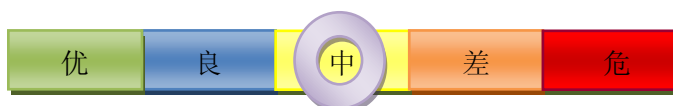




CNCERT互联网安全威胁报告

2013 年 7 月

总第 31 期



摘要：

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2013 年 7 月，互联网网络安全状况整体评价为中。主要数据如下：

- 境内感染网络病毒的终端数为245万余个；
- 境内被篡改网站数量为8244个，其中被篡改政府网站数量为606个；境内被植入后门的网站数量为9940个，其中政府网站有463个；针对境内网站的仿冒页面数量为2872个；
- 国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞714个，其中，高危漏洞242个，可被利用来实施远程攻击的漏洞有647个。

热线电话：+8610 82990999（中文），82991000（英文） 传真：+8610 82990399

电子邮件：cncert@cert.org.cn

PGP Key: <http://www.cert.org.cn/cncert.asc>

网址：<http://www.cert.org.cn/>

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 1999 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。

2003 年，CNCERT 在全国 31 个省、直辖市、自治区成立分中心，形成了全国性的互联网网络安全信息共享、技术协同能力。目前，CNCERT 作为国家公共互联网网络安全应急体系的核心技术协调机构，在社会网络安全防范机构、公司、大学、科研院所的支撑和支援下，在协调骨干网络运营单位应急组织、域名服务机构应急组织等国内网络安全应急组织共同处理网络安全事件方面发挥着重要作用。

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 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

CNCERT 的业务能力主要包括：

- **事件发现：**CNCERT 通过多种渠道发现网络攻击威胁和网络安全事件，包括网络安全事件自主发现，国内外合作伙伴的数据和信息共享，以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等。
- **通报预警：**CNCERT 依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等。为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。
- **应急处置：**对于自主发现和接收到的事件报告，CNCERT 筛选危害较大的事件进行及时响应和协调处置，重点处置的事件包括：影响互联网运行安全的事件、波及较大范围互联网用户的事件、涉及重要政府部门和重要信息系统的事件、用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

版权及免责声明

《CNCERT 互联网安全威胁报告》(以下简称“报告”)为国家计算机网络应急技术处理协调中心(简称国家互联网应急中心, CNCERT 或 CNCERT/CC)的电子刊物, 由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处, 其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理, 未经 CNCERT 同意, 任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性, 其中的信息、数据、图片等仅供参考, 不作为您个人或您企业实施安全决策的依据, CNCERT 不承担与此相关的一切法律责任。

编者按:

感谢您阅读《CNCERT 互联网安全威胁报告》, 如果您发现本报告存在任何问题, 请您及时与我们联系, 来信地址为: cncert@cert.org.cn。

本月网络安全基本态势分析

2013 年 7 月，互联网网络安全状况整体评价为中。我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。在我国互联网网络安全环境方面，除境内感染恶意代码的主机数量、针对境内网站的仿冒页面数量较上月有所下降外，其他各类网络安全事件数量均有不同程度的增长。总体上，7 月公共互联网网络安全态势较上月略有恶化。

◆ 基础网络安全

2013 年 7 月，我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未出现省级行政区域以上的造成较大影响的基础网络运行故障，未发生较大以上网络安全事件，但存在一定数量的流量不大的针对互联网基础设施的拒绝服务攻击事件。

◆ 重要联网信息系统安全

政府网站和金融行业网站仍然是不法分子攻击的重点目标，安全漏洞是重要联网信息系统遭遇攻击的主要内因。本月，监测发现境内被篡改政府网站数量为 606 个，较上月 610 个下降 0.7%，占境内被篡改网站比例由 7.6%减少到 7.4%；境内被植入后门的政府网站数量为 463 个，较上月的 360 个增长 28.6%，占境内被植入后门网站比例由 4.1%上升到 4.7%；针对境内网站的仿冒页面数量为 2872 个，较上月的 3160 个下降 9.1%，这些仿冒页面绝大多数是仿冒我国金融机构和著名社会机构。

本月，国家信息安全漏洞共享平台（CNVD¹）共协调处置了 400 起涉及我国政府部门以及银行、民航等重要信息系统部门以及电信、

注1：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，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

