国家互联网应急中心

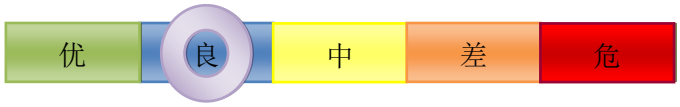
网络安全信息与动态周报

2016 年第 8 期

2 月 15 日-2 月 21 日

CNCERT/CC

本周网络安全基本态势

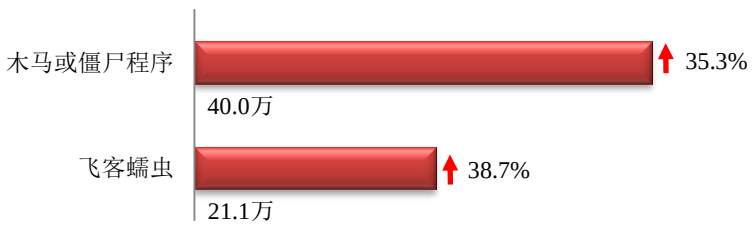


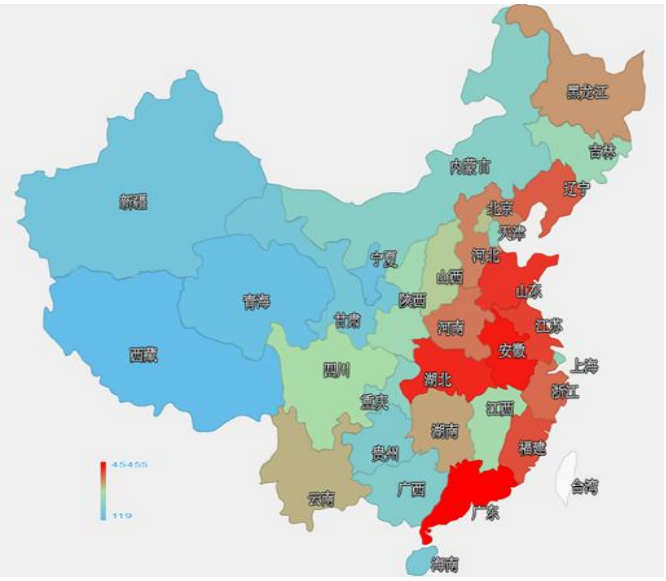
境内感染网络病毒的主机数量	•61.1万	36.5%
境内被篡改网站总数 其中政府网站数量	•4102 •54	1.0% 1.8%
境内被植入后门网站总数 其中政府网站数量	•1738 •39	65.8% 129.4%
针对境内网站的仿冒页面数量	•2015	569.4%
新增信息安全漏洞数量 其中高危漏洞数量	•298 •99	195.0% 312.5%

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 61.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 40.0 万以及境内感染飞客（conficker）蠕虫的主机约 21.1 万。



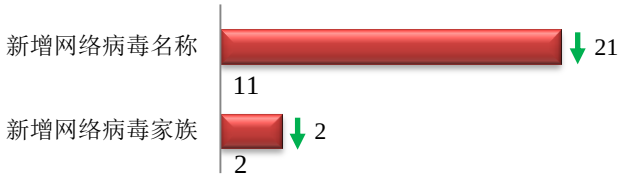


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、安徽省和湖北省。

TOP3

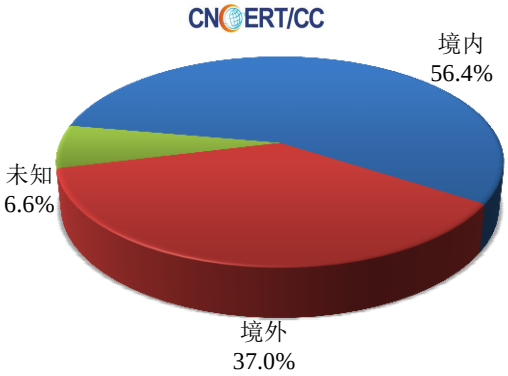
广东省	•约4.5万个（约占中国大陆总感染量的11.4%）
安徽省	•约3.74万个（约占中国大陆总感染量的9.34%）
湖北省	•约3.71万个（约占中国大陆总感染量的9.28%）

