国家互联网应急中心

网络安全信息与动态周报

2016 年第 9 期

2 月 22 日-2 月 28 日

CNCERT/CC

本周网络安全基本态势

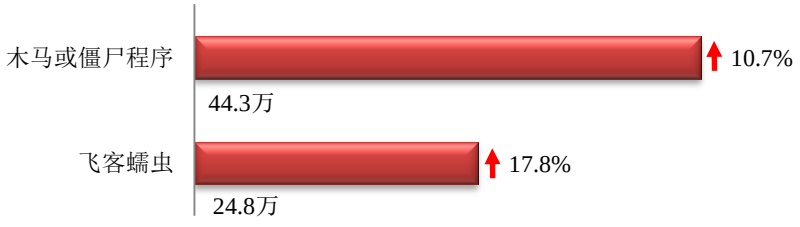
优 | 良 | 中 | 差 | 危

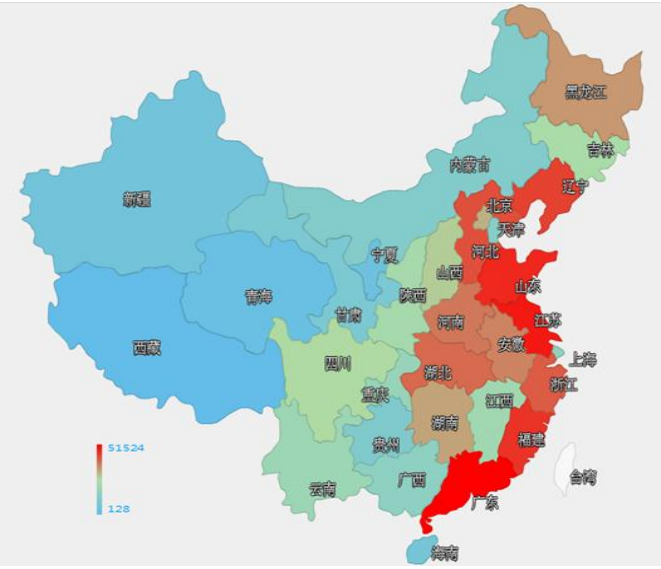
境内感染网络病毒的主机数量	•69.1万	13.1%
境内被篡改网站总数 其中政府网站数量	•4108 •56	0.1% 3.7%
境内被植入后门网站总数 其中政府网站数量	•1779 •45	2.4% 15.4%
针对境内网站的仿冒页面数量	•3462	71.8%
新增信息安全漏洞数量 其中高危漏洞数量	•160 •37	46.3% 62.6%

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 69.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 44.3 万以及境内感染飞客（conficker）蠕虫的主机约 24.8 万。



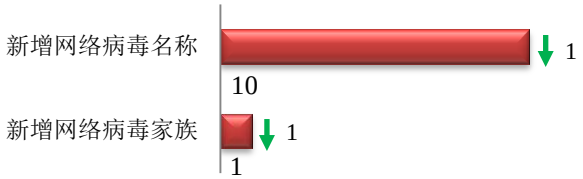


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和山东省。

TOP3

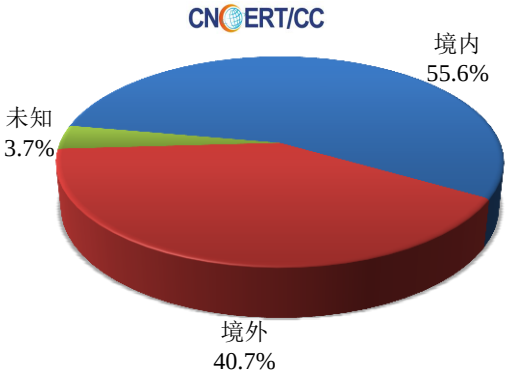
广东省	•约5.2万个（约占中国大陆总感染量的11.6%）
江苏省	•约4.1万个（约占中国大陆总感染量的9.2%）
山东省	•约3.7万个（约占中国大陆总感染量的8.4%）

