国家互联网应急中心

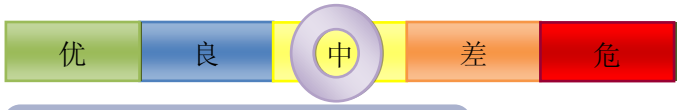
2013 年第 27 期

7 月 1 日-7 月 7 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

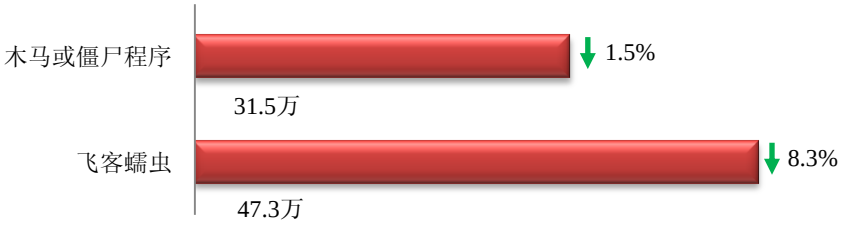


境内感染网络病毒的主机数量	•78.8万	5.7%
境内被篡改网站总数 其中政府网站数量	•6075 •439	23.6% 16.8%
境内被植入后门网站总数 其中政府网站数量	•2460 •102	4.2% 16.4%
针对境内网站的仿冒页面数量	•1058	16.4%
新增信息安全漏洞数量 其中高危漏洞数量	•137 •36	5.5% 37.9%

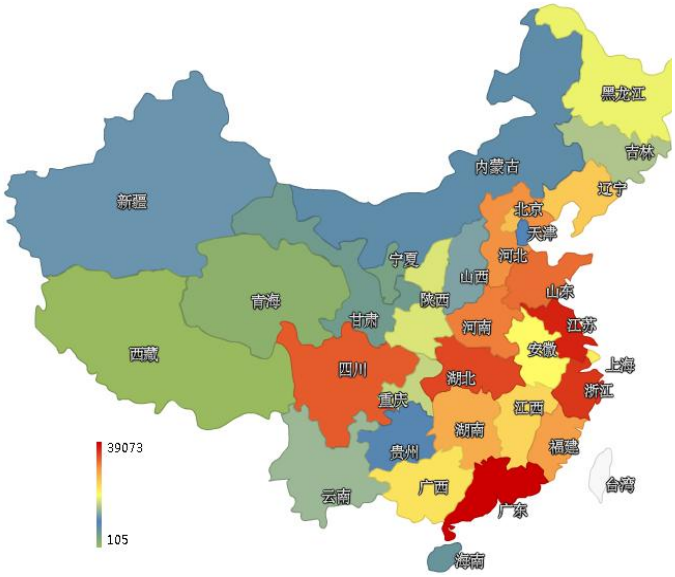
表示数量与上周相同 *表示数量较上周环比增加* *表示数量较上周环比减少*

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 78.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 31.5 万以及境内感染飞客（conficker）蠕虫的主机约 47.3 万。



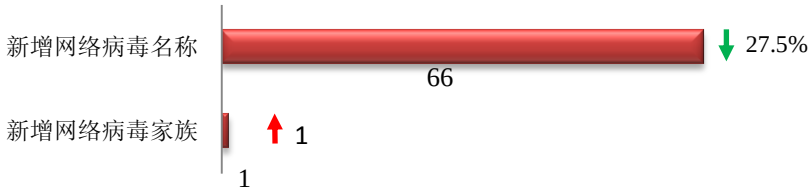
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。



TOP3

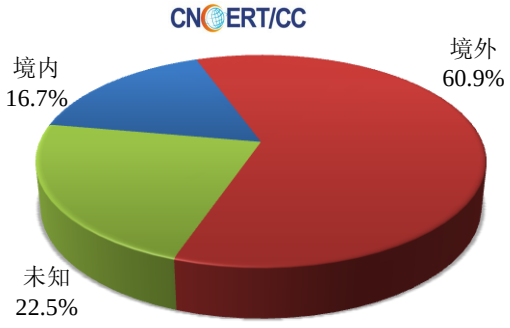
广东省	•约3.6万个（约占中国大陆总感染量的11.4%）
江苏省	•约3.2万个（约占中国大陆总感染量的10.1%）
浙江省	•约2.1万个（约占中国大陆总感染量的6.8%）

