国家互联网应急中心

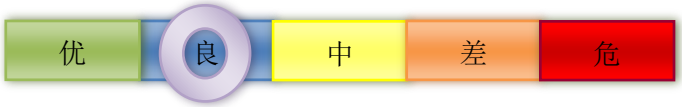
网络安全信息与动态周报

2017 年第 22 期

5 月 22 日-5 月 28 日

CNCERT/CC

本周网络安全基本态势

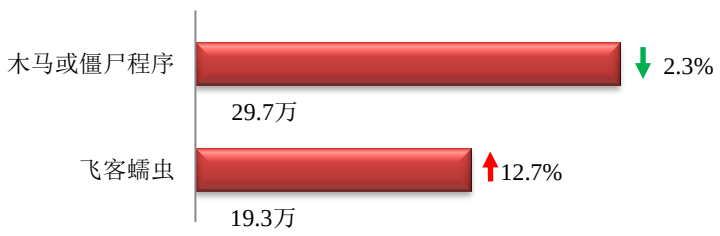


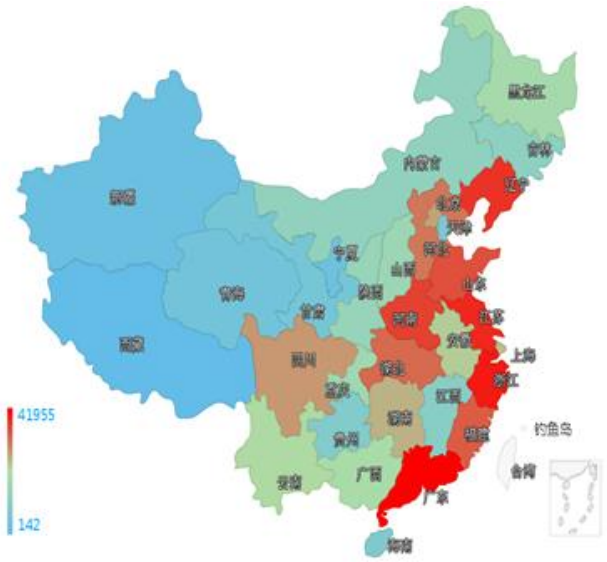
境内感染网络病毒的主机数量	• 49.0万	3.1%
境内被篡改网站总数 其中政府网站数量	• 1,763 • 48	104.3% 26.3%
境内被植入后门网站总数 其中政府网站数量	• 1,984 • 89	16.8% 161.8%
针对境内网站的仿冒页面数量	• 407	33.0%
新增信息安全漏洞数量 其中高危漏洞数量	• 363 • 145	17.5% 4.0%

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 49.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 29.7 万以及境内感染飞客（conficker）蠕虫的主机约 19.3 万。



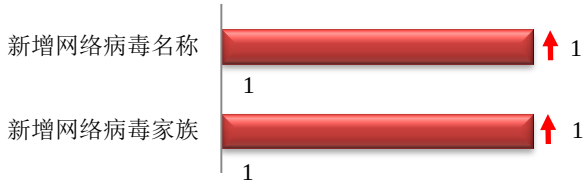


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

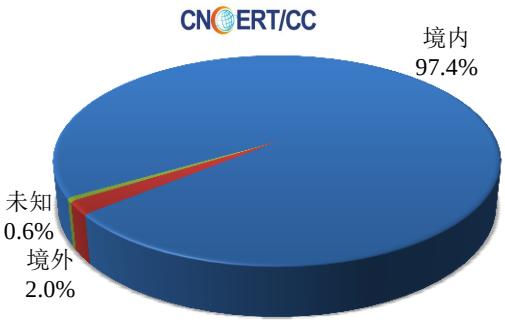
广东省	•约4.2万个（约占中国大陆总感染量的25.8%）
浙江省	•约2.7万个（约占中国大陆总感染量的16.8%）
江苏省	•约2.2万个（约占中国大陆总感染量的13.3%）

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。

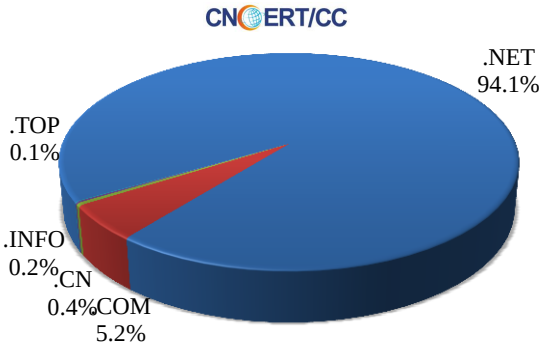


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1088 个，涉及 IP 地址 498 个。在 1088 个域名中，有 2.0%为境外注册，且顶级域为.com 的约占 5.2%；在 498 个 IP 中，有约 3.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 7 个 IP。

