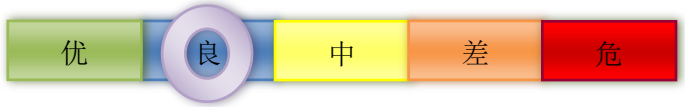
国家互联网应急中心

2016 年第 24 期

6 月 6 日-6 月 12 日

网络安全信息与动态周报

本周网络安全基本态势

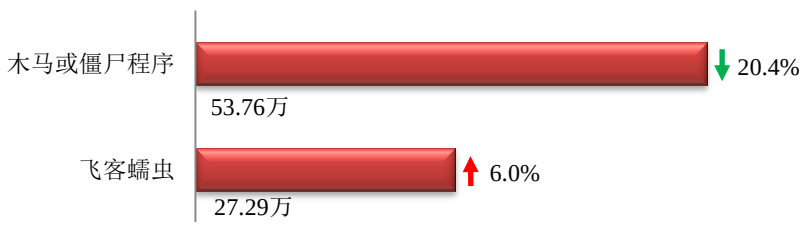


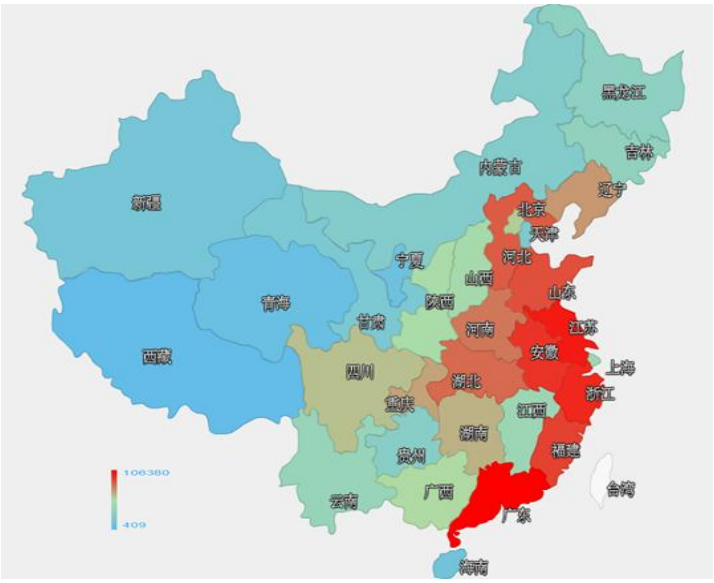
境内感染网络病毒的主机数量	•81.05万	13.1%
境内被篡改网站总数 其中政府网站数量	•2471 •66	20.6% 4.3%
境内被植入后门网站总数 其中政府网站数量	•2581 •80	2.2% 21.2%
针对境内网站的仿冒页面数量	•1444	31.6%
新增信息安全漏洞数量 其中高危漏洞数量	•118 •36	3.5% 200.0%

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 81.05 万个，其中包括境内被木马或被僵尸程序控制的主机约 53.76 万以及境内感染飞客（conficker）蠕虫的主机约 27.29 万。



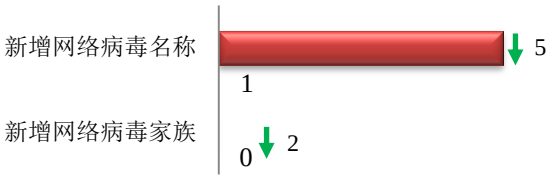


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

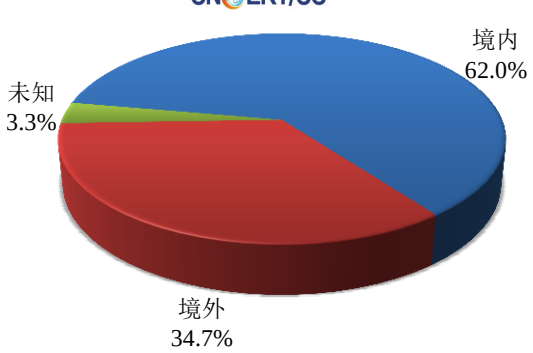
广东省	•约10.6万个（约占中国大陆总感染量的19.8%）
江苏省	•约4.9万个（约占中国大陆总感染量的9.2%）
浙江省	•约4.3万个（约占中国大陆总感染量的8.0%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计无新增。

