国家互联网应急中心

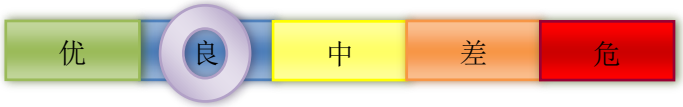
2017 年第 23 期

5 月 29 日-6 月 4 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

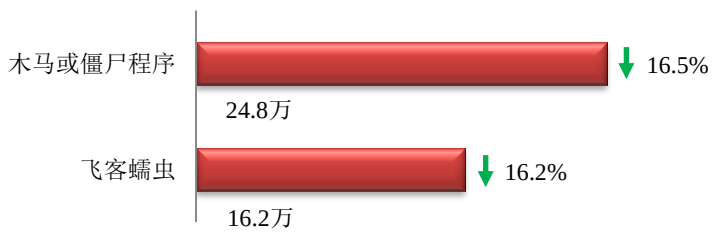


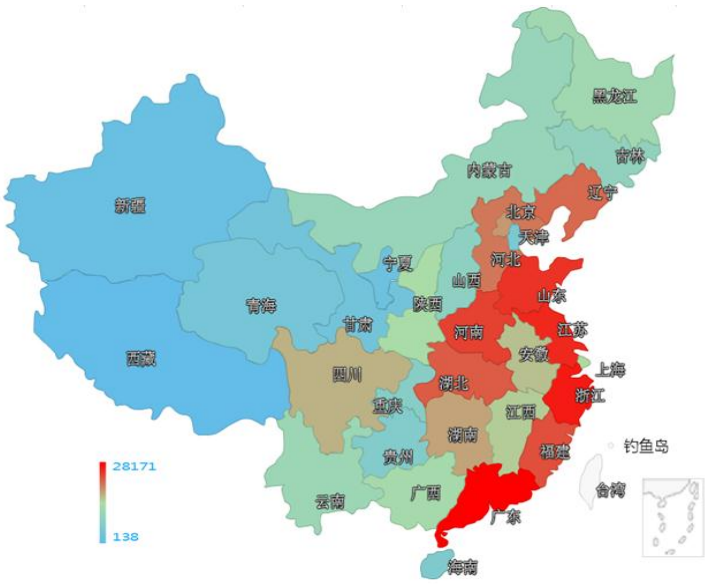
境内感染网络病毒的主机数量	•41.0万	↓ 16.4%
境内被篡改网站总数 其中政府网站数量	•1,236 •37	↓ 29.9% ↓ 22.9%
境内被植入后门网站总数 其中政府网站数量	•1,276 •64	↓ 35.7% ↓ 28.1%
针对境内网站的仿冒页面数量	•374	↑ 22.2%
新增信息安全漏洞数量 其中高危漏洞数量	•157 •54	↓ 56.7% ↓ 62.8%

═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 41.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 24.8 万以及境内感染飞客（conficker）蠕虫的主机约 16.2 万。



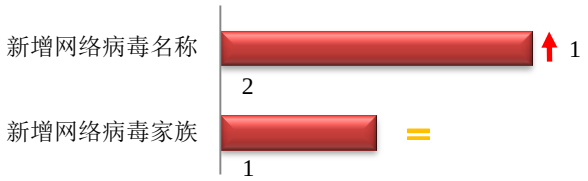


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

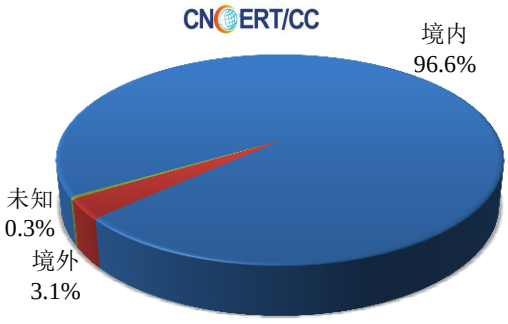
广东省	•约2.8万个（约占中国大陆总感染量的17.4%）
浙江省	•约2.6万个（约占中国大陆总感染量的16.3%）
江苏省	•约2.1万个（约占中国大陆总感染量的13.0%）

