国家互联网应急中心

2015 年第 36 期

8 月 31 日-9 月 6 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

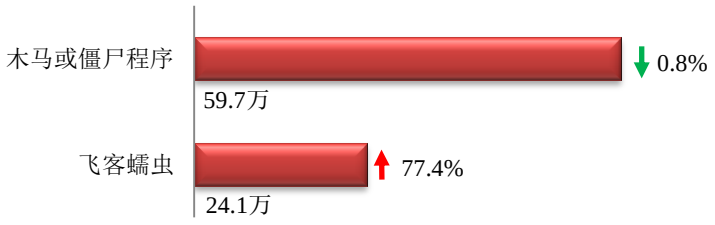
优 | 良 | 中 | 差 | 危

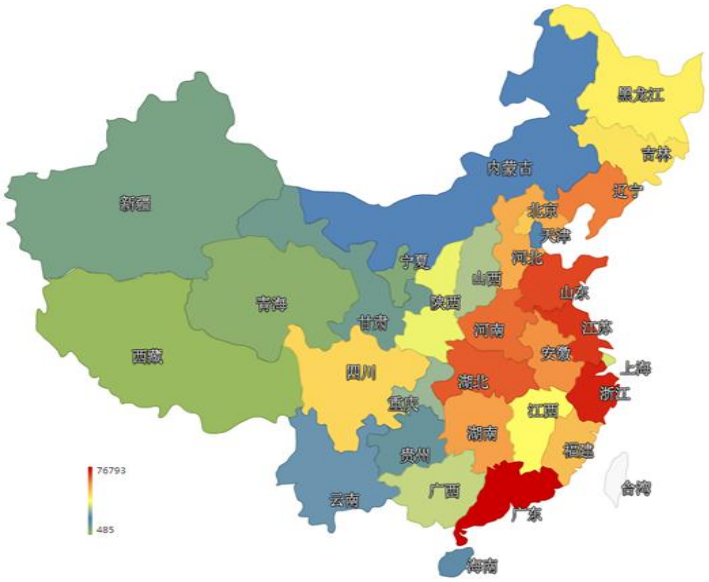
境内感染网络病毒的主机数量	•83.8万	↑ 13.6%
境内被篡改网站总数 其中政府网站数量	•5351 •86	↑ 90.0% ↑ 87.0%
境内被植入后门网站总数 其中政府网站数量	•4013 •136	↑ 1.9% ↓ 21.4%
针对境内网站的仿冒页面数量	•3323	↓ 26.2%
新增信息安全漏洞数量 其中高危漏洞数量	•92 •40	↓ 58.0% ↓ 38.5%

═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 83.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 59.7 万以及境内感染飞客（conficker）蠕虫的主机约 24.1 万。



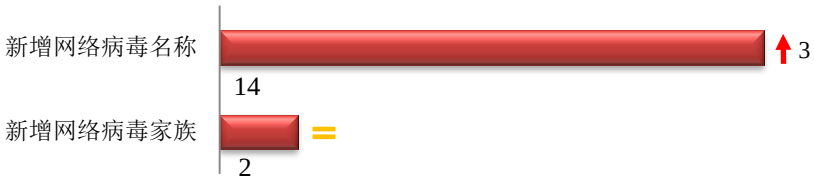


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

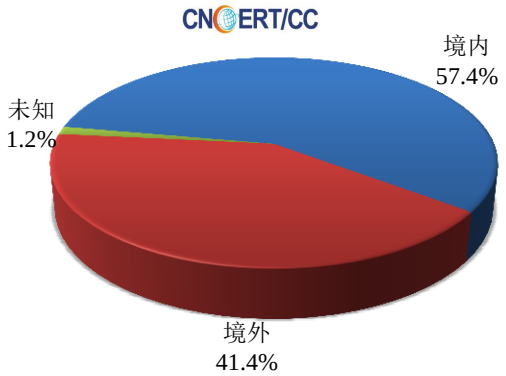
广东省	•约7.7万个（约占中国大陆总感染量的12.9%）
浙江省	•约7.4万个（约占中国大陆总感染量的12.4%）
江苏省	•约5.4万个（约占中国大陆总感染量的9.1%）

