国家互联网应急中心

网络安全信息与动态周报

2016 年第 15 期

4 月 4 日-4 月 10 日

CNCERT/CC

本周网络安全基本态势

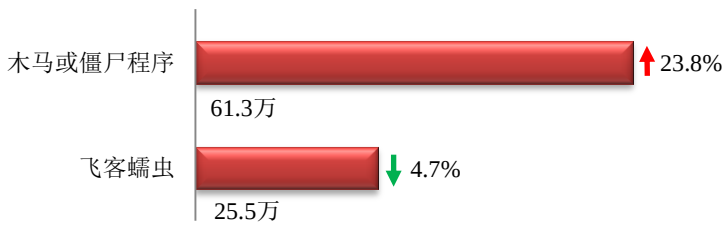
优 | 良 | 中 | 差 | 危

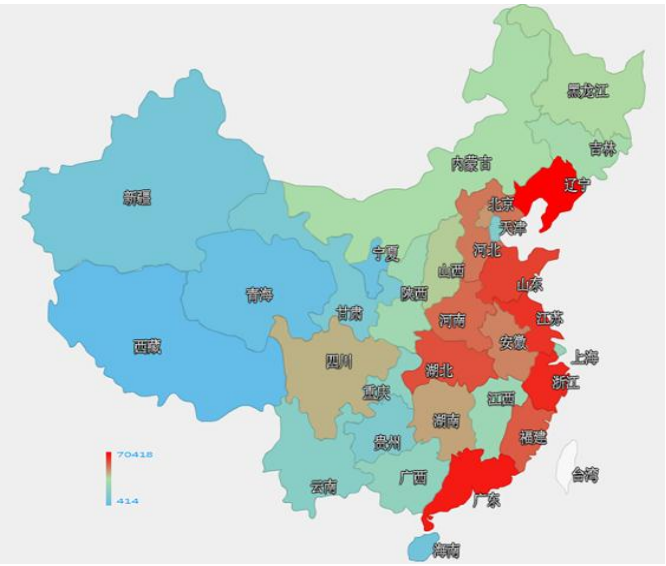
境内感染网络病毒的主机数量	•86.8万	13.8%
境内被篡改网站总数 其中政府网站数量	•2663 •48	37.5% 33.3%
境内被植入后门网站总数 其中政府网站数量	•4441 •279	71.1% 217.0%
针对境内网站的仿冒页面数量	•3724	39.9%
新增信息安全漏洞数量 其中高危漏洞数量	•106 •34	14.0% 54.5%

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 86.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 61.3 万以及境内感染飞客（conficker）蠕虫的主机约 25.5 万。





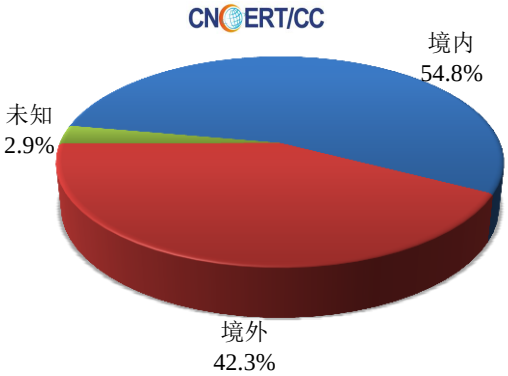
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是辽宁省、广东省和浙江省。

TOP3

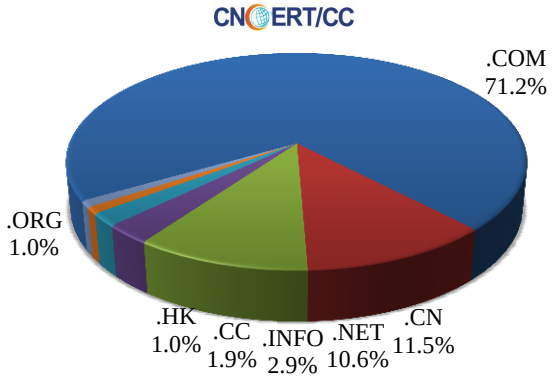
辽宁省	•约7.0万个（约占中国大陆总感染量的11.5%）
广东省	•约5.5万个（约占中国大陆总感染量的9.0%）
浙江省	•约5.3万个（约占中国大陆总感染量的8.6%）

