国家互联网应急中心

2016 年第 3 期

1 月 11 日-1 月 17 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

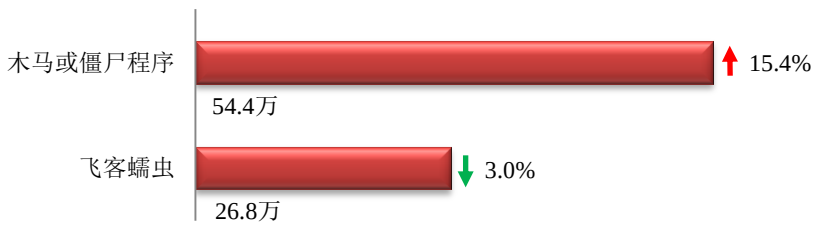
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	•81.2万	↑ 8.6%
境内被篡改网站总数 其中政府网站数量	•4536 •73	↑ 296.9% ↑ 305.6%
境内被植入后门网站总数 其中政府网站数量	•2077 •55	↓ 54.5% ↓ 31.3%
针对境内网站的仿冒页面数量	•6889	↑ 83.6%
新增信息安全漏洞数量 其中高危漏洞数量	•118 •40	↑ 8.3% ↑ 25.0%

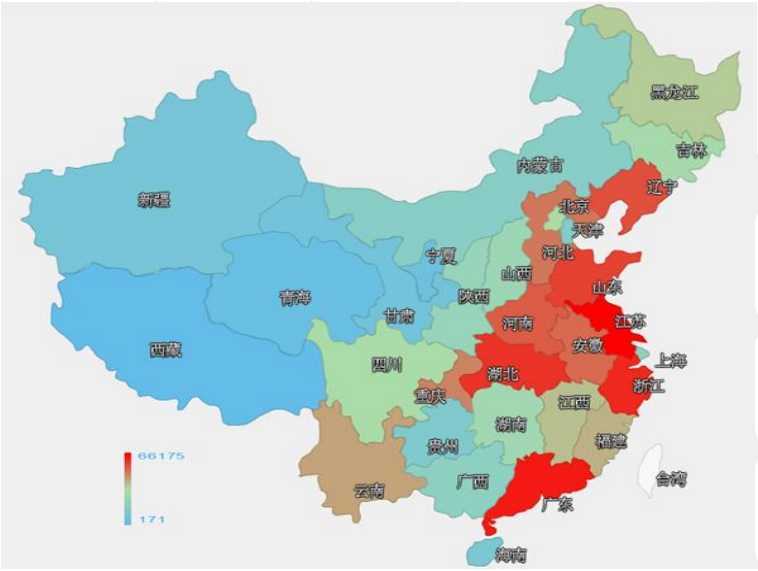
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 81.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.4 万以及境内感染飞客（conficker）蠕虫的主机约 26.8 万。



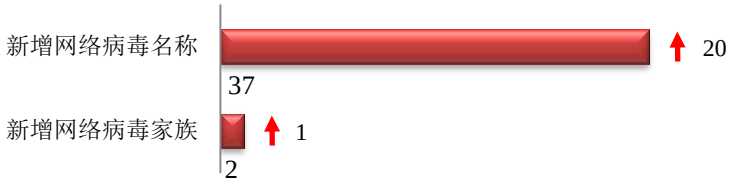
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是江苏省、广东省和浙江省。



TOP3

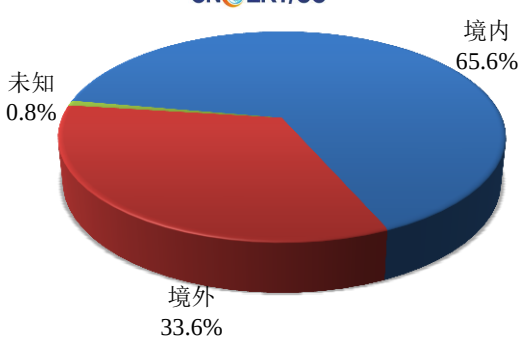
江苏省	•约6.6万个（约占中国大陆总感染量的12.2%）
广东省	•约5.4万个（约占中国大陆总感染量的9.9%）
浙江省	•约5.0万个（约占中国大陆总感染量的9.2%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 37 个，按网络病毒家族统计新增 2 个。

