国家互联网应急中心

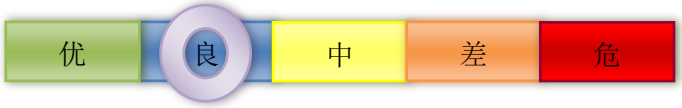
2014 年第 4 期

1 月 20 日-1 月 26 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

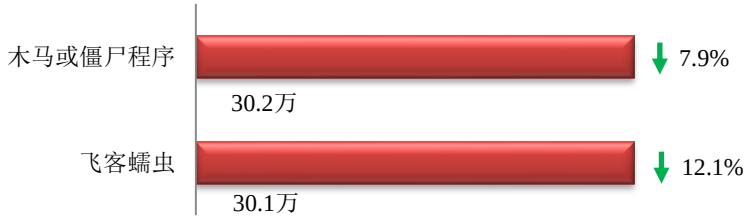


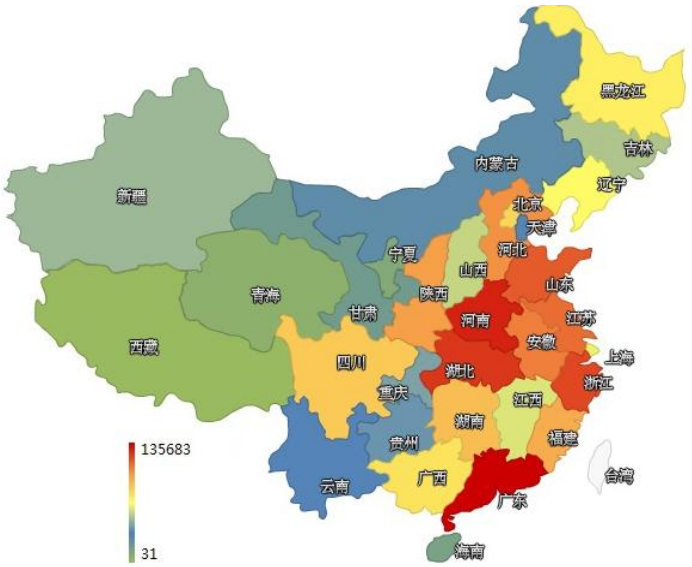
境内感染网络病毒的主机数量	• 60.3万	↓ 10.1%
境内被篡改网站总数 其中政府网站数量	• 4781 • 385	↑ 8.1% ↑ 12.6%
境内被植入后门网站总数 其中政府网站数量	• 2031 • 72	↑ 45.8% ↑ 50.0%
针对境内网站的仿冒页面数量	• 259	↓ 7.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 190 • 45	↓ 24.0% ↓ 25.0%

= 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 60.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 30.2 万以及境内感染飞客（conficker）蠕虫的主机约 30.1 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、河南省和湖北省。

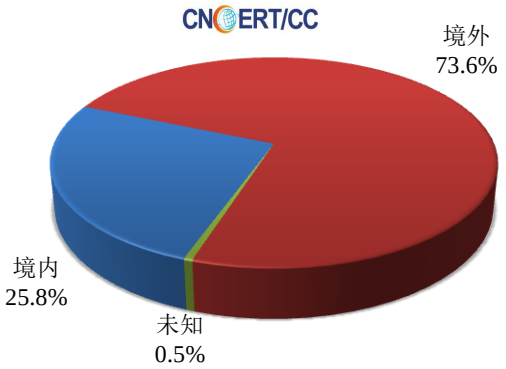
TOP3

广东省	•约14.0万个（约占中国大陆总感染量的44.9%）
河南省	•约1.4万个（约占中国大陆总感染量的4.7%）
湖北省	•约1.4万个（约占中国大陆总感染量的4.7%）

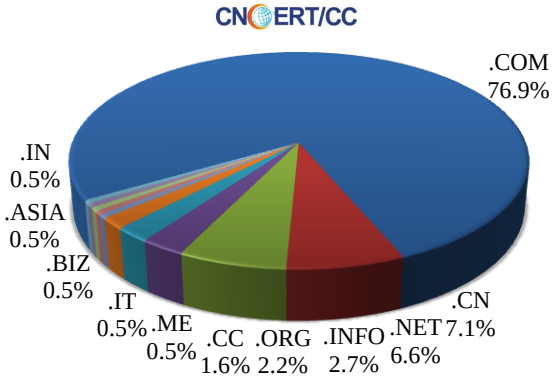
本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 53 个，按网络病毒家族统计新增 2 个。