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 104 个，涉及 IP 地址 295 个。在 104 个域名中，有约 42.3%为境外注册，且顶级域为.com 的约占 71.2%；在 295 个 IP 中，有约 7.8%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 22 个 IP。

本周放马站点域名注册所属境内外分布
(4/4-4/10)



本周放马站点域名所属顶级域的分布
(4/4-4/10)



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。

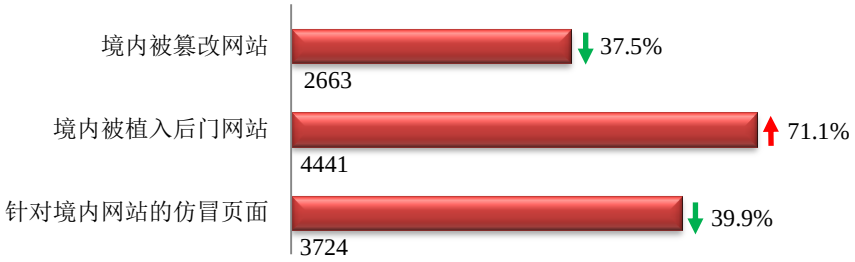
ANVA恶意地址黑名单发布地址

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。

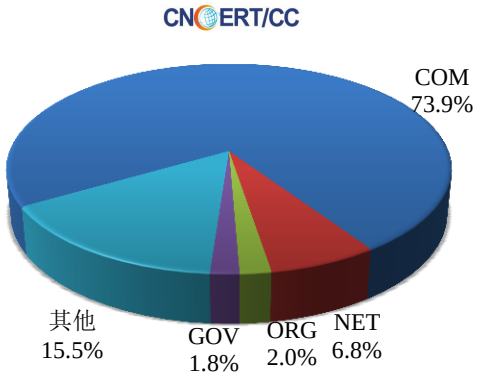
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2663 个；境内被植入后门的网站数量为 4441 个；针对境内网站的仿冒页面数量为 3724。

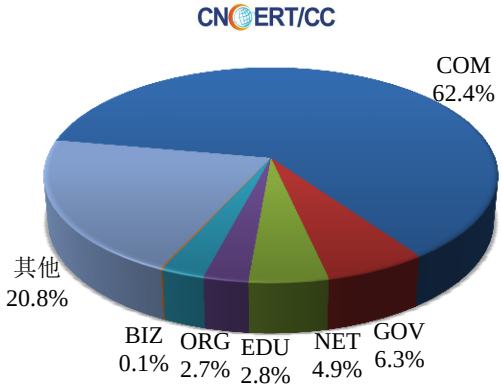


本周境内被篡改政府网站(GOV 类)数量为 48 个（约占境内 1.8%），较上周环比下降了 33.3%；境内被植入后门的政府网站（GOV 类）数量为 279 个（约占境内 6.3%），较上周环比上升了 217.0%；针对境内网站的仿冒页面涉及域名 3335 个，IP 地址 1006 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/4-4/10)

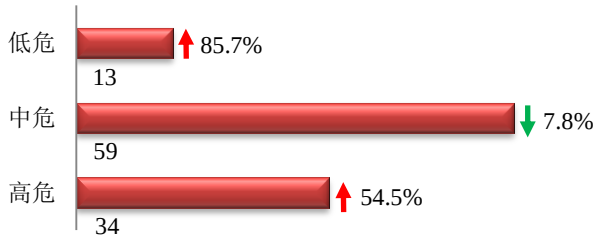


本周我国境内被植入后门网站按类型分布
(4/4-4/10)

