国家互联网应急中心

2015 年第 32 期

8 月 3 日-8 月 9 日

网络安全信息与动态周报

CNCERT/CC

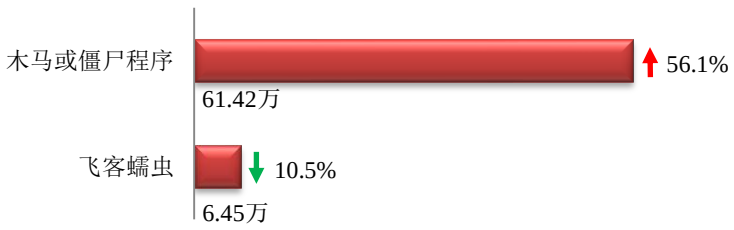
本周网络安全基本态势

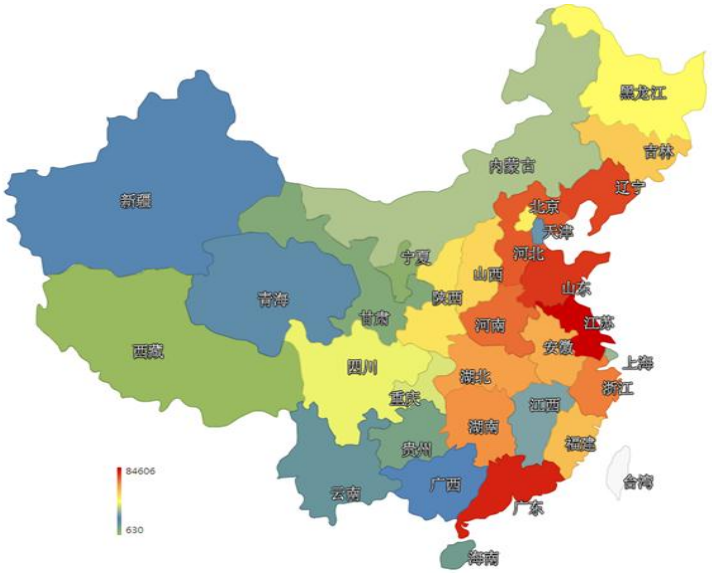
境内感染网络病毒的主机数量	•67.87万	↑ 45.8%
境内被篡改网站总数 其中政府网站数量	•4931 •106	↓ 9.3% ↓ 10.2%
境内被植入后门网站总数 其中政府网站数量	•2885 •125	↓ 39.8% ↓ 13.2%
针对境内网站的仿冒页面数量	•5156	↓ 4.5%
新增信息安全漏洞数量 其中高危漏洞数量	•86 •46	↓ 62.3% ↓ 20.7%

═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 67.87 万个，其中包括境内被木马或被僵尸程序控制的主机约 61.42 万以及境内感染飞客（conficker）蠕虫的主机约 6.45 万。



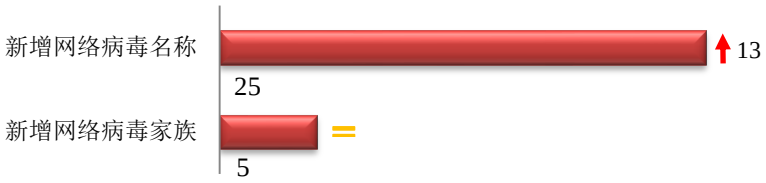


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是江苏省、广东省和山东省。

TOP3

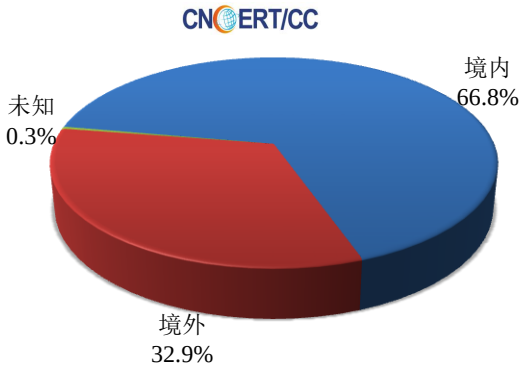
江苏省	•约8.5万个（约占中国大陆总感染量的13.8%）
广东省	•约8.1万个（约占中国大陆总感染量的13.2%）
山东省	•约5.6万个（约占中国大陆总感染量的9.1%）