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 2 个，按网络病毒家族统计新增 1 个。

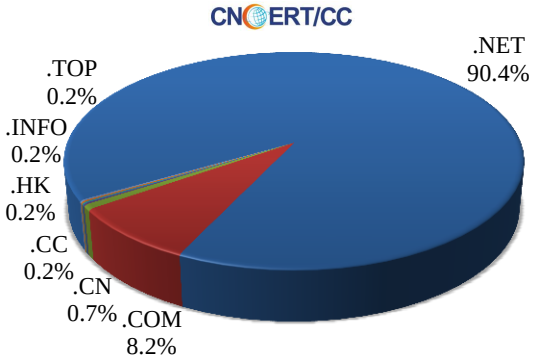


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 586 个，涉及 IP 地址 365 个。在 586 个域名中，有 3.1%为境外注册，且顶级域为.com 的约占 8.2%；在 365 个 IP 中，有约 4.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 5 个 IP。

本周放马站点域名注册所属境内外分布
(5/29-6/4)



本周放马站点域名所属顶级域的分布
(5/29-6/4)



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。

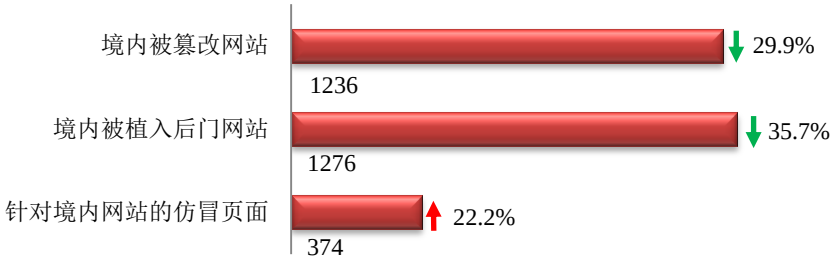
ANVA恶意地址黑名单发布地址

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。

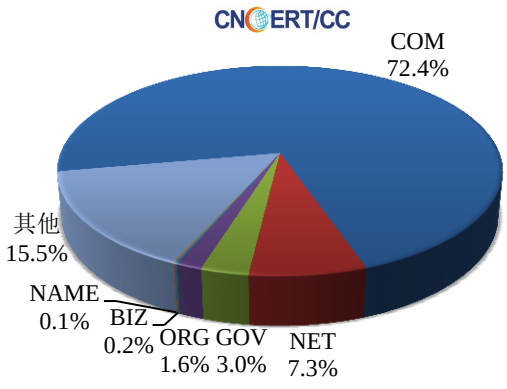
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1236 个；境内被植入后门的网站数量为 1276 个；针对境内网站的仿冒页面数量为 374。

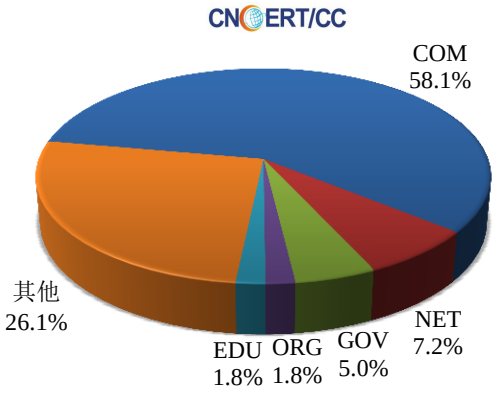


本周境内被篡改政府网站（GOV 类）数量为 37 个（约占境内 3.0%），较上周环比下降了 22.9%；境内被植入后门的政府网站（GOV 类）数量为 64 个（约占境内 5.0%），较上周环比下降了 28.1%；针对境内网站的仿冒页面涉及域名 316 个，IP 地址 156 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/29-6/4)

