国家互联网应急中心

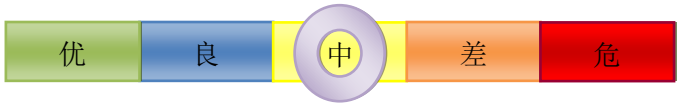
网络安全信息与动态周报

2016 年第 19 期

5 月 2 日-5 月 8 日

CNCERT/CC

本周网络安全基本态势

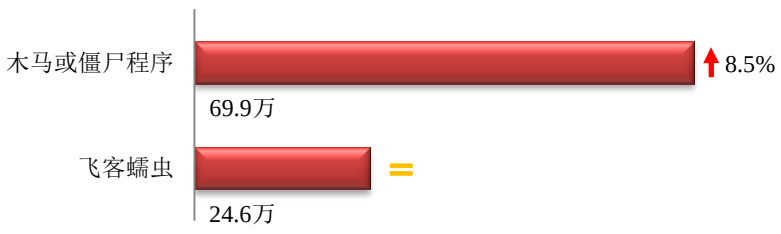


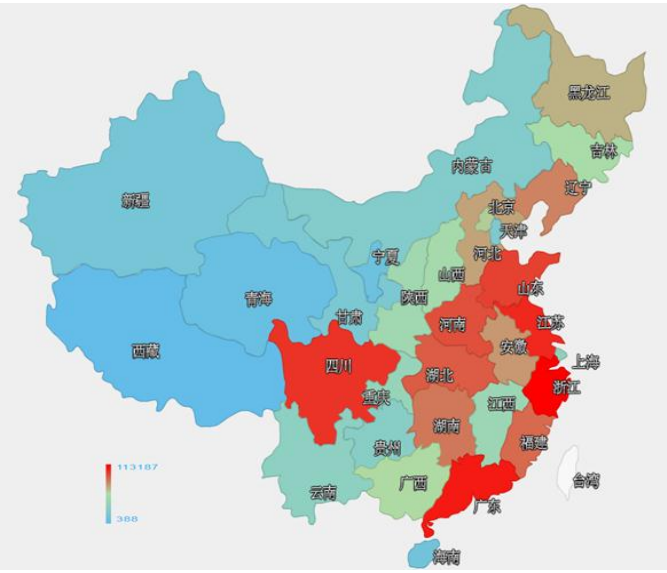
境内感染网络病毒的主机数量	•94.5万	6.1%
境内被篡改网站总数 其中政府网站数量	•3372 •90	18.0% 14.3%
境内被植入后门网站总数 其中政府网站数量	•11128 •325	197.4% 95.8%
针对境内网站的仿冒页面数量	•1976	16.3%
新增信息安全漏洞数量 其中高危漏洞数量	•132 •28	30.9% 39.1%

=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 94.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 69.9 万以及境内感染飞客（conficker）蠕虫的主机约 24.6 万。



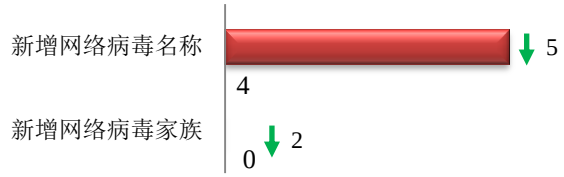


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是浙江省、广东省和江苏省。

TOP3

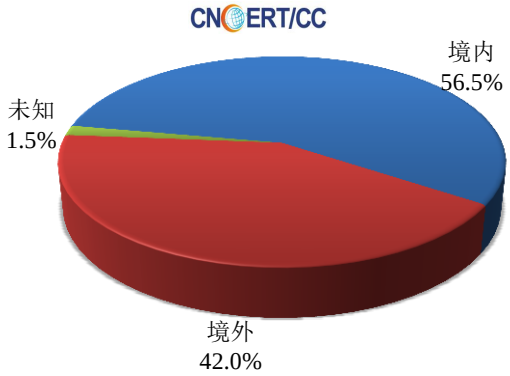
浙江省	•约11.3万个（约占中国大陆总感染量的16.2%）
广东省	•约9.7万个（约占中国大陆总感染量的13.9%）
江苏省	•约7.1万个（约占中国大陆总感染量的10.1%）

