国家互联网应急中心

2015 年第 10 期

3 月 2 日-3 月 8 日

网络安全信息与动态周报

本周网络安全基本态势

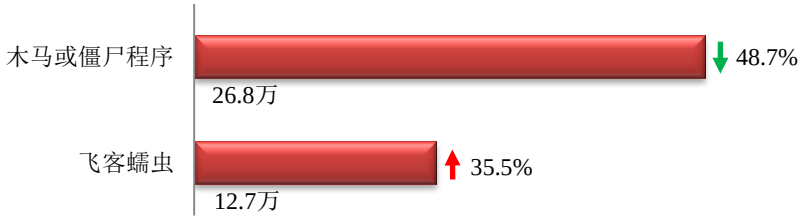
优 良 中 差 危

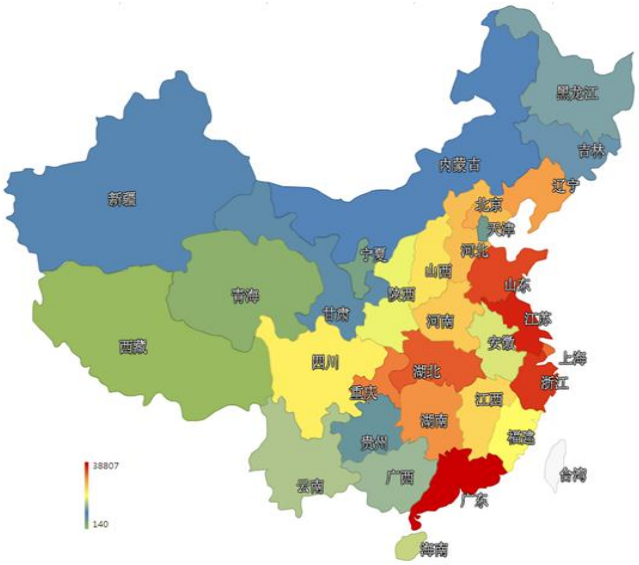
境内感染网络病毒的主机数量	• 39.5万	↓ 35.9%
境内被篡改网站总数 其中政府网站数量	• 3404 • 104	↑ 1.5% ↑ 26.8%
境内被植入后门网站总数 其中政府网站数量	• 1036 • 69	↑ 7.8% ↑ 60.5%
针对境内网站的仿冒页面数量	• 1976	↑ 239.5%
新增信息安全漏洞数量 其中高危漏洞数量	• 133 • 25	↓ 24.0% ↓ 24.2%

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 39.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 26.8 万以及境内感染飞客（conficker）蠕虫的主机约 12.7 万。



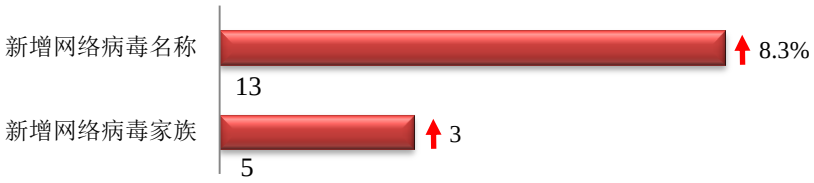


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

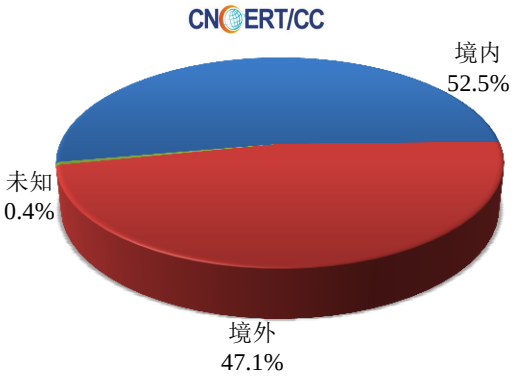
广东省	•约3.9万个（约占中国大陆总感染量的14.5%）
江苏省	•约2.5万个（约占中国大陆总感染量的9.3%）
浙江省	•约2.4万个（约占中国大陆总感染量的9.0%）

