国家互联网应急中心

2016 年第 5 期

1 月 25 日-1 月 31 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

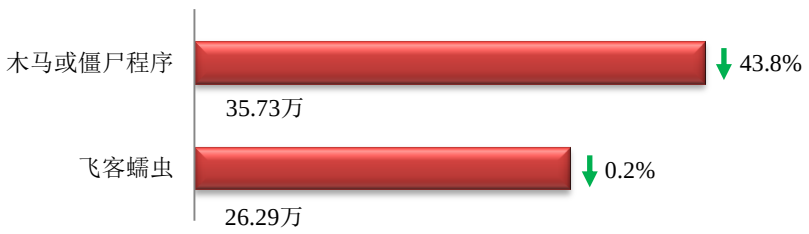
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	•62.02万	↓31.0%
境内被篡改网站总数 其中政府网站数量	•4133 •58	↓3.8% ↓19.4%
境内被植入后门网站总数 其中政府网站数量	•1035 •36	↓15.8% ↓26.5%
针对境内网站的仿冒页面数量	•1826	↓36.1%
新增信息安全漏洞数量 其中高危漏洞数量	•286 •42	↑73.3% ↓25.0%

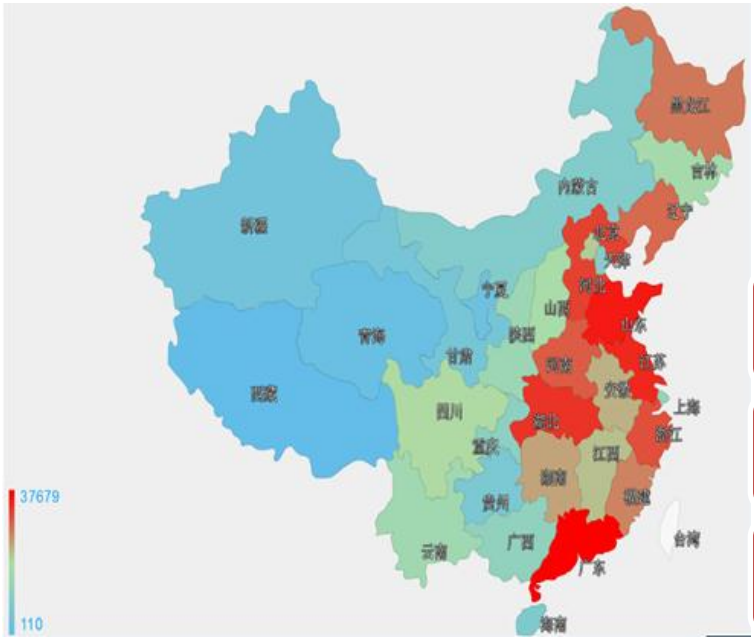
=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 62.02 万个，其中包括境内被木马或被僵尸程序控制的主机约 35.73 万以及境内感染飞客（conficker）蠕虫的主机约 26.29 万。



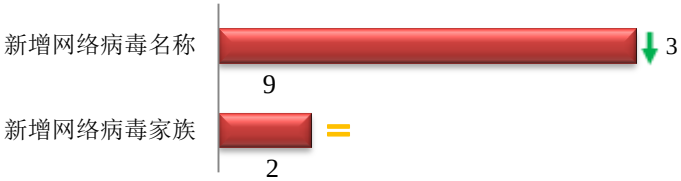
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和江苏省。



TOP3

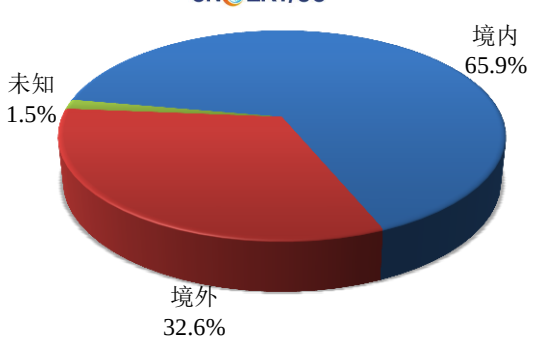
广东省	•约3.8万个（约占中国大陆总感染量的10.5%）
山东省	•约3.3万个（约占中国大陆总感染量的9.2%）
江苏省	•约3.3万个（约占中国大陆总感染量的9.1%）