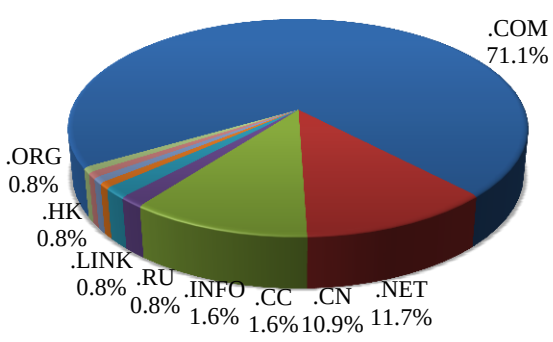


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 128 个，涉及 IP 地址 327 个。在 128 个域名中，有约 33.6%为境外注册，且顶级域为.com 的约占 71.1%；在 327 个 IP 中，有约 14.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 29 个 IP。

本周放马站点域名注册所属境内外分布
(1/11-1/17)



本周放马站点域名所属顶级域的分布
(1/11-1/17)



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。

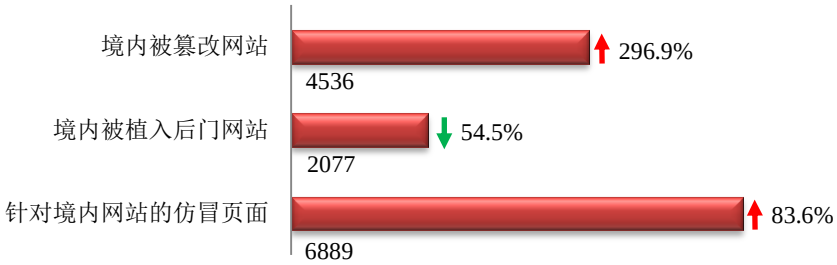
ANVA恶意地址黑名单发布地址

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。

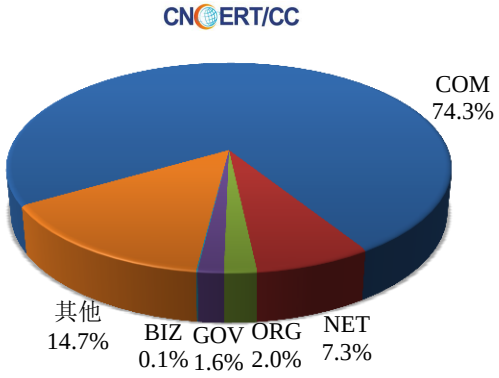
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4536 个；境内被植入后门的网站数量为 2077 个；针对境内网站的仿冒页面数量为 6889。

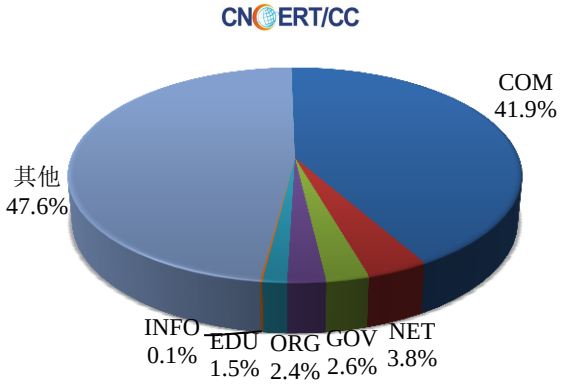


本周境内被篡改政府网站(GOV 类)数量为 73 个（约占境内 1.6%），较上周环比上升了 305.6%；境内被植入后门的政府网站(GOV 类)数量为 55 个（约占境内 2.6%），较上周环比下降了 31.3%；针对境内网站的仿冒页面涉及域名 3251 个，IP 地址 995 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/11-1/17)

