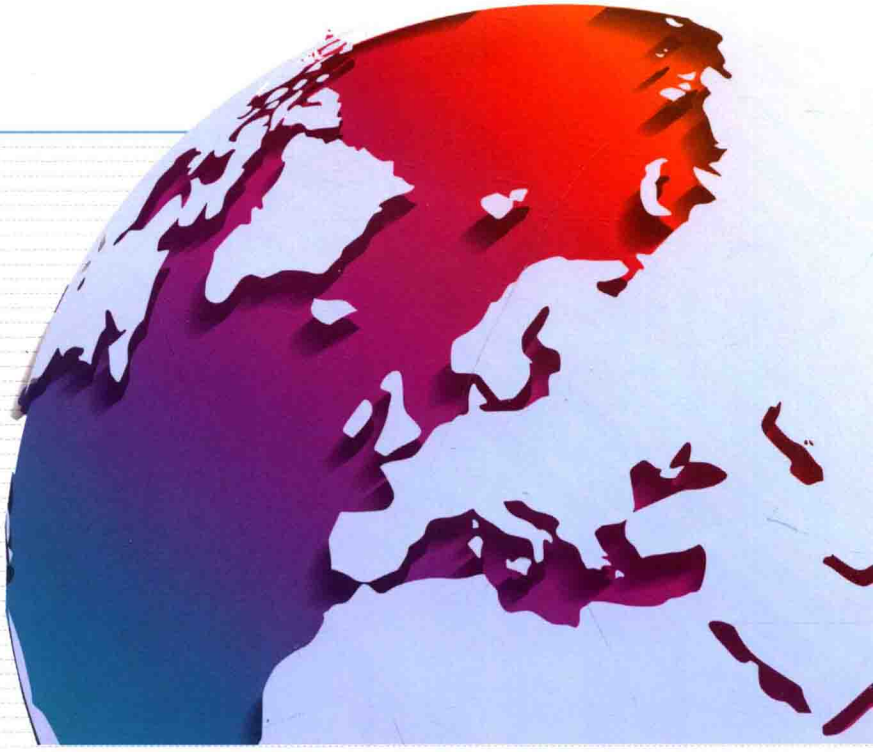
2014年
中国互联网网络安全报告

国家计算机网络应急技术处理协调中心 著

CNCERT/CC



中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

2014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

2014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, 2015.6
ISBN 978-7-115-39215-2

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2014 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2015)第091913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2014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、网络安全企业相关单位报送的大量数据，具有鲜明的行业特色。报告涵盖了我国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，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、网络安全信息通报等情况进行深入细致的分析。

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。

2014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：12　　2015年5月第1版
字数：130千字　　2015年5月北京第1次印刷

ISBN 978-7-115-39215-2

定价：59.00元

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

《2014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　李　佳　纪玉春
委　　员	徐　娜　徐　原　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
	李　挺　陈　阳　李世淙
	党向磊　徐晓燕　王适文
	刘　婧　饶　毓　赵　宸
	肖崇蕙　张　帅　贾子骁
	摆　亮

PREFACE

前言

当前，互联网在我国政治、经济、文化以及社会生活中发挥着越来越重要的作用。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/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 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。

《2014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2014年开展的移动互联网恶意程序治理工作、分布式反射型拒绝服务攻击等专题进行专门介绍，并首次吸纳通信行业的网站安全监测数据。接下来，报告对2014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、国内外网络安全重要活动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2014年网络安全的威胁和形势判断，预测了2015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

2015年3月

THANKS

致谢

《2014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《2014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、恒安嘉新（北京）科技有限公司、北京奇虎科技有限公司、趋势科技（中国）有限公司、深信服科技有限公司、北京安管佳科技有限公司等单位征集了数据素材[1]，特此致谢。

2014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。北京新网数码信息技术有限公司、厦门商中在线科技有限公司、北京新网互联科技有限公司、成都西维数码科技有限公司、厦门三五互联科技股份有限公司、阿里巴巴通信技术（北京）有限公司等单位对国家互联网应急中心事件处置要求及时响应，配合积极；北京奇虎科技有限公司、猎豹