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 4 个，按网络病毒家族统计无新增。

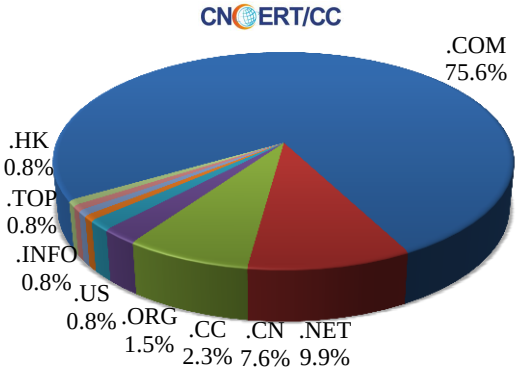


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 131 个，涉及 IP 地址 377 个。在 131 个域名中，有 42.0%为境外注册，且顶级域为.com 的约占 75.6%；在 377 个 IP 中，有约 6.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 38 个 IP。

本周放马站点域名注册所属境内外分布
(5/2-5/8)



本周放马站点域名所属顶级域的分布
(5/2-5/8)



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。

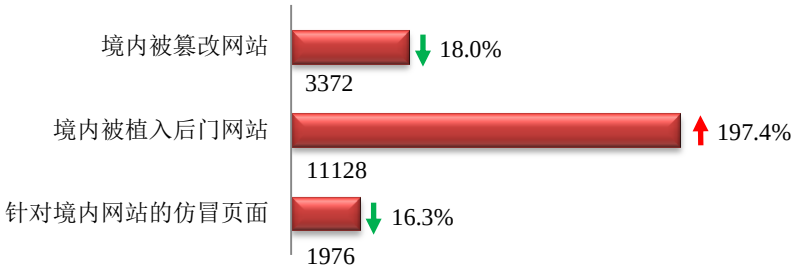
ANVA恶意地址黑名单发布地址

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。

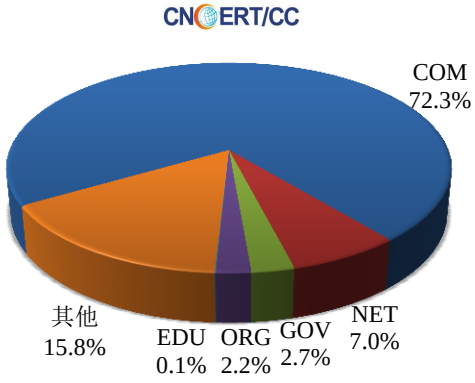
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3372 个；境内被植入后门的网站数量为 11128 个；针对境内网站的仿冒页面数量为 1976。

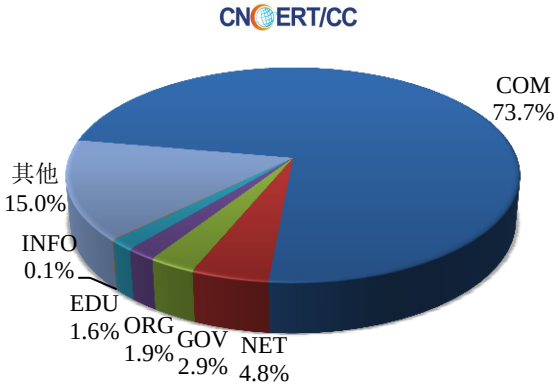


本周境内被篡改政府网站（GOV 类）数量为 90 个（约占境内 2.7%），较上周环比下降了 14.3%；境内被植入后门的政府网站（GOV 类）数量为 325 个（约占境内 2.9%），较上周环比上升了 95.8%；针对境内网站的仿冒页面涉及域名 1781 个，IP 地址 511 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/2-5/8)

