国家互联网应急中心

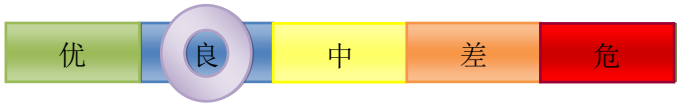
网络安全信息与动态周报

2016 年第 7 期

2 月 8 日-2 月 14 日

CNCERT/CC

本周网络安全基本态势

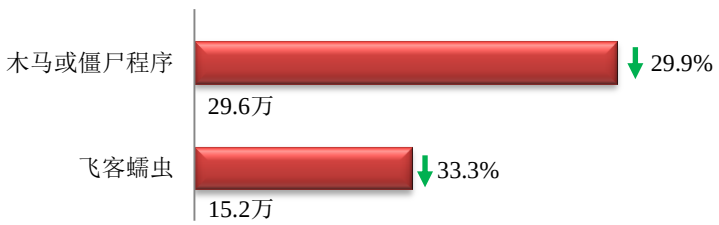


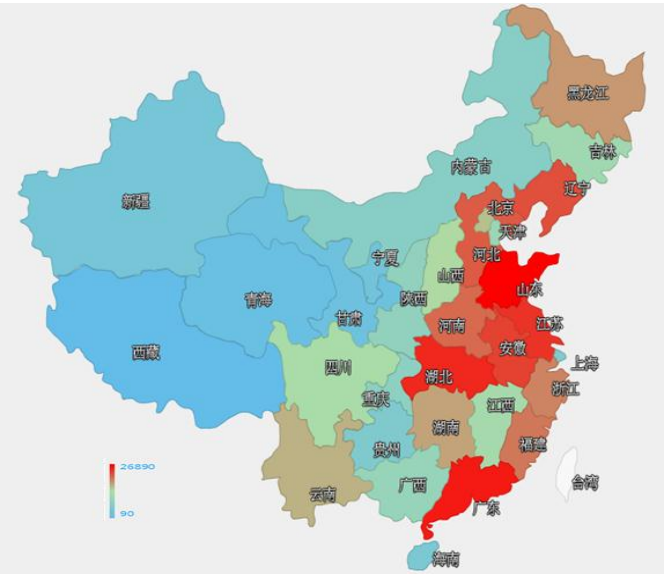
境内感染网络病毒的主机数量	• 44.8万	↓ 31.1%
境内被篡改网站总数 其中政府网站数量	• 4062 • 55	↓ 3.5% ↑ 1.9%
境内被植入后门网站总数 其中政府网站数量	• 1048 • 17	↑ 10.7% ↓ 39.3%
针对境内网站的仿冒页面数量	• 301	↓ 83.0%
新增信息安全漏洞数量 其中高危漏洞数量	• 101 • 24	

= 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 44.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 29.6 万以及境内感染飞客（conficker）蠕虫的主机约 15.2 万。



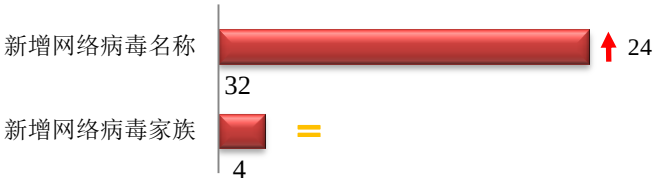


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是山东省、广东省和湖北省。

TOP3

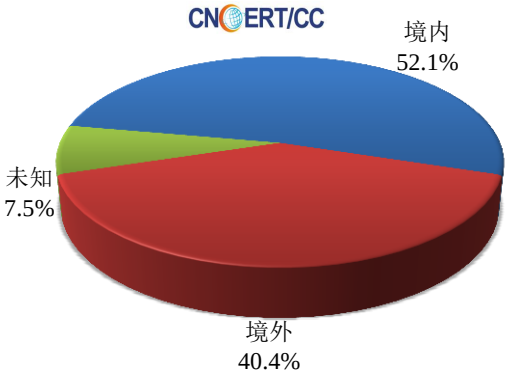
山东省	• 约2.7万个（约占中国大陆总感染量的9.1%）
广东省	• 约2.43万个（约占中国大陆总感染量的8.2%）
湖北省	• 约2.39万个（约占中国大陆总感染量的8.1%）

