

# 2013<sup>年</sup>

## 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

CNERT/CC

  
人民邮电出版社  
POSTS & TELECOM PRESS

# 2013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

CN  ERT/CC

人民邮电出版社  
北京

## 图书在版编目(CIP)数据

2013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,  
2014.5

ISBN 978-7-115-35502-7

I. ①2… II. ①国… III. ①互联网络—安全技术—  
研究报告—中国—2013 IV. ①TP393.408

中国版本图书馆CIP数据核字(2014)第083653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2013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。

## 2013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 2014年5月第1版  
字数: 130千字 2014年5月北京第1次印刷

ISBN 978-7-115-35502-7

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

# 《2013 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 | 王明华 | 严寒冰 | 李 佳 | 贺 敏 | 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 |     |     |
|         | 摆 亮 | 陈 阳 | 李世淙 |     |     |
|         | 党向磊 | 徐晓燕 | 王适文 |     |     |
|         | 刘 婧 | 饶 毓 | 赵 宸 |     |     |

# 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 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、网络安全企业相关部门网络安全工作情况和数据的基础上，《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。

《2013 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、网络安全企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 2013 年开展的防范治理黑客地下产业链专项行动，对 DDoS 攻击的监测分析等进行专题介绍，并吸纳互联网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 2013 年国内外网络安全监管动态、国内网络安全组织发展情况、国内外网络安全重要活动做了阶段性总结。最后，针对当前网络安全的热点和难点问题，对 2014 年网络安全的威胁和形势做出判断。

国家互联网应急中心

2014 年 4 月

# 致 谢 *THANKS*

《2013 年中国互联网网络安全报告》的写作素材均来自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、网络安全企业、安全研究机构以及相关合作单位的大力支持。

在《2013 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网秦天下科技有限公司、北京网御星云信息技术有限公司、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 公司、洋浦科技有限公司等单位征集了专题和数据素材<sup>[1]</sup>，在此一并致谢。

由于编者水平有限，《2013 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] 《2013 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“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，为非政府非盈利的网络安全安全技术中心，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。**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、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 2013 年，CNCERT/CC 已与 59 个国家和地区的 127 个组织建立了“CNCERT/CC 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](mailto: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

|          |                                 |           |
|----------|---------------------------------|-----------|
| <b>1</b> | <b>2013 年网络安全状况综述</b>           | <b>13</b> |
| 1.1      | 我国互联网网络安全总体状况                   | 13        |
| 1.2      | 数据导读                            | 22        |
| <b>2</b> | <b>网络安全专题分析</b>                 | <b>24</b> |
| 2.1      | 防范黑客地下产业链专项行动专题分析（来源：CNCERT/CC） | 24        |
| 2.2      | DDoS 攻击专题分析（来源：CNCERT/CC）       | 28        |
| 2.3      | 从“棱镜”看国内网络安全（来源：安天公司）           | 38        |
| 2.4      | APT 攻击技术研究及防范（来源：网御星云）          | 41        |
| 2.5      | 网上交易服务安全风险分析（来源：奇虎 360 公司）      | 51        |
| <b>3</b> | <b>计算机恶意程序传播和活动情况</b>           | <b>63</b> |
| 3.1      | 木马和僵尸网络监测情况                     | 63        |
| 3.2      | “飞客”蠕虫监测情况                      | 73        |
| 3.3      | 恶意程序传播活动监测                      | 75        |
| 3.4      | 通报成员单位报送情况                      | 77        |
| <b>4</b> | <b>移动互联网恶意程序传播和活动情况</b>         | <b>88</b> |
| 4.1      | 移动互联网恶意程序监测情况                   | 88        |

|          |                          |            |
|----------|--------------------------|------------|
| 4.2      | 移动互联网恶意程序传播活动监测 .....    | 90         |
| 4.3      | 通报成员单位报送情况 .....         | 92         |
| <b>5</b> | <b>网站安全监测情况 .....</b>    | <b>104</b> |
| 5.1      | 网页篡改情况 .....             | 104        |
| 5.2      | 网页挂马情况 .....             | 108        |
| 5.3      | 网页仿冒情况 .....             | 113        |
| 5.4      | 网站后门情况 .....             | 115        |
| <b>6</b> | <b>安全漏洞预警与处置 .....</b>   | <b>119</b> |
| 6.1      | CNVD 漏洞收录情况 .....        | 119        |
| 6.2      | 高危漏洞典型案例 .....           | 123        |
| 6.3      | CNVD 行业漏洞库 .....         | 127        |
| 6.4      | CNVD 漏洞处置情况 .....        | 132        |
| <b>7</b> | <b>网络安全事件接收与处理 .....</b> | <b>134</b> |
| 7.1      | 事件接收情况 .....             | 134        |
| 7.2      | 事件处理情况 .....             | 136        |
| 7.3      | 事件处理典型案例 .....           | 139        |
| <b>8</b> | <b>网络安全信息通报情况 .....</b>  | <b>146</b> |
| 8.1      | 互联网网络安全信息通报 .....        | 146        |
| 8.2      | 行业外互联网网络安全信息发布情况 .....   | 149        |
| <b>9</b> | <b>国内外网络安全监管动态 .....</b> | <b>151</b> |
| 9.1      | 2013 年国内网络安全监管动态 .....   | 151        |
| 9.2      | 2013 年国外网络安全监管动态 .....   | 154        |

|           |                       |            |
|-----------|-----------------------|------------|
| <b>10</b> | <b>国内网络安全组织发展情况</b>   | <b>168</b> |
| 10.1      | 网络安全信息通报成员发展情况        | 168        |
| 10.2      | CNVD 成员发展情况           | 171        |
| 10.3      | ANVA 成员发展情况           | 173        |
| 10.4      | CNCERT/CC 应急服务支撑单位    | 175        |
| <b>11</b> | <b>国内外网络安全重要活动</b>    | <b>178</b> |
| 11.1      | 国内重要网络安全会议和活动         | 178        |
| 11.2      | 国际重要网络安全会议和活动         | 181        |
| <b>12</b> | <b>2014 年网络安全热点问题</b> | <b>186</b> |
| <b>13</b> | <b>网络安全术语解释</b>       | <b>189</b> |

# 2013<sup>年</sup>

## 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

CN  ERT/CC

人民邮电出版社  
北京

## 图书在版编目(CIP)数据

2013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,  
2014.5

ISBN 978-7-115-35502-7

I. ①2… II. ①国… III. ①互联网络—安全技术—  
研究报告—中国—2013 IV. ①TP393.408

中国版本图书馆CIP数据核字(2014)第083653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2013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。

## 2013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 2014年5月第1版  
字数: 130千字 2014年5月北京第1次印刷

ISBN 978-7-115-35502-7

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

# 《2013 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 | 王明华 | 严寒冰 | 李 佳 | 贺 敏 | 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 |     |     |
|         | 摆 亮 | 陈 阳 | 李世淙 |     |     |
|         | 党向磊 | 徐晓燕 | 王适文 |     |     |
|         | 刘 婧 | 饶 毓 | 赵 宸 |     |     |

# 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、网络安全企业相关部门网络安全工作情况和数据的基础上，《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。

《2013 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、网络安全企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 2013 年开展的防范治理黑客地下产业链专项行动，对 DDoS 攻击的监测分析等进行专题介绍，并吸纳互联网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 2013 年国内外网络安全监管动态、国内网络安全组织发展情况、国内外网络安全重要活动做了阶段性总结。最后，针对当前网络安全的热点和难点问题，对 2014 年网络安全的威胁和形势做出判断。

国家互联网应急中心

2014 年 4 月