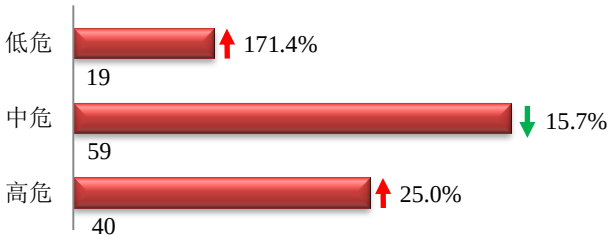


本周我国境内被植入后门网站按类型分布
(1/11-1/17)

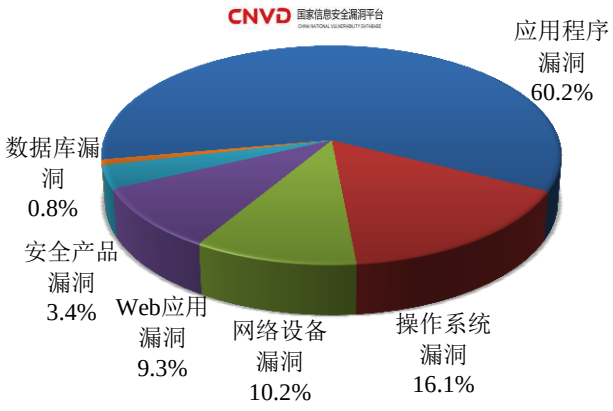


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 118 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
(1/11-1/17)



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

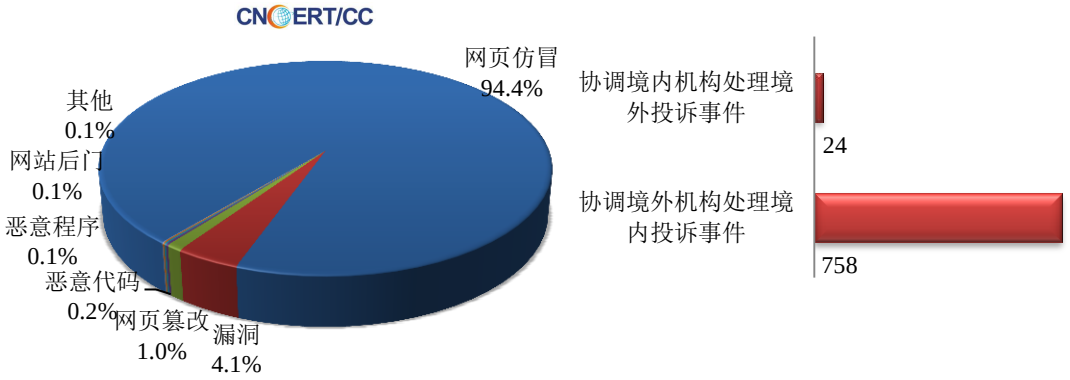
http://www.cnvd.org.cn/webinfo/list?type=4

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 2686 起，其中跨境网络安全事件 782 起。

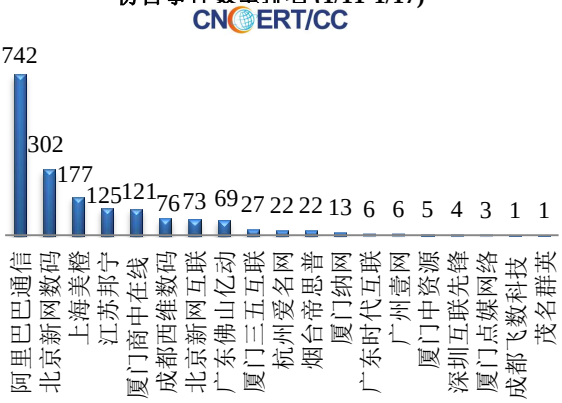
本周CNCERT处理的事件数量按类型分布
(1/11-1/17)



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 2536 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 2423 起和互联网服务提供商仿冒事件 101 起。

