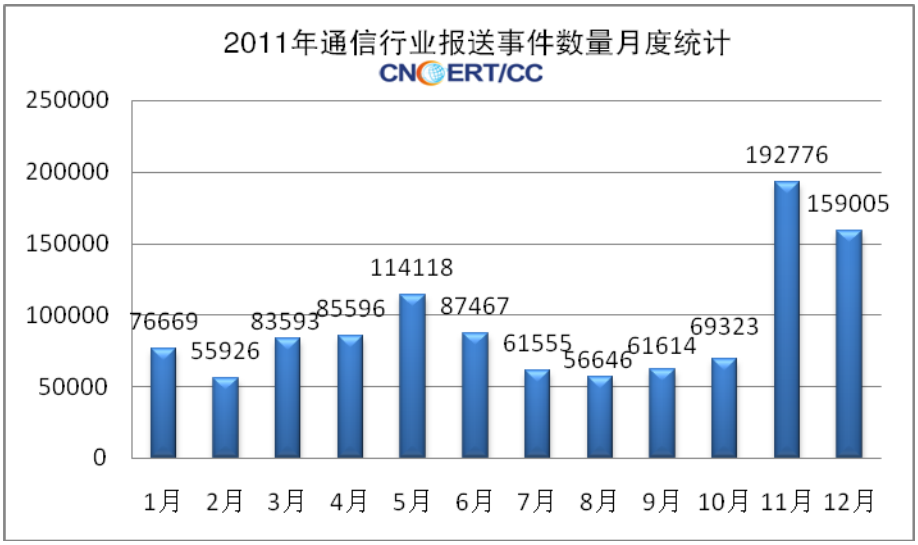
7 网络安全信息通报情况

7.1 互联网网络安全信息通报

2011 年 CNCERT 作为通信行业内的通报中心，协调组织各地通信管理局、中国互联网协会、基础电信运营企业、域名注册管理和服务机构、非经营性互联单位、增值电信业务经营企业以及网络安全企业开展通信行业网络安全信息通报工作。

按照《互联网网络安全信息通报实施办法》规定，各信息通报工作单位每月前五个工作日向 CNCERT 报送前一个月的月度汇总信息；对于监测和掌握的其它重要事件信息和预警信息则需及时报送。2011 年，我中心共收到各单位报送的月度信息 619 份，事件信息和预警信息 962 份。经过全面汇总、整理各类上报信息，结合 CNCERT 网络安全监测和事件处置情况，对网络安全态势和影响较大的网络安全事件进行综合分析研判，全年共编制并向各单位发送《互联网网络安全信息通报》46 期，内容涵盖基础 IP 网络、IP 业务、域名系统、相关单位自有业务系统和公共互联网环境等多方面，为我国政府和重要信息系统、电信运营企业、互联网企业和广大互联网用户进一步提升网络安全工作水平，加强网络安全意识，提供了及时有效的预警和指导。

根据各互联网网络安全信息通报工作单位报送的月度汇总信息[16]，2011 年通信行业报送的网络安全事件数量月度统计如图 7-1 所示。



[16] 各省通信管理局、基础电信业务经营者集团公司汇总的信息主要来自 CNCERT 各省分中心以及基础电信业务经营者省公司/子公司，月度汇总信息事件统计以上述单位报送为基准，未包括域名注册管理和服务机构、增值电信业务经营企业、非经营性互联单位以及安全企业报送的月度信息。

图 7-1　2011 年通信行业事件月度报送数量统计

对上述事件按基础 IP 网络、IP 业务、运营企业自有业务系统、域名系统、公共互联网环境五大类别进行统计，各类别的事件报送数量如图 7-2 所示。可以看到，2011 报送的事件类型仍然主要为公共互联网环境以及基础 IP 网络中的网络安全事件，事件数量均超过去年 2 倍。