传媒、公共卫生、教育等相关行业的漏洞事件。这些事件大多数是网站程序存在 SQL 注入、弱口令以及权限绕过等漏洞，也有部分是信息系统采用的应用软件存在漏洞，可能导致获取后台系统管理权限、信息泄露、恶意文件上传等危害，甚至会导致主机存在被不法分子远程控制的风险。此外，“McAfee ePolicy Orchestrator 多个漏洞”、“Advanced User Tagging Module for vBulletin 'usertag.php' 跨站脚本漏洞”、“YardRadius src/log.c 消息记录格式串漏洞”、“MLM SQL 注入漏洞”等 0day 漏洞影响较为严重，互联网上已经出现针对上述漏洞的攻击代码。

◆ 公共网络环境安全

2013 年 7 月，根据 CNCERT 的监测数据和通信行业报送数据，我国互联网网络安全环境主要指标情况如下：①网络病毒²活动情况方面，境内感染网络病毒的终端数为 245 万余个，较上月下降 15.3%；在捕获的新增网络病毒文件³中，按网络病毒名称⁴统计新增 285 个，较上月下降 22.6%，按网络病毒家族⁵统计新增 3 个，较上月增加 1 个；各安全企业报送的网络病毒捕获数量中，瑞星公司截获的病毒数量较上月增长 9.6%，新增病毒数量较上月大幅增长 57.4%；安天公司捕获的样本总数较上月大幅下降 61.2%，新增病毒种类较上月大幅下降 80.7%；金山公司报送的计算机病毒事件数量较上月下降 3.7%。②网站安全方面，本月境内被篡改网站数量为 8244 个，较上月增长 3.0%；境内被植入后门

注2：一般情况下，恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。其中，网络病毒是特指有网络通信行为的恶意代码。7 月，CNCERT 在对恶意代码进行抽样监测时，对 403 种木马家族和 85 种僵尸程序家族进行了抽样监测。

注3：网络病毒文件是网络病毒的载体，包括可执行文件、动态链接库文件等，每个文件都可以用哈希值唯一标识。

注 4：网络病毒名称是通过网络病毒行为、源代码编译关系等方法确定的具有相同功能的网络病毒命名，完整的命名一般包括：分类、家族名和变种号。一般而言，大量不同的网络病毒文件会对应同一个网络病毒名称。

注 5：网络病毒家族是具有代码同源关系或行为相似性的网络病毒文件集合的统称，每个网络病毒家族一般包含多个变种号区分的网络病毒名称。

的网站数量为 9940 个，较上月增长 13.4%；针对境内网站的仿冒页面有 2872 个，较上月下降 9.1%；各安全企业报送的网页挂马情况中，浪潮公司报送的网页挂马事件数量较上月增长 0.7%，安天公司报送的网页挂马事件数量较上月增长 1.7%，奇虎 360 公司报送的网页挂马事件数量较上月大幅下降 59.6%。③安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 714 个，较上月增长 21.0%。其中高危漏洞 242 个，较上月增长 12.6%；可被利用来实施远程攻击的漏洞有 647 个，较上月增长 22.8%。④垃圾邮件方面，从中国互联网协会垃圾邮件受理举报中心报送数据看，本月共接收 8890 件垃圾邮件事件举报，较上月增长 13.0%。⑤事件受理方面，CNCERT 接收到网络安全事件报告 2744 件，较上月增长 17.3%。数量最多的分别是漏洞类事件 1060 件、网页仿冒类事件 1018 件。

本月重点网络安全信息

◆ 2013 年中国计算机网络安全年会在呼和浩特召开

2013 年 7 月 4 日，2013 年中国计算机网络安全年会（第 10 届）在内蒙古呼和浩特市召开。工业和信息化部张峰总工程师出席大会开幕式并作大会主旨报告，张峰简要回顾了近年来互联网和通信行业主管部门工业和信息化部维护网络安全的方针和工作，并进一步对信息通信行业提出做好网络安全工作的五点要求。一是加强网络安全工作联动，深化跨部门跨行业协调配合。二是加强防护应急能力建设，强化网络安全环境综合治理。三是加强新型网络安全威胁的研究投入，探求有效应对措施与保障技术。四是加强网络安全国际交流合作，推动网络安全领域经验共享。五是加强网络安全宣传教育，促进网络安全防范意识与知识水平提高。国家互联网应急中心副总工程师杜跃进应邀在大会上作了题为“新时代网络安全的应对之路”的报告。

