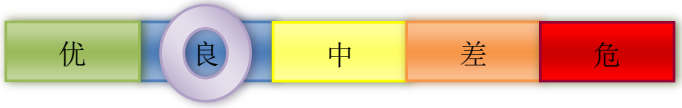
国家互联网应急中心

2014 年第 3 期

1 月 13 日-1 月 19 日

网络安全信息与动态周报

本周网络安全基本态势

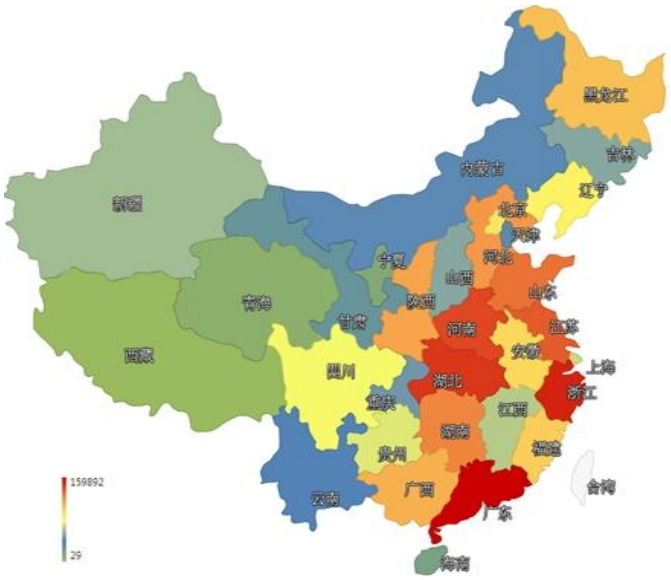


境内感染网络病毒的主机数量	• 67.1万	6.9%
境内被篡改网站总数 其中政府网站数量	• 4421 • 342	9.2% 11.6%
境内被植入后门网站总数 其中政府网站数量	• 1393 • 48	3.7% 15.8%
针对境内网站的仿冒页面数量	• 281	25.3%
新增信息安全漏洞数量 其中高危漏洞数量	• 250 • 60	64.5% 42.9%

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 67.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 32.8 万以及境内感染飞客（conficker）蠕虫的主机约 34.3 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、浙江省和湖北省。

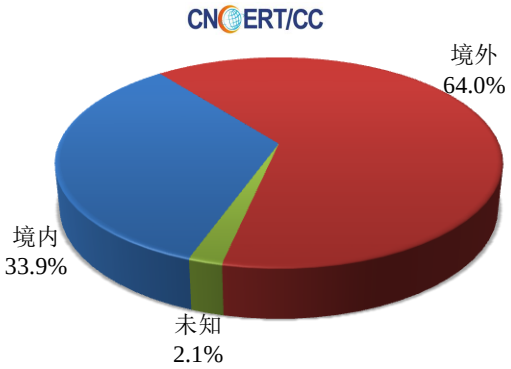
TOP3

广东省	•约16.0万个（约占中国大陆总感染量的48.7%）
浙江省	•约1.6万个（约占中国大陆总感染量的4.8%）
湖北省	•约1.4万个（约占中国大陆总感染量的4.1%）

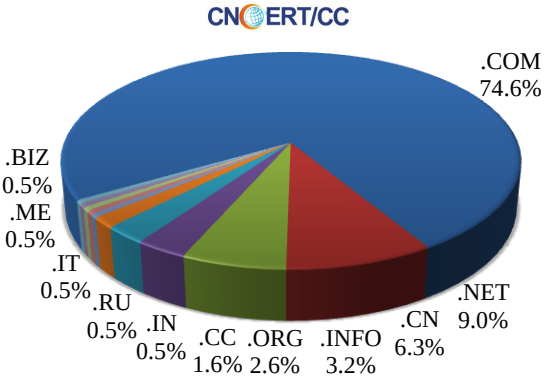
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 56 个，按网络病毒家族统计新增 2 个。

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 189 个，涉及 IP 地址 325 个。在 189 个域名中，有约 64.0%为境外注册，且顶级域为.com 的约占 74.6%；在 325 个 IP 中，有约 29.8%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 81 个 IP。

本周放马站点域名注册所属境内外分布
(1/13-1/19)



本周放马站点域名所属顶级域的分布
(1/13-1/19)