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 14 个，按网络病毒家族统计新增 2 个。

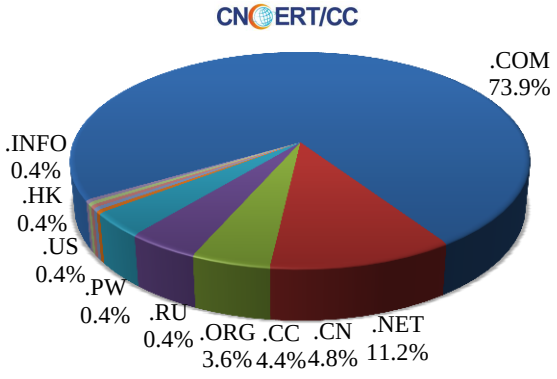


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 249 个，涉及 IP 地址 423 个。在 249 个域名中，有约 41.4%为境外注册，且顶级域为.com 的约占 73.9%；在 423 个 IP 中，有约 25.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 71 个 IP。

本周放马站点域名注册所属境内外分布
(8/31-9/6)



本周放马站点域名所属顶级域的分布
(8/31-9/6)



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。

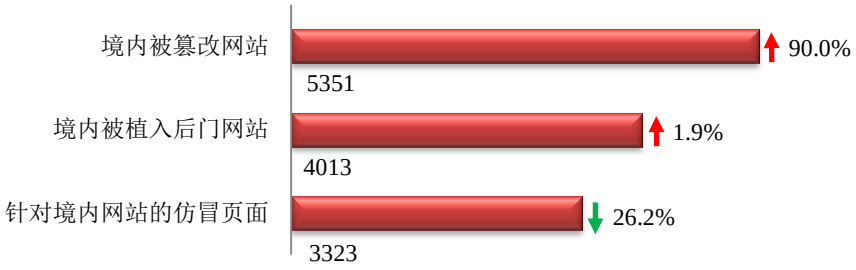
ANVA恶意地址黑名单发布地址

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。

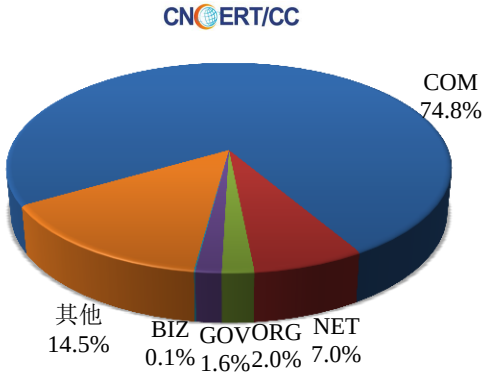
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 5351 个；境内被植入后门的网站数量为 4013 个；针对境内网站的仿冒页面数量为 3323。

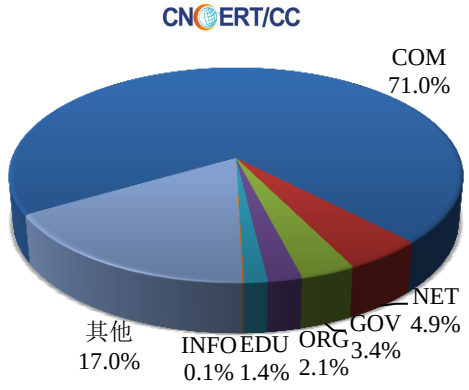


本周境内被篡改政府网站(GOV 类)数量为 86 个（约占境内 1.6%），较上周环比上升了 87.0%；境内被植入后门的政府网站(GOV 类)数量为 136 个（约占境内 3.4%），较上周环比下降了 21.4%；针对境内网站的仿冒页面涉及域名 2685 个，IP 地址 758 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/31-9/6)

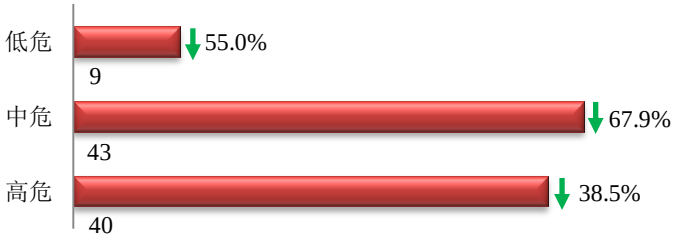


本周我国境内被植入后门网站按类型分布
(8/31-9/6)

