国家互联网应急中心

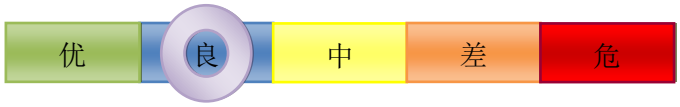
网络安全信息与动态周报

2016 年第 10 期

2 月 29 日-3 月 6 日

CNCERT/CC

本周网络安全基本态势

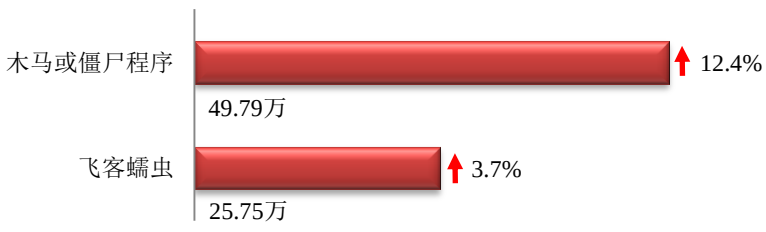


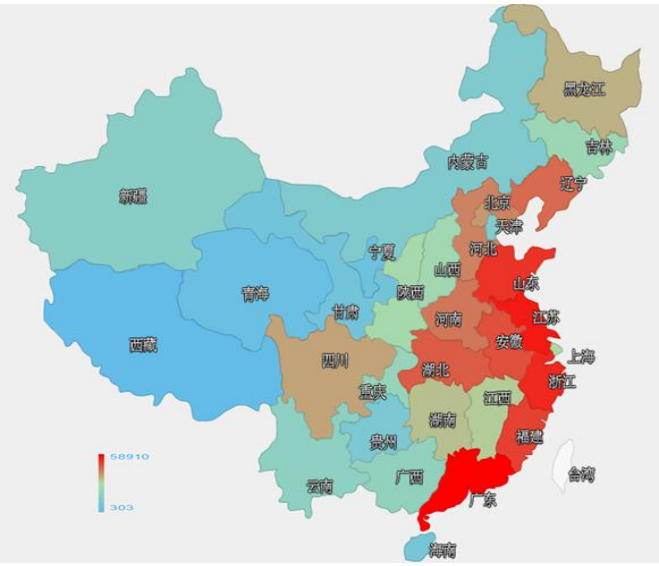
境内感染网络病毒的主机数量	• 75.54万	↑ 9.3%
境内被篡改网站总数 其中政府网站数量	• 3877 • 57	↓ 5.6% ↑ 1.8%
境内被植入后门网站总数 其中政府网站数量	• 1998 • 64	↑ 12.3% ↑ 42.2%
针对境内网站的仿冒页面数量	• 4030	↑ 16.4%
新增信息安全漏洞数量 其中高危漏洞数量	• 102 • 30	↓ 36.3% ↓ 18.9%

= 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 75.54 万个，其中包括境内被木马或被僵尸程序控制的主机约 49.79 万以及境内感染飞客（conficker）蠕虫的主机约 25.75 万。



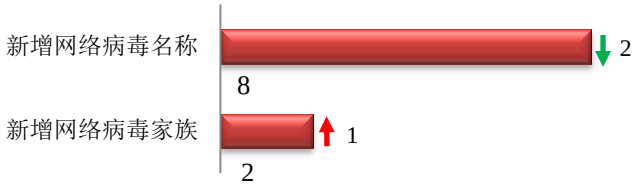


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和浙江省。

TOP3

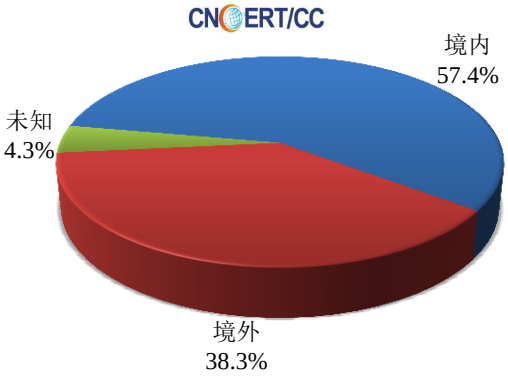
广东省	•约5.9万个（约占中国大陆总感染量的11.8%）
江苏省	•约5.2万个（约占中国大陆总感染量的10.5%）
浙江省	•约3.6万个（约占中国大陆总感染量的7.3%）

