国家互联网应急中心

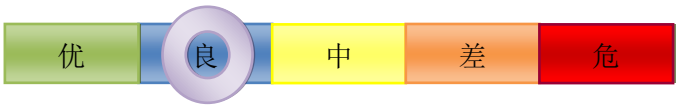
2015 年第 23 期

6 月 1 日-6 月 7 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

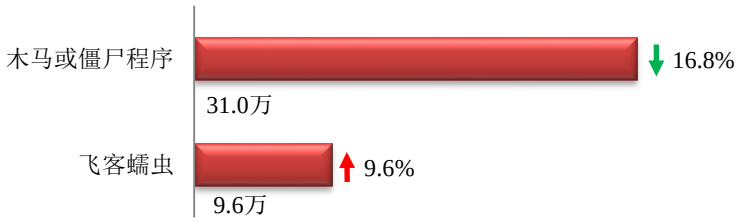


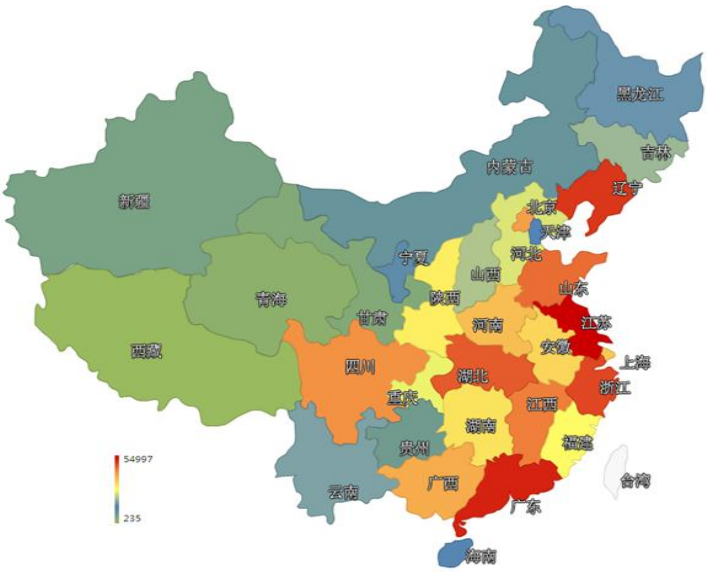
境内感染网络病毒的主机数量	•40.6万	↓11.8%
境内被篡改网站总数 其中政府网站数量	•1722 •51	↓40.7% ↓45.2%
境内被植入后门网站总数 其中政府网站数量	•1967 •110	↓8.6% ↓10.6%
针对境内网站的仿冒页面数量	•3158	↓31.2%
新增信息安全漏洞数量 其中高危漏洞数量	•112 •27	↓26.3% ↓51.8%

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 40.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 31.0 万以及境内感染飞客（conficker）蠕虫的主机约 9.6 万。



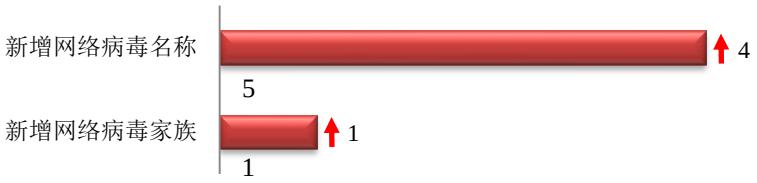


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是江苏省、广东省和辽宁省。

TOP3

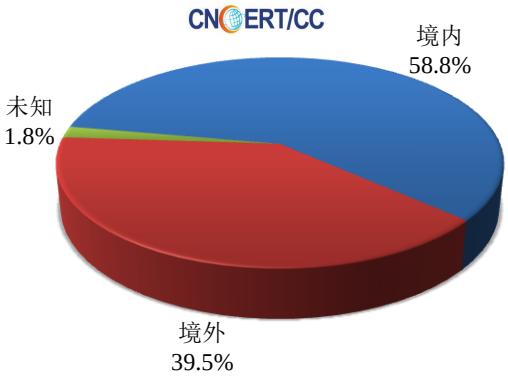
江苏省	•约5.5万个（约占中国大陆总感染量的17.7%）
广东省	•约3.7万个（约占中国大陆总感染量的12.1%）
辽宁省	•约2.8万个（约占中国大陆总感染量的9.1%）