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 182 个，涉及 IP 地址 276 个。在 182 个域名中，有约 73.6%为境外注册，且顶级域为.com 的约占 76.9%；在 276 个 IP 中，有约 27.9%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 77 个 IP。

本周放马站点域名注册所属境内外分布
(1/20-1/26)



本周放马站点域名所属顶级域的分布
(1/20-1/26)



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。

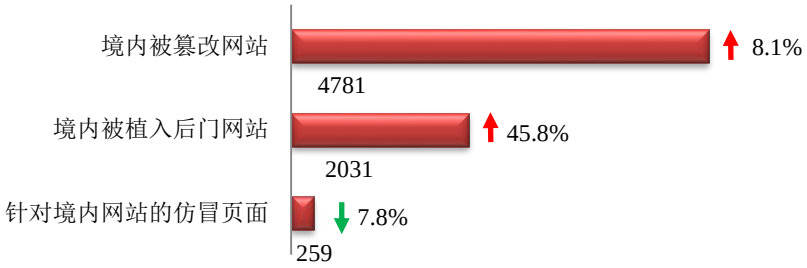
ANVA恶意地址黑名单发布地址

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。

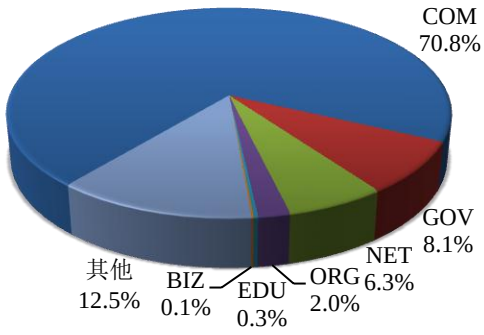
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4781 个；境内被植入后门的网站数量为 2031 个；针对境内网站的仿冒页面数量为 259 个。

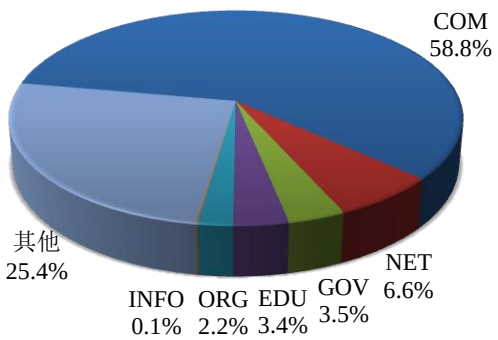


本周境内被篡改政府网站(GOV 类)数量为 385 个（约占境内 8.1%），较上周环比增长了 12.6%；境内被植入后门的政府网站(GOV 类)数量为 72 个（约占境内 3.5%），较上周环比增长了 50.0%；针对境内网站的仿冒页面涉及域名 187 个，IP 地址 118 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/20-1/26)

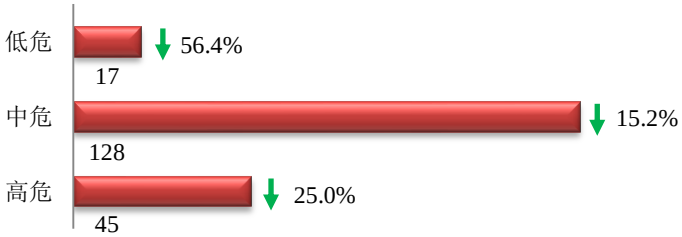


本周我国境内被植入后门网站按类型分布
(1/20-1/26)

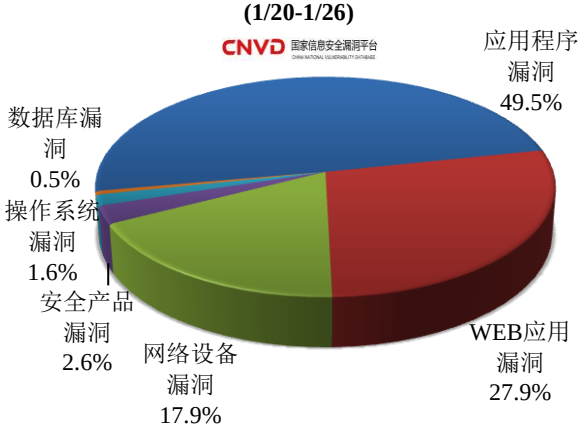


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 190 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
(1/20-1/26)