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 8 个，按网络病毒家族统计新增 2 个。

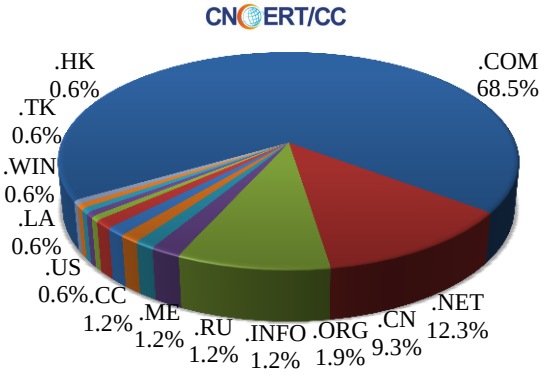


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 162 个，涉及 IP 地址 481 个。在 162 个域名中，有约 38.3%为境外注册，且顶级域为.com 的约占 68.5%；在 481 个 IP 中，有约 9.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 69 个 IP。

本周放马站点域名注册所属境内外分布
(2/29-3/6)



本周放马站点域名所属顶级域的分布
(2/29-3/6)



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。

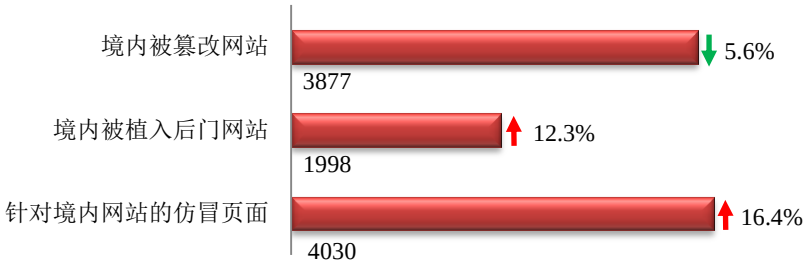
ANVA恶意地址黑名单发布地址

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。

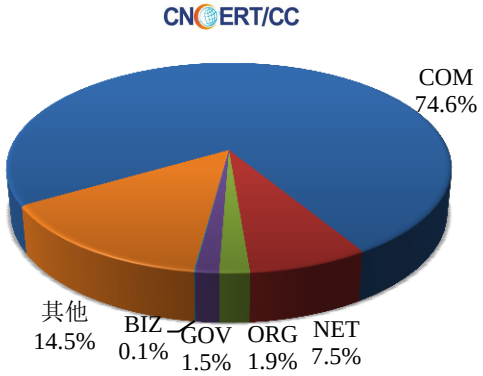
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3877 个；境内被植入后门的网站数量为 1998 个；针对境内网站的仿冒页面数量为 4030。

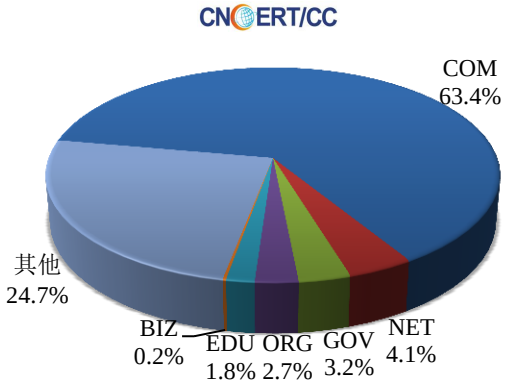


本周境内被篡改政府网站(GOV 类)数量为 57 个（约占境内 1.5%），较上周环比上升了 1.8%；境内被植入后门的政府网站(GOV 类)数量为 64 个（约占境内 3.2%），较上周环比上升了 42.2%；针对境内网站的仿冒页面涉及域名 3328 个，IP 地址 1087 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/29-3/6)

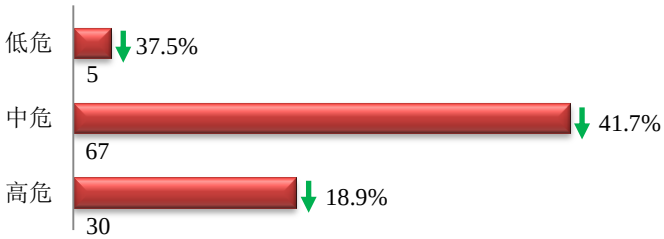


本周我国境内被植入后门网站按类型分布
(2/29-3/6)