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 25 个，按网络病毒家族统计新增 5 个。

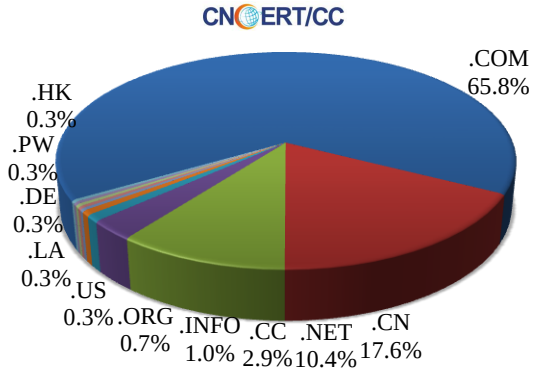


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 307 个，涉及 IP 地址 443 个。在 307 个域名中，有约 32.9%为境外注册，且顶级域为.com 的约占 65.8%；在 443 个 IP 中，有约 19.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 62 个 IP。

本周放马站点域名注册所属境内外分布
(8/3-8/9)



本周放马站点域名所属顶级域的分布
(8/3-8/9)



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。

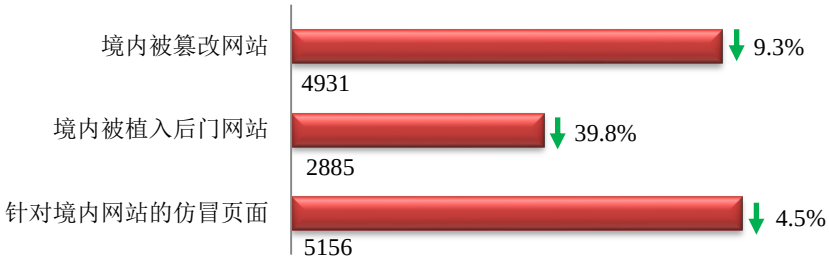
ANVA恶意地址黑名单发布地址

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。

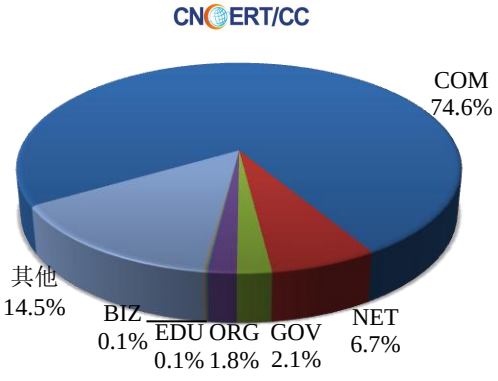
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4931 个；境内被植入后门的网站数量为 2885 个；针对境内网站的仿冒页面数量为 5156。

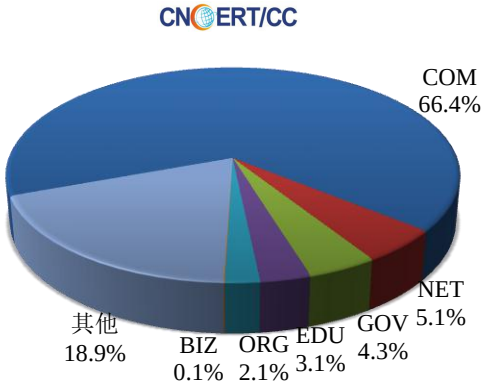


本周境内被篡改政府网站(GOV 类)数量为 106 个（约占境内 2.1%），较上周环比下降了 10.2%；境内被植入后门的政府网站(GOV 类)数量为 125 个（约占境内 4.3%），较上周环比下降了 13.2%；针对境内网站的仿冒页面涉及域名 4047 个，IP 地址 939 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/3-8/9)



