国家互联网应急中心

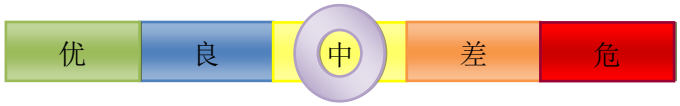
网络安全信息与动态周报

2016 年第 11 期

3 月 7 日-3 月 13 日

CNCERT/CC

本周网络安全基本态势

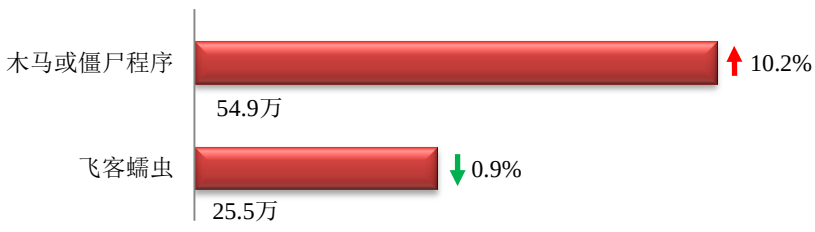


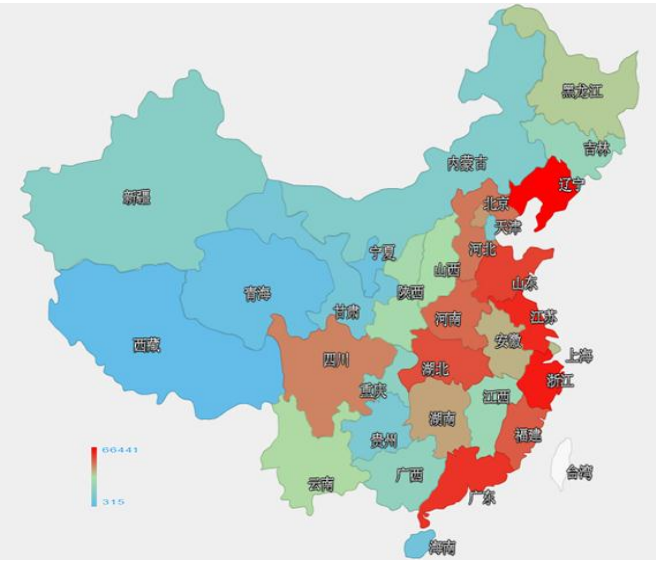
境内感染网络病毒的主机数量	•80.4万	↑ 6.4%
境内被篡改网站总数 其中政府网站数量	•4018 •69	↑ 3.6% ↑ 21.1%
境内被植入后门网站总数 其中政府网站数量	•1767 •81	↓ 11.6% ↑ 26.6%
针对境内网站的仿冒页面数量	•4043	↑ 0.3%
新增信息安全漏洞数量 其中高危漏洞数量	•119 •68	↑ 16.7% ↑ 126.7%

═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 80.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.9 万以及境内感染飞客（conficker）蠕虫的主机约 25.5 万。



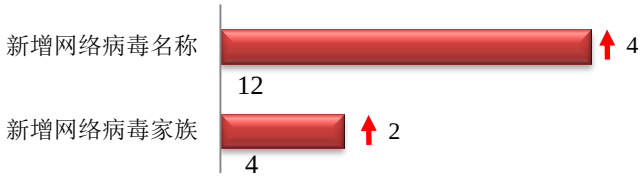


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是辽宁省、浙江省和江苏省。

TOP3

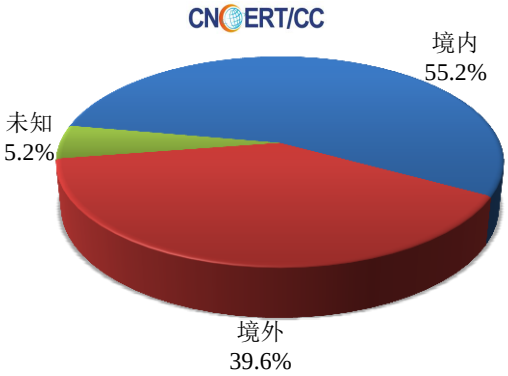
辽宁省	•约6.6万个（约占中国大陆总感染量的12.1%）
浙江省	•约6.5万个（约占中国大陆总感染量的11.9%）
江苏省	•约5.2万个（约占中国大陆总感染量的9.5%）