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 5 个，按网络病毒家族统计新增 1 个。

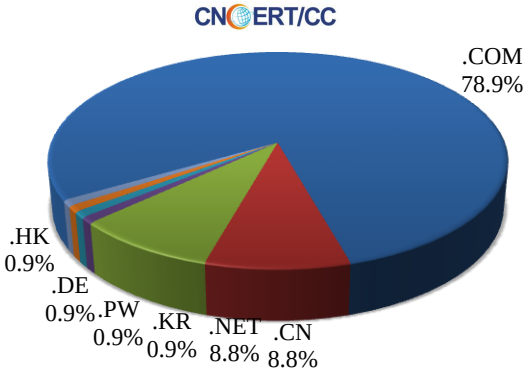


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 114 个，涉及 IP 地址 204 个。在 114 个域名中，有约 39.5%为境外注册，且顶级域为.com 的约 78.9%；在 204 个 IP 中，有约 12.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 24 个 IP。

本周放马站点域名注册所属境内外分布
(6/1-6/7)



本周放马站点域名所属顶级域的分布
(6/1-6/7)



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。

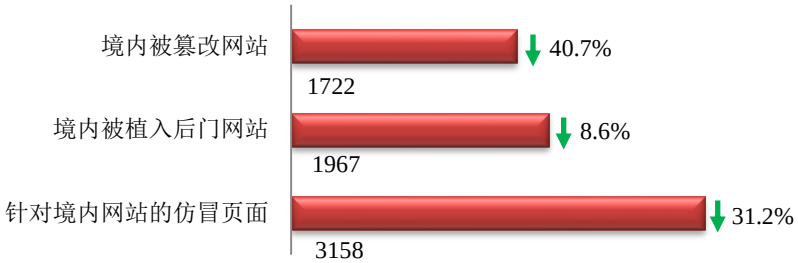
ANVA恶意地址黑名单发布地址

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。

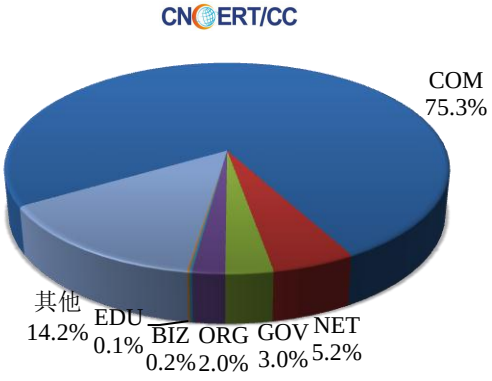
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1722 个；境内被植入后门的网站数量为 1967 个；针对境内网站的仿冒页面数量为 3158。

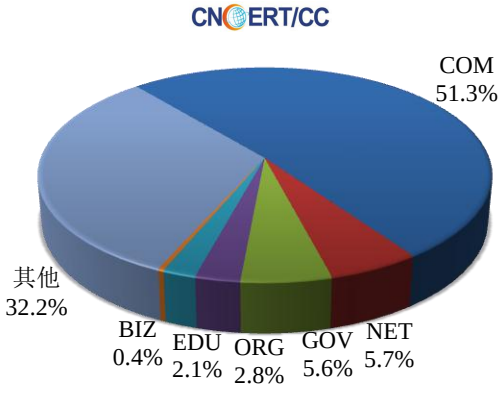


本周境内被篡改政府网站(GOV 类)数量为 51 个（约占境内 3.0%），较上周环比下降了 45.2%；境内被植入后门的政府网站(GOV 类)数量为 110 个（约占境内 5.6%），较上周环比下降了 10.6%；针对境内网站的仿冒页面涉及域名 2484 个，IP 地址 659 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/1-6/7)

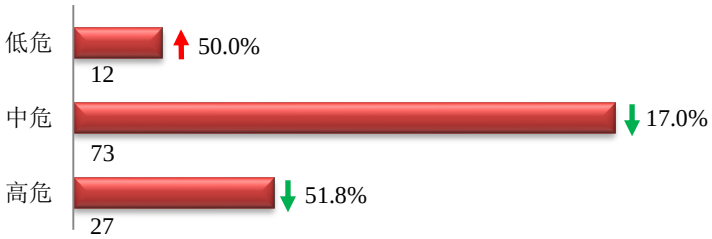


本周我国境内被植入后门网站按类型分布
(6/1-6/7)