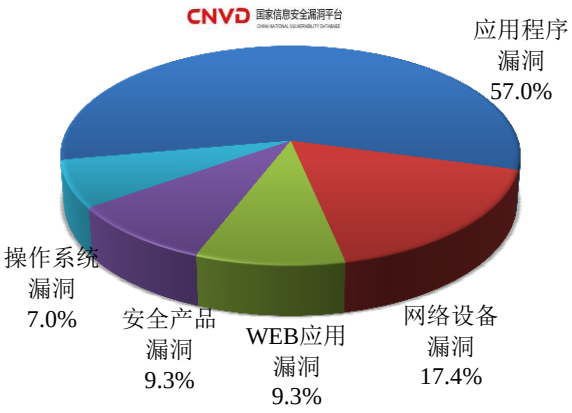
本周我国境内被植入后门网站按类型分布
(8/3-8/9)



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 86 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
(8/3-8/9)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 WEB 应用漏洞、安全产品漏洞。

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

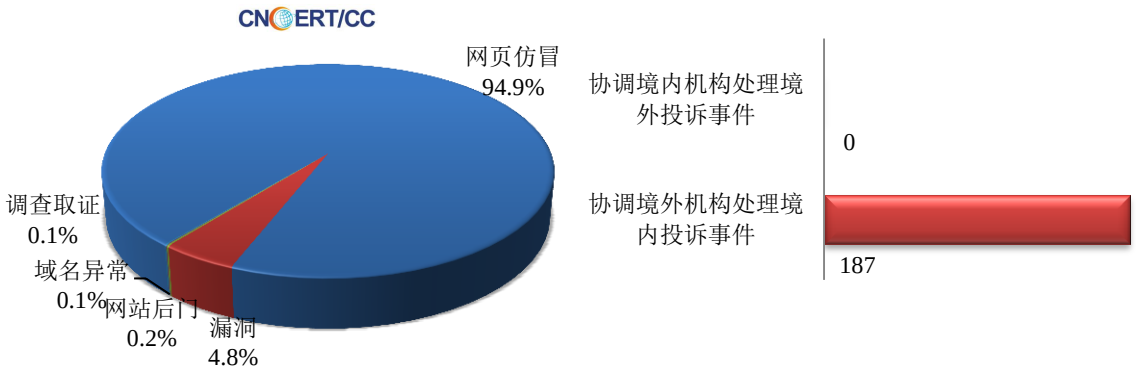
http://www.cnvd.org.cn/webinfo/list?type=4

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

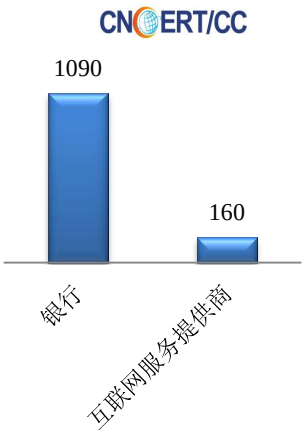
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1317 起，其中跨境网络安全事件 187 起。

本周CNCERT处理的事件数量按类型分布
(8/3-8/9)

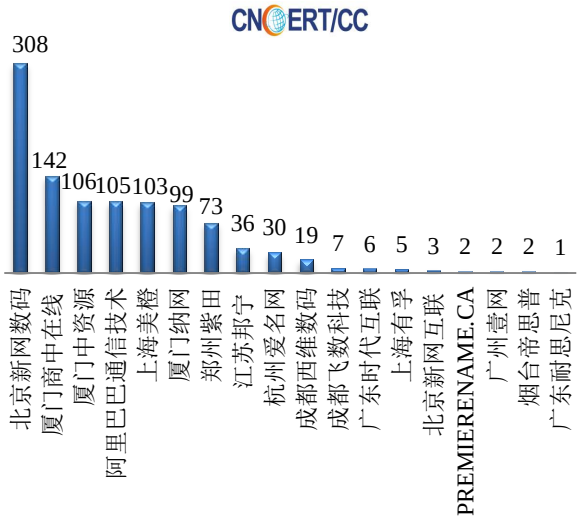


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1250 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1090 起和互联网服务提供商仿冒事件 160 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/3-8/9)