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 12 个，按网络病毒家族统计新增 4 个。

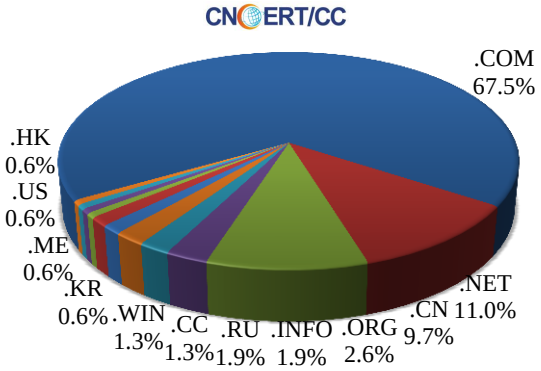


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 154 个，涉及 IP 地址 425 个。在 154 个域名中，有约 39.6%为境外注册，且顶级域为.com 的约占 67.5%；在 425 个 IP 中，有约 9.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 40 个 IP。

本周放马站点域名注册所属境内外分布
(3/7-3/13)



本周放马站点域名所属顶级域的分布
(3/7-3/13)



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。

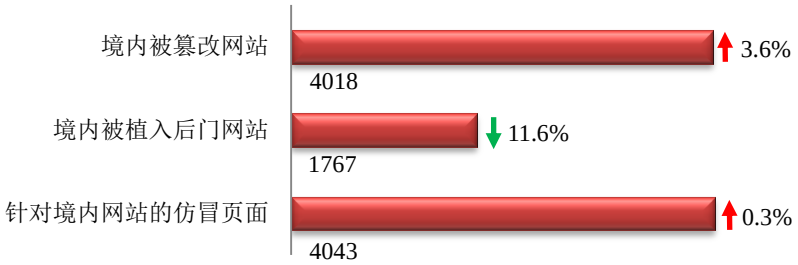
ANVA恶意地址黑名单发布地址

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。

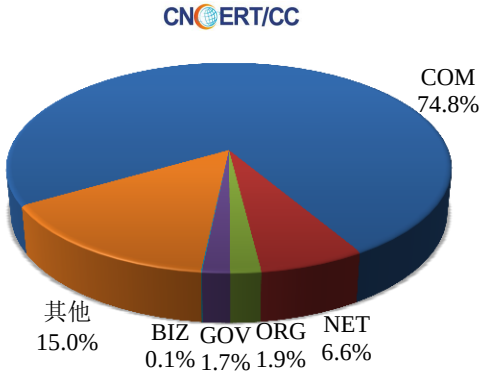
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4018 个；境内被植入后门的网站数量为 1767 个；针对境内网站的仿冒页面数量为 4043。

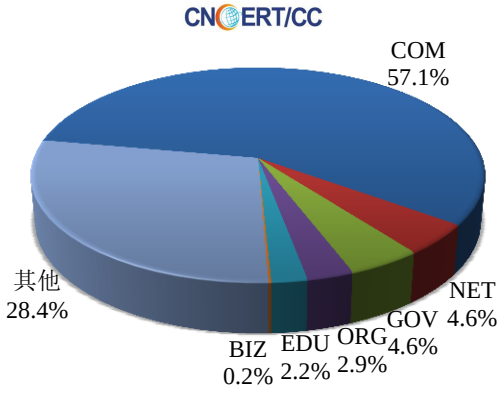


本周境内被篡改政府网站(GOV 类)数量为 69 个（约占境内 1.7%），较上周环比上升了 21.1%；境内被植入后门的政府网站(GOV 类)数量为 81 个（约占境内 4.6%），较上周环比上升了 26.6%；针对境内网站的仿冒页面涉及域名 3491 个，IP 地址 1094 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/7-3/13)

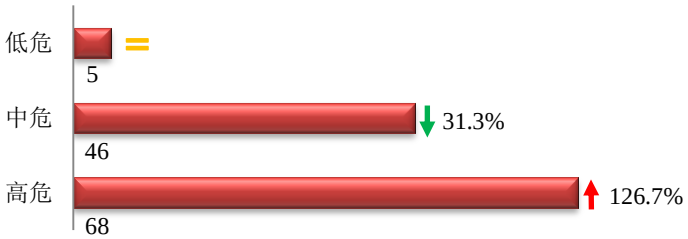


本周我国境内被植入后门网站按类型分布
(3/7-3/13)