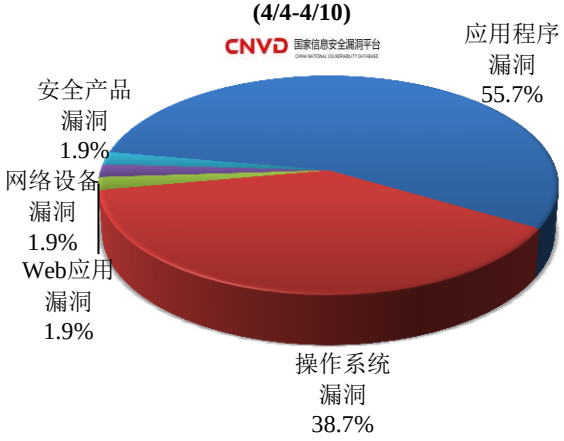


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 106 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
(4/4-4/10)



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

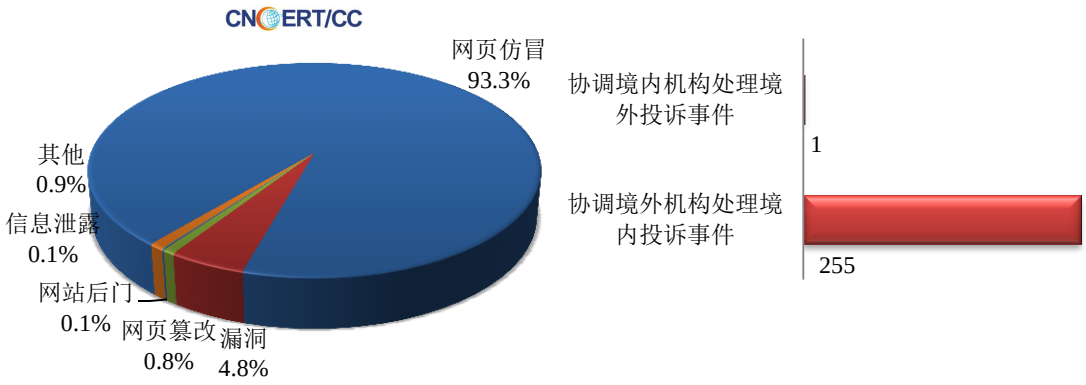
http://www.cnvd.org.cn/webinfo/list?type=4

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 1177 起，其中跨境网络安全事件 256 起。

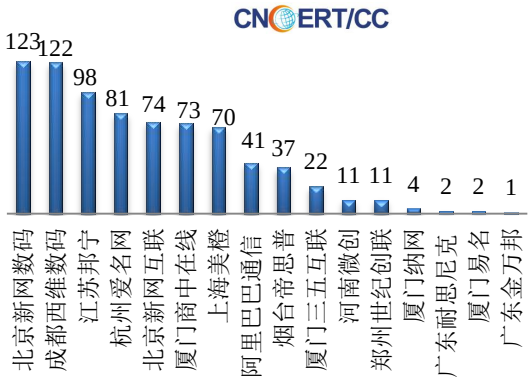
本周CNCERT处理的事件数量按类型分布
(4/4-4/10)



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 1098 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 995 起和互联网服务提供商仿冒事件 90 起。

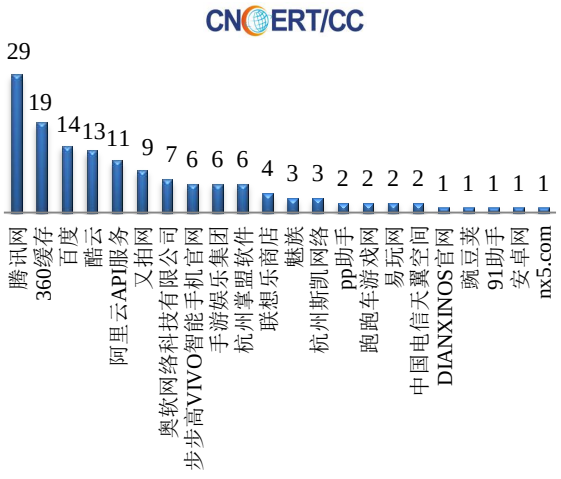
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/4-4/10)

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 (4/4-4/10)



本周，CNCERT 协调 22 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 143 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 (4/4-4/10)



