国家互联网应急中心

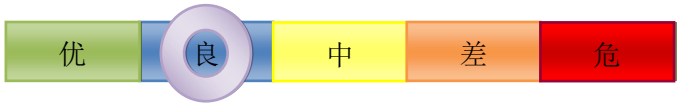
网络安全信息与动态周报

2016 年第 13 期

3 月 21 日-3 月 27 日

CNCERT/CC

本周网络安全基本态势

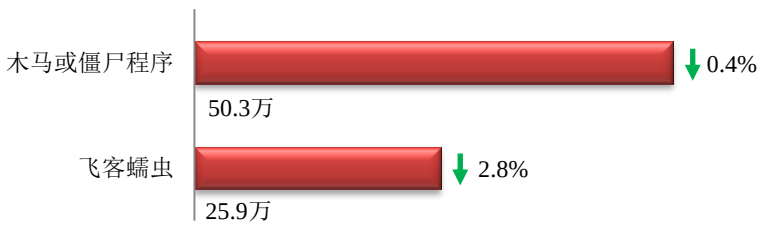


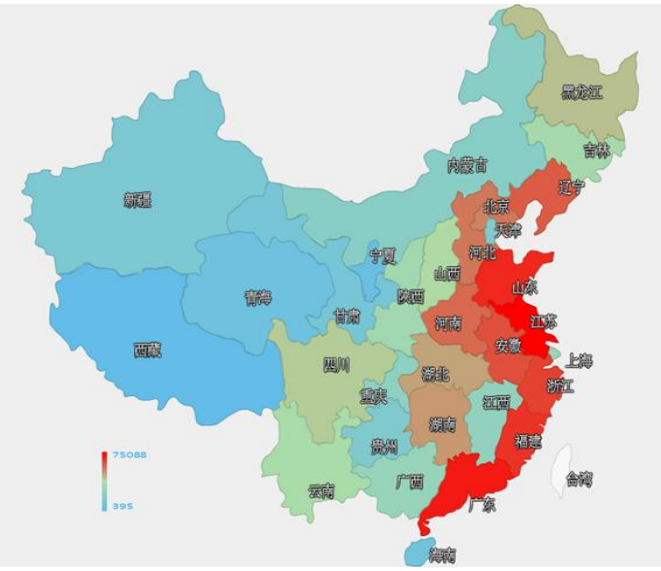
境内感染网络病毒的主机数量	•76.2万	1.2%
境内被篡改网站总数 其中政府网站数量	•4160 •69	10.6% 11.3%
境内被植入后门网站总数 其中政府网站数量	•1949 •88	3.4% 11.1%
针对境内网站的仿冒页面数量	•4211	1.3%
新增信息安全漏洞数量 其中高危漏洞数量	•115 •30	19.6% 57.7%

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 76.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.3 万以及境内感染飞客（conficker）蠕虫的主机约 25.9 万。





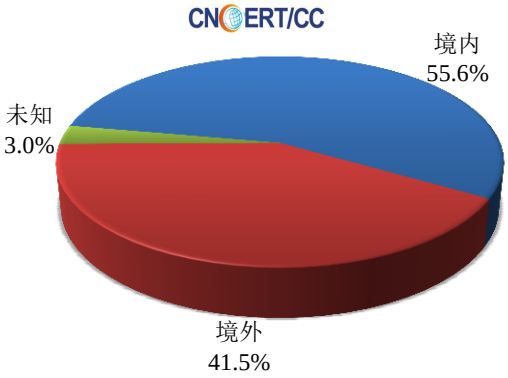
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是江苏省、广东省和山东省。

TOP3

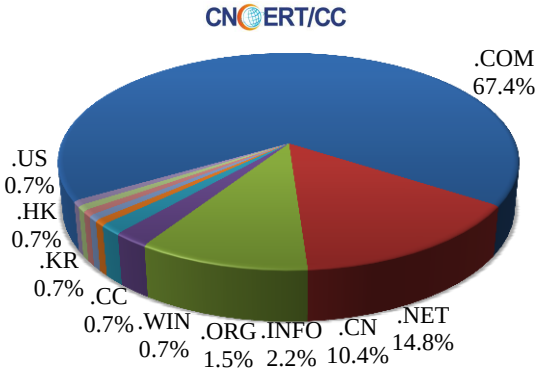
江苏省	•约7.5万个（约占中国大陆总感染量的14.9%）
广东省	•约4.8万个（约占中国大陆总感染量的9.5%）
山东省	•约3.8万个（约占中国大陆总感染量的7.5%）