[1] 《2014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。

移动公司、北京瑞星信息技术有限公司、哈尔滨安天科技股份有限公司等单位向国家互联网应急中心报送了大量有价值的信息通报，起到了很好的预警效果；百度手机助手、PP 助手、木蚂蚁、应用汇、安智网、安卓网、中国移动应用商场积极配合开展移动互联网恶意程序下架和信息报送工作。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，《2014 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。

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“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。

2003 年，国家互联网应急中心在全国 31 个省（自治区、直辖市）成立分中心。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极防御、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。依托“863-917 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。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，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，作为中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 积极开展网络安全国际合作，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 为国际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 的发起者之一。截至 2014 年年底，CNCERT/CC 已与世界上 63 个国家和地区的 144 个组织建立“CNCERT 国际合作伙伴”关系。

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

2014 年网络安全大事记

2014 年 2 月 27 日

中央网络安全和信息化领导小组成立

2014 年 4 月 8 日

网络安全协议 OpenSSL 被曝发现严重安全漏洞，在整个 IT 行业及更广的周边行业引起普遍的恐慌

2014 年 4 月 8 日，XP 停止更新服务

继续使用 XP 的用户无法再 从 Windows Update 接收软件更新，其中包括新的安全升级（它们可帮助电脑抵御有害病毒、间谍软件及其他可能窃取个人信息的恶意软件），非安全性补丁，免费或付费辅助支持，以及在线技术文档更新

2014 年 4 月 15 日

工业和信息化部联合公安部、工商总局共同开展打击治理移动互联网恶意程序专项行动

国内某主要 CDN 服务商的域名服务器遭到大规模异常流量攻击，由于其承载国内大量重要网站的 CDN 加速服务，导致对这些网站的访问均受到严重影响

2014 年 8 月 2 日
七夕当天

一款名为“xx 神器”的安卓系统手机病毒在全国范围蔓延。据统计，超过百万用户感染“xx 神器”，一度引起人们恐慌，被业界称为有史以来最大规模的手机木马

2014 年
6 月

出现一种针对工业控制网络的远程木马“Havex”，利用 OPC 工业通信技术，主要功能是扫描发现系统联网设备，收集工控设备详细信息并秘密回传，预置后门并在必要时接收、执行控制端发送的恶意代码，全球能源行业的数千个工业控制系统曾被其入侵

国家 .cn 顶级域名系统继 2013 年 8 月 25 日之后再次遭受大规模流量攻击，由于系统加强了安全防护措施，未受到严重影响，但在一定程度上反映出我国顶级域名系统面临的严峻外部威胁

2014 年 10 月

爆出 BASH 存在一个安全漏洞，该漏洞直接影响基于 UNIX 的系统，将导致远程攻击者在受影响的系统上执行任意代码

2014 年 9 月 25 日

香港占中期间，我国数十个重要政府网站遭受黑客组织攻击，攻击方式包括：拒绝服务攻击、网页篡改攻击以及数据窃取等

2014 年 9 月 19 日

中国互联网协会反网络病毒联盟发布 2014 年度移动互联网应用自律白名单

2014 年 11 月 19–21 日

首届世界互联网大会在乌镇举行，这是中国举办的规模最大、层次最高的世界级互联网大会，大会以“互联互通 共享共治”为主题，网络安全成为会议的重要议题

2014 年
11 月 24-30 日

国信办联合中央编办、公安部、工业和信息化部等多 8 部门举办首届国家网络安全宣传周

2014 年
12 月

我国多个省份的递归域名解析服务器受到攻击，部分地区的互联网使用受到影响

2014 年
12 月中旬

某大型互联网服务商云平台的一家知名游戏公司遭受拒绝服务攻击，攻击峰值流量超过 450Gbit/s。云平台运行的稳定性直接影响业务的可用性和连续性，而且针对云平台某一目标的攻击，还可能导致其他业务受到牵连，造成大面积用户无法访问或使用

2014 年
12 月 25 日

大量中国铁路客服中心 12306 用户数据在互联网上被疯传贩售，泄露资料包括用户账号、明文密码、身份证、邮箱等敏感信息

CONTENT

目录