国家互联网应急中心

2016 年第 25 期

6 月 13 日-6 月 19 日

网络安全信息与动态周报

本周网络安全基本态势

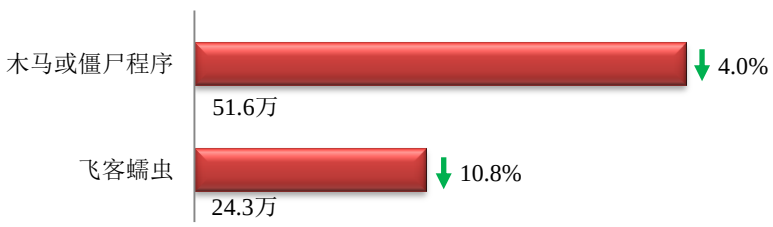
优 | 良 | 中 | 差 | 危

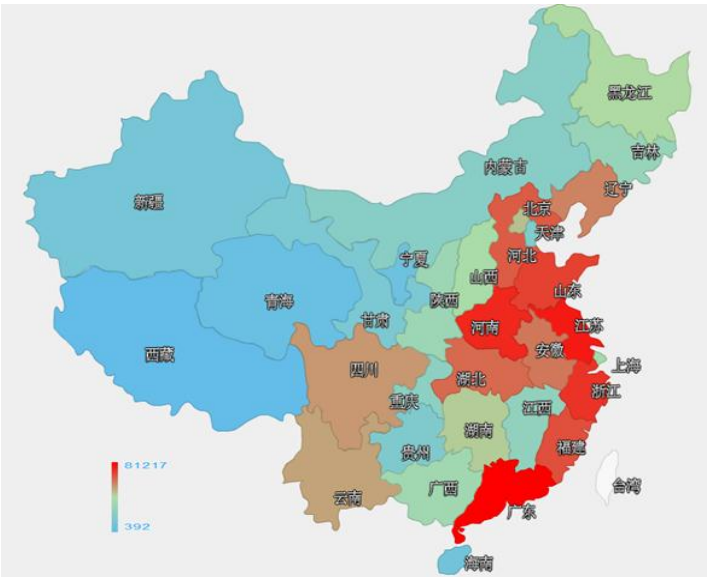
境内感染网络病毒的主机数量	•75.9万	6.3%
境内被篡改网站总数 其中政府网站数量	•3708 •92	50.1% 39.4%
境内被植入后门网站总数 其中政府网站数量	•3309 •93	28.2% 16.3%
针对境内网站的仿冒页面数量	•1870	29.5%
新增信息安全漏洞数量 其中高危漏洞数量	•161 •65	36.4% 80.6%

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 75.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.6 万以及境内感染飞客（conficker）蠕虫的主机约 24.3 万。



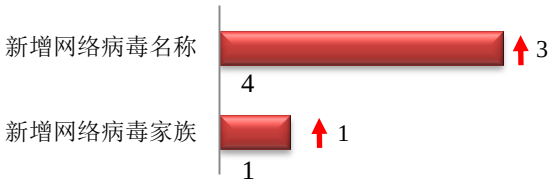


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和河南省。

TOP3

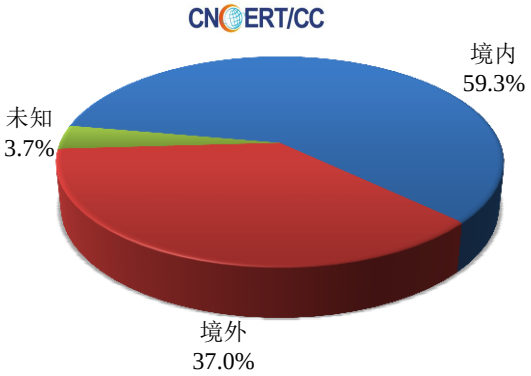
广东省	•约8.1万个（约占中国大陆总感染量的15.7%）
江苏省	•约4.7万个（约占中国大陆总感染量的9.2%）
河南省	•约3.6万个（约占中国大陆总感染量的6.9%）