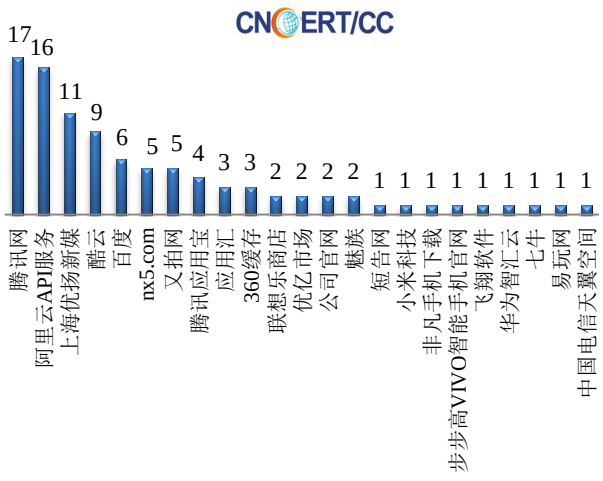
本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(1/11-1/17)

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 (1/11-1/17)



本周，CNCERT 协调 23 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 96 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 (1/11-1/17)



业界新闻速递

1、信安标委换届 我国网络安全标准化提速

新浪网 1 月 15 日消息 1 月 14 日，全国信息安全标准化技术委员会换届大会在京举行。这是 2002 年该委员会成立以来首次换届，委员人数扩充近一倍。中央网信办主任、国家互联网信息办公室主任鲁炜在会议上表示，要快出标准、多出标准，让我国网络安全标准在世界占一席之地。这或意味着我国网络安全标准化工作提速的开始。中国信息安全研究院副院长左晓栋对南都记者介绍，在云计算、大数据、物联网等新领域，目前世界各国都还没有建立起完善的网络安全标准体系，更没有统一的国际标准。鲁炜在会议上明确提出，推进我国网络安全标准化工作，要抓重点突破，快出标准、多出标准；抓国际交流合作，让我国网络安全标准在世界占一席之地。全国信息安全标准化技术委员会（简称“信安标委”）成立于 2002 年，直属于国家标准化管理委员会，主要负责国家网络安全标准申报、立项、评审等工作。信安标委委员、北京数字认证股份有限公司总经理詹榜华对南都记者解释，要落实网络安全标准，不仅技术要跟得上，还需各部门业务协作。例如，信用卡的网络安全就需要信安标委和金标委（全国金融标准化技术委员会）协调合作。这就不难解释委员人数的大幅增加，且涉及中央网信办、工业和信息化部、公安部、国家保密局、国家密码管理局、国家认监委、国家标准委及 10 个相关国家标准化组织。据信安标委秘书长、中国电子技术标准化研究院副院长高林介绍，信安标委 2016 年将重点推进网络可信身份等领域的标准化研究，推动大数据安全、云计算、服务安全、工业控制系统信息安全、智慧城市安全等领域的标准制定工作。

2、英国拟允许司法部门进行黑客活动

腾讯网 1 月 12 日消息 据国外媒体报道，包括苹果、微软、谷歌和 Facebook 在内的科技公司对英国一项最新法律草案表示强烈批评。根据这项法案，司法部门可以对计算机系统进行黑客活动，以获取数据。根据英国最新的《调查权法案》草案，在获得授权的情况下，情报机构、国家安全机构、警方，以及武装力量可以对设备展开黑客活动，从而获取用户数据。政府部门认为，这样的条款是必要的，这将有助于司法部门获得犯罪分子的通信记录。然而科技公司警告称，英国这样做将设置危险的先例，可能被其他国家效仿。这将导致用户不再信任它们的互联网服务，甚至导致业务无法开展。Facebook、谷歌、微软、Twitter 和雅虎等科技巨头已联合向英国议会负责评估这项法案的委员会上书。它们认为，这样的立法是向错误方向迈出的一步。“这可能会导致产品或服务被引入风险或漏洞。这将是非常危险的先例。我们呼吁政府三思。”这些科技公司还提出，当前的草案并未包含任何对网络整体性和信息安全的要求，也没有包含关于政府部门应当告知企业漏洞存在的要求。它们表示：“我们呼吁政府进一步澄清，政府部门采取的行动不会给用户或企业造成新的风险或漏洞。”