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 13 个，按网络病毒家族统计新增 5 个。

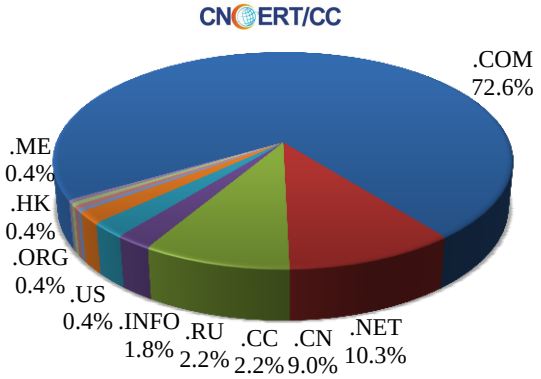


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 223 个，涉及 IP 地址 248 个。在 223 个域名中，有约 47.1%为境外注册，且顶级域为.com 的约占 72.6%；在 248 个 IP 中，有约 26.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 35 个 IP。

本周放马站点域名注册所属境内外分布
(3/2-3/8)



本周放马站点域名所属顶级域的分布
(3/2-3/8)



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。

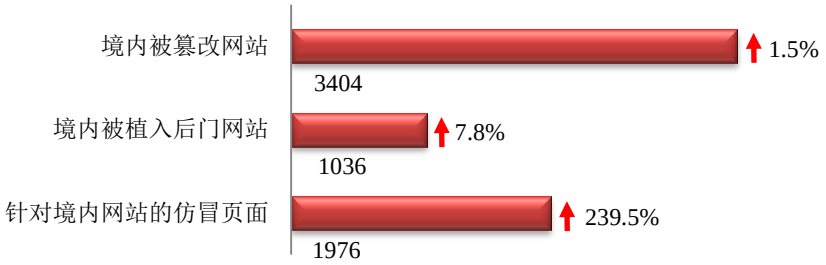
ANVA恶意地址黑名单发布地址

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。

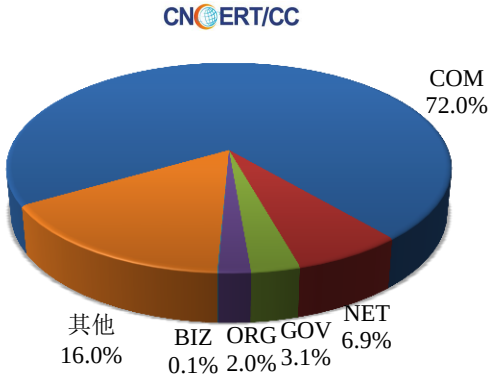
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3404 个；境内被植入后门的网站数量为 1036 个；针对境内网站的仿冒页面数量为 1976。

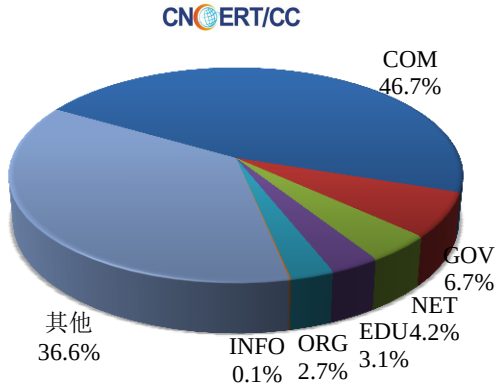


本周境内被篡改政府网站(GOV 类)数量为 104 个（约占境内 3.1%），较上周环比上升了 26.8%；境内被植入后门的政府网站(GOV 类)数量为 69 个（约占境内 6.7%），较上周环比上升了 60.5%；针对境内网站的仿冒页面涉及域名 1588 个，IP 地址 450 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/2-3/8)

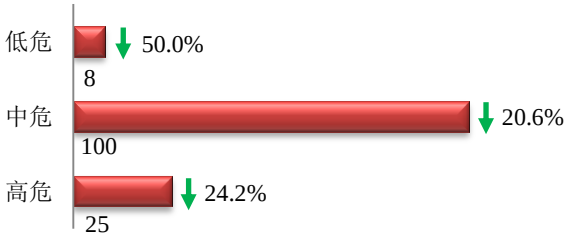


本周我国境内被植入后门网站按类型分布
(3/2-3/8)