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

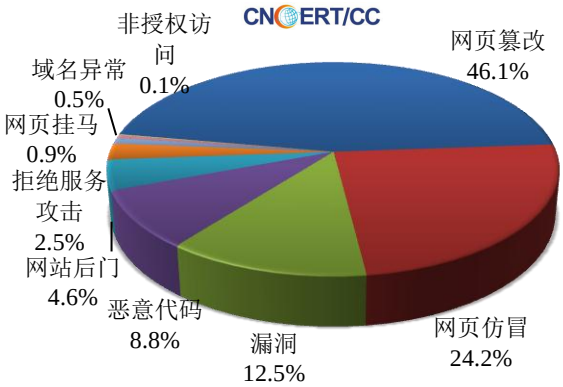
http://www.cnvd.org.cn/webinfo/list?type=4

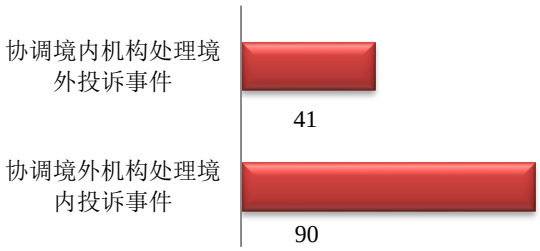
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 857 起，其中跨境网络安全事件 131 起。

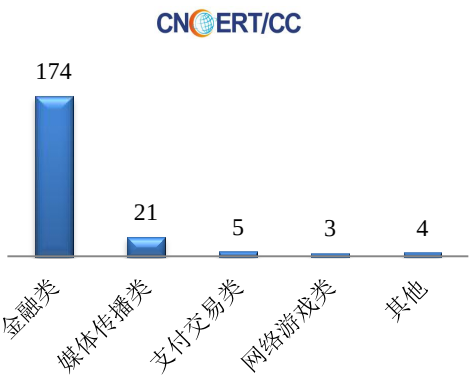
本周CNCERT处理的事件数量按类型分布
(1/20-1/26)



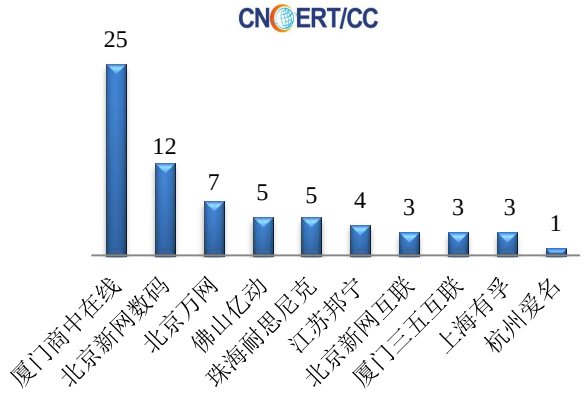


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 207 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含工商银行等金融类仿冒事件 174 起和湖南卫视等媒体传播类仿冒事件 21 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(1/20-1/26)



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 (1/20-1/26)



业界新闻速递

1、中共中央设立国家安全委员会 习近平任主席

新华网 1 月 24 日消息 中共中央政治局 1 月 24 日召开会议，研究决定中央国家安全委员会设置；听取关于一年来贯彻执行中央八项规定情况的汇报，研究部署下一步改进作风工作。会议决定，中央国家安全委员会由习近平任主席，李克强、张德江任副主席，下设常务委员和委员若干名。中央国家安全委员会作为中共中央关于国家安全工作的决策和议事协调机构，向中央政治局、中央政治局常务委员会负责，统筹协调涉及国家安全的重大事项和重要工作。

2、2013 年香港网络信息安全事故激增 专家呼吁提高警惕

新华网 1 月 21 日消息 香港生产力促进局下属的香港电脑保安事故协调中心 1 月 21 日发布消息称，2013 年共接获网络安全事件 1593 起，较 2012 年增加 52%，第四季度发现有超过 8300 部“隐形僵尸”电脑。协调中心高级顾问梁兆昌表示，涉及网络安全的事故越来越隐蔽，不少遭入侵的电脑用户对其被用作发动网上攻击毫不知情。协调中心对安全事故的上升趋势及“隐形僵尸”电脑的数据作进一步分析显示，勒索软件、僵尸网络、针对网站及移动设备的攻击将在今年激增，市民及企业应小心防范。梁兆昌建议各界加强安全措施，特别是中小企业及公众人士应加强注重保护敏感资料，除要定期备份数据，并储存在一个安全的离线地方，以降低勒索软件袭击风险外，还要在传输文档时使用较强的加密方法；市民大众也要在个人移动设备上安装一定的安全软件，并在使用互联网时采用不易破解的密码及双重认证，时刻提防来历不明的软件和网站链接。