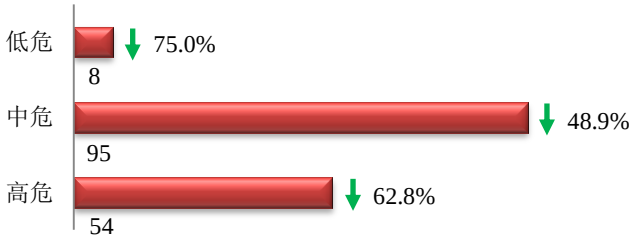


本周我国境内被植入后门网站按类型分布
(5/29-6/4)

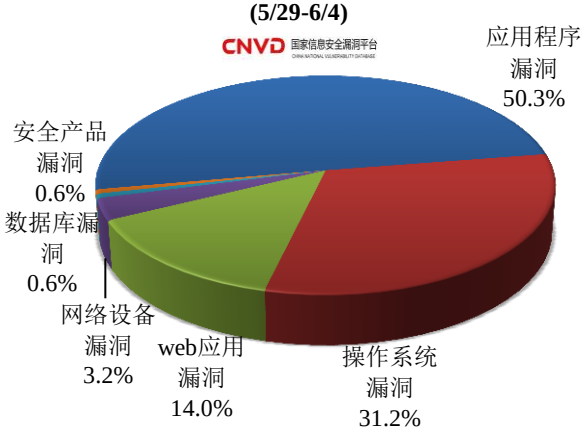


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 157 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
(5/29-6/4)



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

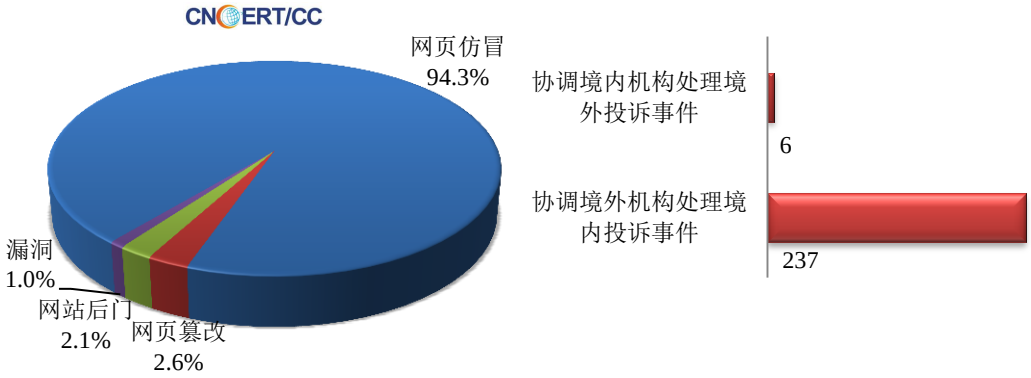
http://www.cnvd.org.cn/webinfo/list?type=4

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

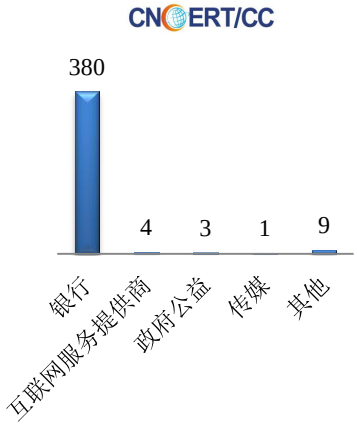
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 421 起，其中跨境网络安全事件 243 起。

本周CNCERT处理的事件数量按类型分布
(5/29-6/4)

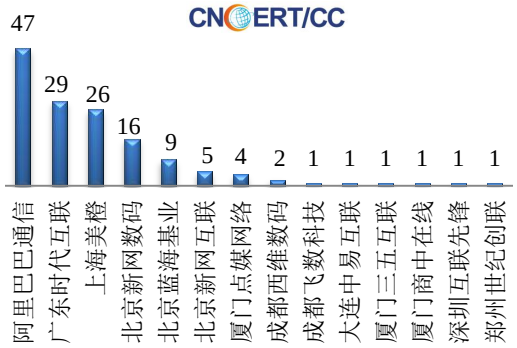


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 397 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 380 起和互联网服务提供商仿冒事件 4 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(5/29-6/4)