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 4 个，按网络病毒家族统计新增 1 个。

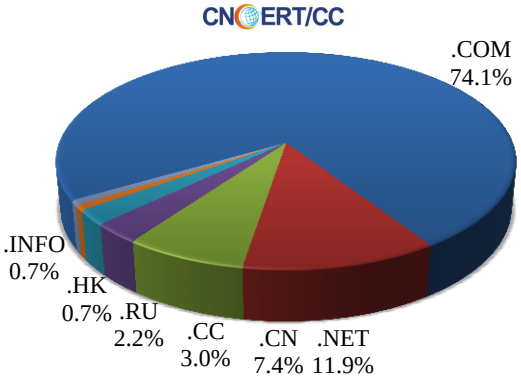


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 135 个，涉及 IP 地址 299 个。在 135 个域名中，有 37.0%为境外注册，且顶级域为.com 的约占 74.1%；在 299 个 IP 中，有约 8.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 25 个 IP。

本周放马站点域名注册所属境内外分布
(6/13-6/19)



本周放马站点域名所属顶级域的分布
(6/13-6/19)



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。

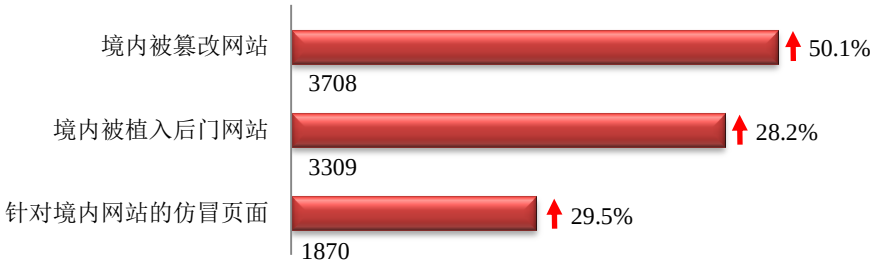
ANVA恶意地址黑名单发布地址

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。

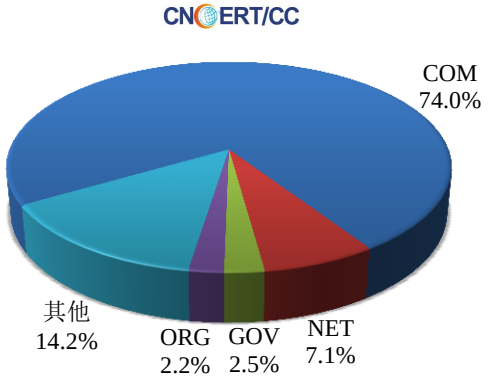
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3708 个；境内被植入后门的网站数量为 3309 个；针对境内网站的仿冒页面数量为 1870。

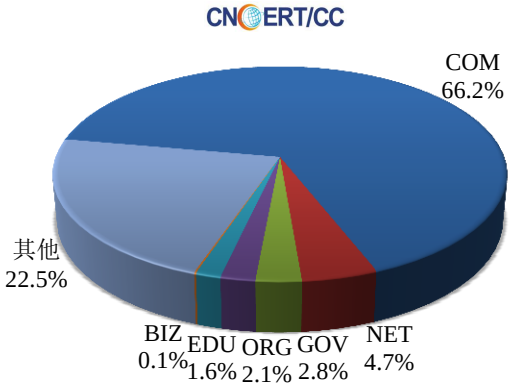


本周境内被篡改政府网站（GOV 类）数量为 92 个（约占境内 2.5%），较上周环比上升了 39.4%；境内被植入后门的政府网站（GOV 类）数量为 93 个（约占境内 2.8%），较上周环比上升了 16.3%；针对境内网站的仿冒页面涉及域名 1104 个，IP 地址 380 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/13-6/19)

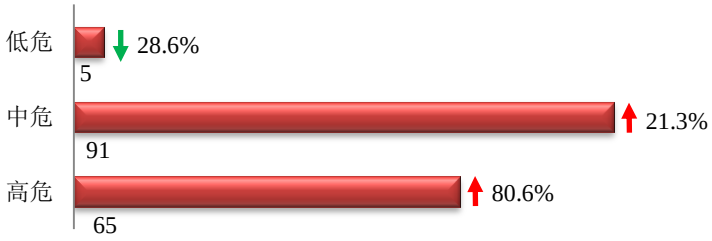


本周我国境内被植入后门网站按类型分布
(6/13-6/19)