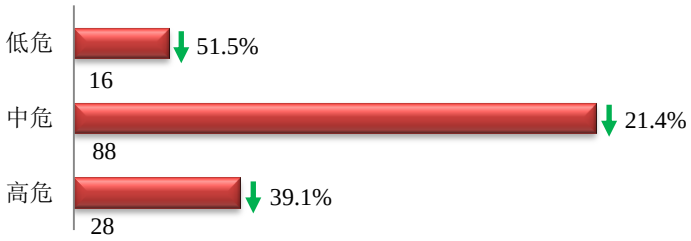


本周我国境内被植入后门网站按类型分布
(5/2-5/8)

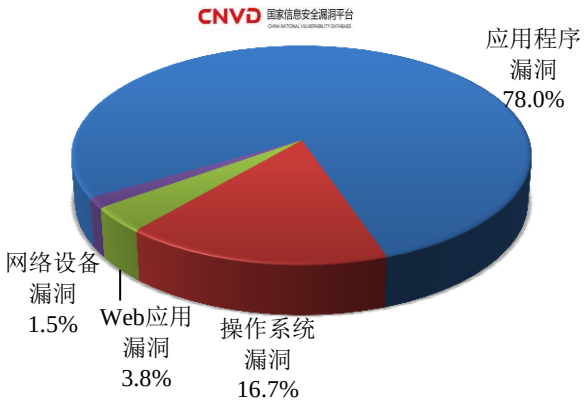


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 132 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
(5/2-5/8)



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 Web 应用漏洞。

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

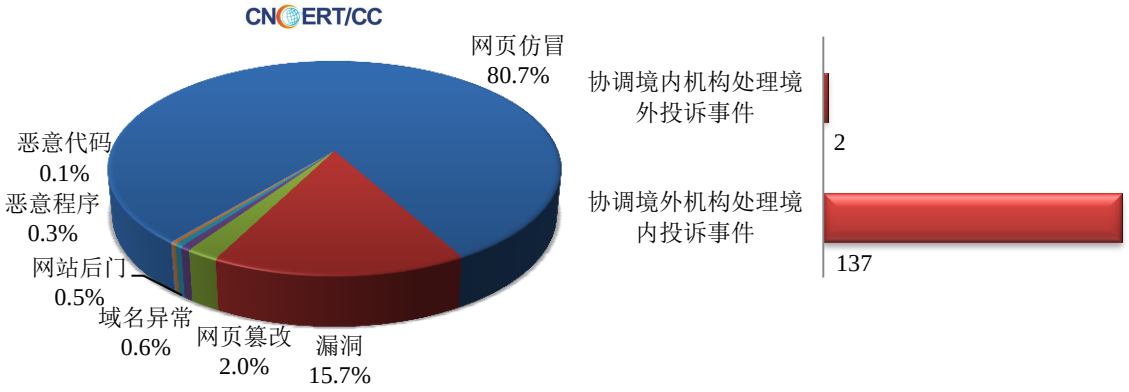
http://www.cnvd.org.cn/webinfo/list?type=4

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 789 起，其中跨境网络安全事件 139 起。

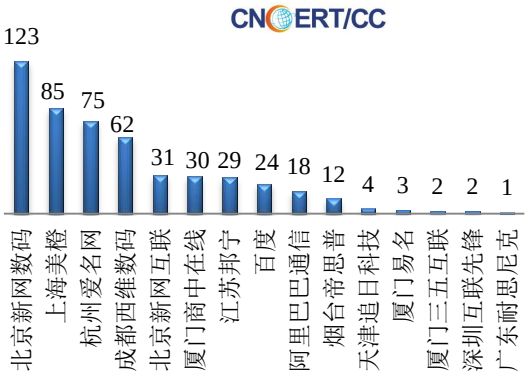
本周CNCERT处理的事件数量按类型分布
(5/2-5/8)



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 637 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 492 起和互联网服务提供商仿冒事件 136 起。