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 9 个，按网络病毒家族统计新增 2 个。

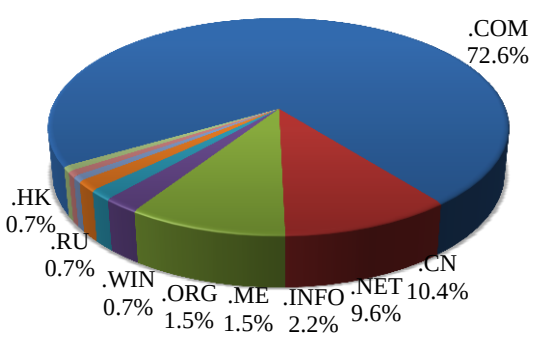


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 135 个，涉及 IP 地址 304 个。在 135 个域名中，有约 32.6%为境外注册，且顶级域为.com 的约占 72.6%；在 304 个 IP 中，有约 10.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 51 个 IP。

本周放马站点域名注册所属境内外分布
(1/25-1/31)



本周放马站点域名所属顶级域的分布
(1/25-1/31)



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。

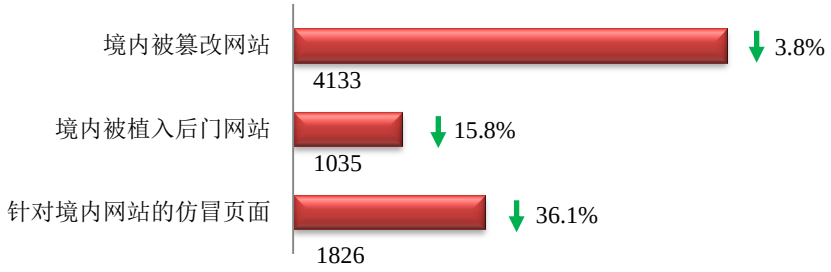
ANVA恶意地址黑名单发布地址

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。

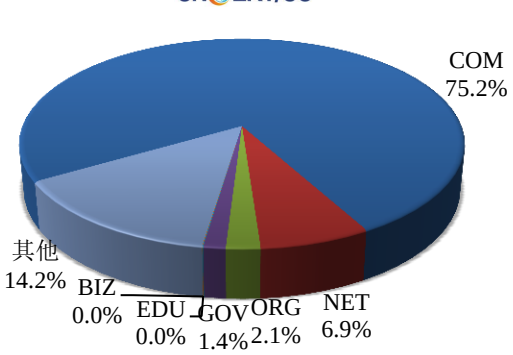
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4133 个；境内被植入后门的网站数量为 1035 个；针对境内网站的仿冒页面数量为 1826。

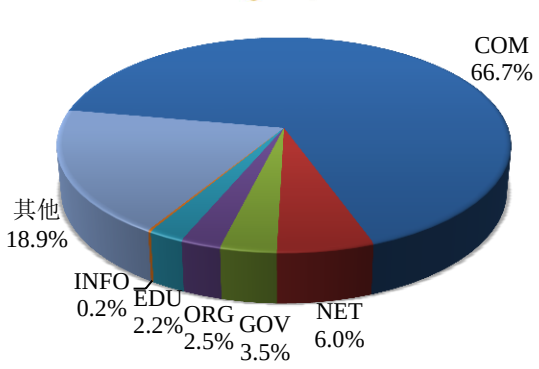


本周境内被篡改政府网站(GOV 类)数量为 58 个（约占境内 1.4%），较上周环比下降了 19.4%；境内被植入后门的政府网站(GOV 类)数量为 36 个（约占境内 3.5%），较上周环比下降了 26.5%；针对境内网站的仿冒页面涉及域名 1569 个，IP 地址 515 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/25-1/31)

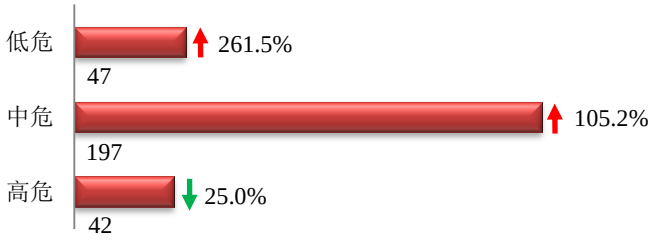


本周我国境内被植入后门网站按类型分布
(1/25-1/31)

