国家互联网应急中心

2015 年第 15 期

4 月 6 日-4 月 12 日

网络安全信息与动态周报

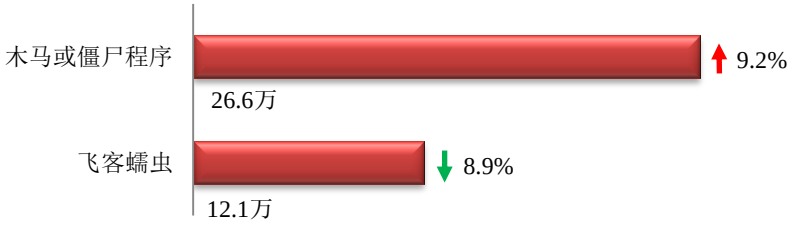
本周网络安全基本态势

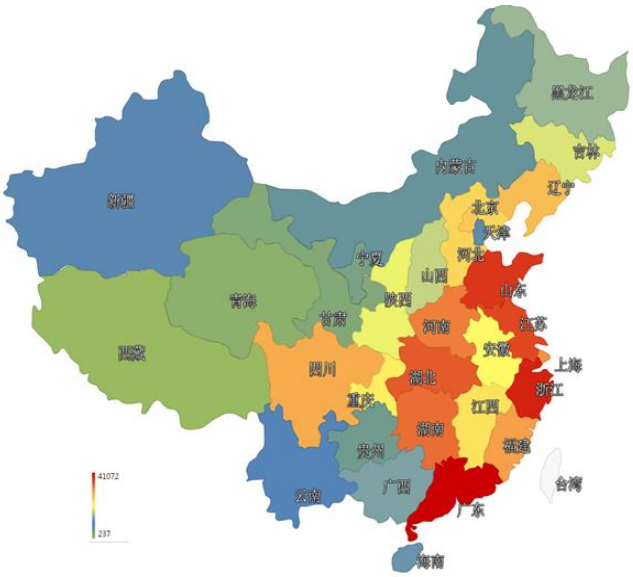
境内感染网络病毒的主机数量	•38.7万	2.8%
境内被植入后门网站总数 其中政府网站数量	•2088 •282	36.1% 41.0%
针对境内网站的仿冒页面数量	•5115	9.4%
新增信息安全漏洞数量 其中高危漏洞数量	•112 •37	14.5% 14.0%

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 38.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 26.6 万以及境内感染飞客（conficker）蠕虫的主机约 12.1 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、浙江省和山东省。

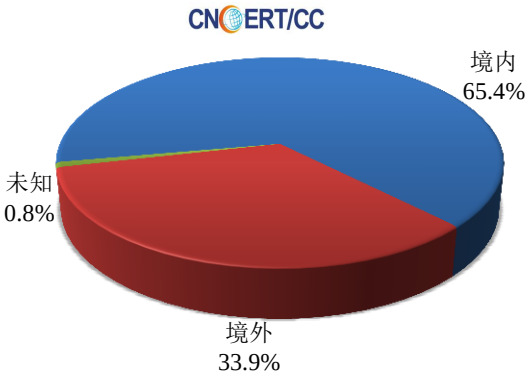
TOP3

广东省	•约4.1万个（约占中国大陆总感染量的15.4%）
浙江省	•约2.4万个（约占中国大陆总感染量的8.9%）
山东省	•约2.1万个（约占中国大陆总感染量的7.8%）

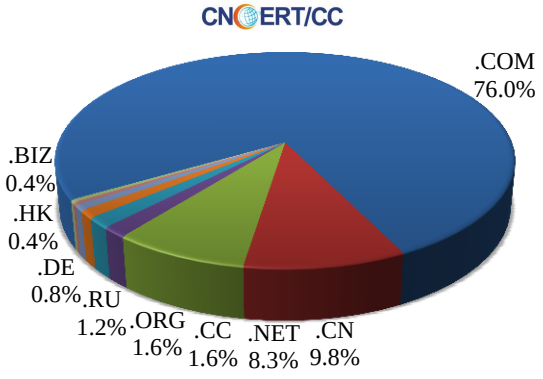
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 23 个，按网络病毒家族统计新增 2 个。

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 254 个，涉及 IP 地址 386 个。在 254 个域名中，有约 33.9%为境外注册，且顶级域为.com 的约占 76.0%；在 386 个 IP 中，有约 12.7%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 49 个 IP。