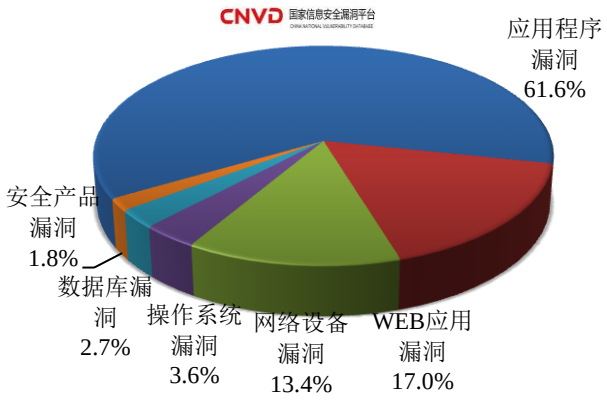


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 112 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
(6/1-6/7)



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

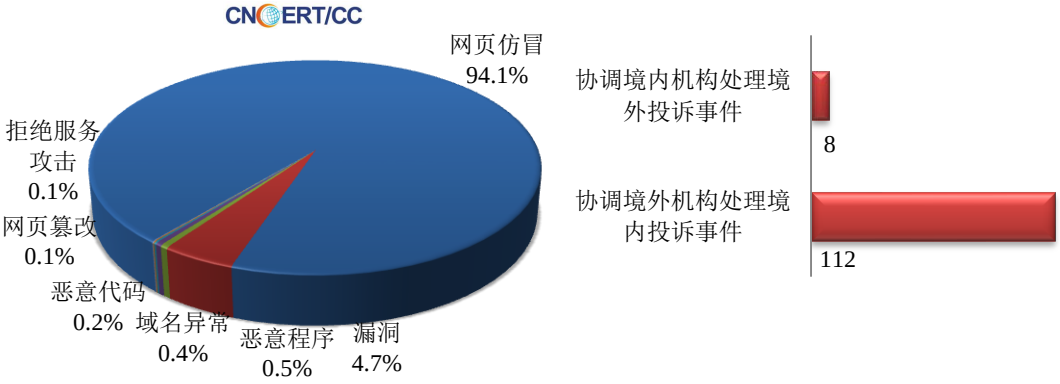
http://www.cnvd.org.cn/webinfo/list?type=4

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

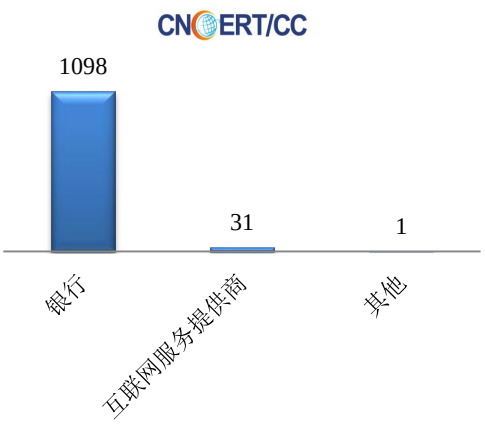
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1201 起，其中跨境网络安全事件 120 起。

本周CNCERT处理的事件数量按类型分布
(6/1-6/7)

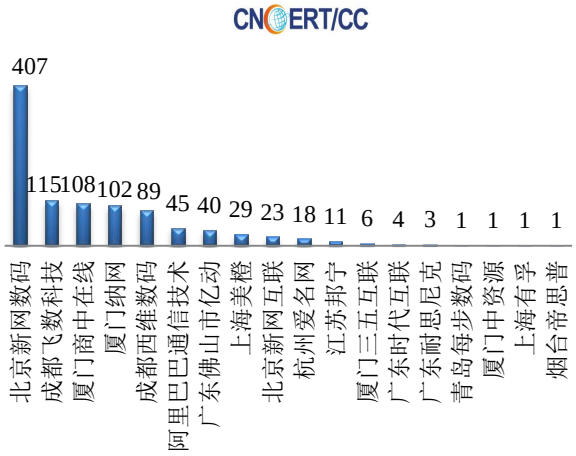


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1130 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1098 起和互联网服务提供商仿冒事件 31 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/1-6/7)