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。

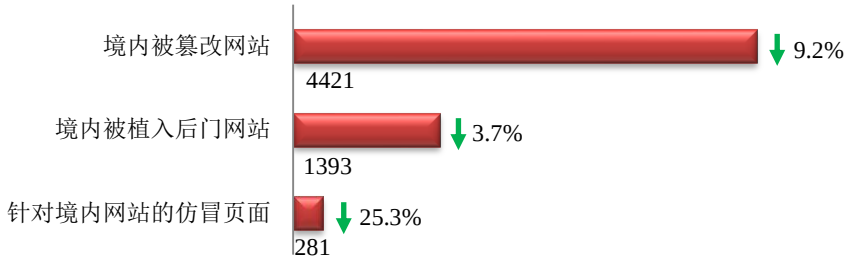
ANVA恶意地址黑名单发布地址

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。

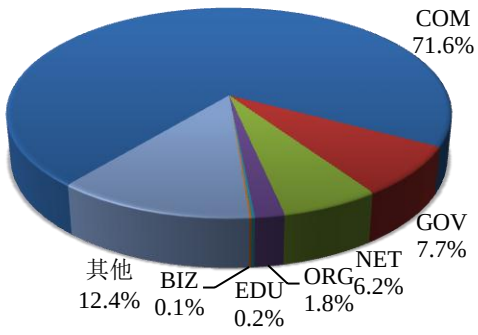
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4421 个；境内被植入后门的网站数量为 1393 个；针对境内网站的仿冒页面数量为 281。

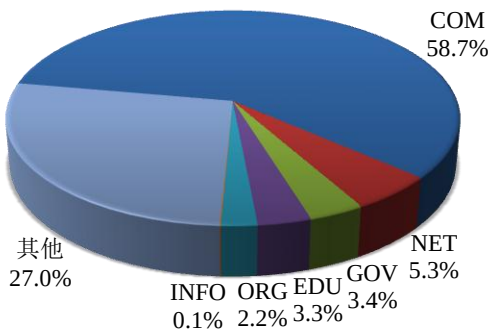


本周境内被篡改政府网站(GOV 类)数量为 342 个（约占境内 7.7%），较上周环比下降了 11.6%；境内被植入后门的政府网站(GOV 类)数量为 48 个（约占境内 3.4%），较上周环比下降了 15.8%；针对境内网站的仿冒页面涉及域名 208 个，IP 地址 131 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/13-1/19)

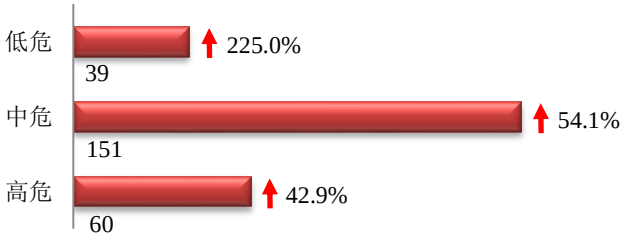


本周我国境内被植入后门网站按类型分布
(1/13-1/19)

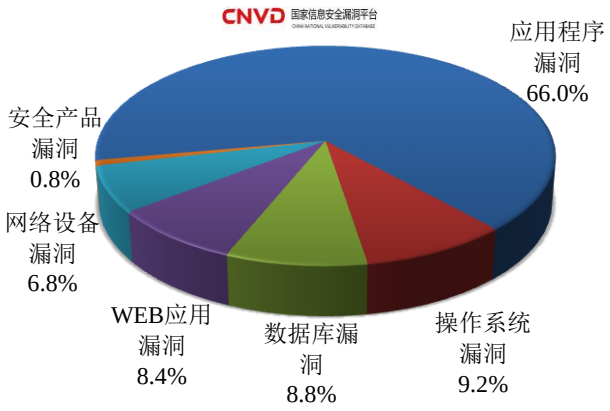


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 250 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(1/13-1/19)