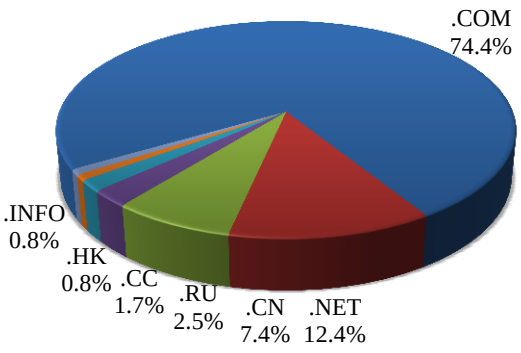


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 121 个，涉及 IP 地址 292 个。在 121 个域名中，有 34.7%为境外注册，且顶级域为.com 的约占 74.4%；在 292 个 IP 中，有约 8.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 20 个 IP。

本周放马站点域名注册所属境内外分布
(6/6-6/12)



本周放马站点域名所属顶级域的分布
(6/6-6/12)



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。

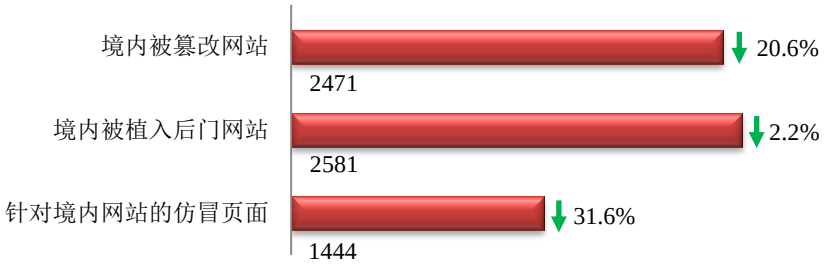
ANVA恶意地址黑名单发布地址

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。

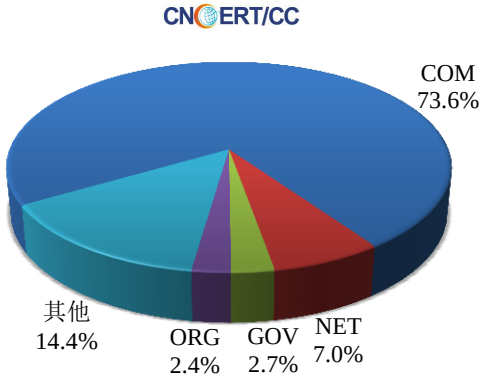
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2471 个；境内被植入后门的网站数量为 2581 个；针对境内网站的仿冒页面数量为 1444。

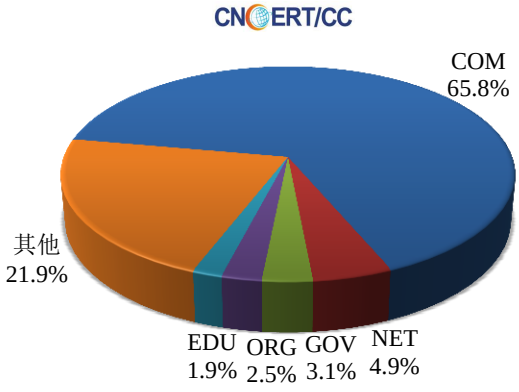


本周境内被篡改政府网站（GOV 类）数量为 66 个（约占境内 2.7%），较上周环比下降了 4.3%；境内被植入后门的政府网站（GOV 类）数量为 80 个（约占境内 3.1%），较上周环比上升了 21.2%；针对境内网站的仿冒页面涉及域名 1048 个，IP 地址 366 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/6-6/12)

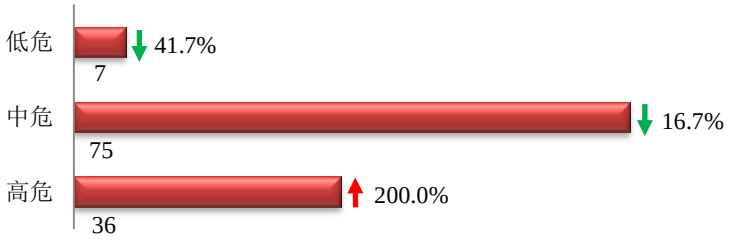


本周我国境内被植入后门网站按类型分布
(6/6-6/12)

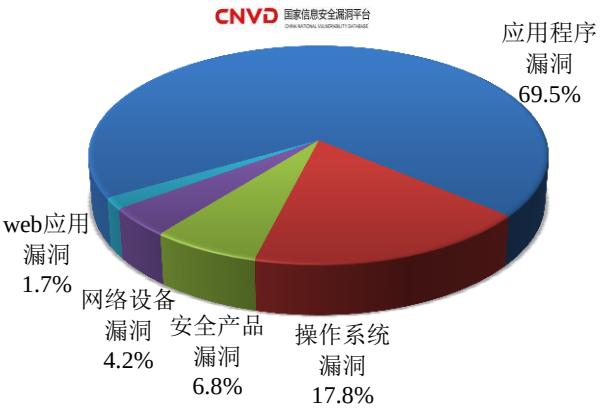


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 118 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
(6/6-6/12)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和安全产品漏洞。