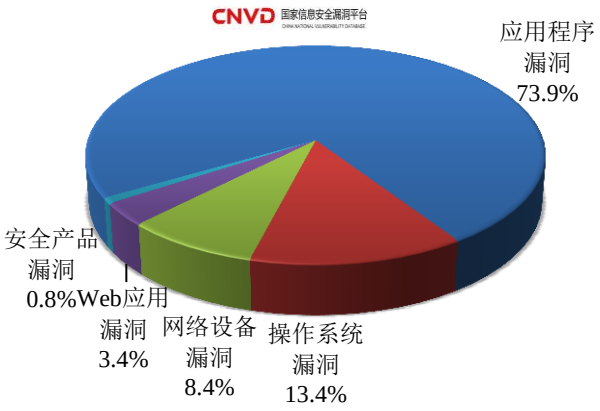


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 119 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(3/7-3/13)



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

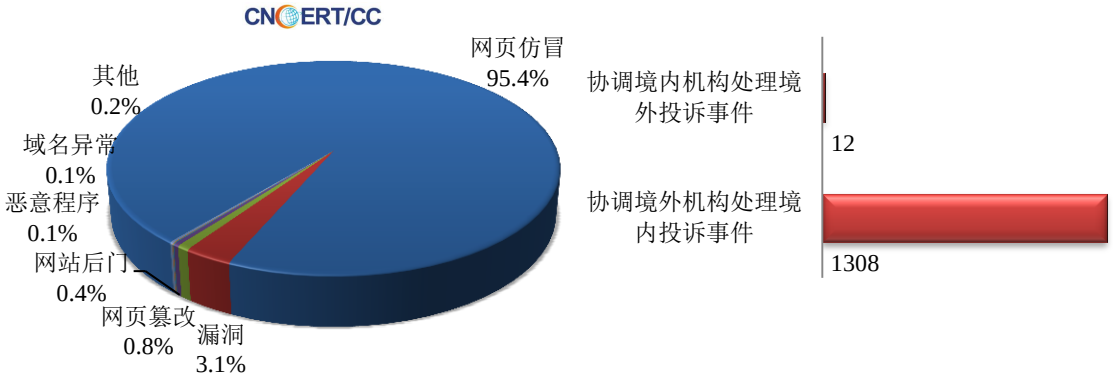
http://www.cnvd.org.cn/webinfo/list?type=4

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 3868 起，其中跨境网络安全事件 1320 起。

本周CNCERT处理的事件数量按类型分布
(3/7-3/13)



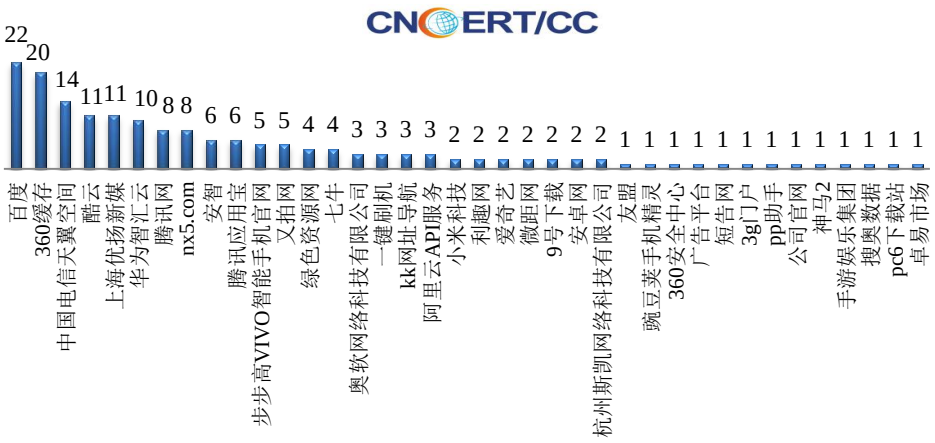
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 3692 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 3396 起和互联网服务提供商仿冒事件 291 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/7-3/13)

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 (3/7-3/13)

本周，CNCERT 协调 38 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 173 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
(3/7-3/13)



业界新闻速递

1、韩美拟强化网络安全合作 共同研发应对网络袭击技术

环球网 3 月 7 日消息 据韩联社 3 月 6 日报道，韩国未来创造科学部 3 月 6 日表示，未来部次官（副部长）崔在裕当地时间 3 月 3 日在美国与美国国土安全部科学与技术局副秘书雷金纳德·布拉泽斯举行会谈，商定加强两国网络安全合作。双方决定将全面加强三个领域的合作，具体包括共同开发技术、进一步分享全球网络威胁信息，加强网络安全政策对接。在共同研发技术领域，双方将联合划拨网络安全研发预算，携手研发最新网络袭击应对技术。在信息共享领域，韩美两国将深入发展现有两国网络应急小组之间威胁信息共享体系。在政策合作方面，双方将推动网络安全领域司长级会议实现常态化，共谋政策合作并携手应对网络袭击。