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 10 个，按网络病毒家族统计新增 1 个。

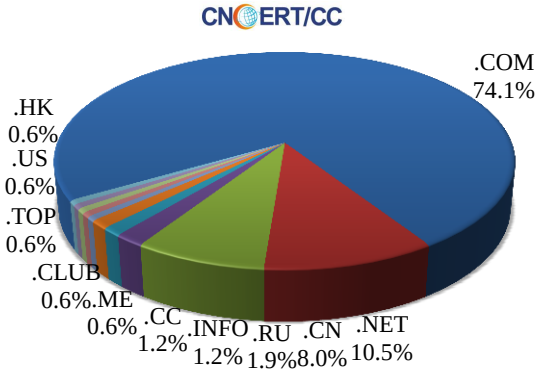


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 162 个，涉及 IP 地址 498 个。在 162 个域名中，有约 40.7%为境外注册，且顶级域为.com 的约占 74.1%；在 498 个 IP 中，有约 9.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 56 个 IP。

本周放马站点域名注册所属境内外分布
(2/22-2/28)



本周放马站点域名所属顶级域的分布
(2/22-2/28)



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。

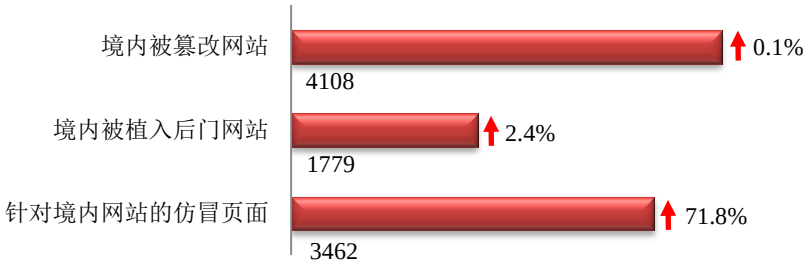
ANVA恶意地址黑名单发布地址

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。

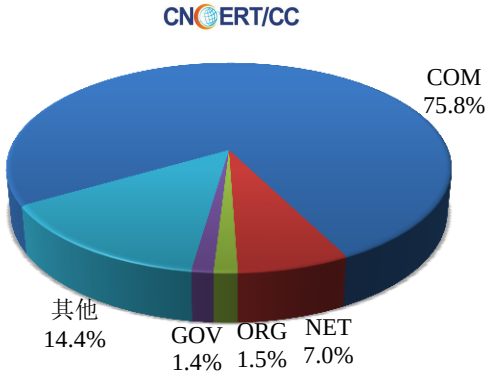
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4108 个；境内被植入后门的网站数量为 1779 个；针对境内网站的仿冒页面数量为 3462。

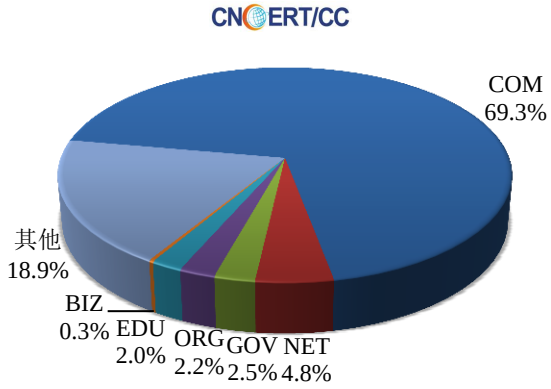


本周境内被篡改政府网站(GOV 类)数量为 56 个（约占境内 1.4%），较上周环比上升了 3.7%；境内被植入后门的政府网站(GOV 类)数量为 45 个（约占境内 2.5%），较上周环比上升了 15.4%；针对境内网站的仿冒页面涉及域名 3055 个，IP 地址 743 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/22-2/28)

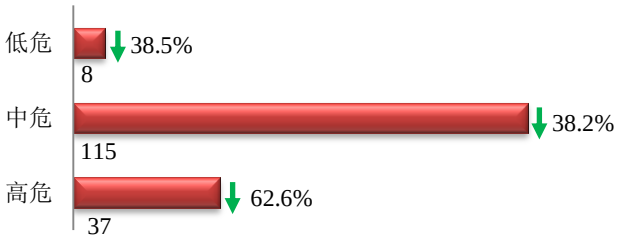


本周我国境内被植入后门网站按类型分布
(2/22-2/28)