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

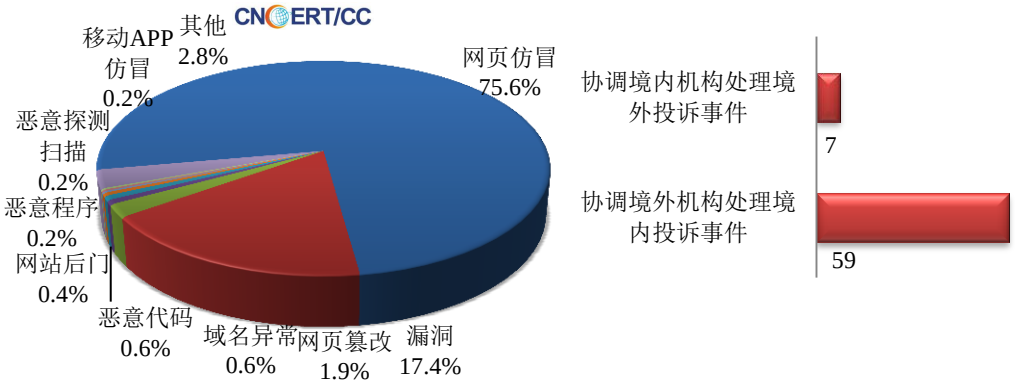
http://www.cnvd.org.cn/webinfo/list?type=4

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

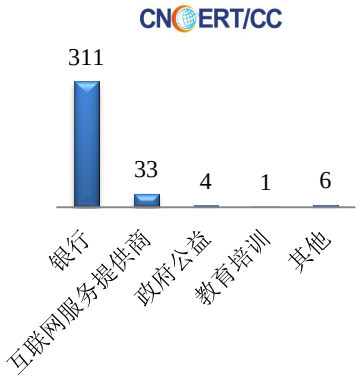
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 471 起，其中跨境网络安全事件 66 起。

本周CNCERT处理的事件数量按类型分布
(6/6-6/12)

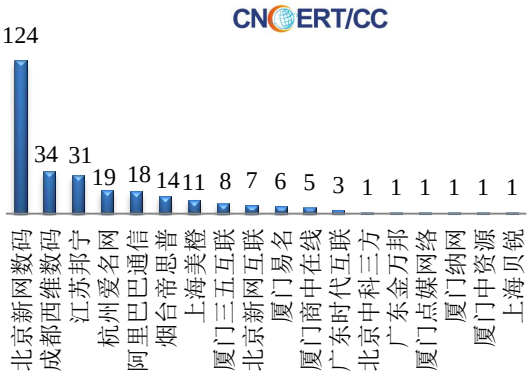


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 355 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 311 起和互联网服务提供商仿冒事件 33 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/6-6/12)

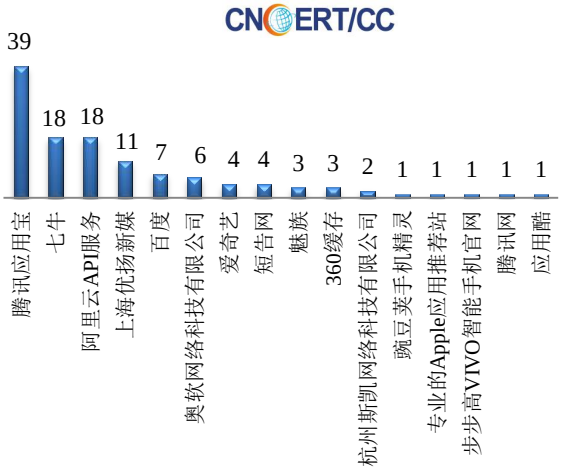


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/6-6/12)



本周，CNCERT 协调 16 个应用商店及挂载恶意程序的域名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 120 个。

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 (6/6-6/12)