本周放马站点域名注册所属境内外分布
(4/6-4/12)



本周放马站点域名所属顶级域的分布
(4/6-4/12)



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。

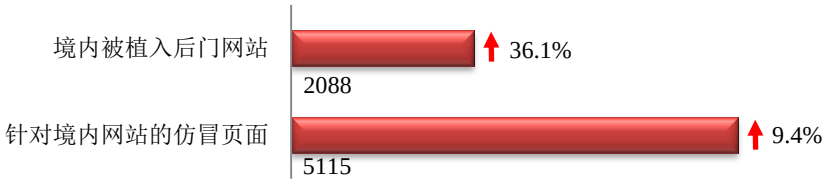
ANVA恶意地址黑名单发布地址

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。

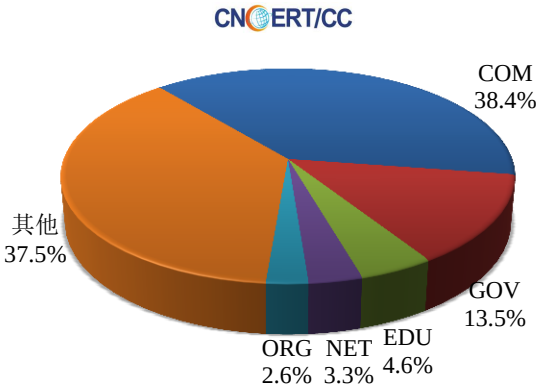
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 2088 个；针对境内网站的仿冒页面数量为 5115。



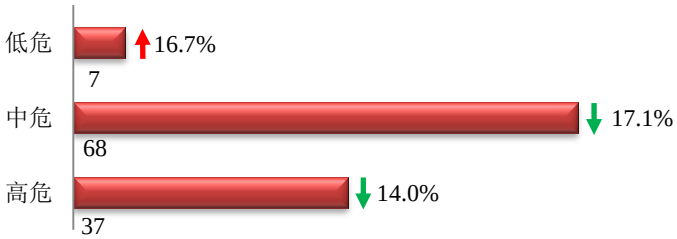
本周境内被植入后门的政府网站(GOV 类)数量为 282 个（约占境内 13.5%），较上周环比上升了 41.0%；针对境内网站的仿冒页面涉及域名 4564 个，IP 地址 1119 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(4/6-4/12)

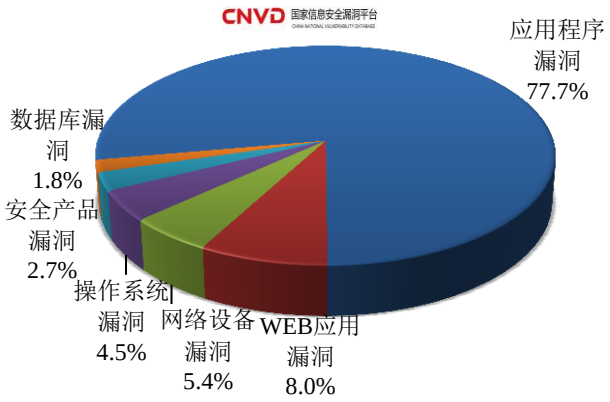


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 112 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
(4/6-4/12)



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 WEB 应用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

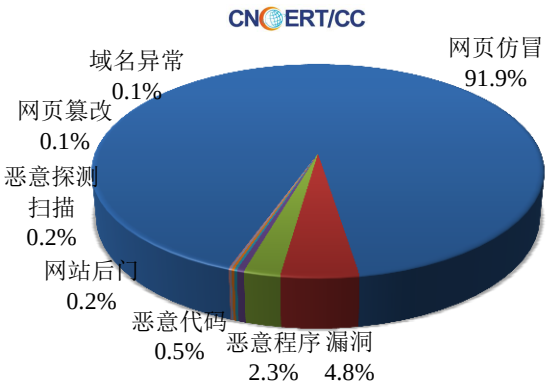
http://www.cnvd.org.cn/webinfo/list?type=4

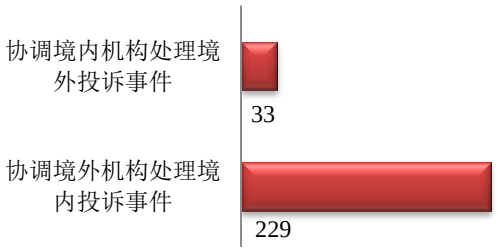
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1102 起，其中跨境网络安全事件 262 起。