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数据库漏洞。

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

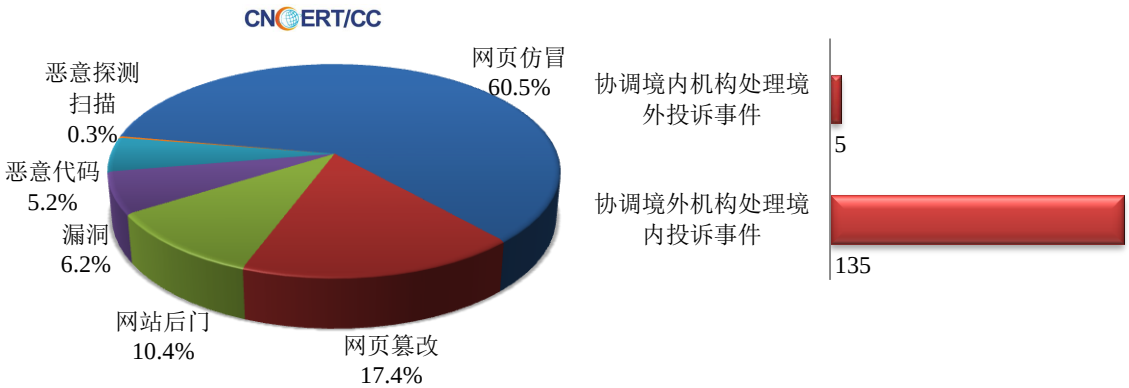
http://www.cnvd.org.cn/webinfo/list?type=4

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

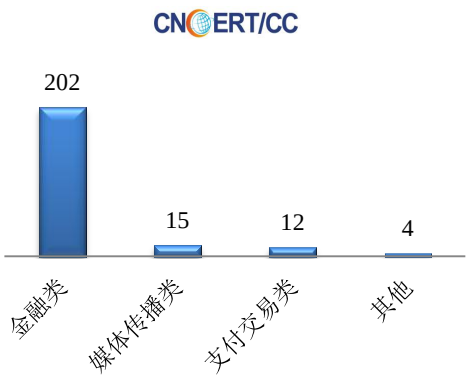
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 385 起，其中跨境网络安全事件 140 起。

本周CNCERT处理的事件数量按类型分布
(1/13-1/19)

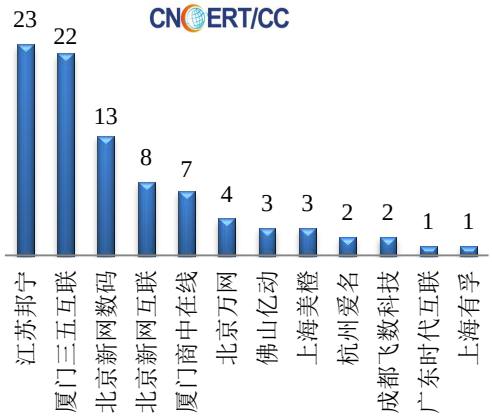


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 233 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含工商银行等金融类仿冒事件 202 起和湖南卫视等媒体传播类仿冒事件 15 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/13-1/19)

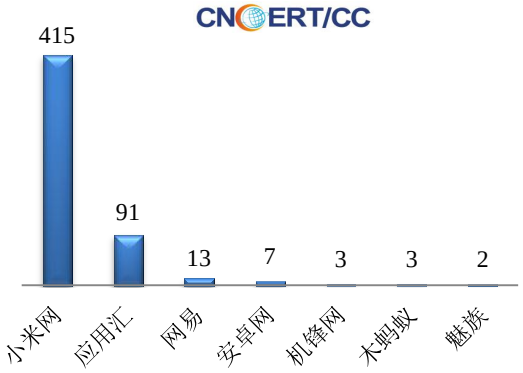


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/13-1/19)



本周，CNCERT 协调 7 家应用商店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 534 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 (1/13-1/19)



业界新闻速递

1、工信部：尽快出台新增骨干直联点鼓励政策

凤凰网 1 月 14 日消息 工信部网站 1 月 14 日消息，为了加快新增骨干直联点设立工作，更好发挥新增点作用，工信部发布相关指导意见。意见提出尽快出台新增点鼓励扶持政策、及时签订新增点互联协议、抓紧制订新增点设立方案、切实抓好新增点工程建设等具体任务。意见提出的目标为，未来 1 到 2 年，完成新增七个骨干直联点的设立工作并投入运行；完成总共不少于 700G 的骨干网间互联，基本消除网间通信质量障碍；骨干网络节点升级改造全面完成，相关网间通信质量监测、应急保障、安全运行维护及保护、网络信息安全等配套系统完成建设并投入运行；相关配套管理制度初步建立，管理流程顺畅，基本满足新增点安全平稳运行需要。