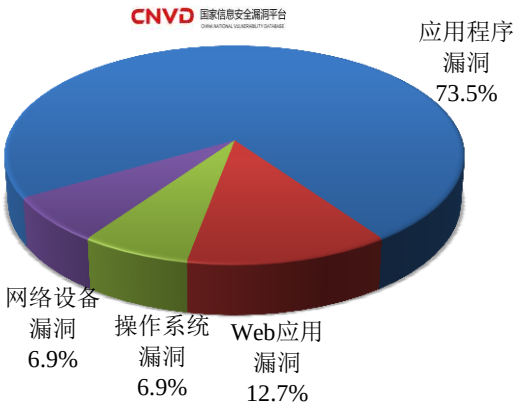


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 102 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
(2/29-3/6)



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 应用漏洞和操作系统漏洞。

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

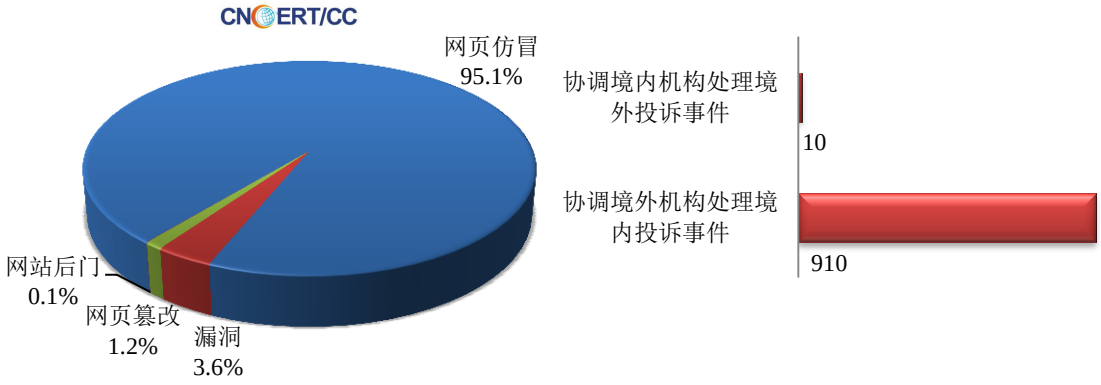
http://www.cnvd.org.cn/webinfo/list?type=4

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 3113 起，其中跨境网络安全事件 920 起。

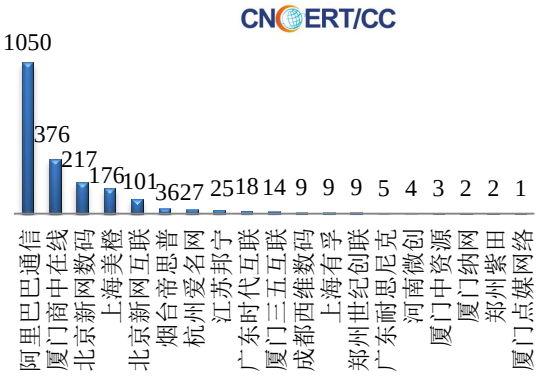
本周CNCERT处理的事件数量按类型分布
(2/29-3/6)



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 2962 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 2760 起和互联网服务提供商仿冒事件 197 起。

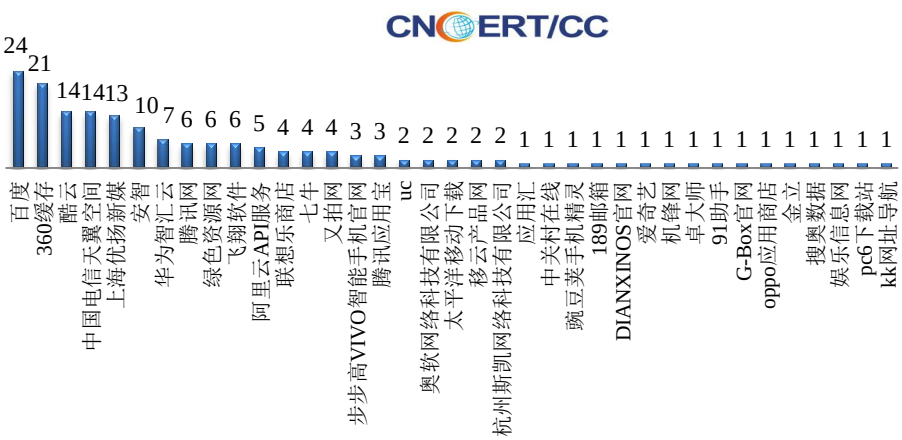
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/29-3/6)