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 66 个，按网络病毒家族统计新增 1 个。

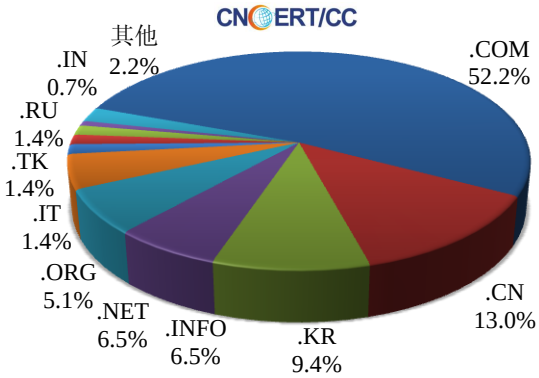


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 138 个，涉及 IP 地址 224 个。在 138 个域名中，有约 60.9%为境外注册，且顶级域为.com 的约占 52.2%；在 224 个 IP 中，有约 58.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 95 个 IP。

本周放马站点域名注册所属境内外分布
(7/1-77)



本周放马站点域名所属顶级域的分布
(7/1-7/7)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

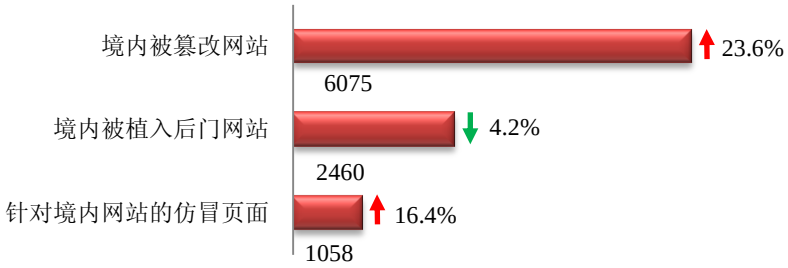
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

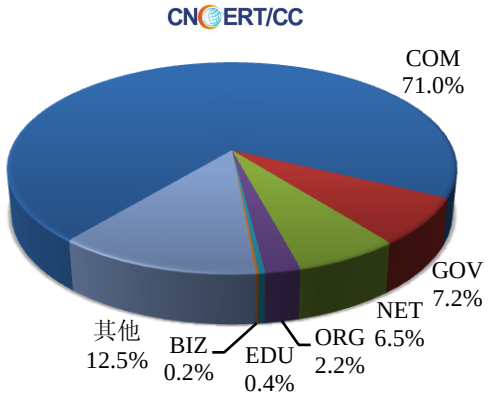
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 6075 个；境内被植入后门的网站数量为 2460 个；针对境内网站的仿冒页面数量为 1058 个。

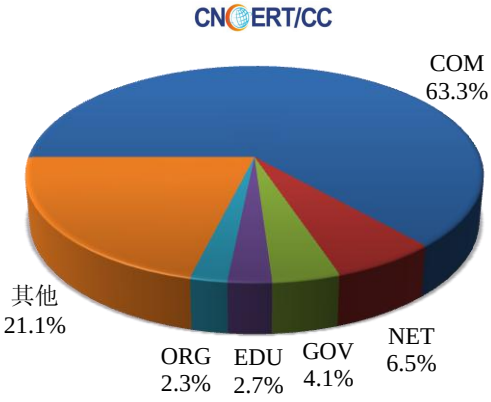


本周境内被篡改政府网站(GOV 类)数量为 439 个（约占境内 7.2%），较上周环比增长了 16.8%；境内被植入后门的政府网站(GOV 类)数量为 102 个（约占境内 4.1%），较上周环比减少了 16.4%；针对境内网站的仿冒页面涉及域名 711 个，IP 地址 242 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/1-7/7)

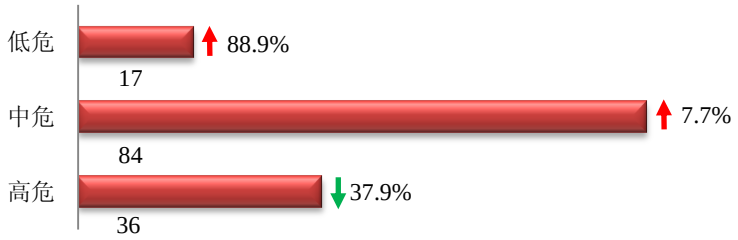


本周我国境内被植入后门网站按类型分布
(7/1-7/7)