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 135 个，涉及 IP 地址 370 个。在 135 个域名中，有约 41.5%为境外注册，且顶级域为.com 的约占 67.4%；在 370 个 IP 中，有约 9.2%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 24 个 IP。

本周放马站点域名注册所属境内外分布
(3/21-3/27)



本周放马站点域名所属顶级域的分布
(3/21-3/27)



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。

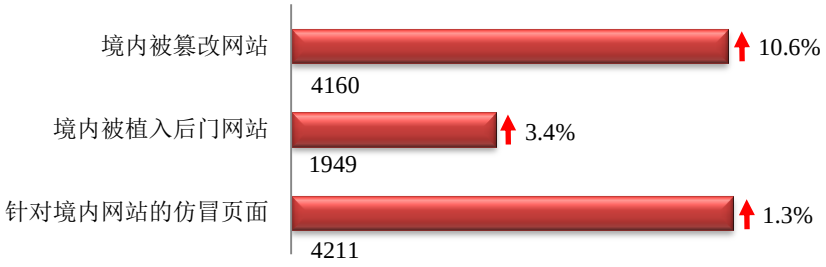
ANVA恶意地址黑名单发布地址

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。

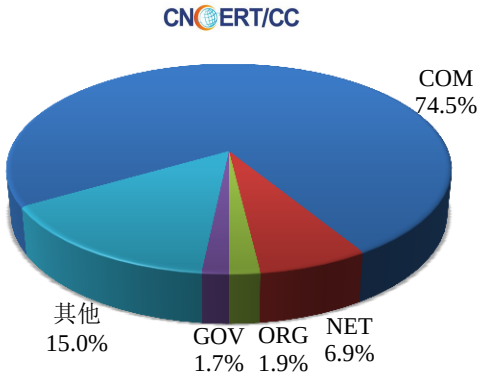
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4160 个；境内被植入后门的网站数量为 1949 个；针对境内网站的仿冒页面数量为 4211。

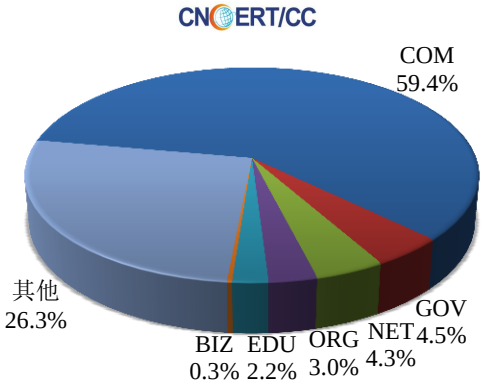


本周境内被篡改政府网站(GOV 类)数量为 69 个（约占境内 1.7%），较上周环比上升了 11.3%；境内被植入后门的政府网站(GOV 类)数量为 88 个（约占境内 4.5%），较上周环比下降了 11.1%；针对境内网站的仿冒页面涉及域名 3476 个，IP 地址 1092 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/21-3/27)

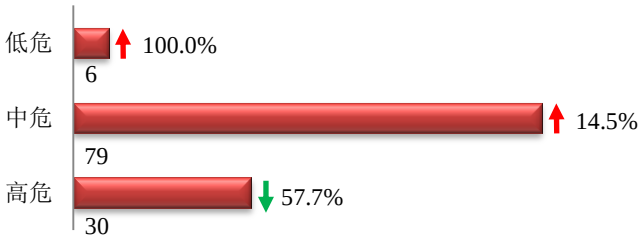


本周我国境内被植入后门网站按类型分布
(3/21-3/27)

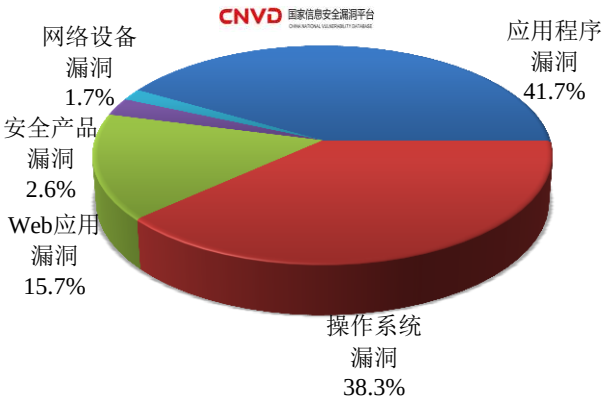


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 115 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
(3/21-3/27)