2013 年中国计算机网络安全年会由国家互联网应急中心主办，历经十年发展，目前已成为国内外网络安全领域进行技术业务交流的重要平台。工业和信息化部总工程师张峰、内蒙古自治区政府副秘书长曹晓斌、内蒙古自治区通信管理局局长乌力吉、工业和信息化部通信保障局副局长熊四皓、大会组委会主席国家互联网应急中心主任黄澄清、中国通信学会副理事长兼秘书长张新生、科学技术部高新技术发展及产业司处长王春恒、中国电子学会副秘书长林润华、国家互联网应急中心副主任云晓春等贵宾出席了开幕式。来自政府和重要信息系统部门、行业企业、高校和科研院所等单位的代表共四百余人参加了本次会议。

◆ 45 家单位荣获第五届 CNCERT 网络安全应急服务支撑单位称号

为强化公共互联网网络安全应急技术体系建设，促进我国网络安全应急服务的规范化和本地化，结合互联网网络安全应急工作以及国

内网络安全服务行业的发展需要，CNCERT 于 2013 年 5 月份启动了第五届 CNCERT 网络安全应急服务支撑单位的评选工作。评选分为初审和现场答辩两个环节。共计收到 65 个单位的申请材料，有 54 个单位通过初审。2013 年 7 月 3 日，CNCERT 在内蒙古自治区呼和浩特市举行了第五届 CNCERT 网络安全应急服务支撑单位评选会议。来自工业和信息化部、中国信息安全认证中心、CNCERT、国家网络安全技术研究所的相关专家组成了评选委员会，从企业实力、应急技术能力、应急服务规范、支撑 CNCERT 工作情况等方面出发，遵循公开、公平、公正的原则，对通过初审的参选单位进行了细致的评估和审查。会议最终评选出 8 个国家级网络安全应急服务支撑单位和 37 个省级网络安全应急服务支撑单位。

CNCERT 自 2004 年开始启动了“CNCERT 网络安全应急服务支撑单位”的选拔工作。经过九年发展，应急服务支撑单位已成为我国互联网网络安全应急体系的重要组成部分，为维护互联网网络安全做出了积极贡献，在国家重大活动期间为保障网络安全发挥了重要的技术支撑作用。

◆ CNCERT 组织召开第一届中日韩互联网应急年会

2013 年 7 月 30 日至 31 日，中、日、韩三国的国家互联网应急中心（CERT）领导及操作层面代表相聚在中国上海，召开了第一届中日韩互联网应急年会。会议上，三方回顾了近年来三方在重大安全事件上的合作及自 2005 年起生效的操作标准，提出进一步加强合作，以达到更高效地协调处理重大网络安全事件的目标。

几年来，CNCERT、日本国家互联网应急中心(JPCERT/CC)和韩国国家互联网应急中心(KrCERT/CC)密切协作，成功处置多起涉及中日韩的黑客攻击事件及其它重大网络安全事件，并遏制了危机的蔓延。三方 7*24 小时的热线机制在及时处理重大事件、消除误会等方面发挥了重大作用。

最近，其它地区（如美国和俄罗斯之间）也在积极开展 CERT 组织之间的合作活动。中日韩三方对这样的举措表示欢迎，以此作为建

立互信机制的一个重要方面。中日韩三方 CERT 对其他地区为降低网络安全风险做出的努力表示肯定，并重申三方继续建设区域合作最佳做法的任务和目标，强调要继续在重大网络安全事件上进行协作，提高网络安全水平，改善网络环境，继续为降低地区间网络安全风险做出贡献。

◆ 关于 Android 系统存在签名验证绕过高危漏洞情况的通报

7 月 8 日，CNVD 收录了 Android 操作系统存在一个签名验证绕过的高危漏洞(编号：CNVD-2013-28152)。攻击者利用该漏洞可以篡改合法应用程序的安装文件并植入恶意代码并绕过 Android 系统数字签名验证，进而大规模传播手机恶意程序。受该漏洞影响的 Android 系统版本包括 Android 1.6 至 Android 4.2.2 之间相关版本。CNCERT 研判认为，随着漏洞信息的逐步披露和扩散，有可能被利用发起恶意程序制造和传播的大规模攻击活动，严重威胁 Android 智能终端用户安全。

根据互联网上公开报道称，Android 操作系统生产厂商——谷歌公司确认该漏洞的存在，但未公开漏洞的详细信息。CNCERT 在获知漏洞情况后询问了国内部分 Android 系统手机厂商，相关厂商尚未针对该漏洞采取技术应对措施。相关建议如下：（一）手机厂商可自行对待出厂产品采取一些临时技术措施进行防范，同时对已售产品提供更新程序，以备用户自行下载或在线完成系统更新。（二）应用商店应加强应用程序安全检测，及时发现伪造合法签名的恶意程序。按照工业和信息化部《移动互联网恶意程序监测与处置机制》，配合 CNCERT 做好应用程序的鉴定和处置相关工作。（三）Android 智能终端用户需提高警惕，避免下载不明来源或未知签名的应用程序，如发现应用程序存在恶意行为，请及时卸载并举报。