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 32 个，按网络病毒家族统计新增 4 个。

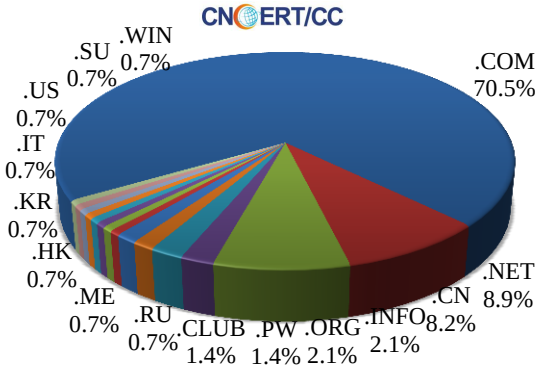


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 146 个，涉及 IP 地址 431 个。在 146 个域名中，有约 40.4%为境外注册，且顶级域为.com 的约占 70.5%；在 431 个 IP 中，有约 9.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 49 个 IP。

本周放马站点域名注册所属境内外分布
(2/8-2/14)



本周放马站点域名所属顶级域的分布
(2/8-2/14)



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。

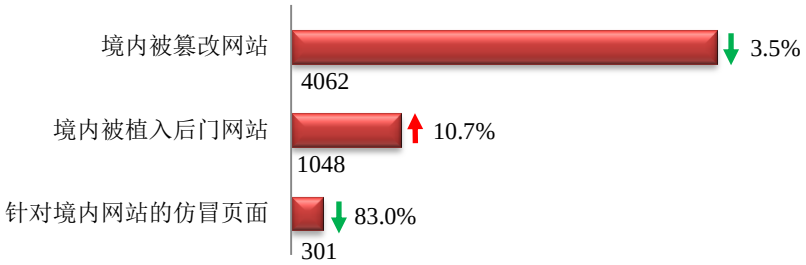
ANVA恶意地址黑名单发布地址

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。

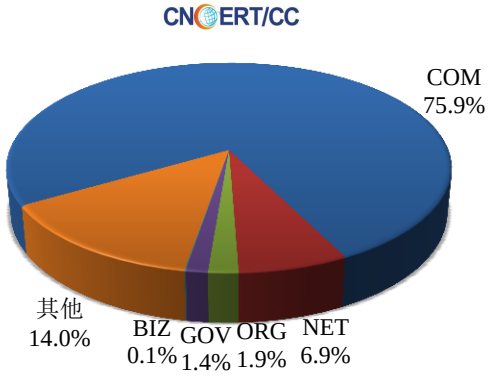
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4062 个；境内被植入后门的网站数量为 1048 个；针对境内网站的仿冒页面数量为 301。

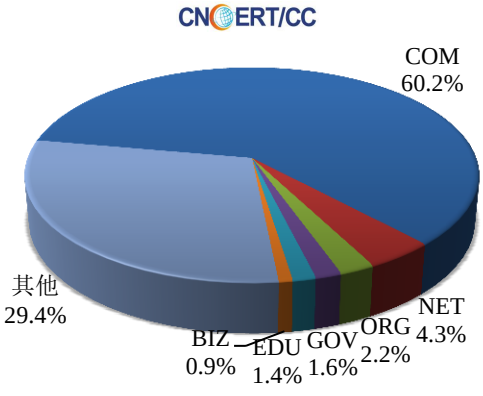


本周境内被篡改政府网站(GOV 类)数量为 55 个（约占境内 1.4%），较上周环比上升了 1.9%；境内被植入后门的政府网站(GOV 类)数量为 17 个（约占境内 1.6%），较上周环比下降了 39.3%；针对境内网站的仿冒页面涉及域名 274 个，IP 地址 138 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/8-2/14)

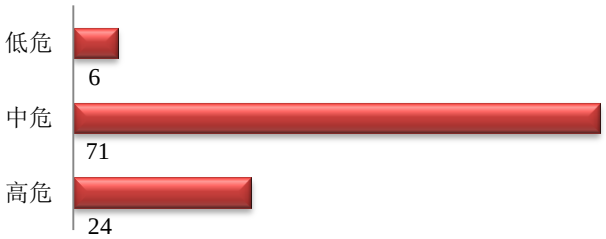


本周我国境内被植入后门网站按类型分布
(2/8-2/14)

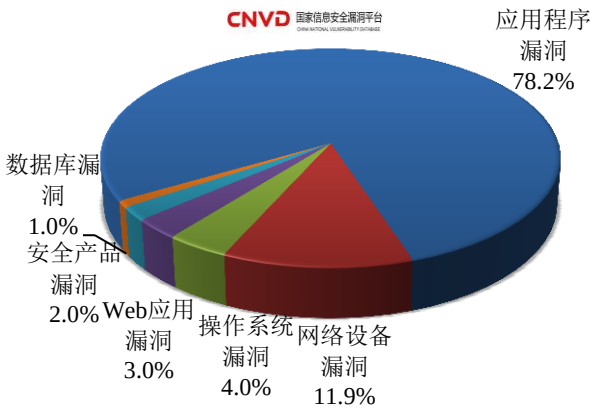


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 101 个，信息安全漏洞威胁整体评价级别为低。



本周CNVD收录漏洞按影响对象类型分布
(2/8-2/14)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备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