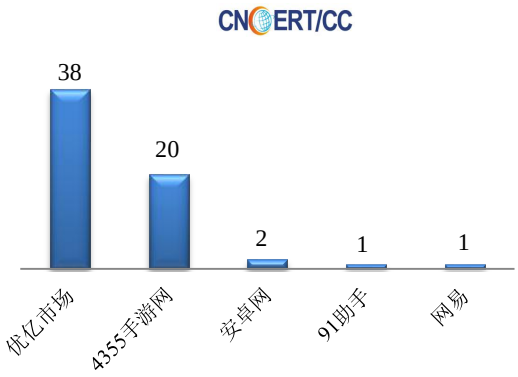


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/1-6/7)



本周，CNCERT 协调 5 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 62 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 (6/1-6/7)



业界新闻速递

1、国家网络安全宣传周启动

人民网 6 月 2 日消息，6 月 1 日，第二届国家网络安全宣传周在京启动。本届宣传周由中央网信办、中央编办、教育部、科技部、工信部、公安部、中国人民银行、新闻出版广电总局、共青团中央、中国科协十部门共同主办，沿用首届“共建网络安全，共享网络文明”主题，将于 6 月 1 日至 7 日在全国各地同步开展。中宣部副部长、中央网信办主任鲁炜在启动仪式上呼吁全社会携起手来，大力培育有高度的安全意识、有文明的网络素养、有守法的行为习惯、有必备的防护技能的新一代“中国好网民”，尤其要突出青少年网络安全宣传教育。启动仪式上，中国工程院副院长陈左宁表示，网络虚拟空间纷繁芜杂，对于心智发育尚未完全成熟的青少年来说，还需要家长、学校和社会给予更多正确地引导，帮助其“适度用网、健康用网、安全用网”。青少年不应成

为网络空间的受害者，而应该在全社会的呵护下，成长为传播“网络空间正能量”的新兴力量。据了解，宣传周设立了启动日、金融日、电信日、政务日、科技日、法治日、青少年日等 7 个主题日，并开展公众体验展、青少年网络安全知识竞赛、全国网络安全宣传作品大赛、“讲述身边的网络安全故事”文章和微视频征集展映、打击网络违法犯罪专题讲座等活动。

2、美参议院通过《美国自由法案》限制政府监听

网易 6 月 3 日消息，根据外国媒体报道，当地时间 6 月 1 日，美国参议院美国参议院以 67 支持票对 32 反对票通过了《美国自由法案》。此项立法将取代即将过期的《爱国者法案》的部分条款，同时加大对政府间谍活动的监管。该法案在上个月已经在众院获得通过，之后法案将被递交给奥巴马进行签署后成为法律，而据此前预计，奥巴马将会签署《美国自由法案》。美国国会为通过立法一直备受压力，因为按照计划，《爱国者法案》的三个规定已于 5 月 31 日过期。《美国自由法案》以更多限制的形式来消弱这部分权力，也旨在遏制政府对美国本土的监控。该法案还将采取措施，推动美国国家安全局的活动更加透明和负责。目前，当政府向海外情报监视法庭（FISC）提请通过监视行动时，都没有谁会提出反对的意见。《美国自由法案》对此做出变革——通过为法院指定的公共倡导者设立新职位，以参与 FISC 诉讼程序。《美国自由法案》的争论一直围绕于国家安全局对美国民众的电话记录监听一事上。《美国自由法案》建立了一系列全新改进的程序来获取美国民众的通话记录，但这些获取需求必须集中在一个明确的“选择项”上，例如客户名称或电话号码。这目的是禁止大量收集客户数据。此外，该法案要求政府公开 FISC 事关重大的舆论观点（尽管政府可以拒绝公布，但这样做定会威胁到国家的安全），以及发布国内间谍活动的详细数据。