3、监听门后德美恢复网监合作

环球网 1 月 11 日消息 据德国媒体 1 月 8 日报道，德国联邦情报局与美国国家安全局恢复了网络监控合作。德国媒体去年爆料称，美国国家安全局自 2008 年起通过德国联邦情报局设在巴特艾布灵的监听站，探听欧洲企业商业活动机密和欧盟以及邻国高级官员的通话。德国情报人士说，监听“帮凶门”事件后，巴特艾布灵的监

听站随即停止向美国国家安全局发送网络监控信息。不过，最新报道称，德美已恢复监听站合作，德国联邦情报局再次开始为美国国家安全局提供信息。巴黎系列恐怖袭击发生后，德国升级了本国的安保措施。报道指出，巴特艾布灵的监听站在监控中东危机国家中发挥重要作用。对于恢复监控合作的报道，德国官员暂未作出回应。

4、担心黑客攻击，五角大楼加强保密措施

新华网 1 月 11 日消息 美国《防务新闻》周刊网站 1 月 9 日报道，由于担心黑客，五角大楼考虑采取更多保密措施。去年 10 月 27 日，五角大楼批准了“远程打击轰炸机”项目合同，但拒绝透露详情，其中包括不公布哪家分包商将为主要承包商诺思罗普-格鲁曼公司提供支持。与此同时，美国空军负责军需采购事务的阿诺德·邦奇中将称，“鉴于保密和加强安保的需要”，这些细节内容将不对外公布。现在，美国国防部负责采购、技术和后勤的副部长弗兰克·肯德尔正在发出警告，这样严格的保密措施可能常态化。肯德尔在接受本刊记者独家专访时说，“总而言之，国防部正在转变态度，将采取更为严格的措施保护我们的信息”，这将体现在减少信息公开——更多的项目最终可能被列为机密。原因何在？这是因为存在着一种威胁，即实力相当的对手可能窃取这些数据，并迅速转而用来对付美国。肯德尔说：“如果我们让更多有关这些攻击对象和目标的信息落入对手手中，那么他们的攻击就会更有效。因此，我们现在需要更积极地保护我们的信息，保护我们领先于对手的优势。”分析人士一致认为五角大楼的用意是好的，但质疑对更多的项目采取保密措施能否真的提高安全性。

5、朝鲜核试验后，韩国提升网络防御等级

至顶网 1 月 11 日消息 在上周朝鲜进行了核试验，韩国军方已将网络安全防御级别提高，并通过这种方式，达到“一种预防措施”的目的。路透社援引韩国联合通讯社（the South Korean Yonhap News Agency）报道称，韩国已经增加了网络防御体系里面的值班人数。早在 2013 年为应对朝鲜网络袭击，韩国政府决定斥资 98 亿韩元（约合人民币 5.4 亿元）构建智能网络防御系统，提高国防、金融和能源等主要信息通信网安全性能。“智能网络”通过设置可拦截网络攻击的路由器来阻止黑客攻击，这种智能路由器可在判断连接者的安保等级后自动允许其通过。再加上运用先进的加密技术，即使遭到黑客袭击也不会泄露信息。该项目被称为“韩国版 GIG（Global Information Grid）”项目。韩国和美国曾在 2015 年 5 月曾表示加强网络安全协调工作，共同抵制朝鲜方面的网络攻击。目前,为防范朝鲜发动网络攻击，韩军将情报作战防御系统“INFORCON”级别由平时的第 5 级上调至第 4 级。“INFORCON”是韩国军方为了保护军事网络、防止网络袭击，于 2001 年 4 月实行的情报作战防御系统。

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：张帅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158