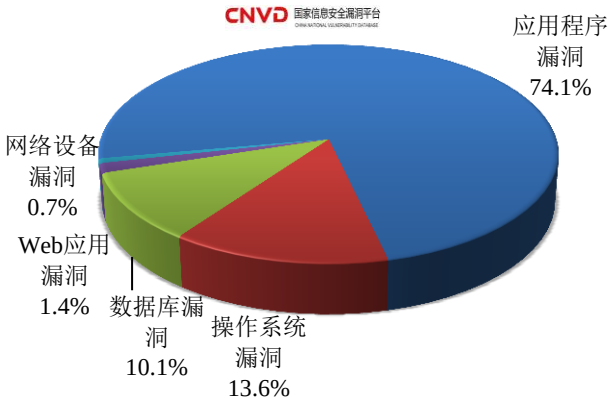


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 286 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
(1/25-1/31)



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数据库漏洞。

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

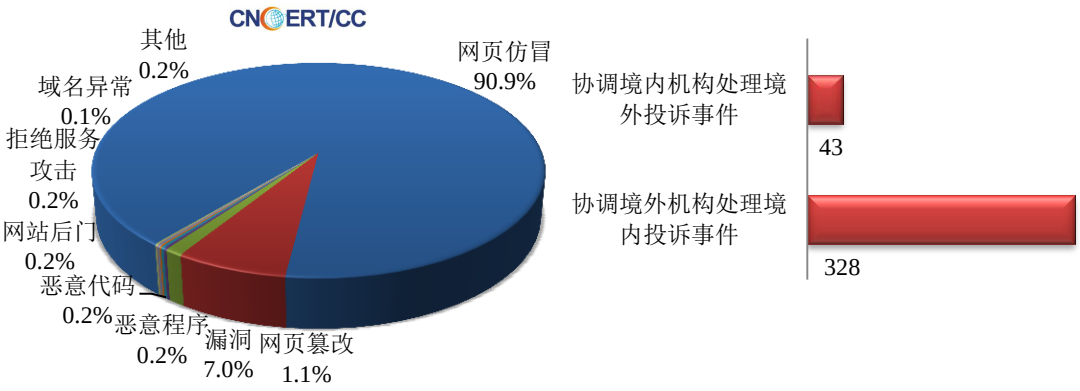
http://www.cnvd.org.cn/webinfo/list?type=4

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

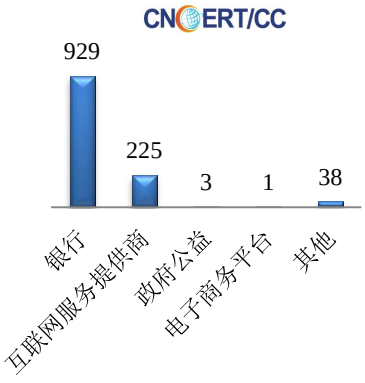
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1316 起，其中跨境网络安全事件 371 起。

本周CNCERT处理的事件数量按类型分布
(1/25-1/31)

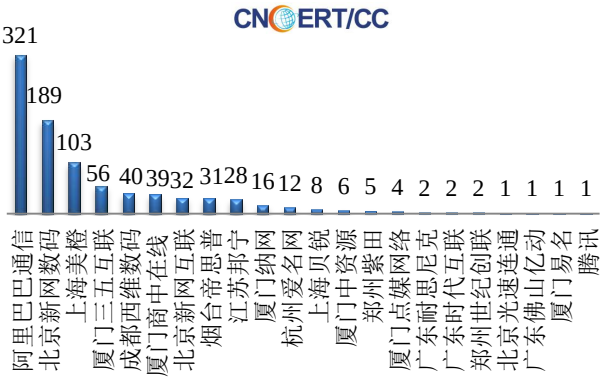


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1196 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 929 起和互联网服务提供商仿冒事件 225 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(1/25-1/31)

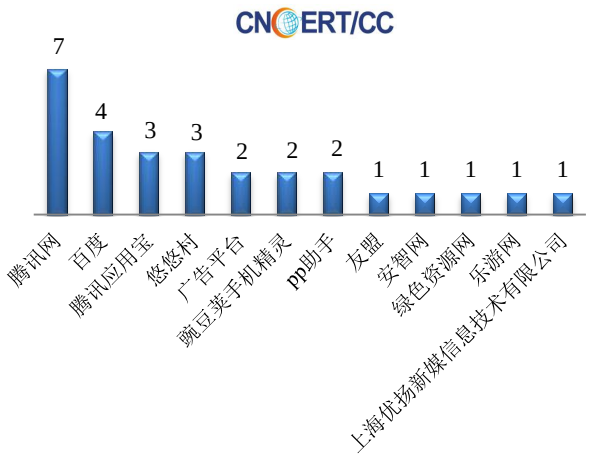


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/25-1/31)



本周，CNCERT 协调 12 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 28 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 (1/25-1/31)