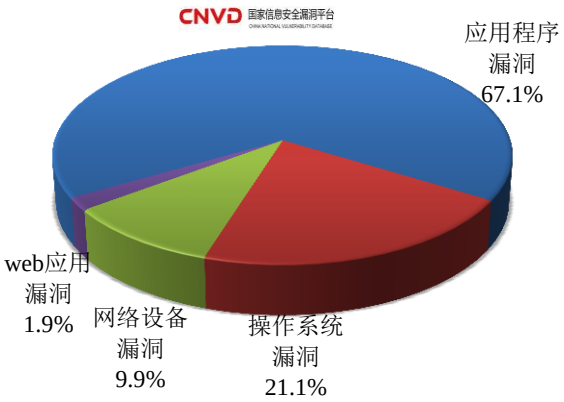


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 161 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(6/13-6/19)



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

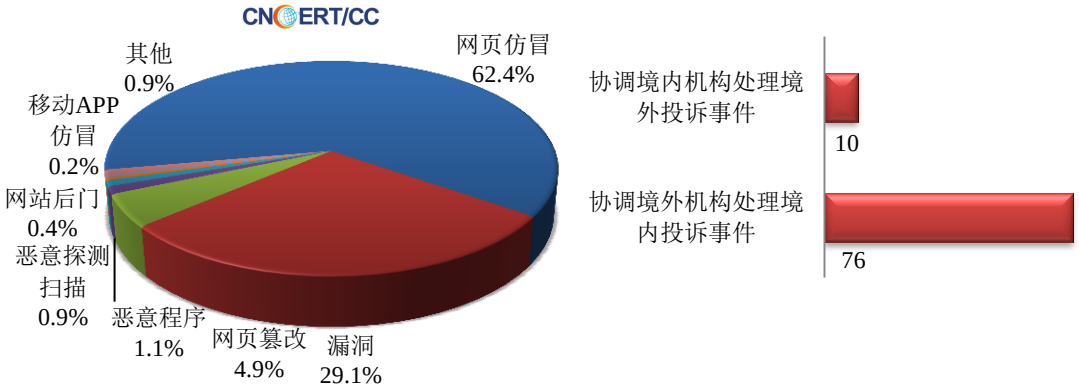
http://www.cnvd.org.cn/webinfo/list?type=4

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

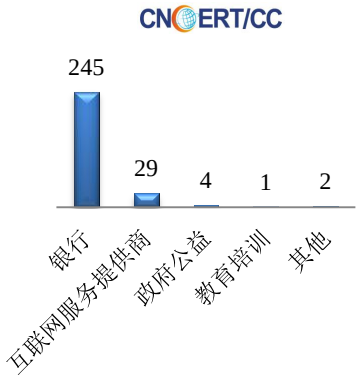
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 450 起，其中跨境网络安全事件 86 起。

本周CNCERT处理的事件数量按类型分布
(6/13-6/19)

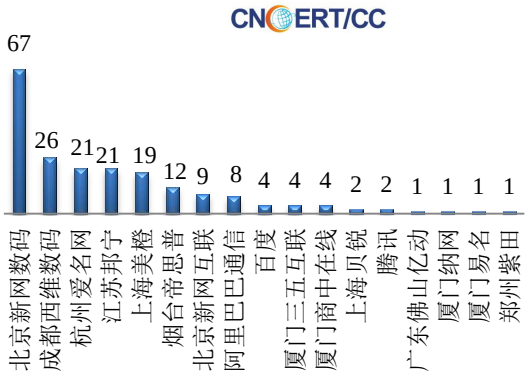


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 281 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 245 起和互联网服务提供商仿冒事件 29 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(6/13-6/19)