◆ 关于 Apache Struts2 远程命令执行高危漏洞和开放重定向高危漏洞的情况通报

7 月，CNVD 收录了 Apache Struts 存在一个远程命令执行漏洞

和一个开放重定向漏洞利用漏洞，可发起远程攻击，轻则窃取网站数据信息，严重的可取得网站服务器控制权，构成信息泄露和运行安全威胁。

CNVD 对远程命令执行漏洞(CNVD-2013-28972)和开放重定向漏洞 (CNVD-2013-28979) 的评级为“高危”，由于 `redirect:` 和 `redirectAction:` 此两项前缀为 Struts 默认开启功能，因此 Apache Struts 2.3.15.1 以下版本受到漏洞影响。厂商已经发布 Apache Struts 2.3.15.1 以修复此安全漏洞，建议 Struts 用户及时升级到最新版本。CNCERT/CNVD 将继续跟踪事件后续情况，做好国内相关用户受影响情况的监测和预警工作。同时，请国内相关单位做好信息系统应用情况排查工作，及时采取措施。

◆ 安卓签名漏洞疯狂爆发 正版应用遭遇“寄生虫”

7 月下旬，利用 Android 操作系统签名漏洞的 Skullkey 扣费木马犹如“寄生虫”般寄生于正常 APP 中并开始疯狂传播。CNCERT 监测发现在第三方应用市场“安丰市场”中存在 6645 个利用签名漏洞被植入 Skullkey 扣费木马的恶意 APP。Skullkey 扣费木马利用 Android 操作系统签名漏洞，可向正常 APP 中植入恶意程序，在用户不知情的情况下，通过后台发送扣费短信，并屏蔽回执短信。此外，该木马还可以在后台读取手机中的通讯录信息，同时具备向联系人发送广告或欺诈短信的权限。

CNCERT 通过对“安丰市场”中存在的 6645 个利用签名漏洞被植入 Skullkey 扣费木马的恶意 APP 进行分析发现，经济类 APP 和安全类 APP 逐渐成为黑客入侵的新目标。根据“安丰市场”网站的下载次数统计显示，这些恶意 APP 的累计下载总次数已超过 200 万次。CNCERT 已第一时间通知“安丰市场”下架所有 6645 个恶意 APP，并彻底删除相应的 APP 下载链接。同时，将 6645 个恶意 APP 信息和相应 URL 下载链接通过中国反网络病毒联盟（ANVA）向全社会进行黑名单发布。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2013 年 7 月，境内感染网络病毒的终端数为 245 万余个。其中，境内被木马或僵尸程序控制的主机 IP 为 112 万余个，环比下降 8.2%；境内感染飞客蠕虫的主机 IP 为 133 万余个，环比下降 20.5%。

➤ 木马僵尸网络监测数据分析

2013 年 7 月，CNCERT 监测发现境内 112 万余个 IP 地址对应的主机被木马或僵尸程序控制，按地区分布感染数量排名前三位的分别是广东省、江苏省、浙江省。

木马或僵尸网络控制服务器 IP 总数为 14,681 个。其中，境内木马或僵尸网络控制服务器 IP 数量为 11,514 个，按地区分布数量排名前三位的分别为广东省、江苏省、云南省。境外木马或僵尸网络控制服务器 IP 数量为 3,167 个，主要分布于美国、韩国、中国香港。其中，位于葡萄牙的控制服务器控制了境内 467,875 个主机 IP，控制境内主机 IP 数量居首位，其次是位于美国和韩国的 IP 地址，分别控制了境内 342,499 个和 100,701 个主机 IP。

➤ 飞客蠕虫监测数据分析

2013 年 7 月，CNCERT 监测到全球互联网 1316 万余个主机 IP 地址感染飞客蠕虫，按国家或地区分布感染数量排名前三位的分别是中国大陆、印度、巴西。