2、韩国情报院称朝鲜黑客攻击韩方政府官员智能机

比特网 3 月 10 日消息 韩国国家情报院（NIS）称：朝鲜黑客已经攻入韩国一些关键政府官员的智能手机。上周二，韩国国家情报院（NIS）表示：在二月下旬和三月上旬间，朝鲜完成其第四次核试验后，来自朝鲜的网络间谍从韩国主要官员的智能手机中窃取了大量敏感数据和文本消息等。朝鲜已经对韩国发起了无数次的网络攻击。朝鲜黑客曾对专门为网上银行提供安全服务器的大型软件公司发起攻击，还对两个省级铁路运营商的员工发动了网络钓鱼活动，还曾往受害者的移动设备发送含有恶意链接的短信等。安全专家认为，朝鲜的黑客正在掀起针对韩国重要基础设施发起网络攻击的新热潮，其中包括铁路交通控制系统等。“朝鲜已经启动了一系列针对我国网络空间的攻击行动”，NIS 说：“他们似乎已经准备对韩国的银行网络进行大规模的网络袭击行动。”“如果攻击行为实现，势必将导致重大的金融混乱，如银行网络瘫痪以及存款无法转移等问题。”面对朝鲜的步步紧逼，韩国共同民主党（Minjoo Party）表示，首尔正在加强对朝鲜的密切关注，并努力建立、通过反网络恐怖活动的法律，现在正在等待国民议会，希望通过法律形式给予 NIS 更多的监督权力。但同时也担心新的法律可能会给予政府不合理窥视政治对手的机会。

3、“2016 台湾资讯安全大会”开幕

新华网 3 月 7 日消息 “2016 台湾资讯安全大会”3 月 7 日在台北开幕，众多信息安全业者及研究人员汇聚一堂，探讨在新形势下为信息安全构建“铜墙铁壁”之道。记者在大会现场看到，电视屏幕上滚动着介绍前沿信息安全技术的信息，业内人士三五成群聚在一起热烈探讨。据大会主办单位《iThome 电脑报周刊》的总编辑吴其勋介绍，超过 60 家信息安全厂商参与今年大会，展示 100 多款最新的信息安全技术和数百款信息安全产品。大会将重点围绕 IT 基础建设安全、网际网络安全、行动装置安全以及资料安全等四方面的信息安全技术议题展开。同时，今年的大会规划了新兴安全威胁论坛、安全情资论坛、金融科技安全论坛、云端安全论坛及数位政府安全论坛等五场专业论坛，以进一步探讨信息安全新兴趋势及产业专属议题。丰富多彩的专业人士演讲是此次大会的重要特色。据了解，今年大会共安排了 60 多场信息安全领域演讲，其中包括近十场“大会主题演讲”。吴其勋表示，去年的台湾资讯安全大会吸引超过 2000 人参加，预计今年大会参加人数将突破 3000 人。

4、澳大利亚多个大型银行官方手机应用遭黑客攻击

中新网 3 月 11 日消息 据澳大利亚“新快网”3 月 10 日报道，澳大利亚大型银行的数百万客户，尤其是安卓系统使用者，正遭一项恶意程序盗取银行信息，甚至连双重安全验证都不起作用。据报道，目前澳大利亚联邦银行（Commonwealth Bank）、西太银行（Westpac）、国民银行（National Australia Bank）和澳新银行（ANZ Bank）的用户们现在都处于遭受攻击的风险之中。该恶意程序会一直“潜伏”在感染了病毒的设备里，用户打开有关的银行客户端，就会弹出一个伪造的登陆窗口，使用者的用户名和密码就这样被盗取。该恶意程序模仿了澳大利亚、新西兰和土耳其的 20 家银行的手机银行客户端，还有 PayPal、eBay、Skype、WhatsApp 等应用的登陆页面。该程序的攻击目标除了澳大利亚的四大银行外，还有其他的一些金融机构，比如：本迪戈银行（Bendigo Bank）、圣乔治银行（St. George Bank）和西澳银行（Bankwest）等。据悉，该程序在盗取登陆信息的同时，还能拦截手机利用短信发送双重安全验证的验证码，随后它会将验证码转发给黑客。小偷们一旦有了这些信息，不论身处何地都能够轻松地绕开银行的安全防护措施，直接登录到受害人的网上银行账户中进行转账。电脑安全软件公司 ESET 的高级研究员菲茨杰拉德（Nick FitzGerald）表示，随着时间的推移，该恶意程序已经变得更为复杂了，因为黑客也在不断地升级该软件以破解更多银行安全措施。菲茨杰拉德表示：“这对于澳大利亚和新西兰的银行业而言，是一个严重的打击，我们不能掉以轻心。”他还指出，“虽然现在只有 20 家银行的客户端遭到攻击，但是不排除这群犯罪分子会继续升级程序，攻击更多的银行客户端。”