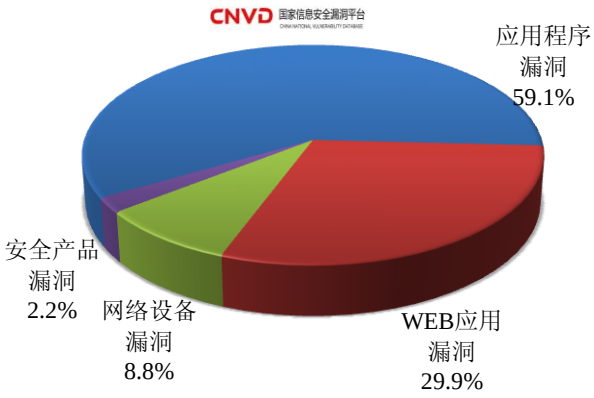


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 137 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象类型分布
(7/1-7/7)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 web 应用漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

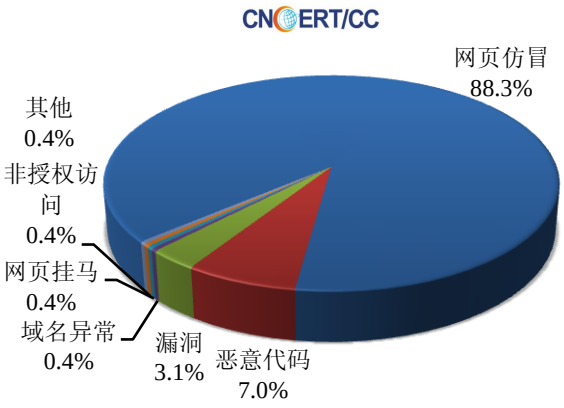
http://www.cnvd.org.cn/publish/main/47/index.html

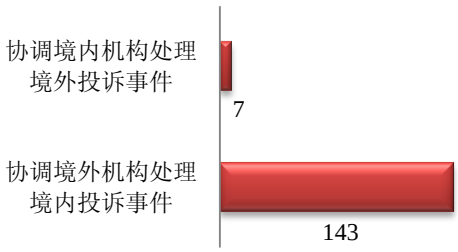
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 257 起，其中有跨境网络安全事件 150 起。

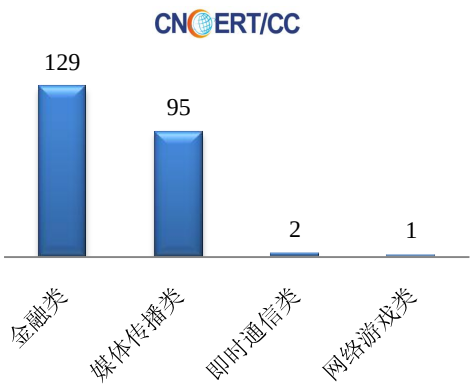
本周CNCERT处理的事件数量按类型分布
(7/1-7/7)



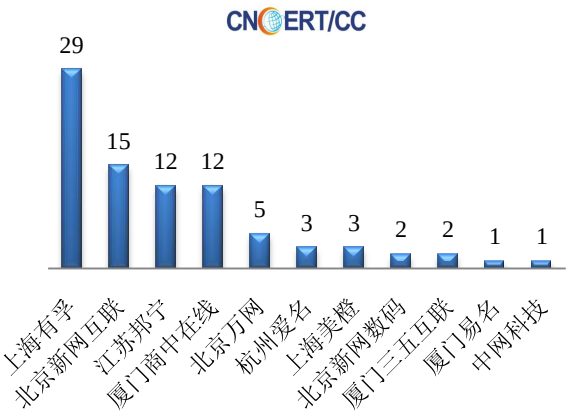


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 227 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含建设银行等金融类仿冒事件 129 起和湖南卫视等媒体传播类仿冒事件 95 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(7/1-7/7)

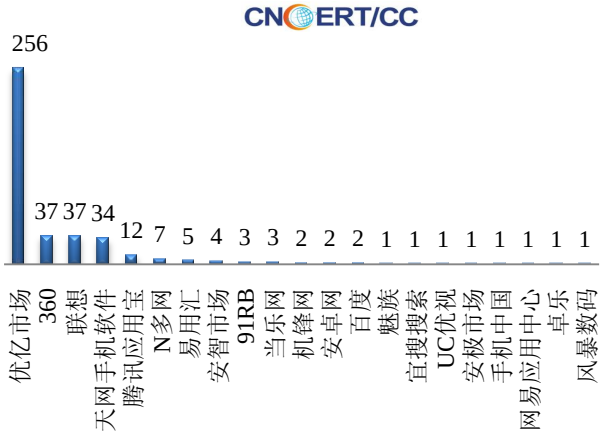


本周CNCERT协调境内域名注册机构处理
网页仿冒事件数量排名 (7/1-7/7)