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。

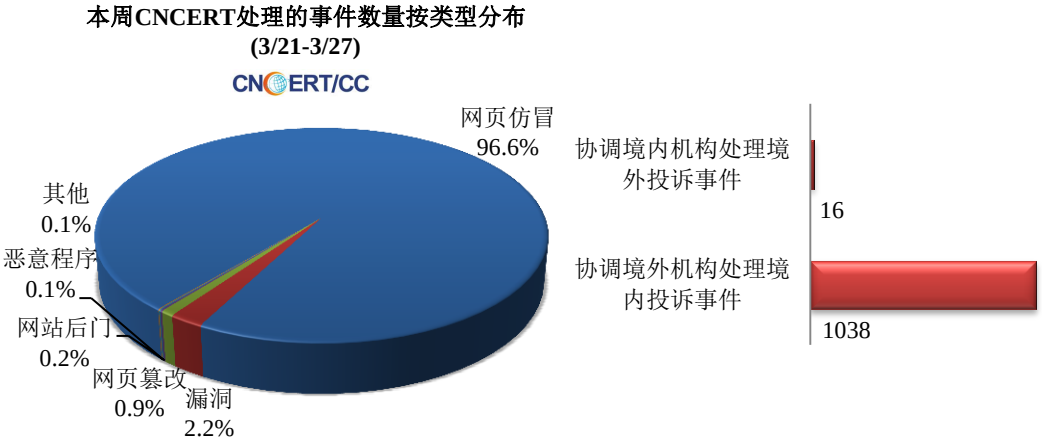
CNVD漏洞周报发布地址

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

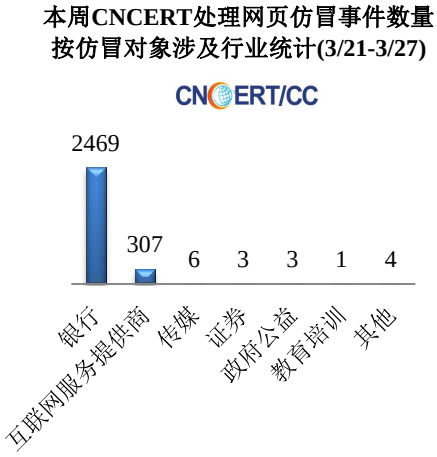
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

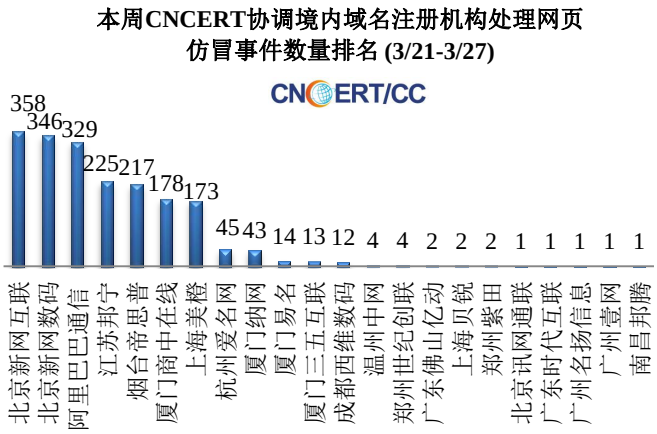
本周事件处理情况

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 2891 起，其中跨境网络安全事件 1054 起。



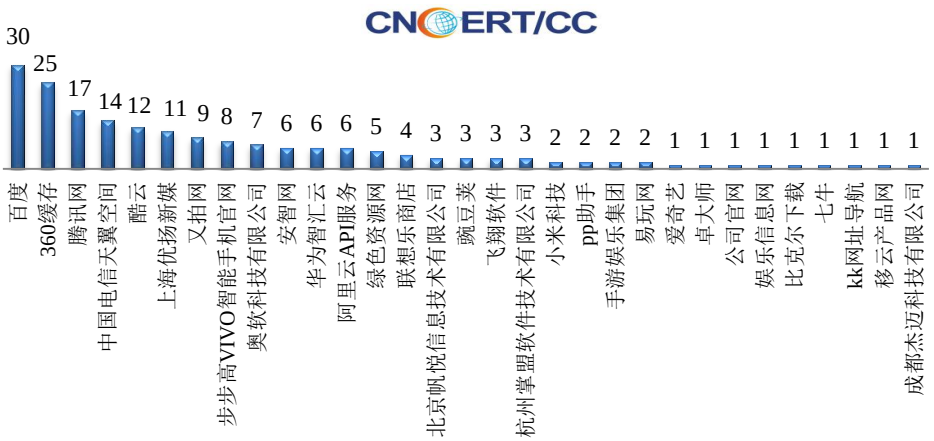
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 2793 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 2469 起和互联网服务提供商仿冒事件 307 起。