3、法国增赛博防御预算 军方遭网络攻击两年翻两番

中新网 1 月 22 日消息 据中国国防科技信息网报道，法国国防部长让 伊夫 勒 德里安 1 月 21 日称，法国将推出 15 亿欧元的计划，战略重点是在赛博战中保护法国。该计划将在几周后推出，并写入法国未来五年的军事预算中。过去两年内法国国防部受到的网络攻击已经翻了两番：国防部有记录的重大计算机事件 2013 年为 780 件，而在 2011 年只有 195 件。攻击者试图使政府服务器瘫痪或者破坏信息和指挥系统，并通过入侵网络以影响法国部队的海外作战甚至影响其合作伙伴，所以法国必须增加赛博安全预算。法国会与其他欧盟国家合作

或者共享平台和专业知识来拓展防御措施。国防部希望招募更多的 IT 和编程专家来扩大防护、培训现有员工，利用网络技术更好地支持法国军队。法国国防部军备部的赛博分部的人员在未来几年将增加近一倍达 450 人，以致力于研究赛博问题。

4、日本政府新设“网络安全日” 宣传打击黑客对策

中新网 1 月 23 日消息 据日本共同社报道，1 月 23 日，日本政府在官邸召开官房长官菅义伟任主席的信息安全政策会议。政策会议上，内阁官房负责人报告了打击黑客攻击保护政府信息安全的相关工作情况。菅义伟就黑客攻击表示，这是“在国家安全和危机管理上越来越重要的问题。有必要进一步加强支撑信息安全措施的人才培养和体制完善工作”。为针对企业和个人开展有关打击黑客攻击措施的宣传警示工作，会议决定将 2 月的第一个工作日定为“网络安全日”，届时将在东京召集专家举行研讨会。

5、德 1600 万互联网用户信息遭黑客窃取

新华网 1 月 23 日消息 德国信息技术安全局 1 月 21 日证实，德国约 1600 万用户的电子邮箱密码等信息被黑客通过病毒软件盗取。消息披露后引发德国民众测试邮箱和修改密码的狂潮。德国信息技术安全局表示，网络犯罪分子通过一个病毒程序感染了数百万台电脑，进而盗取了用户的电子邮箱及密码等信息，受影响的用户约 1600 万。在通告公众的同时，德国信息技术安全局提供了一个安全测试网站，让公众来检查自己是否不幸“中招”。一天之内，超过 1260 万用户登录该网站进行检测，其中约 88 万用户已确认受影响。由于短时间内大量用户请求验证，目前该网站已经瘫痪。鉴于此次密码和信息被盗的电子邮件地址的数量和规模非常大，相当于德国全部人口中的近五分之一处于危险之中，尽管被盗信息主要涉及电子邮件的用户名及密码，但由于许多网络用户不仅在登录邮箱时使用有关信息，在登录社交网站、网购时同样会使用这些信息，因此，德国民众普遍感到担忧，在验证未果的情况下引发修改密码的狂潮。

6、美奢侈品商店数据库遭攻击 上百万顾客信息泄露

中新网 1 月 24 日消息 据美国媒体 1 月 23 日报道，美国以经营奢侈品为主的高端百货商店内曼·马库斯发表声明称，他们的客户信息数据库遭到黑客攻击，该公司 110 万名顾客的信用卡和借记卡信息可能已被黑客窃取。Visa、MasterCard 和 Discover 已经发现有 2400 个曾在内曼·马库斯和其旗下 Last Call 商店使用的银行卡被盗用。据初步调查显示，内曼·马库斯百货商店的操作系统被恶意安装了黑客软件，致使其顾客的付款信息在 2013 年 6 月 16 日至 10 月 30 日期间可能遭到窃取。目前美国特勤局已开始调查这起网络攻击案件。该公司也正在与第三方情报公司合作，追踪攻击来源。内曼·马库斯公司表示，已经通知所有去年曾在其公司消费的顾客，并已采取有效的保证网络安全的防范措施，以加强信息安全。针对之前全美第二大零售商塔吉特的 4000 万个付款信息及 7000 万条顾客信息遭窃事件，内曼·马库斯公司表示尚不清楚两起事件是否有联系。

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：王明华

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170