本周CNCERT协调手机应用商店处理移动互
联网恶意代码事件数量排名 (7/1-7/7)

本周，CNCERT 协调 21 家应用商店开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 412 个。



本周重点网络安全信息

1、2013 年中国计算机网络安全年会在呼和浩特召开

2013 年 7 月 4 日，2013 年中国计算机网络安全年会（第 10 届）在内蒙古呼和浩特市召开。工业和信息化部张峰总工程师出席大会开幕式并作大会主旨报告，张峰简要回顾了近年来互联网和通信行业主管部门工业和信息化部维护网络安全的方针和工作，并进一步对信息通信行业提出做好网络安全工作的五点要求。一是加强网络安全工作联动，深化跨部门跨行业协调配合。二是加强防护应急能力建设，强化网络安全环境综合治理。三是加强新型网络安全威胁的研究投入，探求有效应对措施与保障技术。四是加强网络安全国际交流合作，推动网络安全领域经验共享。五是加强网络安全宣传教育，促进网络安全防范意识与知识水平提高。国家互联网应急中心副总工程师杜跃进应邀在大会上作了题为“新时代网络安全的应对之路”的报告。

2013 年中国计算机网络安全年会由国家互联网应急中心主办，历经十年发展，目前已成为国内外网络安全领域进行技术业务交流的重要平台。工业和信息化部总工程师张峰、内蒙古自治区政府副秘书长曹晓斌、内蒙古自治区通信管理局局长乌力吉、工业和信息化部通信保障局副局长熊四皓、大会组委会主席国家互联网应急中心主任黄澄清、中国通信学会副理事长兼秘书长张新生、科学技术部高新技术发展及产业司处长王春恒、中国电子学会副秘书长林润华、国家互联网应急中心副主任云晓春等贵宾出席了开幕式。来自政府和重要信息系统部门、行业企业、高校和科研院所等单位的代表共四百余人参加了本次会议。

2、45 家单位荣获第五届 CNCERT 网络安全应急服务支撑单位称号

为强化公共互联网网络安全应急技术体系建设，促进我国网络安全应急服务的规范化和本地化，结合互联网网络安全应急工作以及国内网络安全服务行业的发展需要，国家互联网应急中心（以下简称“CNCERT”）于 2013 年 5 月份启动了第五届 CNCERT 网络安全应急服务支撑单位的评选工作。评选分为初审和现场答辩两个环节。共计收到 65 个单位的申请材料，有 54 个单位通过初审。2013 年 7 月 3 日，CNCERT 在内蒙古自治区呼和浩特市举行了第五届 CNCERT 网络安全应急服务支撑单位评选会议。来自工业和信息化部、中国信息安全认证中心、CNCERT、国家网络安全技术研究所的相关专家组成了评选委员会，从企业实力、应急技术能力、应急服务规范、支撑 CNCERT 工作情况等方面出发，遵循公开、公平、公正的原则，对通过初审的参选单位进行了细致的评估和审查。会议最终评选出 8 个国家级网络安全应急服务支撑单位和 37 个省级网络安全应急服务支撑单位。

CNCERT 自 2004 年开始启动了“CNCERT 网络安全应急服务支撑单位”的选拔工作。经过九年发展，应急服务支撑单位已成为我国互联网网络安全应急体系的重要组成部分，为维护互联网网络安全做出了积极贡献，在国家重大活动期间为保障网络安全发挥了重要的技术支撑作用。

业界新闻速递

1、孟建柱：加强国际合作打击犯罪 维护网络安全

新华网符拉迪沃斯托克 7 月 4 日电 7 月 2 日至 4 日，中共中央政治局委员、中央政法委书记孟建柱出席在俄罗斯符拉迪沃斯托克举行的第四届安全事务高级代表国际会议，就网络和信息安全作主旨发言。孟建柱指出，维护网络和信息安全是各国维护国家安全的重要内容。面对网络信息安全威胁和挑战，各国必须加强合作，共

同承担网络安全责任。他强调，国际社会要积极合作打击各种网络犯罪，加快制订信息安全国际行为准则，坚决反对网络冲突。期间，孟建柱还出席了金砖国家代表团团长非正式会晤，并同金砖国家代表就加强执法安全合作深入交换意见，就共同制订网络和信息安全行为准则达成共识。

