中国科学院网络与信息安全情况通报

第 75 期

（2016 年 10 月 1 日至 10 月 31 日）

办公厅　条财局　　2016 年 11 月 4 日

一、 安全威胁情况

（一）隐患通报

10 月以来，国家互联网应急中心、工业和信息化部电子科学技术情报研究所发出警示，我院纳米器件及相关材料研究部（苏州纳米所）、云南天文台丽江观测站（云南天文台）共 2 个单位 2 个网站存在 SQL 注入及信息泄露等高危漏洞。这些隐患可被黑客利用，轻易获得系统核心控制权限，造成网站重要敏感信息泄漏。办公厅已向相关单位发送《安全隐患告知书》，督促隐患整改。

（二）重大预警

近日，国家信息安全漏洞共享平台（CNVD）收录了 Linux kernel 本地权限提升漏洞（CNVD-2016-09672 漏洞发现者命名为“Dirty COW”漏洞）。该漏洞对于 Linux kernel 2.6.22（2007 年发行版）及以后的版本、Android 操作系统和 Red Hat、Debian、Ubuntu 等流行的 Linux 操作系统发行版本都受该漏洞影响。相关发行版厂商均已发布了漏洞修复程序，CNVD 建议用户尽快升级程序至最新版本。研发人员可重新

编译 Linux 修复此漏洞。Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。Linux 内核的内存管理器在处理写入拷贝（copy-on-write，COW）时存在竞态条件，可破坏专用只读内存映射。低权限的本地用户可利用该漏洞获取其他只读内存映射的写权限，进而可导致权限提升。本地攻击者利用该漏洞可获取管理员权限，并执行进一步操作。提醒院内用户做好应对防范。

国家信息安全漏洞库本月总体风险态势评定为“良”。月度发布漏洞总条目 599 条，较上月增加 14 条，“紧急”和“高危”漏洞占总量的 40.23%。

（三）事件处置

中国科技网网络安全应急小组（CSTCERT）本月监测处理安全事件 335 起，其中垃圾邮件投诉事件 100 起，网络扫描事件 235 起。已处理的网络扫描事件中，3%来自境外，95%来自国内其他运营商，2%来自中国科技网。

二、 案例警示

- **广东警方破获 60 多起新型网络传销犯罪案件。**

近日，在广东省公安厅的统一指挥下，全省 21 市公安机关联手，同步开展“飓风 21 号”打击收网行动，成功摧毁多个新型网络传销犯罪团伙，侦破“恒星币”网络虚拟货币传销案、广东隆富集团涉嫌利用互联网销售纳米产品组织、领导传销案等 60 余宗案件，捣毁窝点 80 余个，抓获犯罪嫌疑人 480 余名，查冻涉案账户 550 余个，冻结涉案资金、房产、商铺等折合人民币约 4 亿余元，涉案金额约 20 余亿元。新型网络传销案件主要有三大特点:

一是名堂多，特别是利用爱心慈善、网络虚拟货币的名

义实施组织、领导传销突出。广东隆富集团传销案的犯罪团伙就是借用宗教宣传，制造其爱心慈善的假象，通过“讲师”讲课洗脑，不断拉人头入会。“恒星币”传销案犯罪团伙则是利用网站、微信等渠道宣传，以高回报等虚假信息诱惑公众购买虚拟货币“恒星币”和所谓的能生产“恒星币”的“矿机”。

二是发展快，依托互联网犯罪发展迅速，对社会危害极大。犯罪团伙以互联网为依托进行宣传，对会员进行系统管理，还设置了网上商城、微信公众号等，通过网络的方式宣传其组织及产品，且多为三无产品。对于购买产品入会的会员给予会员号，会员可在会员系统中查询自己发展新会员以及提成等情况。团伙还通过聘请人员专门管理网站，对会员的提成、计酬进行系统计算。此类新型网络传销犯罪团伙利用网络传播迅速的特性，得以快速扩张规模，会员数动辄几千上万人，甚至10万余人。

三是打击难，犯罪团伙成员之间非接触性、高智能化特征明显。犯罪团伙层层发展会员，均是通过网络、微信，会员上下线之间互不认识，且大多分布在全国各地，甚至在境外。同时，团伙聘请专业的技术团队设计网站、软件，用于管理会员、进行提成和利益分配。

安全提示：网络传销分子即利用网络扩散，又落地推广，“网上”和“网下”双管齐下。广大群众应对当前新型网络传销安全的新形势、新特点予以高度重视，提高安全防范意识，切勿为贪图小利而盲目受骗。

三、热点关注

- **中共中央政治局就实施网络强国战略进行第三十六次集体学习**

中共中央政治局 10 月 9 日下午就实施网络强国战略进行第三十六次集体学习。中共中央总书记习近平在主持学习时强调，加快推进网络信息技术自主创新，加快数字经济对经济发展的推动，加快提高网络管理水平，加快增强网络空间安全防御能力，加快用网络信息技术推进社会治理，加快提升我国对网络空间的国际话语权和规则制定权，朝着建设网络强国目标不懈努力。

习近平在主持学习时发表了讲话。他指出，当今世界，网络信息技术日新月异，全面融入社会生产生活，深刻改变着全球经济格局、利益格局、安全格局。世界主要国家都把互联网作为经济发展、技术创新的重点，把互联网作为谋求竞争新优势的战略方向。虽然我国网络信息技术和网络安全保障取得了不小成绩，但同世界先进水平相比还有很大差距。我们要统一思想、提高认识，加强战略规划和统筹，加快推进各项工作。