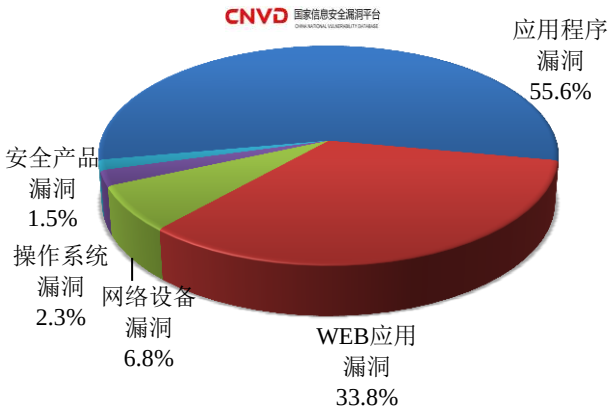


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 133 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
(3/2-3/8)



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

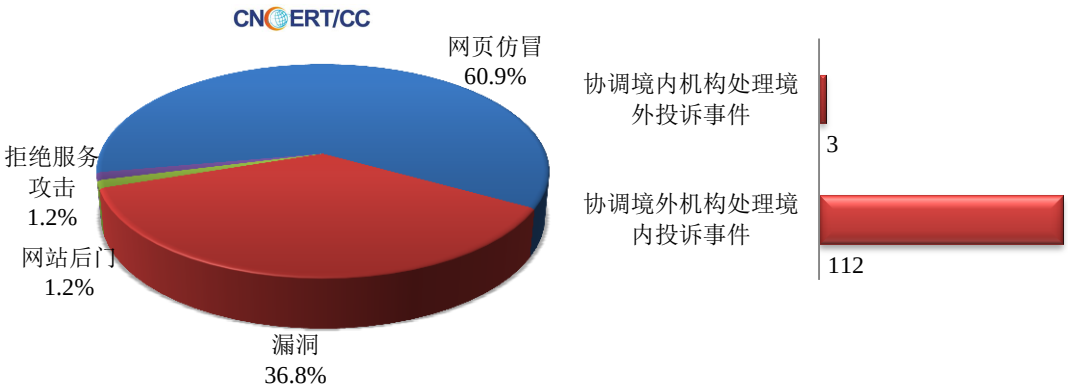
http://www.cnvd.org.cn/webinfo/list?type=4

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

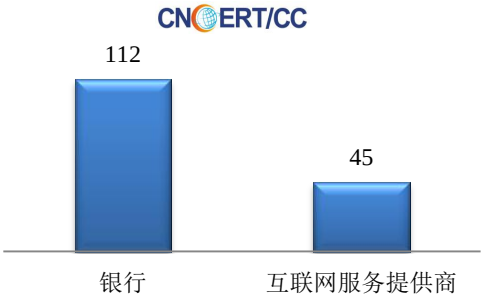
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 258 起，其中跨境网络安全事件 115 起。

本周CNCERT处理的事件数量按类型分布
(3/2-3/8)

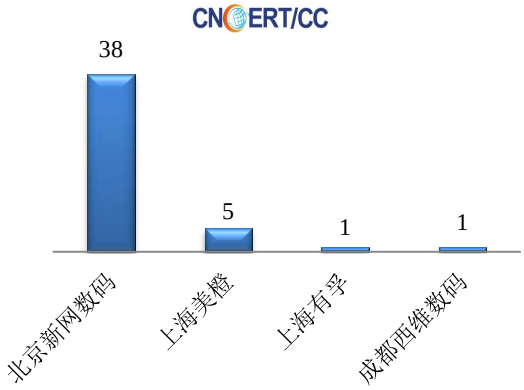


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 157 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含工商银行等银行仿冒事件 112 起和中国移动等互联网服务提供商仿冒事件 45 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/2-3/8)

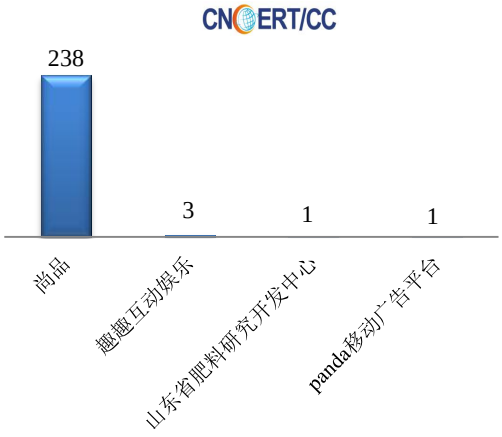


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/2-3/8)



本周，CNCERT 协调 4 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 243 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 (3/2-3/8)