境内感染飞客蠕虫的主机 IP 为 133 万余个，按地区分布感染数量排名前三位的分别是广东省、浙江省、江苏省。

➤ 网络病毒捕获和传播情况

2013 年 7 月，CNCERT 捕获了大量新增网络病毒文件，其中按网络病毒名称统计新增 285 个，按网络病毒家族统计新增 3 个。

网络病毒主要针对一些防护比较薄弱,特别是访问量较大的网站通过网页挂马的方式进行传播。当存在安全漏洞的用户主机访问了这些被黑客挂马的网站后,会经过多级跳转暗中连接黑客最终“放马”的站点下载网络病毒。2013 年 7 月,CNCERT 监测发现排名前十的活跃放马站点域名和活跃放马站点 IP 如表 1 所示。

表 1: 2013 年 7 月活跃放马站点域名和 IP

排序	活跃放马站点域名	排序	活跃放马站点 IP
1	download.cpubln.com	1	122.224.9.35
2	hdmltextvoice.net	2	58.193.0.28
3	www.nbxzywzsnb.com	3	121.10.105.29
4	down.touming5.com	4	204.45.58.36
5	pinterest.com.reports0701.net	5	61.132.227.34
6	qq.liukejun.com	6	61.132.227.23
7	www.go890.com	7	121.10.105.96
8	hi.liukejun.com	8	115.238.237.53
9	dx.kuaibolite.com	9	183.61.189.91
10	www.ah908.com	10	119.147.141.61

网络病毒在传播过程中,往往需要利用黑客注册的大量域名。2013 年 7 月,CNCERT 监测发现的放马站点中,通过域名访问的共涉及有 304 个域名,通过 IP 直接访问的共涉及有 233 个 IP。在 304 个放马站点域名中,于境内注册的域名数为 68 个(约占 22.4%),于境外注册的域名数为 163 个(约占 53.6%),未知注册商所属境内外信息的有 73 个(约占 24.0%)。放马站点域名所属顶级域名排名前 5 位的具体情况如表 2 所示。

表 2: 2013 年 7 月活跃恶意域名所属顶级域名

排序	顶级域名 (TLD)	类别	恶意域名数量
1	.COM	通用顶级域名 (gTLD)	159
2	.CN	中国顶级域名 (ccTLD)	39
3	.KR	韩国顶级域名 (ccTLD)	32
4	.NET	通用顶级域名 (gTLD)	21
5	.INFO	通用顶级域名 (gTLD)	12

◆ 网站安全数据分析

➤ 境内网站被篡改情况

2013 年 7 月, 境内被篡改网站的数量为 8244 个, 境内被篡改网站数量按地区分布排名前三位的分别是北京市、浙江省、上海市。按网站类型统计, 被篡改数量最多的是 COM 域名类网站, 其多为商业类网站; 值得注意的是, 被篡改的 GOV 域名类网站有 606 个, 占境内被篡改网站的比例为 7.4%。

截至 7 月 31 日仍未恢复的部分被篡改政府网站⁶如表 3 所示。

表 3: 截至 7 月 31 日仍未恢复的部分政府网站

被篡改网站	所属部门或地区
www.xxsjj.gov.cn	安徽省宿州市
da.whx.gov.cn	安徽省芜湖市
wjlongmen.huizhou.gov.cn	广东省惠州市
www.tdjyw.gov.cn	广西壮族自治区百色市
wxny.gov.cn	广西壮族自治区来宾市
nyzw.gov.cn	贵州省毕节市
www.gzpxmtj.gov.cn	贵州省六盘水市
www.xhgaj.gov.cn	河北省邢台市
mqgt.gov.cn	河南省商丘市
gyczs.syxxz.gov.cn	湖北省荆门市
tqzfcg.tq.gov.cn	内蒙古自治区兴安盟
www.jxjtw.gov.cn	山东省日照市
www.jxfg.gov.cn	山东省日照市

注6: 政府网站是指英文域名以“.gov.cn”结尾的网站, 但不排除个别非政府部门也使用“.gov.cn”的情况。表格中仅列出了被篡改网站或被挂马网站的域名, 而非具体被篡改或被挂马的页面 URL。

被篡改网站	所属部门或地区
rzdm.gov.cn	山东省日照市
www.rzdm.gov.cn	山东省日照市
wgjsj.gov.cn	陕西省咸阳市
www.lhxzw.gov.cn	云南省德宏傣族景颇族自治州
zjjiashan.lss.gov.cn	浙江省嘉兴市

➤ 境内网站被植入后门情况

2013 年 7 月，境内被植入后门的网站数量为 9940 个。境内被植入后门的网站数量按地区分布排名前三位的分别是北京市、广东省、浙江省。按网站类型统计，被植入后门数量最多的是 COM 域名类网站，其多为商业类网站；值得注意的是，被植入后门的 GOV 域名类网站有 463 个，占境内被植入后门网站的比例为 4.7%。