业界新闻速递

1、中国印尼将搞网络战演习 日媒：树立外交新先例

参考消息网 1 月 28 日消息 日媒称，有关印尼和中国将合作举行网络战演习的新闻，本身对于地区战略关系具有足够重大的意义。与此同时，它显示两国对于网络战所应具备的样式有着超前的理解，这将为各国应如何进行合作以准备应对网络战最有可能带来的冲击树立新的外交先例。据日本外交学者网站 1 月 26 日报道，印尼《时代》周刊报道说，两国将制订一个合作计划，其内容包括“网络战模拟、网络战对策、网络监控、网络危机管理和数据中心恢复计划”等。这一计划的意图似乎并非旨在进行联合军事合作，而是把重点放在政府就网络战对于民用基础设施不可避免的影响所应采取的对策上。日前披露的拟议中的网络协作涵盖四个领域：信息与通信技术战略（出于决策目的的网络安全意识以及国家基础设施发展中的网络安全）；业务和技术的能力建设（在数字刑侦、信息安全、网络安全、网络风险管控、大数据分析及数字经济方面）；网络安全联合研究（加密操作系统、网络法律、网络恐怖主义及网络反情报）；联合行动（网络战模拟、网络战对策及缓解手段、网络监控、网络危机管控及恢复）。这一拟议中的网络关系涵盖范围之广，远远超出了中国与其他发展中国家的同类关系。向印尼媒体透露拟议中与中国的网络合作的官员是印尼国家网络安全信息局的专家穆赫利斯 •艾哈迈迪。他也认同这种看法，即大多数中等大国无法自行确保国家网络安全。他认为，“成功的网络空间危机管控的关键是协作和共享”。

2、工信部决定在浙江试点云计算信息安全管理工作

中国信息产业网 1 月 27 日消息 近日，工信部决定在浙江阿里云计算有限公司开展云计算业务信息安全管理工作试点。据了解，工信部网络安全管理局、中国信息通信研究院相关专家在调研阿里云计算有限公司云计算业务信息安全技术手段建设情况的基础上认为：云计算业务具有 IDC 机房跨省分布、机房间高速互联流量全局调度、承载业务动态迁移流动性强等特点，传统 IDC 业务信息安全技术手段已无法满足监管要求，结合新版电信业务分类目录的发布，亟须完善配套管理措施，开展相关工作试点十分迫切。为此，工信部计划在浙江的阿里云计算有限公司开展云计算业务信息安全管理工作试点。试点工作由中国信息通信研究院会同浙江省通信管理局及相关企业组建试点专项小组，共同制定云计算业务信息安全管理技术标准，通过试点验证标准及技术手段建设方案的可行性、有效性，为新形势下加强云计算业务信息安全管理提供经验。

3、证监会进行跨行业信息安全应急演练

搜狐网 1 月 29 日消息 证监会新闻发言人张晓军 1 月 29 日表示，证监会联合电力电信部门进行证券期货市场信息安全联合应急演练，证监会副主席方星海担任副主任，包括上交所网上信息系统遭遇网络攻击等七个场景的演练。一是针对性强，二是实战型强，三是协同性强。当前，金融信息与网络安全风险已经成为金融风险的形式之一，证监会已经把行业应急演练工作常态化，自 2009 年以来，连续八年开展应急演练，逐步从行业内模拟演练，过度到行业内真实演练，遭到跨行业真实演练，有利于提高证券期货行业整体的安全保障能力。

4、机密文件曝光：美英长期监听以色列空军活动

新华网 1 月 31 日消息 一份最新曝光的机密文件显示，美国和英国长期以来秘密监听以色列空军活动，最早可以追溯到 1998 年。这份文件由美国国家安全局承包商前雇员爱德华•斯诺登获得，29 日经多家媒体披露。报道称，美国国家安全局和英国负责通信技术监控的情报机构“政府通信总部”先前监听过以色列空军针对加沙、叙利亚和伊朗的活动，监听活动代号“无政府主义者”，以塞浦路斯为基地，对象还包括中东地区其他国家。文件显示，英国政府通信总部 2008 年曾在一份报告中称，这一监听活动“必不可少”，能帮助美英“持续了解以军培训、行动以及将来可能在这一地区的行动”。以色列政府对于新披露的监听活动表示遗憾。以安全内阁成员、能源部长尤瓦尔•施泰尼茨说，这种监听活动或许不是针对以色列的“最大秘密”，但显然让以色列感到不满，“我们将不得不考虑更换加密系统”。