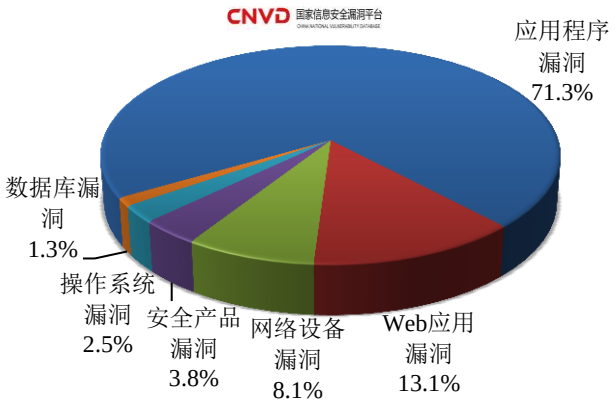


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 160 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
(2/22-2/28)



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 应用漏洞和网络设备漏洞。

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

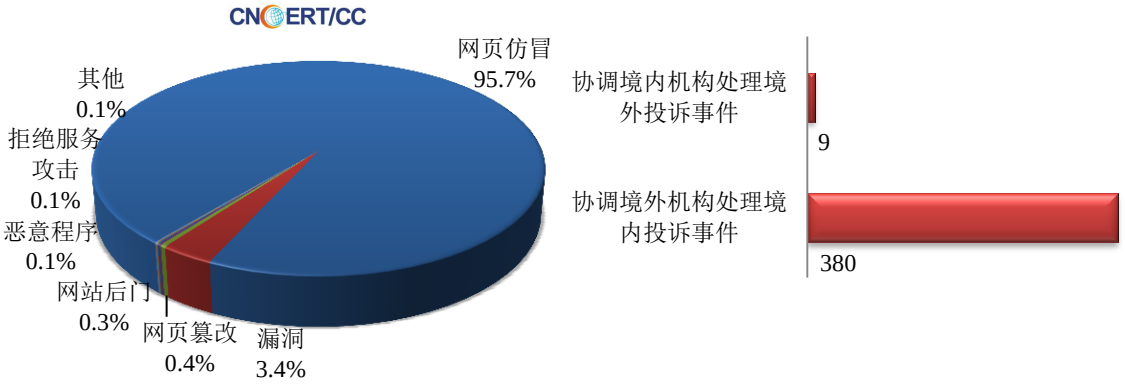
http://www.cnvd.org.cn/webinfo/list?type=4

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 1597 起，其中跨境网络安全事件 389 起。

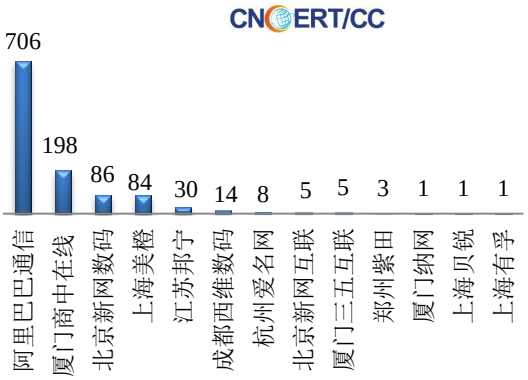
本周CNCERT处理的事件数量按类型分布
(2/22-2/28)



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 1529 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 1472 起和互联网服务提供商仿冒事件 53 起。

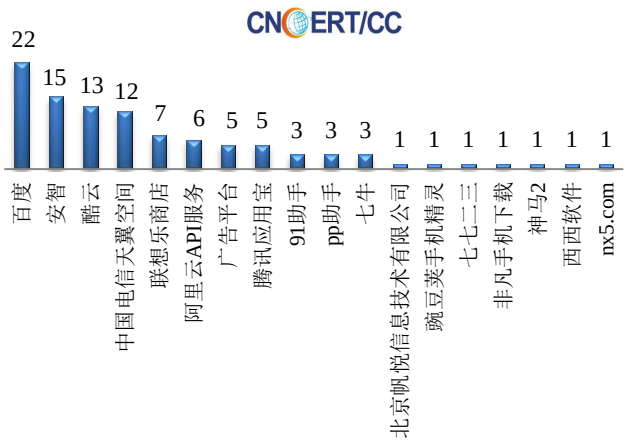
本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(2/22-2/28)

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 (2/22-2/28)