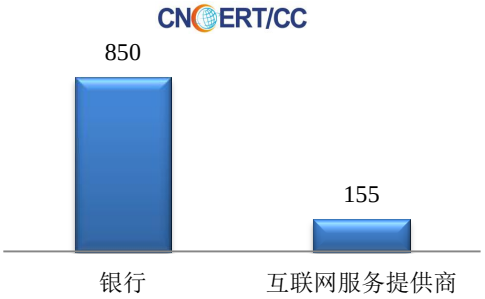
本周CNCERT处理的事件数量按类型分布
(4/6-4/12)



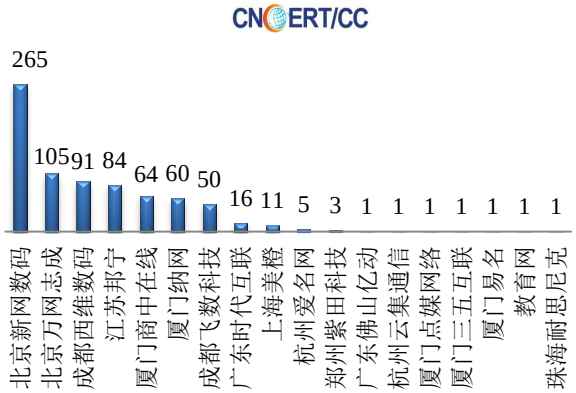


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1005 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 850 起和互联网服务提供商仿冒事件 155 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/6-4/12)

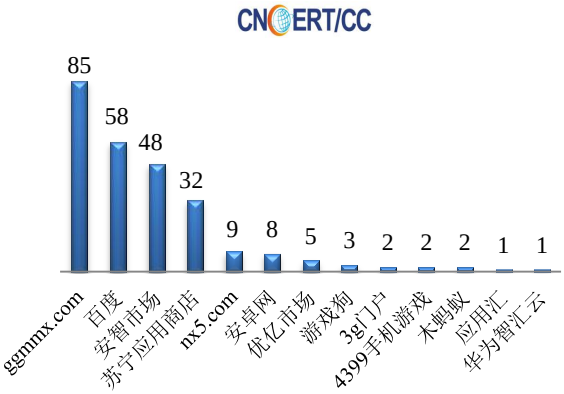


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/6-4/12)



本周，CNCERT 协调 13 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 256 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 (4/6-4/12)



业界新闻速递

1、美媒：美国政府监控国民致电海外长途电话逾 20 年

中新网 4 月 9 日消息 据外媒 4 月 8 日援引美国媒体报道，美国政府自 1992 年起大规模监控美国民众致电海外的长途电话，相关通话纪录除用作打击贩毒活动外，也用于恐袭案调查。这是美国被揭发的大规模监控国民计划中最早开始的一个。报道称，《今日美国报》引述多名美国现任和前任情报及执法部门官员指出，监控计划由毒品管制局及司法部运作，强制电话公司每日交出相关通话记录，直到中情局前雇员斯诺登 2013 年揭露国安局大规模监控后，时任司法部长的霍尔德才在同年 9 月叫停了该计划。据报道，监控计划记下通话号码及通话时间，当局不管被监控者是否有犯罪嫌疑，将数以百万计美国人的长途电话记录存盘，致电目的地包括 116 个政府认为与贩毒有关的国家。联邦调查人员则通过记录，调查贩毒集团在美国的分销网络。报道还指出，当

局同时也利用通话记录调查重大恐袭案，例如 1995 年造成 168 人死亡的俄克拉荷马城政府大楼爆炸案，当局通过这方法确认没有海外恐怖分子参与。“9·11”事件后，这方面的应用更为广泛。

2、美媒：俄黑客入侵白宫电脑系统 奥巴马资料被攫取

环球网 4 月 8 日消息 据俄罗斯《观点报》4 月 8 日消息，美国 CNN 电视台援引与美国政府关系密切的消息人士的话报道称，俄罗斯黑客通过美国国务院系统入侵美国白宫计算机。报道称，去年 10 月份，美国媒体就曾报道疑似来自俄罗斯的黑客可能积极参与了对白宫的攻击行为。但随后白宫发言人乔希•埃内斯并未证实俄黑客尝试入侵网络系统。该官员表示，俄罗斯黑客可能于数月前就已入侵白宫计算机系统。报道称，他们成功攫取机密信息，其中包括本不应该被曝光的奥巴马工作行程细节内容。埃内斯补充指出，被攫取的信息不是秘密内容，但对于国外情报机构具有重要价值。