5、欧盟寻求制定网络安全共同政策 打击跨国网络犯罪

国际在线 1 月 27 日消息 正在荷兰阿姆斯特丹举行的欧盟司法与内政部长非正式会议 26 日重点讨论了网络安全问题。会议提议，欧盟内部各国要加强网络安全信息的分享，寻求制定统一的网络安全政策，并与互联网提供商进行合作，以打击跨国网络犯罪。担任今年上半年欧盟轮值主席国的荷兰将网络安全问题列为任期内的一项重要工作。上一任欧盟轮值主席国卢森堡曾提议于今年秋天讨论有关网络空间司法管辖权的问题，也就是谁有权在数字世界行使法律权力，但荷兰提前将这个问题列入日程。荷兰安全与司法大臣范德斯图尔说，其中一个问题就是各成员国在有关网络安全方面的法规不统一。虽然互联网供应商愿意提供合作，许多供应商也按照法律的要求愿意公开电子记录，但各国有关隐私保护和数据披露的规定不同，从而使跨国网络犯罪的调查陷于混乱。欧盟司法事务委员维耶拉 • 尤罗娃当天表示，网络犯罪没有边境，但欧盟各国却拥有各自的司法管辖权。因此，欧盟需要一个应对网络犯罪的共同政策。据悉，来自各成员国的法律专家将于今年 3 月开会讨论在这方面取得的进展，但目前欧盟委员会还没有出台统一网络安全政策的具体时间。另外，欧盟委员会的官员还将与互联网供应商展开“对话”，以找到精确定位网络攻击的位置的方法，从而使一个国家的警察能更容易地从另外一个国家得到传唤嫌犯的电子证据。

6、荷兰政府计划扩大防止数据泄露的义务范围

中国网信网 1 月 29 日消息 据 telecompaper 2016 年 1 月 22 日报道，荷兰政府计划实施一项针对报告数据泄露和网络安全事件的法律义务。相关法案已经提交议会二院，要求核心部门政府和公司在发生网络安全事件时向国家网络安全中心（National Cyber Security Center）汇报。该法律义务是否会适用于电力、天然气、核能、水、电信、交通运输、金融和政府等领域，尚不能最终确定。这些行业都是国家关键基础设施的组成部分，对事故处理不善可能会直接或间接引发社会混乱。其实该法律义务已经部分存在，但政府想要增加更多条款，加强其法律效力。介于部分行业和业务的敏感性，公共安全与司法部想针对公司和安全专家之间的信息交换建立一个独立线路。国家网络安全中心不仅要具备相应的工具手段，还要具有专业运营知识，以备发生意外情况时能够介入并采取措施。这项举措是为了加强对工业和服务业的数据保护，不涉及私人数据。新法案是建立在一月份刚刚生效的针对私人数据汇报义务之上的。数据保护法（Data Protection Act）和电信法（Telecommunications Act）都包含此类的汇报要求。

7、以色列国家电网遭受有史最大规模网络攻击

搜狐网 1 月 27 日此消息 以色列能源与水力基础设施部部长 Yuval Steinitz 已经披露称，该国电力供应系统受到重大网络攻击侵袭，且已经有多份报告表明勒索软件正是造成事故的直接原因。在 CyberTech 2016 大会上，Steinitz 谈到以色列的网络安全现状时指出“昨天（2016 年 1 月 25 日）我们确认了有史以来出现过的规模最大的网络攻击。”尽管此次针对国家关键性基础设施的攻击活动规模极大，但 Steinitz 指出“其使用的病毒已经被查明，而且我们准备了应急预警方案对其进行处理。”“我们不得不中止了该以色列电力设施当中大量计算机的运行。我们目前正着手处理这一状况，我希望这一严重事故能够很快得到平息，”他表示。相关计算机设备已经关闭了两天，并于 1 月 26 号重新上线。以色列电力局已经向各方记者确认了此次攻击行为，而其出现时机恰好选在了以色列当地的严冬时节。目前尚不清楚到底是谁策划并实施了此次攻击，有消息指出：“我们需要相关网络技术以预防此类攻击行为。针对基础设施的网络 攻击活动能够导致发电站乃至整套能源供应链发生瘫痪，其中涵盖天然气、石油、汽油以及供水系统，并可能造成人员伤亡等严重后果。”“以色列必须认真考虑其日常运作体系可能面临的攻击威胁。关键性基础设施正越来越多地成为安全威胁的指向目标，而且虽然尚缺乏有效的个案研究结论，但业界普遍认为这类状况正有愈演愈烈之势。”

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 2014 年，CNCERT 与 63 个国家和地区的 144 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：吕志泉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158