2、北京网络行业协会“和谐北京 安全网络”会员大会举行

中新网 1 月 16 日消息 1 月 15 日下午，北京网络行业协会 2013“和谐北京 安全网络”年会暨会员大会在北京邮电会议中心举行。北京网络行业协会会长王奇云出席并致辞。来自公安主管部门、协会各会员单位、及《网络信息安全杂志》、《中国信息安全杂志》等相关机构的代表出席了会议。与会代表就互联网大数据时代下网络信息安全相关问题进行了探讨、发言。据了解，北京网络行业协会是由北京地区的 ISP、ICP、IDC，从事信息网络安全技术服务以及产品研究开发、生产制造的企事业单位，信息网络重点保护单位和使用单位，上网服务场所等网络行业单位自愿发起组成的。该协会自 2011 年 11 月 24 日正式对外启动工作，秉承“公平、公正、公开”原则，关注于北京地区的网络安全，为会员需要提供服务，为行业发展做出贡献，同时为相关政府部门的工作提供有力支撑。

3、日本拟设网络救援队 将应对东京奥运会网络安全

中新网 1 月 16 日消息 据日本媒体 1 月 16 日报道，日本政府将在 4 月成立“网络救援队”，负责帮助受到网络攻击的企业收集信息、分析原因以及协助修复。同时该部门也将服务于 2020 年东京奥运会。据报道，该救援队将设在日本独立行政法人情报处理推进机构(IPA)之下，编制为 20 人。着眼于 6 年后的东京奥运会，该救援队将建立提前防范网络攻击、并能尽快恢复正常的体制。报道指出，网络攻击一旦发生，输电线和管道等电力和天然气基础设施受到影响。除了 IPA 平时负责信息收集的电力、天然气、化学、石油和重工业这 5 个行业之外，救援队还将收集通信、金融、航空、铁路、医疗和给排水等广泛行业的信息。此外，该救援队还将进入遭受网络攻击的工厂和发电站展开调查。根据企业的要求，它还将负责发生故障的系统的恢复工作。此前，IPA 只能进入企业的总部，能收集到的信息受到一定局限。在举办奥运会期间，由于比赛计划和结果速报的发布和记录等大都采用 IT 技术，因此很容易成为网络攻击的目标。日本经济产业省将于 2 月邀请曾在 2012 年伦敦奥运会担任网络防护负责人的英国政府相关人士，举行研讨会。

4、欧盟发展进攻性网络能力 大数据、物联网成新“数字战场”

中国信息产业网 1 月 13 日消息 欧洲网络与信息安全局（ENISA）近日发布的最新威胁形势分析报告称，网络攻击已经变得日益复杂、频繁。“几年前，攻击类型和工具针对的是个人电脑，现在目标已经转向移动生态系统。大数据和物联网已经成为新的‘数字战场’。”欧洲国家已经加入发展进攻性网络攻击能力的全球竞赛。ENISA 在报告中称：“网络活动的成熟并非一小撮国家的事情，目前，多个国家都已发展了能够渗入政府及私营目标的能力。”尽管欧盟成员国和其他国家在网络战能力方面保密，不过，英国已经成为全球首个承认发展网络攻击能力的国家，并且与荷兰已经公开呼吁增强网络战的进攻能力。英国国防大臣菲利普·哈蒙德表示，英国在网络情报和监听方面的国防预算不断增加，在全球排名第四位。但是，只加强网络防御能力还不够，英国需要发展在网络空间进行反击的能力；在必要的时候，还应当具有发起攻击的能力。英国、美国、加拿大、澳大利亚和新西兰共同组成了“五眼”情报共享联盟，联盟成员国彼此交换情报和情报评估，并且在行动上与各成员国有广泛的交流。英国将根据与其盟国达成的“五眼”计划共享网络攻击能力。荷兰安全与司法大臣奥普斯特尔腾在 2012 年 10 月请求荷兰议会通过法案，允许荷兰政府为打击犯罪而侵入国内外的计算机。根据今年早些时候公布的澳大利亚《国防白皮书》，澳大利亚一直也在发展自己的网络攻击能力，而美国、以色列、伊朗等国也已经发展了这种技术。