本周，CNCERT 协调 31 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 189 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
(3/21-3/27)



业界新闻速递

1、国家网络安全宣传周活动定于每年 9 月第三周举行

新华网 3 月 26 日消息 经中央网络安全和信息化领导小组批准，中央网信办、教育部、工业和信息化部、公安部、国家新闻出版广电总局、共青团中央等六部门近日联合发布《关于印发〈国家网络安全宣传周活动方案〉的通知》，确定网络安全宣传周活动统一于每年 9 月份第三周举行。《国家网络安全宣传周活动方案》要求，在国家网络安全宣传周活动期间，各省、市、自治区网信办要会同有关部门组织开展本地网络安全宣传周活动。国家有关行业主管监管部门根据实际举办本行业网络安全宣传教育活动。主要活动内容包括制作播放网络安全公益广告和专题节目、开展有奖征集活动和网络安全竞赛、组织网络安全技术研讨交流、发放网络安全科普材料、表彰网络安全先进典型等。国家网络安全宣传周中的开幕式等重要活动，可根据地方实际情况安排在省会城市举行。

2、美联邦政府网络安全漏洞多 总数超 7 万多个

环球网 3 月 23 日消息 据美国“侨报网”3 月 22 日报道，近日出炉的一份审计报告披露，2015 财政年度，美国联邦政府遭遇了 7.7 万多起网络安全事件，其中包括数据被盗或网络出现其它安全漏洞，比 2014 财年增加了 10%。据路透社报道，这份年度审计报告是由联邦政府管理和预算办公室（Office of Management and Budget）发布的。2015 财年网络安全事件之所以显着增加，部分原因是联邦机构发现和识别这类情况的能力有所提高。该报告把“网络事件”（cyber incidents）宽泛地定义为：“对计算机安全策略、可接受的使用策略或计算机安全标准实践的违背、或迫在眉睫的违背威胁。”在如此众多的网络事件中，仅有少数够得上明显的资料外泄。美国国家安全和情报部门长期以来一直发出警告：网络攻击是美国面临的最严重威胁之一。奥巴马上个月在其年度预算申请中请求国会拨款 190 亿美元用于加强联邦政府的网络安全。该数额比去年增加了 50 亿美元。美国联邦政府人事管理办公室（Office of Personnel Management）成了黑客大肆攻击的受害者。该攻击始于 2014 年，但

到去年才被发现。在那期间，大约 2200 万名现职和过去的联邦雇员、承包商的个人资料连同他们家人的资料外泄，其中包括社会安全号、生日、地址及其它个资。该事件促使美国政府启动了一个 30 天的“网络安全冲刺”，旨在加强各联邦机构内的网络安全，方法之一是采用多步骤认证方法。

3、英国央行将启动与英国国家网络安全中心合作

C114 中国通信网 3 月 21 日消息 据英国广播公司 3 月 20 日报道，英国政府宣布新的网络安全中心成立，其首要任务将是与英国央行（Bank of England）合作，针对整个英国金融领域制定新的网络安全标准，包括处理应对可能会影响英国经济发展的网络威胁。去年英国总理曾宣布成立该部门，现已改名为国家网络安全中心。成立目的是为民众提供英国专业的网络知识。任命英国政府通讯总部的高级官员查兰 马丁（Ciaran Martin）为第一负责人，网络安全技术总监伊恩 利维博士（Ian Levy）将成为该部门技术总监。“我们需要建立一个一站式的服务点供政府内外的人们咨询求助。”马修 汉考克（Matthew Hancock）内阁办公室部长向 BBC 新闻透露说他们将致力于成为英国信息安全方面的权威。英国政府通讯总部是网络安全方面的领导机构，但因为它是位于切尔滕纳姆市的一个秘密情报服务中心，对外信息保密。新网络安全中心旨在解决这一信息不透明的问题，应对当前民众对于政府暗箱操作的质疑。该中心不仅与监管机构如银行合作，为私营部门提供咨询服务。还将与其他政府部门，国家基础设施部门，商界以及公众合作。如果某部门或某项业务对国家来说具有潜在风险，信息安全中心更应涉身其中，这就是该中心的职能所在。在未来网络漏洞事件处理中，它将成为起至关重要作用的关键部门。该部门的工作人员强调他们的职能就是保护国家免受网络攻击，做好准备应对处理任何网络攻击，并将犯罪人员绳之以法。英国国家网络安全中心总部设立在伦敦，今年 10 月面向公众开放。