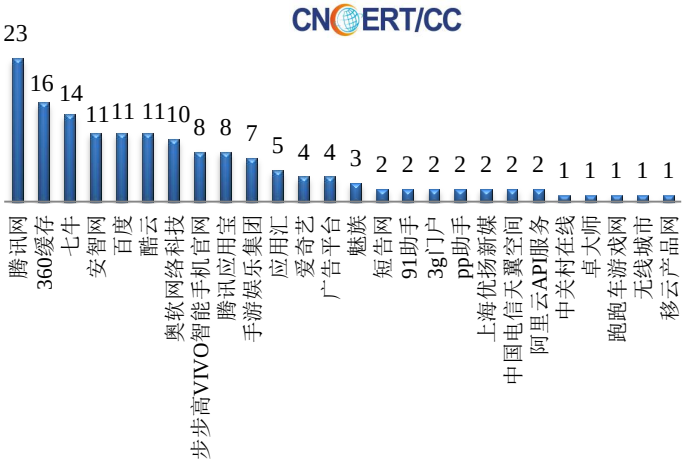
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/2-5/8)

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 (5/2-5/8)



本周，CNCERT 协调 26 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 154 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 (5/2-5/8)



业界新闻速递

1、公安机关将专项整治涉网络诈骗等网络服务平台

新华网 5 月 3 日消息 从即日起至今年 9 月，公安部网络安全保卫局组织全国公安机关网安部门，集中开展涉网络诈骗等多发性犯罪网络服务平台专项整治，以有效遏制此类网络违法犯罪活动，铲除其滋生土壤。据介绍，近年来，网络诈骗、网络盗窃等违法犯罪频发，不法分子通过一些违法违规网络服务平台，传播获取钓鱼木马、个人真实身份和账号信息，利用网络改号电话、短信群发器等大肆实施网络诈骗等违法犯罪活动，严重危害人民群众合法权益。对此，在专项整治期间，公安机关将坚持打击与整治同步，紧盯网上“治安乱点”，对 5 类网络服务平台开展集中整治和专项打击，包括：提供销售网络钓鱼、盗号改号等木马病毒，传播交流黑客攻击破坏、信息窃取和篡改等网络违法犯罪工具方法；贩卖、提供公民个人信息、身份证、银行卡和电话“黑卡”；非法销售“伪基站”和短信群发设备、软件；提供恶意注册、虚假认证、虚假交易服务；抢注和倒卖域名进行诈骗等。同时，公安机关将全面清理具有违法有害内容的信息标题、内容，账号名称和简介，群组名称和简介等信息；全面落实网站、平台开办人、管理人员登记备案和安全技术保护措施；依法查处违法信息高发和安全管理混乱的网络服务平台，对拒不履行法定管理义务、拒不整改构成犯罪的，坚决追究单位和相关人员的法律责任；对网络诈骗、网络盗窃等多发性网络犯罪案件线索，及时组织开展侦查打击，通过此次专项整治有效净化网上环境、规范网上秩序，铲除网上多发性犯罪滋生土壤。

2、韩美两国拟共同研究人工智能打击网络恐怖主义

中新网 5 月 2 日消息 据韩媒报道，韩国未来创造科学部第二次官（副部长）崔在裕和美国国土安全部副部长雷金纳德·布拉泽斯 5 月 2 日商定，韩美将共同研究基于人工智能（AI）的网络安全技术，携手打击网络恐怖主义。双方当天在韩国果川政府办公大楼发表了关于联合研发人工智能技术探测黑客攻击风险威胁杜绝网络恐怖活动的《意向声明》。根据声明，韩美将平摊研发基于人工智能的网络安全技术所需经费，并协商确定具体研发课题。两国还将讨论共享网络安全信息，扩大互联网安全领域的民间合作。崔在裕表示，韩方将与人工智能技术水平领先全球的美国进行合作，全面提升网络安全管理与处置能力，大力支持该领域的韩国企业进军国际市场。