2、中韩将定期举行通信部级战略对话 加强网络安全交流

人民网北京 7 月 2 日电 据工业和信息化部网站消息，6 月 28 日中韩 5G 交流会在北京召开。会议期间，中国 IMT-2020（5G）推进组与韩国 5G 论坛，中国网络应急协调机构 CNCERT 与韩国网络应急协调机构 KrCERT 之间分别签署了《中韩 5G 合作谅解备忘录》和《中韩网络安全合作谅解备忘录》。据韩媒报道，上述备忘录包含共同应对智能型网络攻击、“钓鱼”、DDoS（分布式拒绝服务攻击）等行为的内容。签署此次谅解备忘录后，中韩两国将成立工作小组，互相交流网络保安人才，共享网络威胁信息。韩国未来创造科学部第二次官尹宗录表示，中韩第一次信息通信合作部级战略对话最快将于今年下半年或明年上半年召开首轮会议。

3、2012 中国互联网网络安全报告发布 用户信息成黑客窃取重点

人民网 7 月 4 日消息，国家互联网应急中心（CNCERT）发布了《2012 年中国互联网网络安全报告》。报告显示，2012 年，我国未发生重大网络安全事件。然而，针对我国网络基础设施的探测、渗透和攻击事件时有发生，虽尚未造成严重危害，但高水平、有组织的网络攻击给网络基础设施安全保障带来严峻挑战。据不完全统计，2012 年有 50 余个我国网站用户信息数据库在互联网上公开流传或通过地下黑色产业链进行售卖，其中已证实确为真实信息的数据近 5000 万条。2012 年，网络钓鱼日渐猖獗，严重影响在线金融服务和电子商务的发展，危害公众利益。由于互联网用户通过网络开展的经济活动持续增多，在线销售和支付总额增长迅速，窃取经济利益成为黑客实施网络攻击的主要目标之一。2012 年，移动互联网恶意程序快速繁衍和扩散，危害用户隐私安全，或造成垃圾短信泛滥，给感染用户造成话费损失等，Android 平台成恶意程序重灾区。

4、新加坡军队将建立网络防卫中心抵御黑客袭击

环球网 7 月 1 日消息 据新加坡《联合早报》7 月 1 日报道，新加坡国防部长黄永宏透露，新加坡武装部队为提升对抗网络袭击的能力，将成立网络防卫行动中心(Cyber-Defence Operations Hub，简称 CDOH)，以更全面并系统地防御日益严峻的网络袭击威胁。新成立的网络防卫行动中心将从新加坡国防部、武装部队和国防科技机构现有的人员当中调用这方面的专门人才，执行探测、识别、控制和消除网络威胁的工作。该中心将全天候运作，除了检测和应对网络威胁，必要时它也能快速修复新家坡的军事网络。此外，网络防卫行动中心还将与新加坡资讯通信科技安全局(Singapore Infocomm Technology Security Authority，简称 SITSA)合作，以获取最新的资讯安全科技和了解网络威胁。

5、应对上半年连续出现的黑客事件 韩国出新规加强互联网安全措施

人民网 7 月 5 日消息 据《朝鲜日报》报道， 为系统应对类似“3.20”、“6.25”这样的网络威胁，韩国未来创造科学部 7 月 4 日公布了《国家网络安保综合对策》。根据该对策的内容，为了及时应对分布式拒绝服务（DDoS）等网络攻击，将在总统府青瓦台新设网络应对组织来发挥控制塔的作用。国情院将担任实务总管，与未来部、国防部等部门进行合作。同时还决定在 2014 年前构筑“网络威胁信息共享系统”，扩大与民间部门的信息共享。与此同时，发电站、铁路、港口以及水电站等国家基础设施的内部网按照规定必须与外部网分离。为了增强网络安全，将在 2017 年前培养 5000 多名应对黑客攻击的“反黑客”人员。此外，韩国金融委员会 7 月 4 日表示已制定《金融计算机安保强化综合对策》，该规定包括金融公司若发生重大计算机事故，首席执行官（CEO）将

有可能受到“停职”等严惩，以及大型金融公司的内部网和外部互联网应当分离等内容。

6、俄军网罗 IT 人才打造专门打击网络威胁独立部队

环球时报消息 俄罗斯国防部长绍伊古 7 月 4 日在与多名高校校长和社会代表会面时表示，俄军将到地方高校网罗 IT 人才，为年底成立打击网络威胁的独立部队“科技连”输送人才。绍伊古表示，首个“科技连”将从地方高校招收 35 名士兵，并将建在沃罗涅日军事科技中心，这一中心拥有设备完善的实验室，可以为海军、航空、航天及其他各个领域的科研机构培养人才。未来还将在各个军兵种中推广成立“科技连”。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网路安全技术协调组织，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，开展中国互联网上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。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 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。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990316