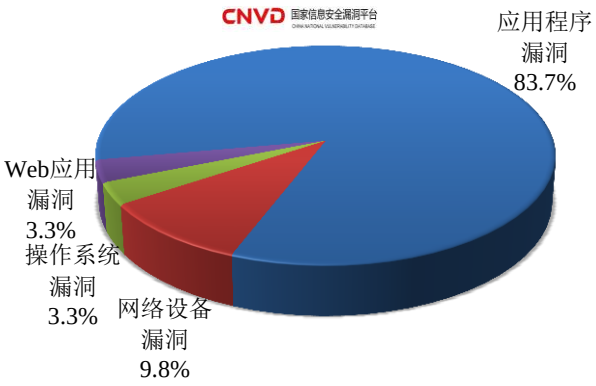


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 92 个，信息安全漏洞威胁整体评价级别为低。



本周CNVD收录漏洞按影响对象类型分布
(8/31-9/6)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和操作系统漏洞。

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

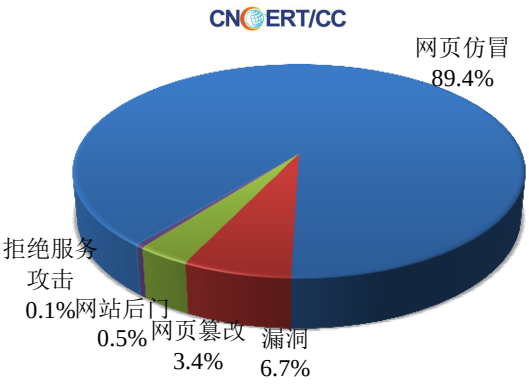
http://www.cnvd.org.cn/webinfo/list?type=4

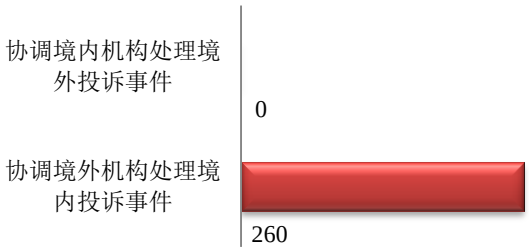
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1072 起，其中跨境网络安全事件 260 起。

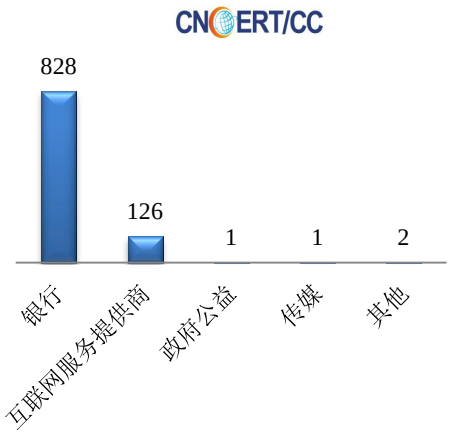
本周CNCERT处理的事件数量按类型分布
(8/31-9/6)



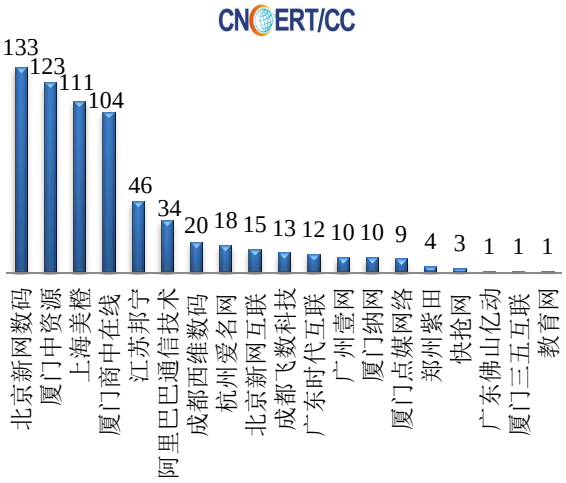


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 958 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 828 起和互联网服务提供商仿冒事件 126 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/31-9/6)

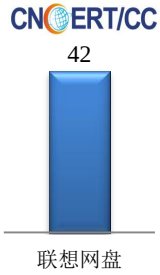


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/31-9/6)



本周，CNCERT 协调 1 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 42 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 (8/31-9/6)