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 11 个，按网络病毒家族统计新增 2 个。

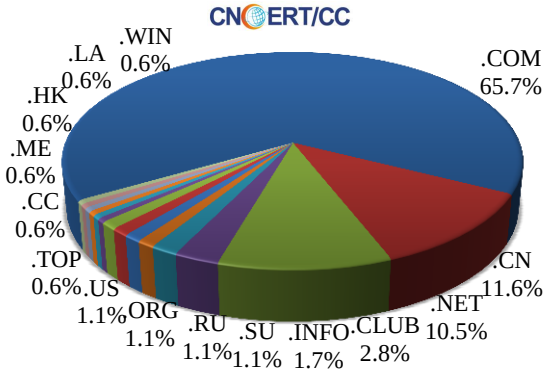


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 181 个，涉及 IP 地址 531 个。在 181 个域名中，有约 37.0%为境外注册，且顶级域为.com 的约占 65.7%；在 531 个 IP 中，有约 8.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 71 个 IP。

本周放马站点域名注册所属境内外分布
(2/15-2/21)



本周放马站点域名所属顶级域的分布
(2/15-2/21)



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。

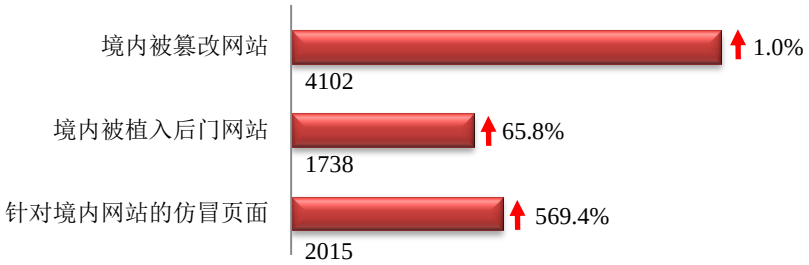
ANVA恶意地址黑名单发布地址

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。

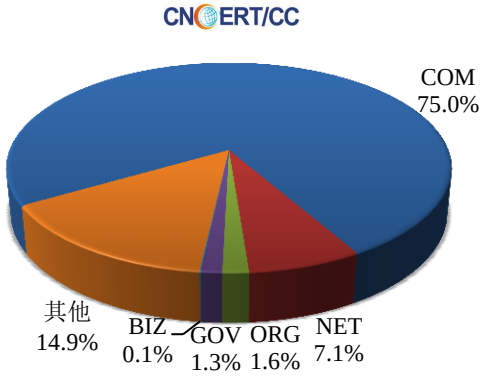
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4102 个；境内被植入后门的网站数量为 1738 个；针对境内网站的仿冒页面数量为 2015。

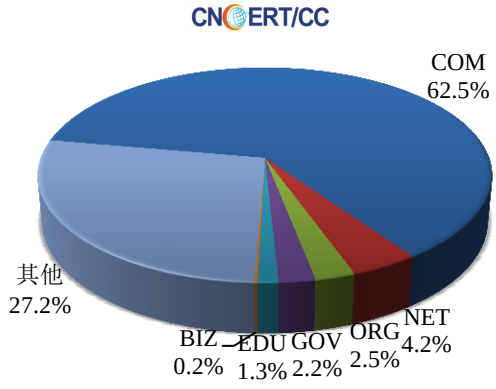


本周境内被篡改政府网站(GOV 类)数量为 54 个（约占境内 1.3%），较上周环比下降了 1.8%；境内被植入后门的政府网站(GOV 类)数量为 39 个（约占境内 2.2%），较上周环比上升了 129.4%；针对境内网站的仿冒页面涉及域名 1842 个，IP 地址 387 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/15-2/21)

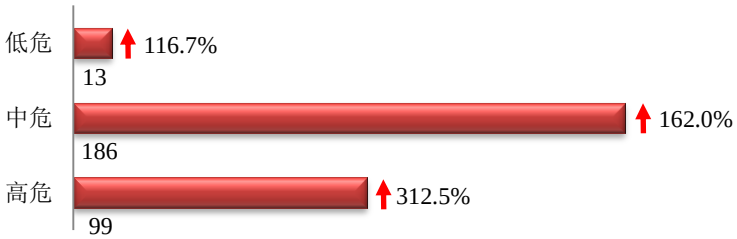


本周我国境内被植入后门网站按类型分布
(2/15-2/21)