业界新闻速递

1、中方回应美方关切信息安全新规:望美正确冷静客观处理

国际在线 3 月 3 日消息 针对美国总统奥巴马对中国反恐法草案中涉信息安全有关内容表示关切，中国外交部发言人华春莹 3 月 3 日在北京回应表示，立法问题属于中国内政，希望美方正确、冷静、客观处理。另外，各国都高度关注信息安全问题并采取措施保障自身信息安全，这无可指摘。华春莹说，“中方一向坚决反对利用信息技术优势或利用提供信息技术产品的便利条件实施网络监控，一贯支持并推动在联合国框架下制订网络空间国际规则。当前网络空间事端频发，尽早制定指导各方行为的统一规范尤为重要。中国同有关国家早在 2011 年 9 月向联大提交了“信息安全国际行为准则”草案，今年 1 月又提交了更新草案，其目的是以维护网络空间和平与稳定为宗旨，在坚持尊重国家主权、不干涉内政、和平解决争端等原则的基础上，强化互联网公平治理，建立网络空间信任措施。”华春莹表示，希望美方建设性参与相关讨论，尽早就此达成国际共识，共同构建和平、

安全、开放、合作的网络空间秩序。

2、上海加快完善信息安全保障体系 推动地方立法

中国日报网 3 月 6 日消息 3 月 5 日，上海市智慧城市信息安全保障工作会议举行。会议表示，面对信息安全事件高发的新常态，上海市将加快完善信息安全保障体系，推动个人信息保护和关键信息基础设施防护等地方立法。据分析，目前上海的信息安全工作面临四方面挑战：一是中央对上海提出了建设具有全球影响力的科创中心的要求；二是城市运行已高度依赖网络和信息系统，信息安全事件高发将成为新常态；三是移动互联网、物联网、大数据等新技术将使信息安全面临新情况；四是市民对打击涉网犯罪、保护个人信息安全等方面提出了更多新期待。面对挑战，上海将重点做好政府公共数据资源开放、网上政务大厅、信用报告在线查询等重点项目的安全保障，加强基础网络、重要网站和信息系统、城市生命线系统及重要工控系统的梳理和检查。此外，上海市还将加快推动立法，营造良好的社会环境；并通过自主创新技术的转化应用、吸引信息安全领军人物来沪发展等举措，充分发挥各类市场主体对于保障信息安全的作用。

3、斯诺登曝新西兰参与美英“五只眼”窃听计划

中国日报网 3 月 6 日消息 据新西兰主流媒体《新西兰先驱报》3 月 5 日公布据信由美国“棱镜门”爆料人爱德华·斯诺登提供的文件，显示新西兰情报机构政府通信安全局在“五只眼”情报监听联盟中负责搜集南太平洋地区国家的情报，并把相关信息分享给美国、加拿大、英国和澳大利亚。此次公开的文件主要是一份日期标注为 2009 年 7 月的“最高机密”报告。报告显示，新西兰政府通信安全局在南太平洋地区多个国家搜集情报信息，并与“五只眼”盟友美国、加拿大、英国和澳大利亚分享这些信息。根据这份报告，新西兰情报机构在太平洋地区的“目标国家”包括所罗门群岛、斐济、基里巴斯、汤加、瓦努阿图、瑙鲁和萨摩亚。新西兰总理办公室 5 日表示，斯诺登获取的信息“过时”，并质疑文件内容的真实性。新西兰政府通信安全局 5 日拒绝评论相关信息。这一机构表示，其从事的所有活动均获得授权并接受独立审查。一些分析人士表示，南太平洋国家在新西兰竞选联合国安理会成员国的过程中给予一定帮助，此次信息公开可能令新西兰政府尴尬。