本周放马站点域名注册所属境内外分布
(5/22-5/28)



本周放马站点域名所属顶级域的分布
(5/22-5/28)



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。

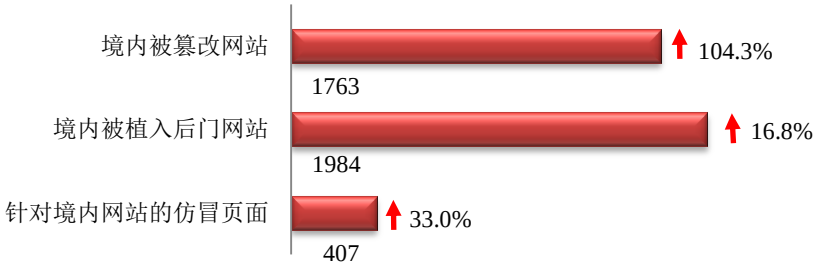
ANVA恶意地址黑名单发布地址

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。

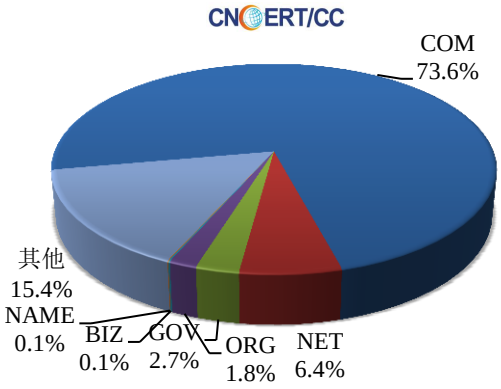
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1763 个；境内被植入后门的网站数量为 1984 个；针对境内网站的仿冒页面数量为 407。

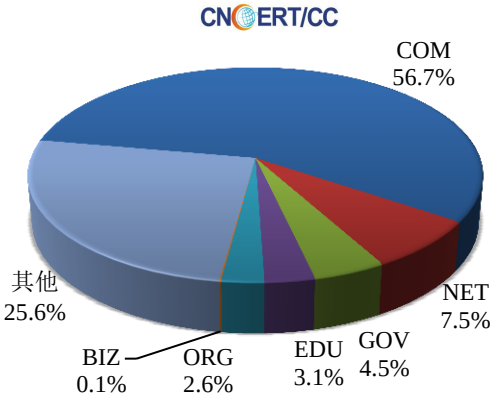


本周境内被篡改政府网站（GOV 类）数量为 48 个（约占境内 2.7%），较上周环比上升了 26.3%；境内被植入后门的政府网站（GOV 类）数量为 89 个（约占境内 4.5%），较上周环比上升了 161.8%；针对境内网站的仿冒页面涉及域名 343 个，IP 地址 165 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/22-5/28)

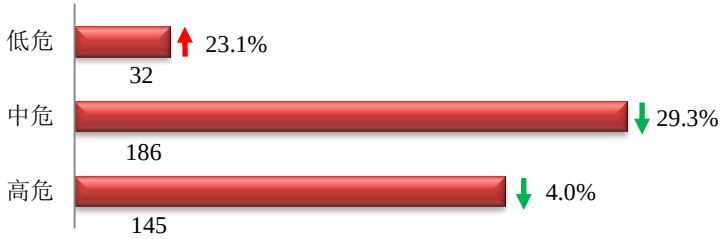


本周我国境内被植入后门网站按类型分布
(5/22-5/28)

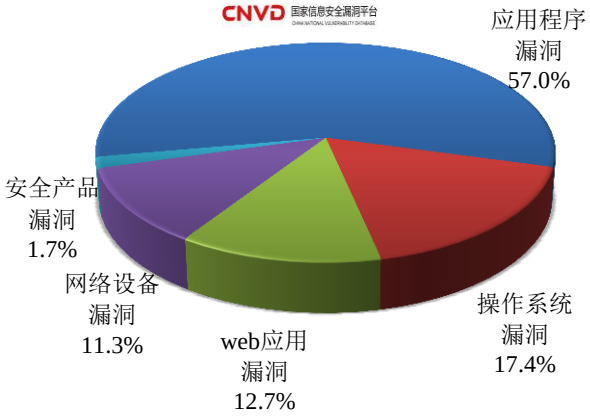


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 363 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
(5/22-5/28)