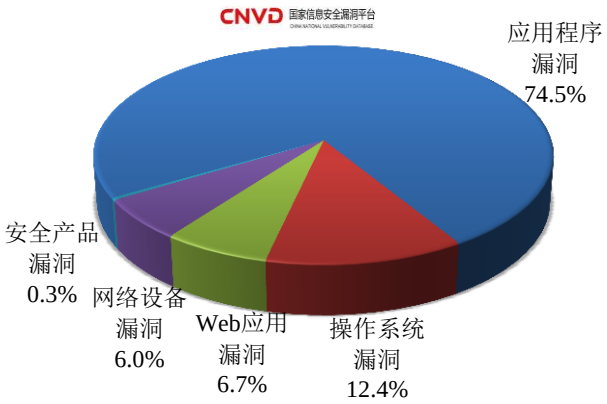


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 298 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
(2/15-2/21)



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

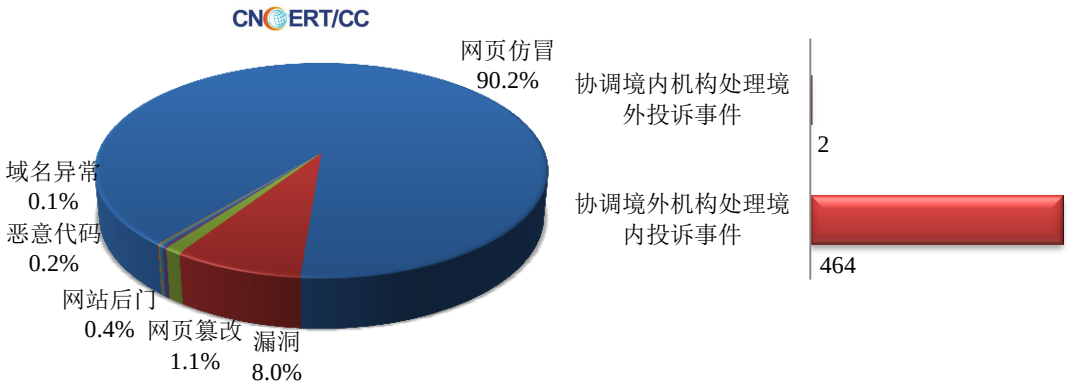
http://www.cnvd.org.cn/webinfo/list?type=4

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

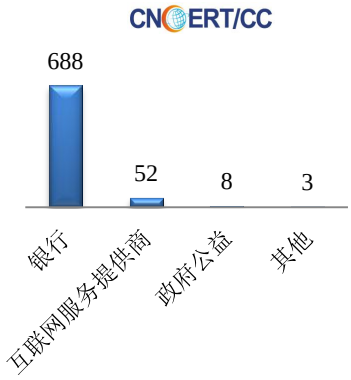
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 833 起，其中跨境网络安全事件 466 起。

本周CNCERT处理的事件数量按类型分布
(2/15-2/21)

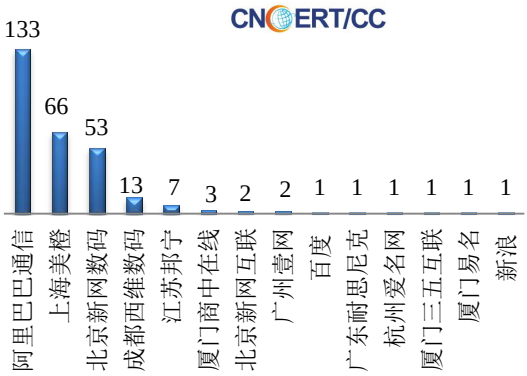


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 751 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 688 起和互联网服务提供商仿冒事件 52 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(2/15-2/21)



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 (2/15-2/21)



业界新闻速递

1、美国成立网络安全促进委员会 提升网络安全环境

央视网 2 月 18 日消息 美国总统奥巴马当地时间 17 日宣布任命前白宫国家安全事务助理多尼隆担任网络安全促进委员会主席，新委员会的主要任务是帮助联邦政府、私营企业和公民个人改善网络安全环境，为提升美国长期网络安全提供一份“路线图”。多尼隆曾于 2010 年至 2013 年担任美国总统国家安全事务助理，是一位在网络安全领域有丰富经验的政策专家。奥巴马同时任命 IBM 公司前首席执行官彭明盛担任委员会副主席。奥巴马当天在白宫与多尼隆等会晤时表示，网络安全促进委员会的工作范围非常广泛，包括确保联邦政府数据库运行更加安全，提升政府部门软硬件水平，保护其不受黑客攻击，推动政府更有效地与金融、基础设施等“关键