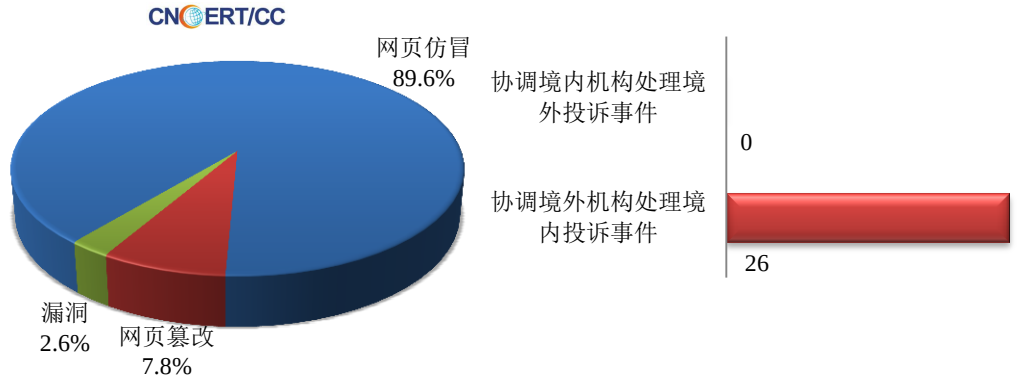
http://www.cnvd.org.cn/webinfo/list?type=4

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 77 起，其中跨境网络安全事件 26 起。

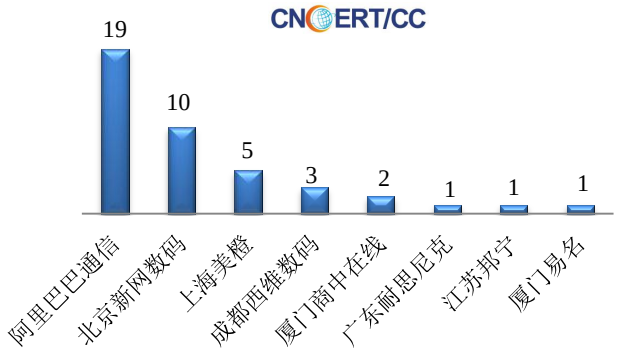
本周CNCERT处理的事件数量按类型分布
(2/8-2/14)



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 69 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包含银行仿冒事件 69 起。

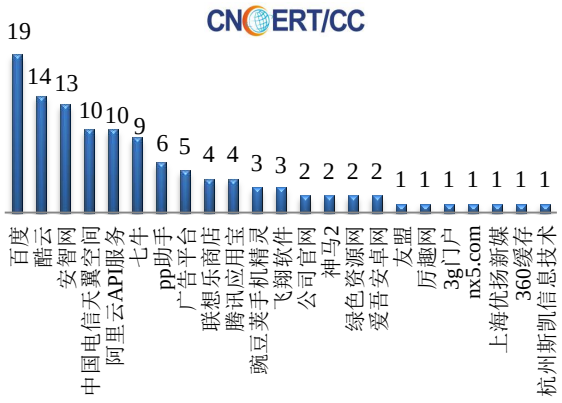
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/8-2/14)

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 (2/8-2/14)



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 (2/8-2/14)

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 115 个。



业界新闻速递

1、奥巴马政府推出《网络安全国家行动计划》

新华网 2 月 10 日消息 美国总统奥巴马 2 月 9 日推出《网络安全国家行动计划》，将从加强网络基础设施建设、加强专业人才队伍建设、加强与企业的合作、加强民众网络安全意识宣传以及寻求长期解决方案 5 个方面入手，全面提高美国在数字空间的安全。为支持这一行动计划，奥巴马在当天提交给国会的 2017 财政年度预算中提议拿出 190 亿美元用于加强网络安全，比今年提高超过三分之一，其中 31 亿美元用于更新改造美国联邦政府落后的电脑系统。奥巴马还计划仿照美国公司的运行模式，设立联邦首席信息安全官，负责联邦政府网络安全政策与行动的规划与执行。白宫在一份背景声明中说，这是美国政府首次设立专职的高级官员主管网络安全。在加强专业人才队伍建设方面，奥巴马表示，将通过提供奖学金以及免除学生贷款等方式招募最好的人才为政府服务。此外，美国内政部将把民用网络防御团队数量扩大至 48 支；美国军方的网络司令部正在组建 133 支共计 6200 人的网络部队。该部队目前已开始参与一些网络行动，按计划将于 2018 年开始全面运行。在加强与企业的合作方面，奥巴马政府 8 日启用一个新的国家网络安全机构，以推动政府与企业共同研发并部署先进网络技术。在长期解决方案方面，奥巴马下令成立由国会、企业界和学术界代表组成的“国家网络安全促进委员会”，任务是为美国政府提供今后 10 年网络安全方面的建议，并在今年年底前向他提交一份相关路线图。奥巴马当天还签署了一份行政命令，设立一个常设机构“联邦隐私委员会”，组成人员为各个联邦机构的隐私保护官员，负责制定并落实各个联邦机构的隐私保护政策。