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 (2/29-3/6)



本周，CNCERT 协调 37 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 170 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
(2/29-3/6)



业界新闻速递

1、美国明年将加大对网络安全的投入

网易 2 月 29 日消息 美国国防部部长阿什顿·卡特称，美国国防部提交的 2017 年预算中加大了对网络安全的投入，达 70 亿美元，比 2016 年预算中的 55 亿美元有所增加。该预算是卡特上任以来国防部准备的首份预算。卡特称，这部分经费将用于建造更多的网络训练基地，测试网络工具，培训国防部的网络力量和发展新的攻击性网络武器。卡特在本月初的发言中称，这将帮助国防部进一步提升网络防御能力，为美国的网络战士建立更多的训练基地，发展网络工具和基础设施，提高网络攻击能力。

2、美政府拟重谈军控协议 简化网络安全设备进口

环球网 3 月 3 日消息 据美联社 3 月 1 日报道，美国一名立法人员近日表示，奥巴马政府计划重新拟定部分军备控制协议，以便进口与窃听和监控软件有关的工具，因为这些技术常被用来确保计算机网络安全。据悉，美国政府将在 12 月份讨论此事，其中会涵盖 2013 年由 41 个国家通过的一项规定。报道称，这将给有助于有关部门精确追踪黑客活动，同时不会给国家网络安全和研究造成负面影响。此前，行业组织和立法人员一直对此抱有怨言。当地时间 2 月 29 日，美国国会网络安全会议联合主席吉姆•朗之万发布声明，披露了美国政府的决定，即确保各国讨论如何清除用于创造或支持窃听及监控软件研究工具和技术的语言。朗之万说：“国际网络安全政策是一个新领域，为了保护网络安全，大家团结一致是至关重要的。”白宫曾表示，支持用于合法网络安全活动的网络入侵工具在海外流通。29 日，白宫向美国国务院和商业部提及了这些问题，但后者拒绝对此做出评论。去年 5 月，美国商业部下属的工业及安全局提议禁止转移攻击工具，认为这种攻击软件可通过使用“零日攻击”、修改新漏洞和特殊的恶意软件允许“管理员”访问系统。

3、美军将加大对 IS 网络攻击 破坏其指挥和通讯系统

中新网 3 月 1 日消息 美防长卡特 2 月 29 日在美国防部表示，美国网络司令部将加大对“伊斯兰国”的网络攻击，进一步破坏其指挥和通讯系统。美国打击“伊斯兰国”行动近期取得进展。在美军空袭的协助下，伊拉克安全部队重新夺回军事重镇拉马迪的控制权，并逐渐向摩苏尔、拉卡等地逼近。美防长卡特与美军参谋长联席会议主席邓福德 29 日在记者会上表示，为配合空、地作战行动，美国网络司令部将运用技术手段对“伊斯兰国”发动网络攻击，进一步破坏其指挥和通讯系统。卡特说，发动网络攻击是美军在战场上的最新尝试。美军在这一领域有着强大的实力，这也是网络司令部的作用所在。从目前情况看，针对“伊斯兰国”的网络攻击已收到成效，美军今后还将加大攻击力度。邓福德表示，美军针对摩苏尔地区“伊斯兰国”目标的网络攻击已经开始。美军试图切断其通讯线路。这会使“伊斯兰国”在该地区更加孤立。他说，由于网络攻击的特点在于“出其不意”，因此美军不会向外界透露具体的作战计划。来自美国防部网站的消息称，卡特与邓福德本月 27 日访问了位于马里兰州米德堡军事基地的网络司令部总部。卡特当天鼓励网络司令部加大对“伊斯兰国”的网络攻击，切断该组织利用网络传播意识形态、招募武装人员以及煽动恐怖袭击的渠道。