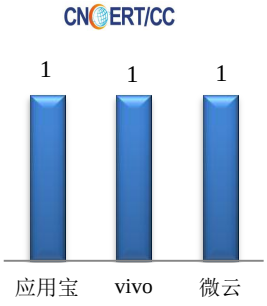


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/29-6/4)



本周，CNCERT 协调 3 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 3 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
(5/29-6/4)



业界新闻速递

1、我国首部网络安全法 6 月 1 日起正式施行

央广网 6 月 1 日消息 从 6 月 1 日起《中华人民共和国网络安全法》正式施行，这是我国第一部全面规范网络空间安全管理方面问题的基础性法律，其中重要的一方面就是要打击防止公民个人信息数据被非法获取、泄露或者非法使用。作为我国网络安全领域的基础性法律，《中华人民共和国网络安全法》的出现在我国网络安全史上具有里程碑意义，明确加强了对个人信息的保护，打击网络诈骗。国家互联网信息办公室网络安全协调局局长赵泽良说：“中国经济和社会已经高度依赖于信息网络。我们制定网络安全法就是要维护网络空间的国家安全，维护公共利益。”网络安全法现有七章 79 条，内容涵盖了网络空间主权、关键信息个人信息保护规则、关键信息基础设施重要数据跨境传输的规则等。另外，它确立了保障网络的设备设施安全，网络运行安全、网络数据安全，以及网络信息安全等各方面的基本制度。其中，针对个人信息泄露问题规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

2、公安部制定网络安全条例 关注大数据保护

金融界 6 月 1 日消息 继网络安全法今起实施之后，我国还将进一步完善国家层面的大数据保护机制，加快推进大数据安全保护法律法规和制度建设。公安部网络安全保卫局副局长李彤透露，目前公安部正在制订网络安全保护条例，拟将大数据、云平台、物联网、工控系统纳入，并进一步完善等级保护措施，重点加强对国家关键基础设施和大数据的安全保护。据悉，公安部已经组织相关单位制订了网络安全等级保护技术标准中的大数据扩展要求，拟今年正式发布实施。在大数据安全检测方面，目前公安部门已经在全国审核推荐了 160 家审计保护的机构。下一步，公安部将依托等级保护、保护联盟等开展等级保护测试指导书，提高评测能力。上半年，公安部开展安全部署工作，下半年将采取技术检测，对大数据子单位履行保护业务。此外，公安机关将严厉打击网络违法犯罪活动，并继续开展专项行动，打击贩卖个人信息的活动，铲除地下产业链。同时，加强国际合作，打击网络犯罪国际合作。同时，密码法草案 4 月向公众征求意见。国家密码管理局副局长何良生表示，密码应用要服务大数据应用和安全保护的大局。“十三五”国家密码发展中，已经有相关的研究，但在加密、数字签名等机制方面，还需要进行深入的研究和探讨。

3、美国空军即将完成各新型网络使命部队建制工作

E 安全 6 月 2 日消息 根据美国空军第二十四联队指挥官兼美国空军网络司令部司令克里斯托弗·韦格曼将军介绍，美国空军目前正加紧建设总计 39 支新型网络使命部队，其将分别负责新型网络作战手段、攻击技术以及安全规程等事务的制定与实施工作。克里斯托弗·韦格曼将军在近期召开的听证会上向立法者们解释称，“各国防使命团队将采取一系列网络安全与防御手段、技术与规程，同时还将配合其定制化网络防御传感器及工具组合，旨在立足军事基地层面实现主动防御能力。”今年 5 月 1 日，美国空军下辖的 39 支网络使命部队全部实