业界新闻速递

1、工信部布局八大领域推进电信和互联网行业网络安全试点示范工作

通信产业网 6 月 12 日消息 近日，为进一步推进电信和互联网行业网络安全技术手段建设，工信部根据《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》和工信部 2016 年重点工作安排，发布《工业和信息化部关于开展 2016 年电信和互联网行业网络安全试点示范工作的通知》，决定继续组织开展电信和互联网行业网络安全试点示范工作（以下简称试点示范）。试点示范是在 2015 年工作基础上，将工作覆盖对象拓展至互联网企业和网络安全企业，包括各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，各互联网域名注册管理和服务机构，各互联网企业，各网络安全企业有关单位。其目的在于继续引导企业加大网络安全投入，加强网络安全技术手段建设，全面提升网络安全态势感知能力，促进先进技术和经验在行业的推广应用，增强企业防范和应对网络安全威胁的能力，切实提升电信和互联网行业网络安全防御能力。试点示范申报项目应为支撑企业自身网络安全工作或为客户提供安全服务的已建成并投入运行的网络安全系统（平台）。项目遴选应综合考虑项目的实用性、创新性、先进性、可推广性，重点考察试点示范项目是否具备良好的应用效果、扎实的实践基础和技术创新性，能否坚持持续改进，发挥综合效益。对于入选的试点示范项目，工业和信息化部将在其申请国家专项资金、科技评奖等方面，按照有关政策予以支持。

2、美将举行大型网络攻击演习 模拟核心设备遭袭击

环球网 6 月 8 日消息 美国“华盛顿自由灯塔”网站 6 月 6 日刊登比尔·格茨的文章称，美国网络司令部本周将举行一场大规模网络攻击演习。而这一持续一个月的大规模演习将模拟国家电网等美国的核心基础设施遭受他国网络攻击的情况。报道称，此次演习代号为“网络守卫 16”，是美国近年来规模最大的年度演习，涉及美国众多军事单位，五角大楼、美国联邦调查局、国土安全部以及非政府部门的人员也参与其中。演习模拟的场景是美国的关键基础设施遭到网络攻击，目的是寻求应对他国通过数字攻击瘫痪美国电网和金融网络的方案。文章称，此次演习将持续一个月，旨在检验跨政府和军队部门之间的安全合作，以及政府与非政府部门在应对网络攻击方面的配合。美国网络司令部担心，联邦政府在保卫电网这个最核心的基础设施的安全力度还不够。去年 12 月，针对乌克兰电网的网络攻击凸显了电网面临的风险。美国联邦调查局从那时起，开始向美国电力公司发布针对美国电网的网络威胁。今年 4 月，美军网络司令部司令罗杰斯担忧地说，他不知道网络司令部能否帮助美国应对电网可能遭遇的多重网络攻击。报道称，一名美国网络司令部发言人拒绝提供“网络守卫 16”演习的演练详情，只表示可以参照去年的演习情况。去年，来自政府、学界、行业和美国盟友的 100 个组织参加了在弗吉尼亚州举行的类似演习。

3、英议会通过新数字监控法案：加强监控也要保隐私

网易 6 月 8 日消息 据路透社报道，英国议会下院周二通过了新的数字监控法，赋予安全机构更广泛的监控职能。在此之前，这部法案经过了一些修正，以更好地保护个人隐私。英国议会下院的议员们以 444 票赞成、

69 票反对的投票结果，通过了《调查权力法案》（Investigatory Powers Bill）。英国内政大臣特丽莎·梅（Theresa May）表示，该法案将有助于“在一个不确定的世界里，保护我们的安全。”在获得英国议会下院的批准后，该法案将呈交至英国议会上院表决。英国议会下院的一些议员对这项法案投了反对票，其中包括来自反对党苏格兰民族党的议员，他们认为该法案对隐私的保护力度不够。去年 11 月，英国首相戴维·卡梅伦（David Cameron）的政府宣布计划制定一部涵盖广泛新权力的法案，该法案将迫使高科技公司将每位用户访问网站的细节存储一年以上的时间，以及明确规定情报机关收集大量数据并侵入私人计算机及智能手机的权限。特丽莎·梅称该法案在监控上的力度是“史无前例的”，同时表示该法案包含了新的保护隐私的条款，要求各机构尽可能考虑用侵扰程度较低的手段来实现同样的目的，并对国会议员、律师和记者进行特殊保护。她告诉议会：“这部法案带来了更大透明度，改进了安全保障措施，加强了对隐私的保护并引入了新的、世界领先的监督机制。”