行业”开展合作、确保行业系统运行更安全，推动美国公民的金融、健康等信息更安全等，以帮助联邦政府、私营企业和公民个人改善网络安全环境，提升美国国家安全。奥巴马说，他将确保国土安全部部长约翰逊、商务部长普里茨克等政府高官与网络安全促进委员会保持密切合作，委员会须于 2016 年 12 月 1 日前形成建议报告提交奥巴马，为提升美国长期网络安全提供一份“路线图”。白宫本月早些时候已宣布计划在 2017 财年斥资 190 亿美元强化网络安全，将资金拨付国防部、联邦调查局、退伍军人事务部和联邦人事管理局等部门，升级政府机构网络安全基础设施，淘汰陈旧的计算机系统，招募优秀的网络安全人才。近年来，美国政府已多次鼓励企业与政府共享网络威胁信息，但出于公民隐私保护等考虑，一些企业不愿共享。目前国土安全部下属的网络安全和通信整合中心是负责推动政府与企业共享网络威胁信息的主要机构。

2、美国网络攻击伊朗计划曝光

网易 2 月 18 日消息 美国《纽约时报》16 日披露，美国曾制订计划，准备在外交途径无法解决伊朗核问题时对伊朗核以及军用和民用设施发动网络攻击。美国军方和情报部门分别拟定了打击计划，其中军方行动的代号名为“宙斯一触即发”，目的是使伊朗防空、通讯系统和关键电网陷入瘫痪。根据美国五角大楼的说法，“宙斯一触即发”行动预计耗资数千万美元，将由数千名美国军事人员参加，试图在伊朗电脑网络系统中植入电子设备。美国情报部门也制订了一个更为细化的秘密网络打击计划，旨在使伊朗的福尔多铀浓缩工厂陷入瘫痪。按照计划，美国情报部门将植入蠕虫病毒破坏核设施内的电脑网络系统，以达到拖延甚至彻底破坏这一设施的铀浓缩活动。2010 年，伊朗纳坦兹核设施电脑网络遭名为“震网”的病毒攻击，1000 台铀浓缩离心机瘫痪。美国媒体披露，这种电脑病毒由美国和以色列联合开发，而两国政府都不承认发动过那次网络攻击。即将登陆柏林电影节的纪录片《零日》描绘了伊核协议达成前伊朗和西方的紧张关系，讲述了电脑病毒攻击伊朗纳坦兹核设施如何被发现以及美军内部关于是否进行网络战的争论。美国《纽约时报》说，关于《零日》的报道暴露出“宙斯一触即发”行动的存在。美国白宫、国防部、国家情报总监办公室均拒绝证实这一报道。

3、英国斥巨资帮扶网络安全初创企业

中国信息产业网 2 月 15 日消息 英国政府近日宣布实施“网络安全早期加速项目”，旨在为本国的安全初创企业提供建议和支持。该项目将由“伦敦网络”和贝尔法斯特女王大学安全信息科技中心联合管理。截至目前，已获得 25 万英镑资金，资金将从 3 月开始对外发放。“伦敦网络”是欧洲历史上首个面向网络安全领域的加速项目。该项目想要尝试前人从未涉足的领域，为新一代英国安全公司创造环境，让英国能够自主生产网络防御技术，而不是仅仅消费其他国家创造的产品。据悉，该项目主要是促进英国安全初创企业的发展，帮助这些初创企业学习优秀安全公司的经验，为这些企业提供帮助与支持。英国文化、媒体和体育部部长艾德·韦泽表示，英国强劲增长的数字经济正改变着人们的生活与工作方式。随着科技的发展，人们对安全产品和服务的需求亦将增加。对安全初创企业的资助将确保该类企业可以汲取优秀企业的经验，维护英国网络空间的安全。贝尔法斯特女王大学安全信息科技中心与“伦敦网络”的负责人均表示，双方之间的合作管理将推动英国网络安全企业的创新和发展，为英国安全初创企业注入新的生机与活力，继而维护英国的数字经济霸主地位。据悉，此次资助是英国促进本国安全产业发展的战略之一。近日，英国财政大臣乔治·奥斯本宣布英国拟在 5 年内投资 19 亿英镑应对网络恐怖威胁。此外，英国政府通信总部也开设了一系列的暑期培训班，以培养未来的网络安全专