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 web 应用漏洞。

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

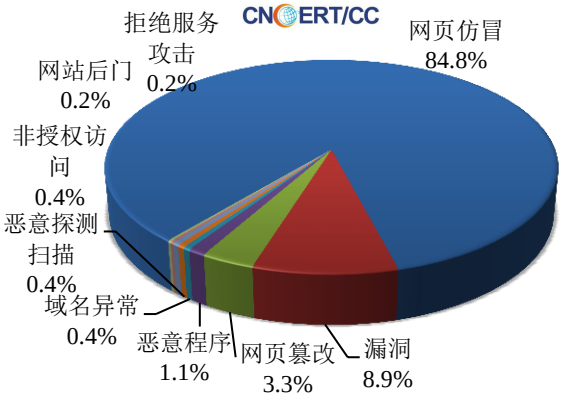
http://www.cnvd.org.cn/webinfo/list?type=4

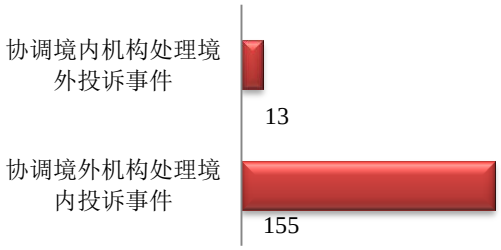
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 448 起，其中跨境网络安全事件 168 起。

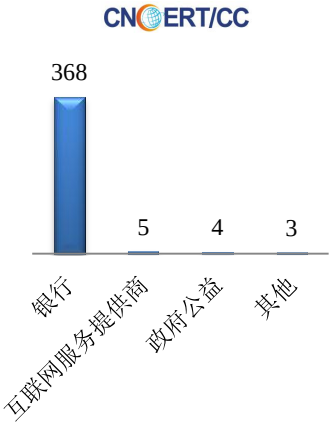
本周CNCERT处理的事件数量按类型分布 (5/22-5/28)



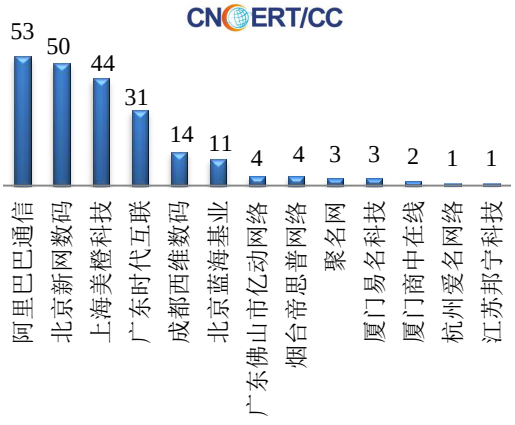


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 380 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 368 起和互联网服务提供商仿冒事件 5 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/22-5/28)



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 (5/22-5/28)