4、俄“Facebook”1.7 亿用户信息被盗 黑市交易仅 1 比特币

凤凰网 6 月 6 日消息 据科技博客 ZDNet 报道，欧洲最大社交网站、俄版“Facebook”——VK.com 网站 1.71 亿名用户的账号信息遭到黑客侵袭。不过令人不可思议的是，黑客将这些用户信息拿到黑市上兜售，开口要价仅为 1 比特币，约合 580 美元。社交网络 VK.com 原名为 vkontakte.ru，是俄罗斯最大的类 Facebook 社交网站，拥有 3.5 亿多名用户，在俄罗斯可谓是一统江湖。据悉，黑客早在 2012 年年末或者 2013 年年初就对该网站实施了攻击，在截获来自 VK.com 网站的数据库中，包括完整的用户名、电子邮件地址以及纯文本密码，很多账号还包括有位置和电话号码信息。但目前尚无确切消息，到底是哪一黑客组织实施了此次攻击。鉴于黑客攻击的时间点——2012 年年末或者 2013 年年初，当时 VK 的用户将近 1.9 亿，因而这一数字很可能就是黑客所盗取客户信息的大约数据。但目前该黑客组织仅在网络黑市上兜售了其中的部分账号数据——涉及 1 亿名账户，容量约为 17GB。不过令人匪夷所思的是，他们在黑市上对这些数据的要价仅为 1 比特币，约合 580 美元。在 VK 网站上的公共搜索引擎当中输入这些账号，发现许多用户名为有效账号。进一步核查发现，少数用户名为无效账号，搜索结果提示这些用户名已不存在或停用。与其中的部分电子邮件进行联系，暂未有回应结果。

5、日本将对 35 个重要单位实施监控 防范网络攻击

中新网 6 月 8 日消息 据日媒报道，日本政府消息人士 6 月 7 日透露，为了针对网络攻击加强防范力度，日本政府已基本决定从 2017 年度开始监控 35 个左右与太空开发、核能等相关的重要单位是否受到攻击。报道称，由于今年 4 月日本的网络对策相关法修订后，原先仅限于日本中央各部门的监控对象将扩大到独立行政法人等，这将是首批新增单位。在 2020 年东京奥运和残奥会到来之前加紧建设网络防御力量。据称，约 35 个单位将以一旦遭到网络攻击可能对国民生活造成重大影响为标准进行选择。2017 年度预算申请中将计提约 10 亿日元（约合人民币 6100 万元）相关费用。具体包括拥有尖端科学技术的日本宇宙航空研究开发机构（JAXA）、新能源和产业技术总合开发机构（NEDO）、日本原子能研究开发机构以及涉及众多个人信息的都市再生机构（UR）等独立行政法人。此前发生个人信息泄露事件的日本年金机构等特殊法人及认证法人中也将指定 5 个左右。预计将在今秋由日本政府的网络安全战略总部最终敲定，2018 年以后还将逐步增加。监控对象的扩大是由于日本年金机构的问题暴露出独立行政法人和特殊法人在网络攻击威胁下的脆弱性。监控业务将由专门负责网络防御工作的独立行政法人“信息处理推进机构”24 小时全天候应对。

6、为防泄密 新加坡将禁公务员电脑接互联网

新华网 6 月 10 日消息 为防止信息泄露，新加坡要求所有公务员使用的公务电脑从明年 5 月起停止接入互联网。新加坡《海峡时报》8 日报道，断网通知已传达给所有政府部门及法定机构，涉及大约 10 万台电脑。这一举措将于 4 月在新加坡资讯通信发展管理局（资信局）试行。政府雇员今后只能用没有接入政府电子邮件系统的个人平板电脑和手机上网。如需用互联网工作，他们可以使用互联网专用终端。另外，如有必要，公务员可以向他们的个人账户发送工作邮件。资信局负责开发、推广和管理新加坡的资讯通信产业。资信局一名发言人说：“新加坡政府经常检查资信局的信息技术（IT）措施，让网络更安全。”《海峡时报》说，在网络安全威胁增加的情况下，这一举措旨在防堵信息由电子邮件或分享文件泄露。在新加坡，即使对电脑使用规定最严格的银行、电讯公司和赌场，切断所有工作电脑互联网连接亦属罕见。出于对员工可能无意间从问题网站下载恶意软件或在网上分享敏感信息的担忧，银行只允许分析师、销售人员和公关人员使用互联网，同时禁止登录文件分享网站、使用网页版电子邮件和浏览色情网站。全球计算机安全组织云安全联盟亚太区执行副主席阿洛伊修斯·张（音译）说，新加坡政府此举意味着回到上世纪 90 年代的做法，当时只允许使用互联网专用终端上网。“恶意程序过去很难从政府网络获取敏感信息，”他说，“现在则难以防止信息由社交媒体和文件分享网站泄露。”

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 2002 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 2015 年，CNCERT 与 66 个国家和地区的 165 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：赵慧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158