家。其主要内容是帮助人们学习如何利用技术维护英国网络安全。

4、韩国金融机构启动应急机制 严防朝鲜黑客攻击

环球网 2 月 15 日消息 据韩联社 2 月 15 日报道，韩国金融界 15 日称，在朝鲜核试和射星、开城工业区关闭导致韩朝局势紧张之际，各大商业银行和保险公司纷纷启动应急工作机制，加强保安系统，以防范来自朝鲜的网络攻击风险。韩国国家网络安全中心于 1 月 8 日发布第四级网络危机警报，2 月 11 日将其上调至第三级，军方也将情报作战防御系统“INFORCON”级别由第四级上调至第三级。此后，韩国友利银行启动应急状况室，增加个人电脑安检次数。新韩银行安排了更多的公休日和夜间值班人员并启动应急工作组。KB 国民银行也增加夜间保安人员，保持 24 个小时应急工作状态，并禁止职员阅览来源不明的电子邮件和附件。此前，朝鲜于 2013 年 2 月进行第三次核试验后针对韩国多家机构和个人发起了大规模网络攻击。同年 3 月韩国多家金融机构和电视台的 4.8 万台服务器、个人电脑和自助终端遭到黑客攻击，同年 6 月，政府机关和媒体服务器遭到分布式拒绝服务（DDOS）攻击。

5、日本 25 个大学等机构曾遭网络攻击但半数未公布

环球网 2 月 15 日消息 据日本共同社 2 月 15 日报道，日本文部科学省管辖的国立大学等 120 个机构中，有 25 个机构在 2013 年度因遭网络攻击而受害，但其中 12 个机构未对外公布此事。官方机构在遭受网络攻击后虽没有公开或进行报告的义务，但出于防止受害进一步扩大并提醒各方引起注意的目的，有必要尽快公布事态。日本文科省表示：“希望在出现重大故障的时候，有关方面能尽到向国民说明的责任。”2013 年 11 月多所大学多功能一体机被曝处于可从外部读取信息的状态后，文科省对 120 个机构实施了调查。在共同社希望其公开相关信息的请求下，文科省公布了调查结果。该调查仅实施了一次，之后未再次实施。调查结果显示，已确认共有 25 个机构共遭受 30 次网络攻击。机构名及受害内容几乎全部被涂黑。公布受害情况的 13 个机构中有一部分是通过政府关于网络攻击的资料来锁定的。同时，在“安全措施是否完善”的设问，大多数机构都回答称“尚有不足”。各大学纷纷表示“旨在提升技能的培训不够”、“专门职员及具有管理能力的人才短缺”，应对措施尚不完善的问题十分突出。

6、黑客攻击土耳其国家警察服务器：公布 17.8GB 数据

网易 2 月 16 日消息 据外媒报道，近日，一名叫做 ROR（RG)的黑客从土耳其国家警察（EMG）服务器盗取了大量数据，现在这些数据已经在网上发布了 BitTorrent 下载链接。ROR（RG）这名黑客还曾是 Adult Friend Finder 数据泄露的幕后黑手，当时他公布了 380 多万用户的高敏感个人信息。这次，ROR（RG）选择同一个网站--The Cthulhu--来公布数据。该名黑客告诉 The Cthulhu，其实早在两年前就已经尝试过攻击土耳其警察局服务器，同时期，他还曾渗透到其他政府系统。两年过后，ROR（RG）仍旧可以访问那些被他攻击过的网站。ROR（RG）表示，他之所以公布这些信息则是因为他相信，土耳其警察内部存在严重的腐败现象。现在，关于土耳其腐败问题和职权滥用的报道络绎不绝。各大国际媒体记者和匿名者（Anonymous）黑客都认为土耳其政府应当为美国记者 Serena Shim 的死负责。对此，匿名者也曾向土耳其政府发起网络攻击，该组织指责土耳其协助叙利亚国内的 IS 成员，甚至还为他们提供医疗帮助。另外，土耳其媒体也已经多次公开指责土耳其政府在镇压公众抗议上采取的暴力滥用现象。虽然此次公布的数据包大约只有 2GB 大，但将其解压之后则有 17.8GB

的信息量。所有数据都以.myd 和.myi 的格式存在。

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：刘军

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158