本周，CNCERT 协调 26 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 220 个。

业界新闻速递

1、2017 中国网络安全年会在青岛隆重召开

E 安全 5 月 23 日讯 2017 年 5 月 22 日-24 日，以“融合促进发展协作共建安全”为主题的 2017 中国网络安全年会（第 14 届）在中国青岛召开。本次大会由工业和信息化部指导，国家互联网应急中心（CNCERT）和中国通信学会联合主办。来自政府和重要信息系统、企业、行业协会、高校和科研院所等单位以及来自 CNCERT 国际合作伙伴的代表共九百余人参加了大会。工业和信息化部党组成员、副部长陈肇雄指出，当前，以互联网为代表的新一代信息技术迅猛发展、加快普及、广泛应用，在支撑经济转型、推动社会进步、深化人文交流、消弭数字鸿沟等方面发挥了积极作用。同时，也带来了一些新问题、新挑战，尤其是，网络安全威胁和风险日益突出，并加快向政治、经济、文化、社会、生态、国防等领域传导渗透，成为世界各国面临的共同难题。陈肇雄表示，我国高度重视网络安全工作。习近平总书记就网络安全工作发表了系列重要讲话，对加强网络空间国际合作，共建网络空间命运共同体提出重要倡议。国家陆续出台了《网络安全法》、《国家网络空间安全战略》和《网络空间国际合作战略》等法律、战略和规划，对网络安全工作作出系统部署。陈肇雄就进一步做好网络安全工作提出四点要求：一是提高认识，切实增强维护网络安全的紧迫感；二是加强创新，不断突破网络安全核心关键技术；三是协同联动，推动形成网络安全保障工作合力；四是开放合作，共同应对网络安全威胁。山东省副省长王书坚指出，山东省始终高度重视网络安全工作，着力提升互联网网络安全技术手段及大数据分析能力，扎实开展打击电信诈骗专项行动，采取多种形式持续开展互联网网络安全威胁治理行动，有效防范处置各类网络安全隐患。并表示维护网络安全成为事关国家安全、国家主权和人民群众合法权益等重大问题。正如习近平总书记指出的那样，网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。同时，维护网络安全迫切需要在核心技术上取得突破，大力发展、积极使用自主可控的技术和产品，争取实现弯道超车，掌握互联网发展主动权，保障互联网安全、国家安全。青岛市市长孟凡利，工程院院士王恩东，工业和信息化部相关司局、有关单位负责同志一同出

席会议。大会为期共 3 天，共 5 个分论坛，同期还举办了 2017 中国网络安全技术对抗赛、第二届 CNCERT 国际合作论坛、网络安全企业领袖高峰论坛，并开展了网络安全防护专题培训。

2、美国 NIST 针对联邦机构发布网络安全框架草案

E 安全 5 月 23 日讯 美国国家标准与技术研究院（NIST）发布指南草案，就联邦机构如何实施 NIST《提升关键基础设施网络安全的框架》提出指导。奥巴马政府于 2014 年发布了这份网络安全框架，描述了关键基础设施操作人员评估和提升防御能力、检测并响应网络攻击的流程。特朗普上周签署网络安全行政令之前，NIST 开始制定新指南草案“机构间 8170 报告”，指导联邦机使用该框架。美国国家安全顾问汤姆·博塞特宣布这项网络安全行政令时表示，私有部门被要求执行该框架，但对联邦机构没有强制要求。他建议联邦部门和机构应践行，并采用同样的 NIST 框架管理以降低风险。NIST 这份草案指出，联邦机构可以使用这份网络安全框架补充现有的 NIST 安全和隐私风险管理标准，以及为响应《联邦信息安全管理法案》制定的指导方针和实践。华盛顿州健康保险交易所的首席信息官柯特·夸克表示，实施这份行政令是政府机构一贯处理网络安全的方式。他肯定了将某框架作为基准是一件好事，尤其涉及到与 NIST 一致的要求时。然而并非所有专家都认为，框架是保护组织机构数字资产的有效过程。FBI 网络部前副助理总监兼白宫无党派国家网络安全委员会委员史蒂文·查彬斯基指出，执行框架相当困难、并且成本昂贵。这并不是因为 NIST 框架不够好，恰恰相反，面对如今不断变化的威胁格局，美国政府缺乏指标衡量 NIST 框架是否或在某种程度上能实现成本效益。如果漏洞缓解耗资少，并且易于实施，当然他不会反对，然而事实却并非如此。NIST 正在征求新草案意见，包括征求机构使用该指南的方式的建议。

3、新加坡政府拨款 17.3 亿美元推进智能国家数字化转型

据外媒 24 日报道，新加坡政府重申拨出 24 亿新西兰元（约合 17.3 亿美元）计划，以快速推动新加坡智能国家数字化转型。该笔资金将用于 2017 新加坡财政信息通信技术（ ICT ）投标，其中主要包括数据分析与物联网（ IoT ）传感器在内的各种技术领域的投资以及必要的通信基础设施的改进。据新加坡政府技术局（ GovTech ）统计显示，中小型企业于 2016 年获得 ICT 合约的三分之二，其通过新加坡资讯通信媒体发展管理局（ IMDA ）项目认证的企业均获得了与各政府机构相关的 90 余个发展项目。IMDA 机构由 GovTech 和智能国家数字政府办公室（ SNDGO ）组成，负责推动智能国家基础设施与应用程序的发展，以及公共部门的数字化转型工作。GovTech 首席行政长官杰奎琳 · 波（ Bernquire Poh ）于本周三在智能国家与数字政府行业年度简报会上表示，他们将继续与 SNDGO 合作并为其提供基础支持、以建立新加坡智能国家。此外，各企业也需提升 ICT 与工程能力，从而快速适应技术格局的变化。