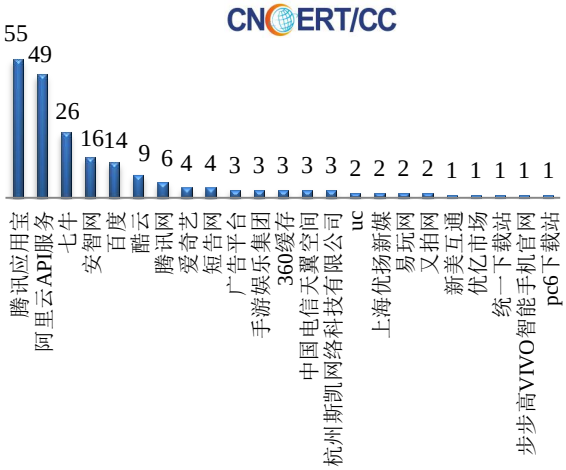


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/13-6/19)



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 211 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 (6/13-6/19)



业界新闻速递

1、第二次中美打击网络犯罪及相关事项高级别联合对话举行

人民网6月15日消息 第二次中美打击网络犯罪及相关事项高级别联合对话6月14日在京举行，国务委员、公安部部长郭声琨与美国国土安全部、司法部全权代表共同主持。郭声琨高度评价去年以来中美网络安全领域执法合作取得的进展。他说，在习近平主席和奥巴马总统高度重视和亲自推动下，双方去年在华盛顿成功举行首次联合对话并达成广泛共识，以坦诚和建设性的态度，在案件协查、信息交流和机制建设等方面开展了密集、务实的交流与合作，取得了丰硕成果。郭声琨指出，加强网络安全合作符合中美两国乃至世界各国共同利益。双方应按照两国元首指明的方向，秉承“依法、对等、坦诚、务实”的原则，切实把联合对话机制打造为中美就网络安全问题进行沟通合作的主渠道，充分发挥其引领作用，进一步增进互信、管控分歧，照顾彼此关切，开展务实合作，实现互利共赢。对话中，中美双方达成广泛共识，通过《中美打击网络犯罪及相关事项热线机制运作方案》，并同意联合发表成果清单，决定于2016年内在华盛顿举行第三次对话。

2、欧洲央行设首个即时网上警报系统应对黑客威胁

环球网6月13日消息 全球近年发生多宗针对银行系统的大型网络攻击，导致巨大损失。据香港《文汇报》6月13日报道，欧洲央行最近设立了首个即時网上警报系统，该系统可以收集欧元区内18家大型银行的数据，而且明年将该系统覆盖范围扩展至受欧洲央行管辖的130家银行。孟加拉央行2月时曾遭黑客入侵，损失8100万美元。欧洲央行随即试行实时警报系统。欧洲央行副行长米肖称，欧洲央行主要收集那些造成巨额损失以及严重影响银行声誉的“显著入侵事故”，并将分析黑客攻击的趋势，提前警告可能成为入侵目标的银行。欧洲央行还计划与美联储及英伦银行等分享情报。

3、北约正式将网络确定为战场

cnBeta.COM6月18日消息 据德国《画报（Bild）》报道,6月14日北大西洋公约组织（NATO）秘书长斯托尔滕贝格（Jens Stoltenber）在比利时布鲁塞尔的一场新闻发布上宣布，“网络”将正式成为各北约成员国的战场。这也意味着对北约成员国中任何一国的攻击将被视为对整个联盟的攻击，所有成员国应援助受攻击国家。北大西洋公约第五条规定指出，其成员国中的一国遭受攻击时将被视作对所有成员国的攻击，所有成员国应作出回应。到现在为止，这些攻击包括来自空中，海上和陆地的军事攻击。目前大多数北约成员国已经确定将网络作为一个正式的战场，并在他们的军队建立了网络安全部门。比如美国海军陆战队和美国海军今年就宣布将成立全新的网络安全部门，开展网络空间防御行动。2015年4月，拥有Fancy Bear、 Sofacy、APT28、 Sednit、Pawn Storm或Strontium等多个绰号的俄罗斯黑客组织就曾对北约军事基地发动网络攻击。

4、俄称美打响网络大战 4年前已入侵百万电脑

新浪网6月15日消息 俄罗斯东方新观察网站6月13日报道称，多年前，美国便已开始在网络空间展开积极的进攻行动。2013年以前，华盛顿的军情部门便已进行过200多次类似行动。此后，其数量不断上升、规模