3、美对“伊斯兰国”展开网络战

新华网 5 月 8 日消息 近日，驻伊拉克美军将领表示，美国正在对“伊斯兰国”组织发动网络攻击，限制该组织的网络联络及招募新成员的能力。美国防部长卡特表示，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。这项行动表明，在多次发布《网络空间行动战略》、整合网络战力量、组建网络司令部后，美军网络战的作战范围正在不断拓展，行动力度进一步加强。奥巴马在美国中央情报局讨论对付“伊斯兰国”组织战略的专题会议中表示：“我们的网络行动正在干扰它的指挥控制以及通讯。”这一表态指出了此次美军网络战行动的两大重点。首先，削弱“伊斯兰国”的军事指挥控制能力。据报道，美军发动的此次网络攻击主要打击重点是“伊斯兰国”指挥系统和通信网络，具体打击目标包括位于“伊

斯兰国”控制区域的两大主要作战基地——伊拉克第二大城市摩苏尔与“伊斯兰国”首都拉卡，这两处地区承载着大量的网络传输任务，是“伊斯兰国”网络力量的重要核心。通过干扰压制其指挥控制、通信通联，削弱“伊斯兰国”指挥人员对武装力量的控制。第二，阻断“伊斯兰国”宣传信息的传播。该组织经常通过社交媒体与潜在的支持者沟通，包括脸书、推特等社交网络及软件在内，利用加密手段在应用软件上建立“帮助桌面”，为全球各地的恐怖分子提供技术指导。此次网络战行动中，美通过封锁控制“伊斯兰国”网站和账户，有效打击了其利用网络进行宣传渗透、征兵等行为以及资金流动和转移等活动。

4、英国推出首套面向网络安全领域的扩展认证项目

搜狐网 5 月 3 日消息 Cyber Security Challenge UK 公司已经推出了英国国内首套面向网络安全领域的扩展项目认证（简称 EPQ）方案。这项已经正式亮相的认证旨在帮助解决英国本土的网络安全技能人才缺失现状，其计划帮助高校学生对网络领域实现全面而深入的理解——从风险管理到数字化取证皆包含在内。这项认证由 Cyber Security Challenge UK 负责设计，同时亦受到包括（ISC）2 在内的众多独立网络教育机构的支持。该认证将由 Heart of Worcestershire 学院负责管理并受到伦敦城市行业协会的审定。基于国家职业标准（简称 NOS）网络安全共识要求的 EPQ 认证属于一项三级资质（相当于 AS 级别），其价值高达 70 UCAS 点。EPQ 认证亦被纳入英国各地的现有教育框架，可作为 14-19 文凭的组成部分或者独立资质。该项目的教育合作伙伴能够为任何个人提供课程——无论其身为在校学生还是已经工作。EPQ 不仅能够被直接纳入高校学业当中，亦可作为独立技能提供给通过 Cyber Security Challenge UK 公司注册的申请人。在校学生可以通过在线课程进行学习，并根据自身表现拿到由伦敦城市行业协会颁发的资质。

5、黑客入侵希腊央行网站 警告其他央行

环球网 5 月 5 日消息 据英国路透社 5 月 4 日报道，一名希腊央行官员 4 日表示，希腊央行 3 日成为激进黑客团体“匿名者”（Anonymous）的下手目标，网站服务中断。这名不愿具名的官员表示，“攻击时间延续了数分钟，并成功入侵了央行安全系统。唯一受到此次阻断服务攻击（DoS）影响的是我们的网站。”匿名者是在 2003 年成立，以盖伊福克斯（Guy Fawkes）的面具作为其网络黑客标志。该团体在 YouTube 的一段视频中表示，“奥林匹斯将会陷落。几天之前我们宣布重新启动伊卡洛斯(Icarus)行动。今日我们已经不间断地攻破希腊央行网站。”“这标志着为期 30 天攻击全球央行网站的开始。”

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：李佳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158