业界新闻速递

1、水利部审议通过全国水利信息化“十三五”规划

中国证券网 4 月 6 日消息 4 月 6 日从水利部网站获悉，4 月 5 日，水利部召开网络安全与信息化领导小组第一次全体会议，安排部署水利网络安全与信息化重点工作。会议审议通过了《全国水利信息化“十三五”规划》《水利部信息化建设与管理办法》，以及水利部网络安全与信息化领导小组工作制度和 2016 年工作要点。水利部部长、水利部网络安全与信息化领导小组组长陈雷就加快推进水利网络安全和信息化建设提出明确要求。一要全力抓好水利信息化“十三五”规划实施。将创新作为重要驱动力，深化信息技术与各项水利工作的融合，积极研究大数据、云计算、物联网、移动互联等技术应用，强化信息化对水利各业务领域的服务与支撑，推进各类信息化资源整合共享，最大程度发挥水利信息化资源的效率。二要着力加强水利网络与信息安全保障工作。遵循“积极利用、科学发展、依法管理、确保安全”的国家网络安全总体方针，做好水利网络安全顶层设计，建立完善网络与信息安全管理责任和制度体系。进一步加强和完善安全防护能力建设，建设和完善网络与信息安全监控系统，加强网络与信息安全预警和数据备份恢复能力建设。三要进一步强化水利信息化建设与管理。强化安全管理和运行维护，不断创新和改进管理机制，做到运行维护工作流程清晰，管理规范。四要建立健全水利部门政府网站体系。大力推进水利部门政府网站集约化建设，打造更加及时、准确、有效的水利信息发布、互动交流和公共服平台。五要充分发挥领导小组工作机制作用。水利部网络安全与信息化领导小组要充分发挥统一领导作用，网信办要加强协调、指导、监督和检查。各司局、各单位要把网络安全和信息化作为一把手工程，主要领导亲自抓、带头用、负总责，确保各项工作落到实处。

2、美计划于五年内投入 350 亿美元加强网络安全 应对各方挑战

环球网 4 月 6 日消息 据联合早报网 4 月 6 日消息，美国国防部长卡特于 4 月 5 日在华盛顿战略与国际研究中心（CSIS）发表讲话演讲时说：“我们不仅要从海陆空天领域，还需要从网络空间来应对面临的五大挑战。”在此前的演讲中，卡特将俄罗斯、中国、朝鲜、伊朗和恐怖主义称为美国当前面临的五大挑战。卡特表示，美国一方面依靠高科技“增强了自己的实力，赢得了更多机会”，但同时也出现了一些弱点，他说：“我们的敌人企图将弱点加以利用，因此，我们要在五年内将网络安全方面的预算增至 350 亿美元，应对网络安全威胁。”

3、英媒：美国宣布对 IS 发动网络战 首次用网络武器

环球网 4 月 10 日消息 据英国《每日电讯报》网站 4 月 7 日报道，美国政府宣布要对“伊斯兰国”组织（IS）发动网络战。这是美国首次公开将网络攻击作为一种作战手段。报道称，美国会用网络武器库削弱“伊斯兰国”组织的在线通信网络并破坏该组织获取资金、进行贸易的渠道。美国国防部长阿什顿·卡特说：“网络攻击手段将扰乱他们指挥武装力量的能力，干扰他们策划阴谋的能力，削弱他们的财力以及雇用士兵的能力。”“伊斯兰国”组织的网络能力已经有翔实的资料佐证。巴黎袭击事件发生后的那周内，该组织发布了一份安全手册，泄露了部分网络战术。报道称，包括脸书和 Telegram 在内，一些公司已经加入这场对“伊斯兰国”组织的网络战。例如，脸书网站每天收到逾百万份有关违禁内容的报告，内容从色情到恐怖主义。报道称，打击“伊斯兰国”

组织的网络战，将是 2009 年美国国防部组建网络安全力量后网络司令部首次执行任务。该军种目前有 4900 名雇员，美国希望将其发展为拥有 6187 人的网络部队。此举是美国对“伊斯兰国”组织军事行动的一部分。美国希望网络战可以帮助军方在不派遣更多军人进入该地区的情况下扩大军队的活动范围。