也日益膨胀。某些媒体所刊载的个别文章中甚至提及，早在 4 年前，美国人便已“入侵”了全球逾百万的电脑及局域网络，并期望在位于犹他州的数据中心启用后，将“入侵”范围再扩大数倍。可以笃定地说，美国其实已打响了电磁频谱领域的世界大战，且正在全球大肆“攻城略地”。相关证据并不匮乏，其中还包括中情局特工以及国会议员的公开承认。报道称，在此背景下，美国电子硬件专家协会所起草的、题为《信息时代的电子战》秘密报告的公开，自然会引发人们的担忧。该协会成员包括美国的前防长、中情局及国家安全局等情报机构的前首脑、白宫现任专家及顾问、国会参众两院议员等。这份报告的部分内容被泄露给媒体，从中能够非常明确地窥见华盛顿在网络战中所奉行的方针：“在国家安全领域，最主要的军事战略任务是通过电磁频谱技术，确保美国的战略优势，毫无悬念地实现美国在一切领域的国家目标，完全压制对手达成自身诉求的能力……由于电磁频谱并无地缘政治以及自然意义上的边界，我们便能在任何地方积极展开使用电磁频谱技术的行动，不受现有国界的约束。”报道称，那么，美国究竟对哪些国家实施了网络战？从美国总统奥巴马的众多讲话中不难得出答案：首当其冲的非俄罗斯、伊朗、朝鲜及中国莫属。美国的一系列指令性文件，如 2015 年的国家安全战略、2014 年通过的电磁频谱战略，更是堂而皇之地为本国在网络空间积极进攻，打击白宫所认为的“敌国以及网络空间的敌对玩家”大开绿灯。

5、斯诺登：苏格兰政府一直在监控民众电话和网络活动

新浪网 6 月 14 日消息 以保护隐私、捍卫自由而闻名的爱德华·斯诺登，在 6 月 12 日泄露出的秘密文件中称，苏格兰国家安全局一直在秘密监听民众电话及其网上活动。据 The National 信息显示，苏格兰在英国大规模监听中发挥作用，苏格兰警方有权访问间谍机构收集的大规模元数据（监视目标对象的通话、电子邮件以及网站访问）。此次监视活动由苏格兰记录中心（SRC）具体执行，代号 MILKWHITE。在美国棱镜门、英国 GCHQ 窃听丑闻曝光之后，苏格兰政府的监听事件，再度引发了人们对政府监控和民众隐私被监听问题的讨论。这次代号 Milkwhite 的苏格兰窃听门，其窃听手段和美国国家安全局、英国情报机构政府通信总部（GCHQ）的做法如出一辙。苏格兰纪录中心（SRC）通过访问数以百万的通讯数据，可以掌握用户的电话记录、互联网浏览记录、电子邮件以及 facebook 等社交媒体上的信息日志。结合位置信息，密切监视一个人的所有行动，窥探互联网上所有用户的隐私。以上秘密监视行动的数据，由苏格兰警方访问管理。各界活动家、政治家，都在关注苏格兰公民的自由和安全活动，质疑 SRC 的监控行为。对此，苏格兰政府表示这是“苏格兰警察服务的经营问题”。面对同样的问题，苏格兰警方则表示“苏格兰警方不讨论情报事务。”也就是说，苏格兰拒绝对这件事做出任何解释。

6、日本将测试关键基础设施网络安全

网易 6 月 13 日消息 从明年开始，日本政府将联合该国和美国的一些重要安全机构，共同开展一项预防黑客进行网络攻击的任务，也是一场网络安全演习，目的是测试日本的公共交通、铁路以及电信系统的安全性，为奥运会的顺利举办做好准备。在该项目中，安全人员将对日本的公共交通、铁路以及电信等城市基础设施的网络系统进行一系列的渗透测试，找出这些系统中存在的可能会对城市生活造成实质危害的安全漏洞，并加以修复。据日本《读卖新闻》报道，为更好地保障东京奥运会期间的网络安全，日本政府计划在 2020 年夏季奥运会前创建“工业网络安全促进机构”，负责招聘“白帽子”精英团队，并开展网络安全方面的研发。报道称，该

机构将隶属于日本经济贸易工业部，并将配备网络安全专家，形成日本关键基础设施的防御前线。此外，该机构还将参与针对奥运会的网络战备演习，协调与大学以及美国国土安全部等国外机构之间的工作。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158