5、网络遭侵入 孟加拉国央行被窃 8100 万美元

网易 3 月 13 日消息 孟加拉国中央银行在美国纽约联邦储备银行开设的账户今年 2 月遭黑客攻击，被窃取 8000 多万美元。不过，孟加拉国央行官员披露，由于黑客进行转账操作时拼错了一个英文单词，使银行得以幸运地避免 8 亿多美元损失。路透社 10 日援引孟加拉国央行两名高官的话报道，黑客侵入孟加拉国央行网络后，窃取银行转账安全证书，接着攻击央行在纽约联邦储备银行的账户，发出 30 多条转账申请，要求把账户里的钱转到一些菲律宾和斯里兰卡的实体机构。黑客成功地将总计 8100 万美元的 4 笔钱转账至菲律宾，但在进行第五笔转账时，黑客原本要把 2000 万美元转账至斯里兰卡一个叫“沙立卡基金会”的非营利组织，却把“基金会”的英文“foundation”拼成了“fandation”。这引起了这笔转账的中转银行德意志银行的注意，后者随即要求孟

加拉国央行核实信息。央行察觉账户被盗，立即终止交易。一名央行官员说，被终止的转账申请总额大约 8.5 亿至 8.7 亿美元。路透社记者发现，“沙立卡基金会”并非在斯里兰卡注册的非营利组织，眼下找不到该组织的联络方式。尽管未能全部得手，黑客还是窃取 8100 万美元。这是史上金额最大的银行盗窃案之一。孟加拉国央行表示，正与菲律宾反洗钱机构合作，已追回部分被盗款项。

6、奥巴马：科技界应在国会采取行动前妥协

腾讯网 3 月 13 日消息 3 月 12 日，据彭博社报道，美国总统奥巴马周五表示，像 FBI 正迫使苹果帮助解密的 iPhone 等智能手机，不应该被允许成为政府机构无法进入的“黑盒子”。他称科技界应该积极与政府配合，而非将问题扔给国会。奥巴马前往得克萨斯州奥斯汀市举办的年度科技娱乐界盛会“西南偏南”（SXSW），并发表演讲称：“如果你的观点是不管发生什么事，你都支持加密，那么我们就应该和可以重塑黑盒子。我认为，我们不该打破已经维持了 200 或 300 年的平衡，但很多人正将盲目迷恋手机置于其他价值观之上。”奥巴马是有史以来首位在 SXSW 演讲的现任美国总统。现在，FBI 正试图迫使苹果帮助调查人员解密加州圣贝纳迪诺市枪击案犯赛义德·法鲁克（Syed Farook）使用的 iPhone。苹果正对抗法庭要求其协助政府调查的裁决，称那将危及其加密技术。支持苹果立场的科技公司包括亚马逊、微软、Facebook 以及谷歌母公司 Alphabet 等。周四，政府提交了一份备忘录，认为苹果公司只需要派出 6 名员工，仅用 2 周时间就可以解密法鲁克的手机。尽管在与苹果解密大战中，白宫支持 FBI 的立场，但据说奥巴马本人认为，在隐私保护和满足执法机构需要之间维持平衡非常重要。苹果和其他科技公司认为，在加密产品中建立“后门”将让它们在与外国对手竞争时处于不利地位。它们还警告称，许多国家可能要求科技公司配合政府进行类似的调查。奥巴马称，妥协是有可能的，科技界必须提供帮助。他说：“我猜想，答案恐怕需要归结到如何开发一套系统，既让加密尽可能强大，钥匙尽可能安全，同时当我们遇到最重要的问题时，能够允许最少的人访问数据。”

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：顾笑南

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158