业界新闻速递

1、国务院印发《促进大数据发展行动纲要》

中国政府网 9 月 5 日消息 经李克强总理签批，国务院日前印发《促进大数据发展行动纲要》（以下简称《纲要》），系统部署大数据发展工作。《纲要》提出，要加强顶层设计和统筹协调，大力推动政府信息系统和公共数据互联开放共享，加快政府信息平台整合，消除信息孤岛，推进数据资源向社会开放，增强政府公信力，引导社会发展，服务公众企业；以企业为主体，营造宽松公平环境，加大大数据关键技术研发、产业发展和人才培养力度，着力推进数据汇集和发掘，深化大数据在各行业创新应用，促进大数据产业健康发展；完善法规制度和标准体系，科学规范利用大数据，切实保障数据安全。《纲要》明确，推动大数据发展和应用，在未来 5 至 10 年打造精准治理、多方协作的社会治理新模式，建立运行平稳、安全高效的经济运行新机制，构建以人为本、

惠及全民的民生服务新体系，开启大众创业、万众创新的创新驱动新格局，培育高端智能、新兴繁荣的产业发展新生态。《纲要》部署三方面主要任务。一要加快政府数据开放共享，推动资源整合，提升治理能力。二要推动产业创新发展，培育新兴业态，助力经济转型。三要强化安全保障，提高管理水平，促进健康发展。健全大数据安全保障体系，强化安全支撑。《纲要》还明确七方面政策机制。一是建立国家大数据发展和应用统筹协调机制。二是加快法规制度建设，积极研究数据开放、保护等方面制度。三是健全市场发展机制，鼓励政府与企业、社会机构开展合作。四是建立标准规范体系，积极参与相关国际标准制定工作。五是加大财政金融支持，推动建设一批国际领先的重大示范工程。六是加强专业人才培养，建立健全多层次、多类型的大数据人才培养体系。七是促进国际交流合作，建立完善国际合作机制。

2、三网融合方案公布完善网络信息安全和文化安全管理体系

观察者网 9 月 5 日消息 国务院近日公布三网融合方案，推动广电电信双向进入。在多地进行各种试点多年之后，三网融合方案终于公布。据中国政府网消息，国务院办公厅近日印发全新的《三网融合推广方案》（以下简称《方案》），加快在全国全面推进三网融合方案，推动信息网络基础设施互联互通和资源共享。通知中称，三网融合方案是党中央、国务院作出的一项重大决策，如今试点阶段各项任务已基本完成。三网融合方案公布，《方案》提出六项工作目标。一是将广电、电信业务双向进入扩大到全国范围，并实质性开展工作，二是网络承载和技术创新能力进一步提升，三是融合业务和网络产业加快发展，四是科学有效的监管体制机制基本建立，五是安全保障能力显著提高，六是信息消费快速增长。《方案》明确，一要在全国范围推动广电、电信业务双向进入。各省（区、市）结合当地实际确定业务开展地区，电信、广电行业主管部门按照相关政策要求和业务审批权限开展业务许可审批，加快推动 IPTV 集成播控平台与 IPTV 传输系统对接，加强行业监管。二要加快宽带网络建设改造和统筹规划。三要强化网络信息安全和文化安全监管。完善网络信息安全和文化安全管理体系，加强技术管理系统建设和动态管理。四要切实推动相关产业发展。为保障三网融合工作的全面推进，《方案》确立了四项保障措施。一是建立健全法律法规，为广电、电信业务双向进入提供法律保障。二是落实相关扶持政策，支持三网融合共性关键技术、产品的研发和产业化，推动业态创新。三是提高信息网络基础设施建设保障水平。四是完善安全保障体系，加快建立健全监管平台。

3、俄新法规定公民数据只能存于境内服务器

环球网 9 月 1 日消息 据俄罗斯国际文传电讯社报道，俄罗斯《个人数据保护法》于 1 日生效。该法规定：俄罗斯公民的个人信息数据只能存于俄境内的服务器中，以实现数据本地化；任何收集俄罗斯公民个人信息的本国或者外国公司在处理与个人信息相关的数据，包括采集、积累和存储时，必须使用俄罗斯境内的服务器；个人信息不止包括姓名、住址、出生日期等，而是与公民身份相关的任何信息。并规定，在一些特殊情况下可以在俄境外的服务器上处理个人信息数据：执法、行使国家机关和地方政府的权力，以及以达成国际协议为目的的行为。俄罗斯联邦通讯、信息技术和大众传媒监督局将履行监督职责，违法的公司将会被起诉，除此之外还将被处以最高达 30 万卢布的罚款。该局官员表示，个人信息数据的跨境传输是允许的，但是必须存储在俄罗斯境内。数据的副本可能会暂时存放在国外，但仅限于需要使用的期间内。例如，俄罗斯公民的个人数据可以被传输到境外的宾馆或者医院，但是在公民结束休息或者结束治疗后，宾馆和诊所中的俄公民个人数据应当被删除。