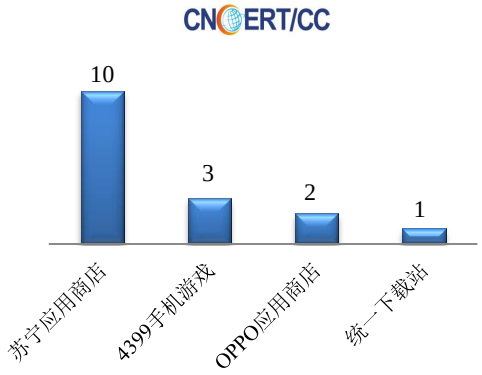


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/3-8/9)



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 16 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 (8/3-8/9)



业界新闻速递

1、工信部组织开展电信行业网络安全试点示范工作

电子信息产业网 8 月 7 日消息 工业和信息化部日前发出通知，组织开展电信行业网络安全试点示范工作（以下简称试点示范）。通知指出，2015 年试点示范项目的申请主体为基础电信企业集团公司或省级公司，试点示范项目为已建或在建（含已立项）的网络安全管理系统或技术平台。试点示范项目遴选以“示范效果好、实用价值高、推广潜力大”为标准，重点考察试点示范项目是否具备实践基础、较强的技术或管理创新性和良好应用效果；是否具有普遍适用性、可复制性和推广价值；能否坚持持续改进，发挥综合效益。工业和信息化部对于入选的试点示范项目，在其申请国家专项资金、科技评奖等方面，将按照有关政策予以支持。2015 年电信行业网络安全试点示范重点引导方向包括企业内部集中化安全管理、网络和信息系统资产安全管理、数据安全保

护、抗拒绝服务攻击、云平台安全防护、域名系统安全及其他创新性显著、安全防护效果突出、示范价值较高的项目等。基础电信企业集团公司统一负责本集团范围内的项目申报工作，2015 年 9 月 30 日前向工业和信息化部统一提交申报材料。各基础电信企业集团公司（包括省级公司）每个领域的申报项目不超过 3 个。工业和信息化部（网络安全管理局）组织对各基础电信企业集团公司的申报材料进行审核，并组织专家在现场考察基础上进行项目遴选，通过遴选的项目，将在工信部所属相关媒体和网站予以公布。

2．独立后的 ICANN 管理运营方案文件征求意见

天极网 8 月 5 日消息 据外媒报道称，近日有一份有关独立之后互联网名称和数字地址分配机构 ICANN 如何管理运营的文件出台，开始面向行业和政府征求意见，且征求意见工作将于 9 月 8 日截止。方案涉及 ICANN 管理工作如何交接以及国际社会如何共同来管理国际互联网等。方案指出，新的 ICANN 总部仍将设立在美国加州，由利益攸关方共同管理；建议在 ICANN 内部设立一个独立的下属机构，完成 ICANN 的技术管理职能；原由美国政府负责的有关职能将转交给 ICANN 来完成；对于 ICANN 的工作考核将向国际利益攸关方转交，而国际利益攸关方中不直接包括各国政府或政府间的组织。

3、美军网络安全领导开会商讨如何实现更好安保工作

环球网 8 月 7 日消息 据美国《国防新闻》8 月 4 日报道，在数百万美国人遭受美国历史上最大的数据泄露事件之后，美国网络防御领域最高军事领导人在 4 日举办会议，商讨如何更好地确保美国网络安全。奥巴马政府在今年夏天人事管理办公室网络被入侵并导致 2150 万美国公民个人信息泄露后，加倍努力确保政府网络安全。此次研讨会又提出了国防安全新关联。根据国防战略研究所的网站上公布的议程，研讨会将重点放在“政策、执行以及技术，旨在维护关键网络并允许在网络域自由操作”。报道说，最近几年，美国军事领导人一直致力于加强维护网络安全能力，包括寻找更好的方法让“网络战士”可以进入进攻战场作战，使他们可以收集情报并削弱敌人的沟通能力。在美国海军陆战队里，网络顾问已经被加入到了海陆空任务规划人员中。据报道，美国的网络海军陆战队参加了 2014 年秋天一次大规模两栖军事演习。网络操作人员当时的任务是监控模拟敌人在城市运作中的通信。他们致力于提取大量电子信号，并将它们转化为可操作的情报并提供给地面诸部队。