4、苹果谷歌确认正修复 Freak 信息安全漏洞

新浪网 3 月 4 日消息 北京时间 3 月 4 日早间消息，苹果和谷歌周二表示，它们正在修复近期发现的“Freak”信息安全漏洞。这一漏洞影响了移动设备和 Mac 电脑。发现该漏洞的研究人员指出，利用这一网页加密技术的漏洞，黑客可以窃取苹果 Safari 和谷歌 Android 浏览器的用户通信。苹果发言人表示，苹果已经开发了补丁，并将于下周推送。谷歌发言人则表示，谷歌也已开发了补丁，并已提供给合作伙伴。不过她并未透露，普通用户将于何时收到这一补丁。谷歌通常并不会直接推送 Android 系统的更新，而是将更新提供给设备商和运营商，由它们来发布。《华盛顿邮报》报道称，这一漏洞导致苹果和谷歌产品的用户在访问数十万网站时容易遭到攻击。这些网站包括 Whitehouse.gov、NSA.gov 和 FBI.gov 等。报道援引约翰·霍普金斯大学密码学专家马修·格林（Matthew Green）的说法称，Whitehouse.gov 和 FBI.gov 已经进行了修复，而 NSA.gov 仍然存在漏洞。9 名研究人员发现，他们可以强迫网页浏览器使用一种针对美国政府监管规定蓄意弱化的加密形式。美国政府的规定禁止美国公司出口最强的加密标准。然而，在使用较弱的加密形式时，他们可以在几小时内破解加密系统。在这种情况下，黑客可以很容易窃取数据，并对这些网站发起攻击。谷歌发言人表示，谷歌已建议所有网站关闭对不太安全的加密形式的支持。她同时指出：“Android 浏览器与大部分网站，包括谷歌网站的连接，并不存在这样的漏洞。”

5、日本将 48 个组织指定为遭网络攻击时的合作对象

环球网 3 月 2 日消息 据日本共同社 3 月 1 日报道，日本政府相关人士 3 月 1 日透露，为应对网络攻击已开始加强官民一体的合作，日本政府根据 2014 年 11 月通过的《网络安全基本法》，于 2 月 10 日将 NTT 及主要机场的运营公司等负责“重要基建”的 48 个企业或组织指定为要求合作的对象。当因网络攻击受害严重时将要求这些企业或组织提供信息及有关资料。为迎接 2020 年东京奥运会，制定日本国内的网络攻击对策成为当务之急。日本政府认为，为了迅速应对网络攻击造成的损害及查明原因，与社会影响较大的重要基建企业等合作不可或缺。指定的 48 个企业或组织包括各高速公路公司及部分铁路公司（JR）、NHK、日本银行、日本红十字会等。合作要求将由政府“网络安全战略总部”秘书处“内阁网络安全中心”提出，该中心于 1 月新设。48 个企业或组织在因网络攻击严重影响自身业务的情况下，以及发生重大信息泄漏、自身服务器成为针对他国的网络攻击的跳板时，将被要求给予合作。基本法规定，各省厅等行政机构有义务遵循该法提供合作，地方政府和国立大学与上述 48 个企业或组织一样，根据该法在政府提出要求时需进行合作。另一方面，电力和燃气等重要基建有关的民间企业依据战略总部制定的行动计划对政府的要求需给予合作，但并没有具体的法律规定。

6、越南黑客窃取 10 亿电邮地址 销售仿冒软件牟利

网易 3 月 7 日消息 据路透社报道，美国司法部于周五表示，2 名越南人以及 1 名加拿大人受到指控，理由是他们用欺诈手段在网络上窃取了 10 亿条电邮地址，并向这些地址发送垃圾邮件推销仿冒的软件产品。司法部将此次事件描述为美国历史上“最大规模数据泄露案件之一”。该部门拒绝透露遭泄露的电邮地址来自哪些公司，虽然看上去该案件与电邮营销公司 Epsilon 在 2011 年遭受的大规模袭击有关。依据安全博客作者布莱恩·科瑞斯（Brian Krebs）的说法，作为 Alliance Data Systems 的一个部门，Epsilon 是众多受害者之一。该事件发生后，Epsilon 的众多客户，包括花旗集团及摩根大通在内，纷纷向自己的消费者发出了提醒。科瑞斯指出，政府在新闻通稿中称，“美国众议院于 2011 年 6 月 2 日对该事件展开过质询并听取了证词。”美国贸易委员会亦对该事件举行过听证会。其中的一名武姓越南嫌犯已于去年 3 月被引渡回美国，并于本周四承认了上述罪行。一名阮姓越南籍嫌犯仍然逍遥法外。另一名被告是现年 33 岁的加拿大人戴维曼纽尔·桑托斯·达斯瓦（David-Manuel Santos Da Silva），达斯瓦已于上月在佛罗里达机场遭到逮捕，并将于本周五出庭。

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：徐晓燕

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170