4、日本政府出台新网络安全战略扩大监管范围

中新网 9 月 4 日消息 据日本媒体报道，日本政府 4 日在内阁会议上正式通过了旨在确保网络空间安全的新指针“网络安全战略”。新的网络安全战略将强化应对向每个日本国民发放一个号码的“个人号码制度”。报道称，鉴于此前发生了日本年金机构信息外泄问题，新战略把网络攻击受害的监管防范对象范围从政府机关扩大到了“独立行政法人”及部分“特殊法人”。新战略还写明，将强化应对向每个日本国民发放一个号码并在行政手续等方面加以利用的“个人号码制度”。为迎接 2020 年东京奥运会和残奥会，日本政府制定新战略作为今后 3 年左右的基本方针。为了防范日益巧妙化的网络攻击，尽早完善应对机制和培养人才成为了课题。作为日本政府网络攻击对策司令塔的“内阁网络安全中心”（NISC）现在把中央省厅作为监管对象，今后将逐步扩展至与中央省厅共同承担公共业务的独立行政法人及特殊法人等。为减少黑客入侵的途径，新战略提出把处理重要信息的政府机构信息系统与网络隔断开来。鉴于国会 3 日通过了 2018 年起可在用户自愿的前提下适用于银行存款账户的《个人号码法》修正案，新战略规定将强化防止个人信息外泄措施。日本政府力争通过 NISC 构筑全面监管中央和地方政府的机制，确保个人号码制度顺利实施。

5、英国反犯罪局网站遭报复式黑客攻击

新华网 9 月 2 日消息 英国国家反犯罪局网站 1 日因遭到“分布式拒绝服务攻击”而短暂瘫痪，著名黑客组织“蜥蜴小队”在社交网站推特上声称对这次攻击负责。截至发稿时，英国国家反犯罪局网站已恢复正常。该机构一名发言人说，这次攻击并没有造成安全漏洞，也未影响该机构正常运转，“最多只是给我们网站的用户带来短暂不便”。分布式拒绝服务攻击是黑客的一种常用攻击手法，主要通过发送大量服务需求占用网络资源，最终使网络瘫痪。这种技术能将多个计算机联合起来作为攻击平台，对一个或多个目标网站发动攻击，从而成倍提高破坏效果。就在这次黑客攻击发生前几天，英国国家反犯罪局宣布在一次全国行动中拘捕了 6 名青少年，他们涉嫌利用“蜥蜴小队”开发的软件对多个网站实施分布式拒绝服务攻击，导致它们瘫痪。这些嫌疑人目前已被保释。英国国家反犯罪局发言人说，他们的网站对黑客来说是比较明显的目标，受到这类攻击可以说是“家常便饭”。

6、Mozilla 承认缺陷数据库遭入侵黑客对火狐用户发动攻击

凤凰网 9 月 6 日消息 北京时间 9 月 6 日消息，据科技网站 ComputerWorld 报道，Mozilla 昨天表示，一名不明身份的黑客入侵了其 Bugzilla 缺陷追踪数据库，窃取了与 53 个危急缺陷有关的信息，并利用其中至少一个缺陷对火狐浏览器用户发动攻击。Bugzilla 是 Mozilla 开发者用来记录出现的问题，讨论解决方案的开放源代码追踪数据库，其中部分信息只向特权帐户开放。Mozilla 当地时间周五表示，“一名黑客入侵了一个特权帐户，下载了火狐和 Mozilla 其他产品的缺陷信息。”Mozilla 安全团队联合负责人理查德·巴尼斯（Richard Barnes）昨天在官方博客上发文称，“我们认为黑客利用窃取的信息对火狐用户进行了攻击。”Mozilla 8 月 6 日发布补丁软件，修正了黑客用来攻击火狐用户的缺陷。据 Mozilla 称，黑客至少早在 2014 年 9 月就通过特权帐户访问了 Bugzilla，但有迹象表明，黑客访问 Bugzilla 的时间比这个时间要早一年。Mozilla 已经采取措施提高 Bugzilla 的安全性，其中包括要求特权帐户重新设置密码、采用双因子身份认证技术。巴尼斯还表示，Mozilla“减少了特权帐户数量，限制了特权用户能执行的操作”。Mozilla 建议火狐用户升级到 8 月 27 日发布的火狐 40，该版本修正了被黑客获得信息的所有缺陷。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373