习近平强调，网络信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的技术创新领域，是全球技术创新的竞争高地。我们要顺应这一趋势，大力发展核心技术，加强关键信息基础设施安全保障，完善网络治理体系。要紧紧牵住核心技术自主创新这个“牛鼻子”，抓紧突破网络发展的前沿技术和具有国际竞争力的关键核心技术，加快推进国产自主可控替代计划，构建安全可控的信息技术体系。要改革科技研发投入产出机制和科研成果转化机制，实施网络信息领域核心技术设备攻坚战略，推动高性能计算、移动通信、量子通信、核心芯片、操作系统等研发和应用取得重大突破。

习近平强调，世界经济加速向以网络信息技术产业为重

要内容的经济活动转变。我们要把握这一历史契机，以信息化培育新动能，用新动能推动新发展。要加大投入，加强信息基础设施建设，推动互联网和实体经济深度融合，加快传统产业数字化、智能化，做大做强数字经济，拓展经济发展新空间。

习近平指出，互联网新技术新应用不断发展，使互联网的社会动员功能日益增强。要传播正能量，提升传播力和引导力。要严密防范网络犯罪特别是新型网络犯罪，维护人民群众利益和社会和谐稳定。要发挥网络传播互动、体验、分享的优势，听民意、惠民生、解民忧，凝聚社会共识。网上网下要同心聚力、齐抓共管，形成共同防范社会风险、共同构筑同心圆的良好局面。要维护网络空间安全以及网络数据的完整性、安全性、可靠性，提高维护网络空间安全能力。

习近平指出，随着互联网特别是移动互联网发展，社会治理模式正在从单向管理转向双向互动，从线下转向线上线下融合，从单纯的政府监管向更加注重社会协同治理转变。我们要深刻认识互联网在国家管理和社会治理中的作用，以推行电子政务、建设新型智慧城市等为抓手，以数据集中和共享为途径，建设全国一体化的国家大数据中心，推进技术融合、业务融合、数据融合，实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务。要强化互联网思维，利用互联网扁平化、交互式、快捷性优势，推进政府决策科学化、社会治理精准化、公共服务高效化，用信息化手段更好感知社会态势、畅通沟通渠道、辅助决策施政。

习近平强调，要理直气壮维护我国网络空间主权，明确宣示我们的主张。现在，各级领导干部特别是高级干部，如果不懂互联网、不善于运用互联网，就无法有效开展工作。

各级领导干部要学网、懂网、用网，积极谋划、推动、引导互联网发展。要正确处理安全和发展、开放和自主、管理和服务的关系，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力，把网络强国建设不断推向前进。

● **第五届全国信息安全等级保护技术大会成功召开**

2016 年 10 月 10 日，第五届全国信息安全等级保护技术大会在云南昆明成功召开。来自中央国家机关有关部门、部分中央企业、公安机关、信息安全通报机制成员单位和技术支持单位、信息安全等级测评机构、信息安全企业、科研院所等单位代表共计 550 余人参加了本届大会。本届大会由公安部第三研究所承办，公安部网络安全保卫局、中央网信办网络安全协调局、工信部网络安全管理局、国家密码管理局、国家保密局、中国科学院办公厅为本届大会指导单位。公安部第三研究所胡传平所长、公安部网络安全保卫局郭启全总工程师、云南省公安厅党委委员胡水旺副厅长、国家密码管理局赵丹主任、中国科学院办公厅高春东副主任以及工信部网络安全管理局、中央网信办网络安全协调局有关领导出席会议并致辞。

本届大会重点围绕新技术新应用环境下信息安全等级保护、关键信息基础设施和大数据安全、国内外网络安全政策与策略、网络安全态势监测与预警处置等主题开研讨交流。

全国信息安全等级保护技术大会作为重要行业部门、网络安全监管部门、信息安全领域科研院所及其专家学者、信息安全企业等交流研讨等级保护技术平台，促进信息安全各相关方共同分享贯彻落实国家信息安全等级保护制度的技

术成果和最佳实践，推动等级保护关键技术的研发、应用以及解决新技术新应用安全问题，为深入推进落实国家信息安全等级保护制度发挥了重要作用。

● **美国域名服务商遭大规模 DDoS 攻击**

美国《纽约时报》10 月 22 日报道，美国东部时间 10 月 21 日 7 时 10 分，美国主要域名服务商“动态网络服务”公司（Dynamic Network Services，简称 Dyn，音译为“迪恩”公司）宣称遭到大规模分布式拒绝服务攻击，超过 1000 台域名服务器受到影响。攻击分为三波次：7 时 10 分“动态网络服务”公司遭到第一波次攻击；11 时 52 分遭到第二波次攻击；17 时遭到第三波次攻击。由于“动态网络服务”公司为大型网站提供域名解析服务，事件导致美国东海岸地区大量网站域名解析服务中断或延迟，其中包括推特、脸谱、亚马逊、纽约时报、华尔街日报、贝宝等。

据“动态网络服务”公司发布的公告称，攻击者利用名为“未来”（Mirai）的恶意软件，感染大量物联网设备形成僵尸网络（包括网络摄像头、数字录像机和路由器等），然后向“动态网络服务”公司的域名解析服务器发起网络攻击，造成域名解析服务中断。该公司称发现了“数千万与‘未来’僵尸网络有关的 IP 地址”。目前，美国国土安全部和联邦调查局正在对事件开展调查。

发：院属各单位，院机关各部门。

编印：荆　涛