本周，CNCERT 协调 18 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 101 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 (2/22-2/28)



业界新闻速递

1、中国互联网网络安全威胁治理联盟在京成立

新华网 2 月 26 日消息 国家互联网应急中心 2 月 26 日在京宣布，中国互联网网络安全威胁治理联盟正式成立，首批共 89 家企业申请加入联盟。据互联网应急中心相关负责人介绍，互联网应急中心联合业内机构、企业自 2015 年 7 月启动了“互联网网络安全威胁治理行动”，通过投诉举报、关键数据共享、威胁认定、协同处置、信息发布等多项措施取得了显著治理效果。据了解，“行动”针对分布式拒绝服务攻击、网页篡改等与互联网黑产密切相关的事件进行重点处置。据统计，行动期间共接到网民举报网络安全事件 109972 起，处置网络安全事件 71220 起，发布黑名单地址 54614 条。危害较大的分布式拒绝服务攻击事件次数由行动前的日均 1491 起下降到目前日均 265 起，下降 82.2%；境内被篡改网站相比行动前下降 21.4%，其中被篡改政府网站相比下降了 56.2%。为巩固“行动”成果，建立互联网网络安全威胁治理长效机制，互联网应急中心联合业内成立了中国互联网网络安全威胁治理联盟，成员单位涵盖网络安全产业链上下游企业。联盟的成立，为行业提供了公共沟通交流平台，加强互联网网络安全威胁信息共享、相互协作，将有效打击互联网黑色产业链，净化网络安全环境，树立我国负责任网络大国的良好形象。

2、维基解密公开机密文件 称美国国安局窃听世界多国领袖

央广网 2 月 25 日消息 据中国之声《央广新闻》报道，维基解密网站近日公开机密文件称，美国国家安全局为了地缘政治而窃听世界多国领袖。网站形容这次发布的文件是由媒体机构公布的最高级别的机密文件。有美国调查记者接受俄罗斯 RT 电视台访问时认为，美国还积极地收集各国的经济情报。凤凰卫视报道，维基解密表示，美国国家安全局窃听了 2008 年潘基文与默克尔的会晤，两人当时讨论如何应对气候变化问题。俄罗斯 RT 电视台引述维基解密创始人阿桑奇的话称，美国窃听是为了保护自己最大的石油公司。此外维基解密还表示，美国监听了日本、欧盟、以色列以及意大利等国领导人的会晤。美国的调查记者拉斯曼（音）在接受 RT 电视台访问时说，这说明美国的监听不只在政府监，而且也在收集经济情报，“他们有一个非常高效的机构，但也十分恐怖，他们无处不在，监控着一切。”

3、美将设立“监察专员”防止欧盟公民数据被滥用

网易 2 月 28 日消息 据路透社报道，路透社获得的一份文件显示，在美国与欧盟本月达成新的数据共享协议后，美国已经开始对其批量收集的欧盟公民数据在使用上进行限制。美国与欧盟达成新的被称为“隐私盾牌（Privacy Shield）”的数据共享协议，让企业能够方便地将个人数据传送给美国。该协议的一个关键内容，是明确规定了那些个人信息可以被使用，从而防止个人信息被“一刀切”和“任意”地使用。根据新的数据协议，华盛顿同意在美国国务院内设立一个新的职位，以处理欧盟数据保护机构转交的投诉及查询。双方还将制定一个替代性纠纷解决机制来化解争端，并每年对协议进行联合审查。美国国家情报总监办公室总法律顾问罗伯特•利特（Robert Litt）在致美国商业部的信中称，批量收集的公民数据只能用于 6 个特定目的，其中包括反恐和网

络安全等。重要的是，美国当局不仅将采取措施反对不加区别地收集数据，这些措施还将同样用于保护通过跨大西洋电缆传输的信息。这解决了欧盟公民一个主要的担忧，即美国对本土以外收集到的信息给予更少地保护。“隐私盾牌”协议将首次让欧洲人有一种途径，能对美国代理商访问其根据该协议传输的数据提出投诉。路透社获得的另一封信件显示，欧盟司法专员维拉·朱洛娃（VeraJourova）、美国国务卿克里承诺设立一位“监察专员”来处理这类投诉。该信件透露，美国国务院副国务卿凯瑟琳·诺维利（Catherine Novelli）将担任这一职位，并确保一旦美国代理商超范围访问个人数据，将采取相应补救措施。