现初步作战能力，这些部队同时也属于国防部长办公室总计 133 支网络安全力量中的组成部分。根据五角大楼方面发表的声明，各支队伍将在 2018 年年底之前实现最终作战能力。各团队被划分为不同类别，具体包括国家特派小组、网络保护小组、网络作战小组与网络支持小组等等——其将全部面向各类进攻与防御性网络行动。

4、斯诺登证实美国向日本提供谍报监控系统

cnBeta.COM6 月 2 日消息 据日本共同社报道，“棱镜门”的爆料者爱德华•斯诺登近日在莫斯科接受了独家采访，证实了美国国安局（NSA）曾向日方提供绝密的信息监控系统，佐证了日本政府可以大量监控个人邮件及通话等。斯诺登敲响警钟称，目前正在日本参院审议的写进“合谋罪”宗旨的《有组织犯罪处罚法》修正案将正式认可大规模收集个人信息。斯诺登称，NSA 向日方提供了被称为“XKEYSCORE”的大规模监控邮件及通话等的监控系统。该系统不仅针对国内，还可收集全世界几乎所有的通讯信息。美国网络媒体“Intercept”4 月公开了据称是斯诺登曝光的 2013 年 4 月 8 日的一份文件，内容为使用提供给日本的“XKEYSCORE”，NSA 要员向上层要求在日本实施训练。斯诺登就合谋罪指出：“这是日本大规模监控的开端。日本至今为止不存在的监控文化也将成为日常。”

5、奥地利政府全力争取即时通讯监控权限，致力打击恐怖犯罪分子

HackerNews5 月 30 日消息 据外媒 5 月 29 日报道，奥地利社会民主党（SPÖ）与奥地利人民党（ÖVP）目前正全力争取公民即时通讯应用程序的监控权限，致力打击恐怖犯罪分子袭击活动。安全专家表示，奥地利政府还将于今年 10 月国会选举结束后取消匿名移动设备 SIM 卡的使用。曼彻斯特竞技场于近期发生的恐怖袭击事件，推动了奥地利政府针对打击恐怖袭击活动的国家监督措施的讨论。联邦宪法保护与反恐局局长 Peter Gridling 表示，恐怖袭击活动迫在眉睫且具有显著破坏风险。ÖVP 于今年 3 月提交了一份针对以往数据保留的后续措施并提议更新法律，以便监控公民通讯应用程序 Whatsapp 与 Skype。目前，奥地利政府已批准一项安全方案，允许政府监控公民 Skype 与 Whatsapp 使用权限。据悉，该方案措施存在一个主要问题，即在不使用加密算法后门的监控软件情况下，无法实现端到端加密通信的监控。另外，奥地利政府正协商讨论另一项安全措施，针对匿名移动设备 SIM 卡的最终调节。

6、Hadoop 服务器人为配置不当，或致全球数据泄露达 5,120 TB

HackerNews6 月 4 日消息 网络犯罪分子近期开始针对配置不当的 Hadoop Clusters 与 CouchDB 服务器展开攻击活动。目前全球因 Hadoop 分布式文件系统（HDFS）配置不当导致的数据泄露或达 5,120 TB。据搜索引擎 Shodan 分析显示，全球将近 4500 台设备因使用 Hadoop 分布式文件系统（HDFS）时配置不当，致使服务器出现数据泄露现象，这些服务器主要位于美国（1,900）、中国（1,426）、德国（129）与韩国（115）等。调查显示已暴露的 HDFS 多数托管于云端，其中涉及亚马逊的有 1,059 个服务器、阿里云 507 个服务器。据 Shodan 创始人约翰 • 马瑟利（John Matherly）透露，今年早些时候出现的针对数据库的勒索软件仍在发生，不仅危害着 MongoDB 同时也影响 HDFS 的部署。目前，约翰 • 马瑟利在线分享了如何使用搜索引擎 Shodan 复制检测设备的所有必要步骤。此外，安全专家建议企业设备管理人员在安全模式下，按照指令说明正确配置 Hadoop 服务器。

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 2016 年，CNCERT 与 69 个国家和地区的 185 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：张腾

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158