4、勒索软件 WannaCry 幕后开发者或来自中文国家

据外媒 26 日报道，威胁情报公司 Flashpoint 针对数十张勒索软件 WannaCry 赎金票据进行了语言分析，其幕后开发者或来自讲中文的国家。全球勒索软件 WannaCry 于近期肆意爆发，攻击者利用 SMB 漏洞开展网络攻击活动。上周，Google 、卡巴斯基等安全公司相继发布声明，指出勒索软件 WannaCry 与朝鲜黑客 Lazarus 存有潜在联系。随后，安全专家根据 WannaCry 赎金票据进行分析后表示，票据内容主要包含中文（ 简体与繁体 ）、韩语、俄语等 28 种语言，其中中文内容极其准确流利。此外，中文票据中使用的某些术语进一步帮

助安全专家缩小了地理范围。例如：赎金票据中出现的 “ 礼拜 ” 一词，主要在华南、香港、台湾或新加坡地区常见，而 “ 反病毒 ”、“ 杀毒软件 ” 等词语在中国大陆比较常见。值得注意的是，中文赎金票据中所包含的内容并未存在其他版本注释，且格式较长、版式略有不同；而英文版赎金票据虽然看起来很好，但它包含一些主要的语法错误，这表明开发人员的母语并非英语，或受教育程度不高。Flashpoint 分析表明，攻击者可能利用朝鲜黑客组织 Lazarus 代码作为混淆以欺骗调查人员，亦或是朝鲜 APT 组织内部招募了以中文为母语的开发者。

5、新蠕虫“永恒之石”来势汹汹：利用 NSA 七大黑客工具

E 安全 5 月 23 日 WannaCry 勒索病毒余波未平，如今又出现了更变本加厉的 EternalRocks（“永恒之石”）新病毒，永恒之石来势汹汹，竟利用了 7 个 NSA 漏洞利用。根据 GitHub 上的介绍，“永恒之石”是 2017 年 5 月上旬浮出水面的一款网络蠕虫（自我复制蠕虫），目前已知最早的样本为 5 月 3 日的：fc75410aa8f76154f5ae8fe035b9a13c76f6e132077346101a0d673ed9f3a0dd。这款蠕虫通过公开的（影子经纪人泄露的 NSA 工具）SMB 漏洞利用（ETERNALBLUE、ETERNALCHAMPION、ETERNALROMANCE、ETERNALSYNERGY）及相关应用程序（DOUBLEPULSAR、ARCHITOUCH 和 SMBTOUCH）进行传播。永恒之石蠕虫利用服务器信息块（SMB）共享网络协议中的漏洞，去感染未修复的 Windows 系统。与 WannaCry 不同的是，“永恒之石”不会捆绑破坏性的恶意软件的有效载荷（至少现在不会）。这款病毒不具有“Kill Switch”功能，因此无法被轻易阻止。WannaCry 会提醒受害者遭遇了勒索病毒感染，而“永恒之石”会安静、隐藏地待在受害者的电脑中。一旦进入电脑，“永恒之石”会下载 Tor 个人浏览器（可用来匿名浏览网页和发送邮件），并向这款蠕虫的隐藏服务器发送信号。之后，“永恒之石”在接下来的 24 个小时内不会有任何动作，它会静静等待直到服务器响应，开始下载并自我复制。这就意味着，安全专家想要获取该蠕虫病毒的更多信息来研究，将会滞后一天。安全公司 Plixer CEO 迈克尔 • 帕特森称，这款病毒甚至“自称”WannaCry，试图向安全研究人员隐藏身份。根据研究人员对永恒之石的早期分析显示，这款病毒利用了 7 个 NSA 黑客工具，而 WannaCry 仅仅部署了两个漏洞进行扩散。Vectra Networks 欧洲、中东和非洲（EMEA）总监马特 • 沃姆斯利评论称，永恒之石是 WannaCry 群体扔出第二个“重磅”炸弹，因为“永恒之石”更黑暗、更精炼，除了针对的目标群体相同。在未被发现的情况下，“永恒之石”可以使用 SBM 文件共享协议，快速传遍互联网和私有网络，迅速感染未打补丁的系统，并且，不依赖用户点击网络钓鱼电子邮件进行链接。

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 2016 年，CNCERT 与 69 个国家和地区的 185 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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158