2013 年 7 月，境外 4481 个 IP 地址通过植入后门对境内 7961 个网站实施远程控制。其中，境外 IP 地址主要位于美国、中国香港和韩国等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，位于美国的 IP 地址共向境内 1719 个网站植入了后门程序，侵入网站数量居首位，其次是位于中国香港和位于韩国的 IP 地址，分别向境内 1413 个和 842 个网站植入了后门程序。

➤ 境内网站被仿冒情况

2013 年 7 月，CNCERT 共监测到针对境内网站的仿冒页面有 2872 个，涉及域名 1767 个，IP 地址 543 个，平均每个 IP 地址承载 5 个仿冒页面。在这 543 个 IP 中，境外占 83.8%，主要位于美国和中国香港。

◆ 漏洞数据分析

2013 年 7 月，CNVD 收集整理信息系统安全漏洞 714 个。其中，高危漏洞 242 个，可被利用来实施远程攻击的漏洞有 647 个。受影响的软硬件系统厂商包括 Apache、Adobe、Cisco、Google、HP、IBM、Linux、Microsoft、Oracle 等。

根据 CNVD 的代码验证结果，本月共出现了 168 个 0day 漏洞，

其中影响较为严重的是“McAfee ePolicy Orchestrator 多个漏洞”、“Advanced User Tagging Module for vBulletin 'usertag.php' 跨站脚本漏洞”、“YardRadius src/log.c 消息记录格式串漏洞”、“MLM SQL 注入漏洞”。互联网上已经出现针对上述漏洞的攻击代码，为避免受到漏洞影响，请广大用户及时采取补丁修复、提高主机操作系统安全防范等级等防御措施。

根据漏洞影响对象的类型，漏洞可分为操作系统漏洞、应用程序漏洞、WEB 应用漏洞、数据库漏洞、网络设备漏洞（如路由器、交换机等）和安全产品漏洞（如防火墙、入侵检测系统等）。本月 CNVD 收集整理的漏洞中，按漏洞类型分布排名前三位的分别是应用程序漏洞、WEB 应用漏洞、操作系统漏洞。

◆ 网络安全事件接收与处理情况

➤ 事件接收情况

2013 年 7 月，CNCERT 收到国内外通过电子邮件、热线电话、网站提交、传真等方式报告的网络安全事件 2744 件（合并了通过不同方式报告的同一网络安全事件，且不包括扫描和垃圾邮件类事件），其中来自国外的事件报告有 68 件。

在 2744 件事件报告中，排名前三位的安全事件分别是漏洞、网页仿冒、恶意代码。

➤ 事件处理情况

对国内外通过电子邮件、热线电话、传真等方式报告的网络安全事件，以及自主监测发现的网络安全事件，CNCERT 每日根据事件的影响范围和存活性、涉及用户的性质等因素，筛选重要事件进行协调处理。

2013 年 7 月，CNCERT 总部以及各省分中心共同协调处理了 2705 件网络安全事件。各类事件处理数量中漏洞、网页仿冒类事件处理数量较多。

附：术语解释

● 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

● 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

● 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意程序分类说明如下：

1. 特洛伊木马（Trojan Horse）

特洛伊木马（简称木马）是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马⁷、网银木马⁸、窃密木马⁹、远程控制木马¹⁰、流量劫持木马¹¹、下载者木马¹²和其它木马七类。

2. 僵尸程序（Bot）

僵尸程序是用于构建大规模攻击平台的恶意代码。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、Http 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

3. 蠕虫（Worm）

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意代码。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕

注7：盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。

注8：网银木马是用于窃取用户网银、证券等账号的木马。

注9：窃密木马是用于窃取用户主机中敏感文件或数据的木马。

注10：远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。

注11：流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。

注12：下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒（Virus）

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的恶意代码。

5. 其它

上述分类未包含的其它恶意代码。

随着黑客地下产业链的发展，互联网上出现的一些恶意代码还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意代码的主要用途参照上述定义进行归类。

● 僵尸网络

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件等。

● 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

● 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

● 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

● 网页挂马

网页挂马是通过在网页中嵌入恶意代码或链接，致使用户计算机在访问该页面时被植入恶意代码。

● 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器的攻击事件。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（二）收件人无法拒收的电子邮件；（三）隐藏发件人身份、地址、标题等信息的电子邮件；（四）含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

- 路由劫持

路由劫持是通过欺骗方式更改路由信息，以导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，以达到不正当的目的。