4、美国安局被曝监听日本政要和大企业通信 未明确提及安倍

央广网 8 月 3 日消息 据中国之声《新闻纵横》报道，日前，维基揭秘网公开多份文件，称美国国家安全局监听日本政要和大型企业的通信，时间最早可追溯到 2007 年，即安倍晋三第一次出任日本首相期间。对此，美国驻日大使馆拒绝发表评论。美国国务院副发言人马克·托纳 31 号在例行新闻发布会上表示，美方没有收到日方提出的正式或非正式抗议。维基揭秘网公开的文件中，有 5 份标注来自美国国安局的文件涉及监听日本，所涉监听对象的电话有 35 个。文件内容没有明确提及日本首相安倍，但现任经济产业大臣宫泽洋一等日本政要、日本中央银行行长黑田东彦、三菱集团旗下天然气公司等大企业，都在美国监听范围之内。日本被视作美国在亚太地区的关键盟友之一，两国经常在防务、经济和贸易问题上保持通气。被公开的美国国安局文件则显示，除正常接触以外，美国在致力于了解日本政府和企业背后的动作和考量。

5、互联网公司将需要遵守欧盟新网络安全法规

网易 8 月 7 日消息 据路透社报道，思科、谷歌、亚马逊等互联网公司将需要遵守一项新的欧盟网络安全法

规。该法规将强制要求它们采取严格的安全措施，它们可能还需要向政府机构汇报严重的网络安全漏洞事件。对于《网络与信息安全指令》，欧盟成员国和欧盟立法委员之间的洽谈一度陷入僵局，因为它们对是否将注入搜索引擎、社交网络、电商网站、云计算提供商的数字平台纳入其中存在分歧。欧盟议会成员希望该法规仅覆盖它们认为关键的行业，如能源、交通运输和金融。但在经过数个月的磋商后，数字平台将会受到该法规管制，尽管它们要履行的安全义务相对没那么繁重。成员国将可以在 9 月的会议上发表自己的意见和选择偏好，在那之后完整的法律文本起草工作将会启动。数字领域的公司反对被纳入该法规的管制范围。思科政务高级经理克里斯·戈夫（Chris Gow）表示，“我们很高兴看到数字服务平台受到一种不同制度的管制，但我们很失望相关机构并没有认识到决定安全风险的是对云服务的使用，而不是服务本身。”欧盟委员会和部分成员国认为，由于互联网服务被广泛使用，大量企业依赖于网络，因此该类服务也应当遵守安全法规和通告要求。目前，还没有泛欧洲的网络安全法规，只有电信运营商需要遵守事件通告要求。

6、美媒体称美国防部电邮系统遭俄黑客攻击

新华网 8 月 7 日消息 美国媒体 8 月 6 日报道称，由于遭到俄罗斯黑客所谓“精密的网络攻击”，美国防部参谋长联席会议电子邮件系统已被迫关闭近两周。美国多家媒体引述五角大楼官员的话确认发生了网络攻击。率先曝出黑客攻击事件的美国国家广播公司援引未透露姓名消息来源的话说，没有机密信息被盗走或泄漏，只有非机密的账号和电子邮箱遭到了攻击。但是在对此次攻击展开调查期间，五角大楼关闭了参谋长联席会议的电邮系统。据报道，有官员说，网络攻击似乎依赖于某种形式的自动化系统。该系统可以在一分钟内快速聚集大量的数据，并将所有信息发送到几千个账号中。该官员还声称，俄罗斯黑客疑似通过加密的社交媒体账号策划了这起精密的网络攻击。报道说，这起攻击发生在 7 月 25 日，大约有 4000 名军人和文职人员的工作受到影响。

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：徐原

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373