4、丹麦情报机构 PET 宣布开设“黑客学院”

网易 3 月 21 日消息 丹麦情报机构 PET（Politiets Efterretningstjeneste）已于上周宣布打造一所“黑客学院”，旨在培养出进攻和防御向的黑客。这所学校定于今年 8 月 1 号开学，具体地点是个秘密。培训将涉时 4.5 个月，包括了三大模块——据悉，培训会在丹麦首都哥本哈根的一个秘密地点展开。学生们在完成课程之后，将可报名加入 PET 的计算机网络探索团队。PET 每年只会吸收少量黑客，招聘条件和丹麦皇家海军的特种兵部队一样高，其中包括了一系列的心理测试。与其它拥有影子计划却鲜为人知的国家不同，PET 直接在官网上发表了一篇官方声明来阐述自身的计划，甚至还在当地报纸、公共交通和展板上发起了广告攻势。不过，在一份致丹麦《政治报》的声明中，PET 负责人 Lars Findsen 表示并不强制要求参与者们是顶级黑客，只需拥有所需的基础知识即可。这或许是考虑到了该国的地小人少（只有 560 万人），甚至还不到莫斯科的一半。先是网络、IT 基础设施和高级安全；其次是防御黑客攻击；最后是教给参与者们有关进攻向的黑客技巧。

5、韩为防朝网络威胁 开展陆空黑客防御大会

环球网 3 月 24 日消息 据韩联社 3 月 24 日报道，韩国为强化朝鲜网络攻击应对能力，韩国陆空军种 24 日将举行黑客防御大会。据悉，陆军将在当天下午于大田陆军信息通信学校举行“2016 年陆军黑客防御大会”。此次大会将有 98 名网络高手一决雌雄。大会将进行 5 个小时，在这 5 个小时内专家必须以最快的速度探测和正确分析出大会假设的服务器、网络和网页等最新型网络攻击情况。陆军黑客防御大会于 2009 年开始举行，今年已经迎来了第 8 个年头。此次大会分数最高的队伍可以获得陆军参谋总长奖，并且有资格参加今年 5 月份召开

的国防部黑客防御大会。空军当日在第 7 航空通信战队举行“第二届空军网络战士竞演大会”。在决赛中，将有 6 名空军军官展开最后角逐，他们都是从本月 22 日参加预赛的 22 个部队 62 名预赛者中选出的佼佼者。韩国空军方表示，运用网络中心最尖端的武器无法保障在没有网络优势情况下作战成功，所以应具备实战型的对应能力，继续维持最高的网络安保状态。

6、SWIFT 拟指导银行安全操作以规避黑客攻击

环球网 3 月 22 日消息 据《马尼拉公报》3 月 22 日报道，鉴于孟加拉国央行因黑客攻击交易系统而损失 8100 万美元的恶性案件，环球同业银行金融电讯协会（SWIFT）将在下周一发布公告，要求其 3000 多家银行会员开展内控风险审查，并按照其推荐的安全做法开展金融交易。此前，神秘黑客攻破孟加拉国央行交易系统，从其存放于纽约联邦储备银行的账户中窃取 8100 万美元，并将其转移到菲律宾有关银行账户，成为菲迄今发生的最大跨国洗钱案。SWIFT 称该案件是孟加拉央行的内部操作问题，SWIFT 核心信息系统并无漏洞。为防止黑客攻击，SWIFT 对其推荐的安全交易做法进行了总结，并建议银行密切关注最优路径。该领域资深人士肖恩舒克称，SWIFT 虽可建议银行遵循最低安全操作标准，但目前并无专业机构监管各国央行信息安全系统，这意味着各国中央银行标准并不统一，部分央行将更易受到网络攻击。

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 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：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158