4、五角大楼打算 5 年斥资 347 亿美元加强网络安全

腾讯网 3 月 1 日消息 据彭博社报道，美国五角大楼计划在未来 5 年内斥资 347 亿美元，用以加强网络安全。这是美国寻求增强进攻性军事能力努力的一部分，比如支持打击恐怖组织 IS 的公开行动等。卡特没有提及正被用于对付 IS 组织的秘密技术细节，但国防部发布的未来 5 年预算计划显示，其在进攻性网络能力、战略威慑以及防御性网络安全方面的投资日益增加。这份预算计划将向五角大楼所属美国网络司令部、网络任务部队提供资金支持，在必要时候协助地区指挥官进行防御和进攻行动。此举反映出美军公开支持进攻性网络行动的意愿正在增强，许多业内人士表示，这种思维可能鼓励网络攻击性虚拟武器竞赛。五角大楼计划在 2017 财年到 2020 财年，将这部分支出从上个 5 年计划中的 220 亿美元增至 280 亿美元。在 347 亿美元 5 年预算计划中，最大的支出将是 143 亿美元的网络空间活动资金，包括 2017 财年的 28.7 亿美元。这部分开支包括支持网络进攻性行动、破坏敌方行动以及防御性军事行动等。第二大类开支是 105 亿美元的信息安全支出，包括确保电网等国家关键基础设施安全，为五角大楼下属网络犯罪中心提供资金支持等。针对恐怖组织 IS 的网络行动是对美国及其盟友陆地行动和空中行动的补充，它与使用战机或地面传感器进行干扰或窃听等美军标准战略截然不同。

5、美国防部邀黑客攻击五角大楼 称助加强数码防御

环球网 3 月 4 日消息 美国国防部 3 月 2 日发起一项“攻击五角大楼网络”活动，邀请经过审查的外部黑客对国防部一些公开网址进行测试并给予物质奖励。据英国广播公司 2 日报道，美国国防部长卡特在当天发布的一份声明中说，“攻击五角大楼网络”是一项创新举措，有助于加强国防部的数码防御能力，并最终加强美国的国家安全。美国国防部长期以来依赖于内部的“红队”进行网络测试，但目前采取的措施将至少开放自己的部分计算机网络，接受来自工业界和科技界的挑战。实施这样的计划对美国联邦政府来说尚属首次。不过，美国国防部的一位高级官员对媒体表示，更敏感的网络部分，如关键武器计划部分，将不包括在这项计划之内，至少暂时不在计划之内。这位官员说，预计将会有数千名合格的人员参加这项将在 4 月开始的试验计划。美国“连线”网站 2 日说，五角大楼的这项计划将效仿一些像脸谱和谷歌这样的商业公司，向发现网站安全弱点的外部专家提供报酬。报道说，拿出几千美元奖励“好心的黑客”，对在网络技术上投入资金最大的五角大楼来说，不是什么费脑筋的事。美国一家网络安全公司的负责人莫叟利斯认为，这是非常有里程碑意义的事件，会产生“涟漪效应”。该公司另一名高管米克斯表示，这说明“不管你多有钱，即使你是世界上最强大的机构，你总有找不到的病毒，必须和黑客们合作”。

6、波兰数字化部准备推出网络安全战略

中国网信网 3 月 1 日消息 据 telecompaper 2 月 24 日报道，波兰数字化部计划于今年 5 月提交一项全面的网络安全战略，并在 3 月 8 日前听取公众意见。计划中新的网络安全架构将包括一个单一联络点（Single Contact Point），旨在收集全国范围内的网络安全事件信息，并与其他国家的同类机构进行跨境信息交流。关键基础设施运营商、国家网络安全中心和安全操作中心的联络点将为具有重要政治、行政、经济作用的机构、组织和企业，以及国家和部门领域的计算机安全应急响应组（CERT）或计算机安全事件响应组（CSIRT）提供安全保障。该联络点也将为行政管理复杂的政府机构提供分析支持。国家安全威胁报告还将包括对网络攻击风险的评估。波兰的网络安全战略提出将构建组织体系，打造早期预警系统，形成应对威胁和攻击的有序步骤，从而高效处

理威胁或网络攻击。该计战略将于 5 月 4 日敲定，并准备于 5 月 19 日在波兰华沙召开的 CyberGov 会议上提交。波兰数字化部、各省、国家研究中心以及欧盟负责出资实施，并维护国家网络安全体系。

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 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 2015 年，CNCERT 与 66 个国家和地区的 165 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：张艳茹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158