3、美国政府电脑被黑：400 万雇员信息被盗

新浪网 6 月 5 日消息，据路透社报道，美国官员 6 月 4 日透露，黑客通过一次大规模网络攻击入侵了美国人事管理局（OPM）的电脑。由于该部门专门负责收集联邦政府雇员的人事信息，导致 400 万现任和前任员工信息被盗。一位来自美国执法机构的消息人士表示，美方认为外国机构或政府可能是此次攻击事件的幕后主使。美国联邦调查局（以下简称“FBI”）也宣布对此展开调查，并将把犯罪分子绳之以法。OPM 今年 4 月在其 IT 系统中发现了新的恶意活动，而美国国土安全部表示，他们在 5 月初发现该机构的数据被盗。一位要求匿名的美国国土安全部官员称，此次攻击影响了 OPM 的 IT 系统及其存储在美国内政部数据中心的数据，该数据中心由美国多家政府机构共享。该官员不肯透露其他政府机构的数据是否也受此影响。OPM 之前还曾遭受过另外一起网络攻击，美国国务院、邮政局和白宫等许多联邦政府机构的电脑系统也都曾遭遇过很多攻击。“FBI 正在与其他部门合作调查此事。”FBI 在声明中说，“我们对公共和私有部门的系统面临的潜在威胁都很重视，并将继续展开调查，将威胁网络安全的人绳之以法。”OPM 表示，自从黑客事件发生以来，该部门已经部署了额外的安全防范措施，他们也通知了受此影响的 400 万人，并为其提供了信用监控和身份盗窃服务。

4、美国：将日本纳入网络攻击防御保护伞

比特网 6 月 1 日消息，美国宣布将其网络防御保护伞覆盖至日本，以助力其亚洲盟友处理针对军事基地及基础设施（如电网等）的网络攻击。美国-日本网络防御政策工作组织（建于 2013 年）在周六发布的这份联合声明中指出：“我们发现包括由非国家及国家支持的恶意网络攻击者发动的攻击不断增多。”美日两国在四月份发布了一系列新的安全指南，并由此加深在军事方面的合作，而这些指南同时整合了两国的弹道导弹防御系统，并赋予日本在亚洲更大的安全角色，以对抗中国不断增长的军事力量。日本国防部一名官员在周四表示，日本

军队的网络防御单位约有 90 个成员，而美国超过 6000 人。并且随着东京 2020 年举办奥运会的时间越来越近，日本正在不断为抵御网络攻击做准备。目前每过几秒就会检测到政府网站中的可疑活动。美国国防部长在新加坡会见日本国防部长时披露了一个在四月份实施的更加强大的军事网络战略，并强调利用网络武器实施报复。这是继针对企业遭受高级别网络攻击之后做出的，其中包括美国认为是朝鲜实施的索尼影视网络攻击活动。

5、日本 NTT 等 30 家公司将成立跨行业组织应对网络攻击

环球网 6 月 3 日消息，据日本共同社 6 月 3 日报道，日本电信巨头 NTT 于 6 月 2 日透露，负责电力燃气、信息通讯、航空、铁路等重要基础设施的约 15 个行业 30 家公司将于 6 月上旬成立新组织，在应对网络攻击方面展开合作。这些不同行业的企业将横向合作加强网络安全措施，提高防御能力。日本年金机构的养老金信息外泄事件使得各方对网络攻击的关注度进一步高涨，今后将加快制定具体措施。预计将讨论受到网络攻击时迅速实现信息共享，以及培养精通网络安全措施的专家等议题。据称，成立跨行业组织应对网络攻击尚属首次尝试。为了避免成为攻击目标，除了 NTT 以外的公司没有公布名称。今后将呼吁更多企业加入，将来计划使成员达到 40 家以上。

6、安全专家发现黑客可将恶意程序藏在图片中

雷锋网 6 月 4 日消息，印度 Net-Square 公司网络安全专家 Saumil Shah 最近发现了一个恶意程序的漏洞：黑客们可以把恶意程序写到一张普通的图片文件里，人们只要打开看一眼这张看似普通的图片，电脑就会被黑，并将这种隐藏恶意程序命名为 Stegosploit。该 BUG 来源于可以把信息隐藏到图片中的 Steganography 技术。利用这种技术把代码写进图片像素，然后通过 HTML5 的可递交脚本的动态 Canvas 元素还原。这个恶意代码本质是图片的代码和 Javascript 脚本的混合，被称之为 IMAJS。黑客程序可以有很多功能，比如下载和安装间谍软件等。然后把图片上传到网上，当你在浏览器中查看这张图片的时候，恶意程序就会被触发。不过这种代码也不是百分百能让你中招，只能作用于一些安全性较弱的浏览器或网站，并且这种带有恶意程序的图片不会出现在社交网站上。

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 2014 年，CNCERT 与 63 个国家和地区的 144 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：董艳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170