4、英国国防部 4000 万英镑建网络安全中心

安全牛网 4 月 5 日消息 英国国防部（MoD）在一个全新的网络安全中心（CSOC）项目上花费超过 4 千万英镑。该项目用于支撑其网络及 IT 系统防护。这个网络安全中心将在英威尔特郡的科思罕建立，这里同时也是 MoD 耗资 6.9 亿英镑建立的通信中心和其它一些附属设施的大本营。去年 11 月，英国政府推出其“战略性防御及安全性回顾（SDSR）”计划，并称将在 5 年内投资逾 19 亿英镑用于保护英国免受网络攻击并提升其在网络空间的能力。新的 MoD 中心将是这个政府计划的一个重要组成部分。英国防部长 Michael Fallon 表示，英国在网络安全方面处于“世界领先”位置，但在网络安全威胁与日俱增的今天，新的安全运营中心将帮助确保英国的武装力量得以继续安全地运作。“我们在国防上预算的增长意味着较于我们的对手，在网络空间领域我们可以继续保持一个相对领先的位置；同时，也有一些常规性能力的研发。”英国政府表示，新的网络安全中心将在克服网络安全挑战这一方面，帮助英国防部和其他政府部门、盟友以及企业协同工作。

5、黑客攻击菲律宾选举网站 5500 万选民个人信息遭泄露

网易 4 月 8 日消息 据外媒报道，日前，有迹象表明，有黑客组织攻击了菲律宾委员会选举（COMELEC）网站，导致在上面注册的 5500 万名选民的个人信息遭到泄露。当地时间 3 月 27 日，Trend Micro 称，COMELEC 网站遭到一个黑客组织攻击，随后，网站整个数据库的数据被另外一个黑客组织公布在网上。负责该起网络攻击事件调查工作的安全公司指出，现在已经有大量敏感个人数据被曝光在网上，如选民的护照、指纹数据。Trend Micro 称，考虑到注册选民数量的庞大技术，此次攻击可以算是有史以来最大规模的政府数据泄露事件——此前则是美国人事管理办公室（OPM）网络攻击，当时 2000 万名美国人受到波及。Trend Micro 指出，这起攻击事件很有可能跟下个月的国家选举有关。另外获悉，第一个黑客组织还向 COMELEC 发出警告，让他们在自动投票系统中做好安全工作。对此，COMELEC 发言人 James Jimenez 回应，虽然 COMELEC 网站的安全性能不是很高，但 AVS 不同，它用的是一个不同且更加安全的网络。此外，该发言人还补充，目前选举工作进展顺利。

6、黑客组织攻击叙利亚政府网站并曝光 43GB 数据

网易 4 月 10 日消息 据外媒报道，当地时间 4 月 6 日，黑客组织 Cyber Justice Team（网络正义小队）在 MEGA 文件托管服务平台上上传了 10GB 来自叙利亚多个政府以及私营网站的压缩数据，解压后则有 43GB。另外，该组织还在 PasteBin 上上传了来自叙利亚国家网络服务机构一台 Linux 服务器上的密码文件。Risk Based Security(RBS)的分析师们对来自 55 个不同网站域名的 38,768 个文件夹和 247,477 个文件展开了分析。在这 55 个域名中有 25 个属于政府网站（.gov.sy），两个为.org.sy 域名，一个为.com.sy 域名，其余则都是.sy 域名。RBS 在分析文章中指出，他们在第一遍检查过程中有种似曾相识的感觉，后来经查证发现很多都是来自以前的网络攻击。分析师经过仔细分析发现，这些曝光的数据大部分都是通用 Plesk（虚拟主机面板）文件，或是来自 Joomla 和 Cportal（基于 PHP-Nuke 的门户网站）安装的数据。值得一提的是，Cportal 和 PHP-Nuke，它们是已经过时的底层技术，现在基本没什么更新，所以它们的许多漏洞相当于直接曝光在外面。这也进一步确定了泄露数据

来自以前的网络攻击。Cyber Justice Team 在 Twitter 表达了自己这次网络攻击的立场——反对 ISIS、反对阿萨德政权，并称它们是“叙利亚人民的杀手”。

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：常秋妮

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158