4、德国政府批准可利用间谍软件监控可疑公民

腾讯网 2 月 24 日消息 据外媒报道，近日德国内政部发言人宣布，政府已经批准其官员利用 Trojan 间谍软件监控可疑公民。Trojan 是一套专门为攻击用户电脑而设计的间谍软件，一般为网络攻击者或网络盗贼所用，也被称为恶意软件。但德国政府会利用这款软件追踪目标人物在智能手机、iPad 平板和电脑上的聊天记录。实际上，早在去年秋季，德国政府就已经对这一做法表示支持。但据法律规定，如果政府官员想要监控可疑公民的聊天记录等内容，他们需要得到德国法院的许可文件才能进行此项操作。在得到许可后，政府官员利用利用 Trojan 软件进入可疑公民的个人电脑、笔记本和智能手机等智能电子设备。一旦 Trojan 在可疑公民的电子设备上安装完成之后，政府官员便可获得其存储在硬盘中的数据以及在设备上进行的聊天记录等内容，随时追踪可疑公民的具体实时动态。尽管这一做法得到了德国政府的支持，但德国绿党却对这一项目提出了反对意见，绿党的副主席 Konstantin von Notz 表示：“我们也理解政府安全官员的需求和工作职责，但在一个法治国家，这并不代表可以为了满足需求而不折手段，”同时，德国的黑客组织 Chaos Computer Club 也对政府的这一做法和决定持怀疑态度。而在 2008 年德国宪法法院作出的一项判决中显示，只有当遇到威胁公民生命安全或是涉嫌对抗国家的犯罪活动发生时才允许远程控制和监控公民的电脑。

5、俄罗斯将加强涉及国防等多个领域的互联网信息安全

中国网信网 2 月 27 日消息 俄罗斯总统普京 2 月 26 日说，要加强俄罗斯军事和战略设施、互联网信息的安全。普京当天出席俄罗斯联邦安全局会议时说，必须可靠地保护权力机构、军事设施、军工企业、主要学术中心的安全，保护机密信息的安全，制止有些人企图利用民族主义、排外主义和激进主义从事分裂社会的活动。普京说，外国情报机构加强了在俄罗斯的活动，去年抓获的外国间谍和招募人员达到 400 多名，其中 23 人被追究刑事责任。普京说，必须加强公共信息安全，尤其是涉及国防、国家安全、社会秩序、经济金融等领域的信息安全。他说，去年俄罗斯权力机构的官方网站和信息系统曾受到 2400 万次黑客攻击，1600 条有损国家安全的互联网资源被清理。俄国家杜马（议会下院）将于 9 月举行换届选举。普京说，要制止外部势力对国家杜马选举的干涉，根据俄罗斯法律保护国家的利益，对破坏主权的威胁作出相应的反应。普京还表示，确保经济安全仍是安全部门重要工作之一。去年破获了 98 个经济犯罪团伙，2200 人被追究刑事责任。他要求，加强打击腐败、盗窃和挪用公款的活动。

6、韩媒：朝鲜专职黑客达 3000 人 负责海外间谍工作

环球网 2 月 22 日消息 据韩国《中央日报》2 月 22 日报道，朝鲜最高领导人金正恩已下令开展对韩攻击活动的消息经韩国国情院披露后，韩国政府拉响紧急警报。报道称，朝鲜侦察总局接到金正恩的指示后已经开始

着手进行准备的事实曝光后，人们纷纷将关注点聚焦到了负责对韩与海外间谍工作的朝鲜侦察总局。据悉，朝鲜侦察总局共设有 6 个局，是负责培养间谍、谋杀重要人物及网络黑客攻击等业务的对韩挑衅大本营。最近还另设网络部队，正在进一步强化网络战争的能力。侦察总局属下的电子侦察局和网络战争指导局是专门负责开展网络攻击的部队。韩国政府掌握到，该部队仅专业黑客人员就多达 3000 名。2014 年窃取韩国核电站图纸等信息的“韩国水力原子能公司网络攻击事件”以及 2013 年 KBS 和农协等机构电算网瘫痪事件的主谋都被指是朝鲜侦察总局。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158