5、美研究者借数学模型计算网络攻击“最佳时刻”

环球网 1 月 14 日消息 据美国侨报网 1 月 13 日报道，新的数学模型可以预测何时才是发动网络攻击的最佳

时刻。据《科学》报道，研究人员现在可以使用数学模型来构拟计算机黑客的攻击策略，任何个体都可依此确定发动网络攻击的最佳时机。密歇根大学安娜堡分校的政治学家 Robert Axelrod 以研究博弈论中的囚徒困境难题而闻名于世，他的研究对经济学、进化生物学等诸多领域都产生了重要影响。Axelrod 曾提出“理性惊奇时刻”的概念，这个想法认为惊奇要素本身就是一种策略资源，通过对惊奇要素的成本和回报进行模拟，可以让人们采取反直觉的行动。黑客最佳攻击时间的选择取决于随着时间的推移所需承担的不同风险、代价和收益。Axelrod 和心理学家 Rumen Iliev 联手重整了 Axelrod 在 1979 年提出的可预测网络攻击的“理性惊奇时刻”模型，然后将修订后的模型应用在最近的几次网络攻击实例上，其中之一就是美国和以色列政府共同设计了前所未有的复杂的计算机 Stuxnet 蠕虫病毒来破坏伊朗的离心机设备。Axelrod 和 Rumen Iliev 的研究成果 1 月 13 日在线发表于美国《国家科学院院刊》，两人认为他们提出的数学模型可以用来设计未来的网络攻击，而且还可以预测未来网络攻击的各种可能出现的类型。

6、美国在全球 10 万台电脑置入软件 建网络攻击通道

中新网 1 月 15 日消息 据美国媒体 1 月 14 日报道，美国国家安全局(NSA)已经在全球近 10 万台电脑中装置软件，以便美国监督这些电脑，也为发起网络攻击创造一条电子高速公路。尽管植入的多数软件都是为了进入电脑网络，美国国安局越来越多地利用秘密技术进入没有联网的电脑，并修改其数据。根据国安局文件、电脑专家和美国官员提供的信息，国安局自 2008 年就采用的那种技术，依靠电脑中的电路板及 USB 卡发出的无线电波监视不联网电脑。在某些情况下，电波被传送到行李箱大小的中继站，而情报部门可以把中继站建立在距离目标的几英里之外。报道指出，电波频率技术帮助美国情报机构解决了多年来面临的最大问题：打入敌方或者美国伙伴的间谍及黑客似乎无法渗透的电脑。美国称为“量子”(Quantum)的项目已经成功地将软件植入俄罗斯军方网络、墨西哥警察和毒枭的电脑系统、欧盟贸易机构的电脑系统以及反恐伙伴沙特阿拉伯、印度和巴基斯坦等国电脑中。华盛顿战略和国际研究中心网络安全专家刘易斯(James Andrew Lewis)说，情报机构能够打入过去其他人都没有进入的电脑的能力、规模和先进程度都令人惊异。有些力量已经存在相当时间，但是如何渗透系统并植入软件，及使用无线电频率都为美国打开了前所未有的新窗口。

7、韩称朝黑客发含恶意代码邮件 拟盗取重要情报

环球网 1 月 14 日消息 据韩国 news1 通讯社 1 月 14 日消息，韩国未来创造科学部 14 日表示，朝鲜黑客组织近日针对韩国主要政府机构官员发送带有恶意代码电子邮件，试图盗取重要信息，有关部门应该进一步加强网络安全监管。据介绍，朝鲜黑客组织针对韩国外交、统一和国防领域有关机构主要官员发送带有恶意代码的邮件，该邮件被伪装成熟人或某机构的来信，要求收信人对邮箱信息进行确认。2014 年以来，朝鲜黑客发送了没有植入恶意代码的邮件，要求收信人参与问卷调查，邮件中包含“新年对朝政策”等题目。此外，朝鲜黑客还针对韩国网络系统管理水平较低的中小 IT 企业发动攻击，攻击次数呈现大幅增长态势。韩方分析认为，朝鲜可能通过“迂回”方式对韩国政府部门等重要机构发起攻击。

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 1999 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 2013 年，CNCERT 与 59 个国家和地区的 127 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：连丽艳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170