2、美国情报部门表示可通过物联网监控公民

搜狐网 2 月 11 日消息 美国国家情报局局长 James Clapper 确认称，美国政府安全机构有能力利用新兴物联网技术扩展自身监控范围与能力。他于 2 月 9 号的一份提交给美国参议院的威胁评估证明文件中证实了这一点，并通过发言概述了当前可能对美国网络与国家安全造成威胁的各类因素。虽然并没有提到任何政府情报及安全机构的确切名称，但他指出相关机构能够利用此类工具进一步实施监控行为，而安全专家们认为各类同步型智能家居设备可能会进一步简化数据的访问流程。这位情报部门负责人表示，“‘智能化’设备已经广泛存在于电网、车辆——包括自动驾驶车辆——以及家居设备当中，旨在提高执行效率、改进能源节约效果并提升便捷性水平。然而安全行业分析人士指出，大部分此类新型系统会威胁到数据保密性、数据完整性乃至服务连接性。”他同时补充称，“在未来，情报部门可能会利用物联网设备实施识别、监视、监控、定位以及追踪，将相关信息纳入招聘流程或者访问网络或用户的相关凭证。”

3、北约与欧盟加强网络安全合作

新华网 2 月 11 日消息 北大西洋公约组织（北约）2 月 10 日发表声明说，北约与欧盟当天达成一项技术协议以加强网络安全合作。声明说，北约和欧盟都面临着日益严峻的网络威胁，为了更好地应对挑战，两大组织签署了一项技术协议，为双方的网络应急部门加强信息交流和分享实践经验作出安排。北约秘书长斯托尔滕贝格表示，北约和欧盟将共同应对包括传统军事战争和网络攻击在内的新形势下的混合战威胁。北约负责新兴安

全挑战事务的助理秘书长索林·杜卡鲁说，北约与欧盟合作将加强彼此抵御网络攻击的能力，使双方能够更好地避免、防范、检测和应对网络攻击。欧盟对外行动署副秘书长佩德罗·塞拉诺表示，与北约加强网络安全合作是欧盟网络防御政策框架下的五大优先事项之一，当天协议的达成是双方合作中的一个重要进展。声明说，北约和欧盟在网络安全方面开展了长期的合作，欧盟工作人员曾多次参加北约的年度网络防御演习。

4、韩国为防止朝鲜攻击提高网络预警等级

环球网 2 月 14 日消息 据俄罗斯卫星新闻 2 月 14 日消息，在朝鲜进行核试验并发射载有卫星的火箭后，韩国认为其面临可能的来自朝鲜的网络攻击威胁。报道称，韩国负责全国信息系统状态的 INFOCON 系统提高了预警水平。据报道，这一五级制的预警系统，最低级别为五级，最高级别为一级，目前韩国已经将预警级别从四级提高到了三级。韩国外交界消息人士强调，朝鲜对韩国进行网络攻击有很大的可能性，因此不久前他们根据 INFOCON 系统重新设定了预警级别。他还补充说，到目前为止，尚未发现韩国国防部系统遭到朝鲜黑客的袭击，但“这种可能增加了，因此专家们在仔细地观察所有可能的迹象”。朝鲜半岛形势因朝鲜 1 月 6 日进行了第四次核试验和 2 月 7 日发射火箭卫星而恶化。多名专家认为，朝鲜发射火箭卫星是其试验洲际弹道导弹的借口。朝鲜宇宙空间技术委员会 2 月 7 日宣布，朝鲜从平安北道铁山郡的西海卫星发射场将载有“光明星 4 号”卫星的“光明星”号运载火箭发射升空。据了解，卫星轨道高度为 494.6 至 500 千米，它环绕地球飞行的时间为 94 分钟。

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：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158