3、欧美捣毁计算机犯罪网络

新浪网 4 月 9 日消息 北京时间 4 月 9 日晚间消息，美国和欧洲警方周三关闭了一个用于窃取银行密码和进行敲诈的计算机犯罪网络。据悉，该犯罪网络多年来成功地躲避了安全公司和执法部门的追踪。英特尔互联网安全部门技术高管拉贾·萨玛尼（Raj Samani）称，美国联邦调查局（以下简称“FBI”）和欧洲网络犯罪中心（以下简称“ECC”）周三捣毁了该犯罪网络设在欧洲的服务器。这些服务器主要向美国的计算机传网络播恶意代码，已经有上千台计算机被感染。面对日益频繁的网络攻击，一些政府纷纷成立专门部门与互联网安全公司合作，争取在更严重的安全威胁出现之前将其扼杀。ECC 运营总监保罗·吉尔林（Paul Gillen）称，此次捣毁的计算机犯罪网络的功能是作为一个门户站点，为其他想传播自己的恶意代码的犯罪分子提供一个平台。FBI 和 ECC 称，虽然没收了服务器，但尚未逮捕任何人，因为目前还无法判断幕后主使者，以及这些恶意软件将导致怎样的损失。但警方会对服务器中的数据进行分析，然后再通知受害者，确定犯罪人。该犯罪网络所使用的恶意代码被称为“W32/Worm-AAEH”，早在 2009 年就被发现。但由于该恶意代码每天会更新 6 次，因此安全公司很难彻底根除。据萨玛尼称，该恶意程序能切断与安全公司服务器的连接，能禁用可检测到该病毒的安全工具。

4、法语媒体接连遭遇攻击 比国法语区政府网站被黑

中新网 4 月 11 日消息 继法国 TV5Monde 电视台遭遇法语区史上最大规模网络恐袭之后，比利时法语区政府用于发布经济信息的网站 10 日也遭遇黑客攻击。当天，比利时法语区政府用于发布经济信息的网站遭黑客攻击，网页被换成深黑色，并不停地播放由一位未带头巾的女主持人用纯正英语录制的反美视频。该位女主持人在视频中抨击美国及其盟友主导的反恐战争。此间媒体披露，对比国法语区政府网站进行攻击的黑客来自突尼斯一激进组织。该组织曾在今年年初法国巴黎《查理周刊》枪击案发生后对多个法语网站进行攻击。颇为巧合的是，法国 TV5Monde 电视台前一日刚遭到自称是来自极端组织“伊斯兰国”的黑客攻击。当时，自称属于“伊斯兰国”的网络黑客攻陷了法国 TV5Monde 电视台的脸书和推特账户以及该台的网站，贴出了宣扬“圣战”内容的信息，随后还入侵电视台的电脑系统，导致该频道出现黑屏，整个过程持续数小时。显然，法语媒体在防范网络攻击方面问题颇多。比利时鲁汶大学教授、网络安全专家让-夏克·奎斯卡特在接受采访时指出，法语媒体在应对网络安全方面仍存在重大隐患，细节的处理更应得到重视对待。

5、欧洲首家网络安全创新公司成立

中新网 4 月 7 日消息 欧洲首家网络安全创新公司 CyLon 日前在英国成立。CyLon 由企业家、风投公司以及网络安全专家组成，不以盈利为目的，旨在确立英国在全球信息安全创新中的核心地位。据悉，CyLon 将于 2015 年第二季度展开首个为期 12 周的创新项目，受邀参加的企业申请者应提交一份商业构想，最终入围的每位申请者将获得 5000 欧元的“生活补贴”。同时 CyLon 非营利的性质决定了其投资者不会接受创新方案实施后带来的任何股份收益。英国内阁办公室大臣弗朗西斯·麦浩德表示，该举措会协助政府将英国打造为全球电子商务环境最安全的国家之一。英国企业家在为公众、企业、政府和国家基础设施提供更安全的环境方面作出了突出贡献。不过，英国首相卡梅伦近日表示，任何使用高强度加密技术以致无法被安全机构监控的通信业务都将被叫停。这一立场与弗朗西斯的表态存在分歧，并遭到网络安全专家的一致批评。专家称，卡梅伦的立场不仅不切实际，还将扼杀信息安全领域的创新活动。

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：肖崇蕙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170