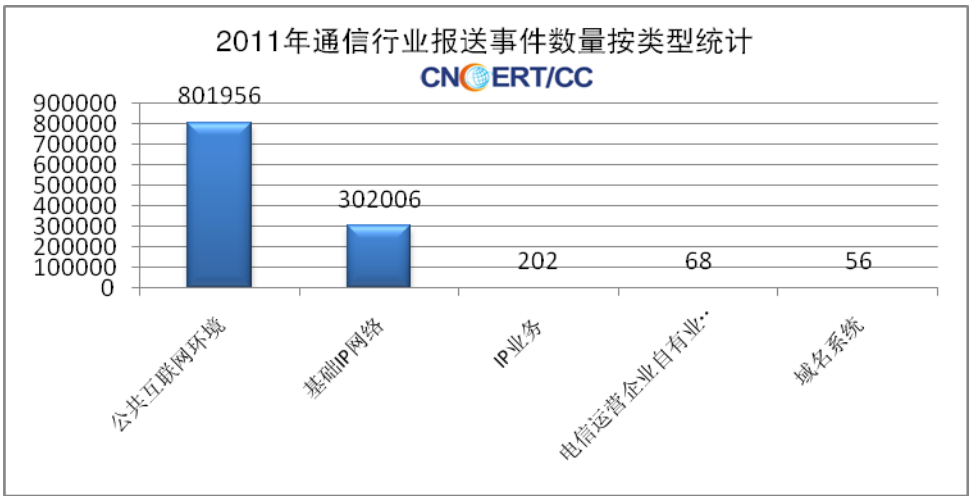


图 7-2　2011 通信行业报送事件数量的分类统计

CNCERT 对公共互联网环境中的网络安全事件按 13 个小类进行统计，分别是计算机病毒事件、蠕虫事件、木马事件、僵尸程序事件、域名劫持事件、网页仿冒事件、网页篡改事件、网页挂马事件、拒绝服务攻击事件、后门漏洞事件、非授权访问事件、垃圾邮件事件和其他网络安全事件。如图 7-3 所示，木马事件数量最多，占公共互联网环境事件总数的比例为 36.6%；其他数量较多的事件类型还有：僵尸程序事件、蠕虫事件和垃圾邮件事件，分别占 22.7%、18.7%和 17.4%。

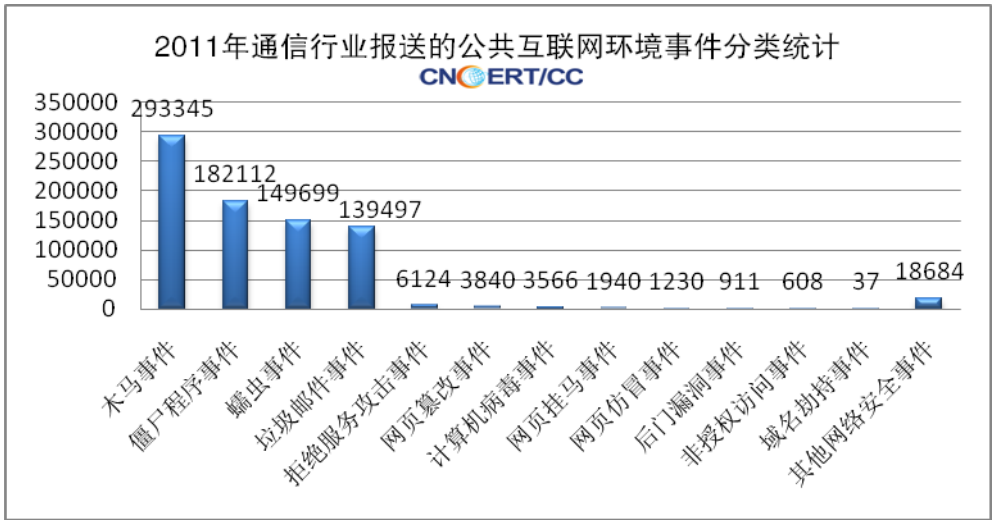


图 7-3　2011 年通信行业报送的公共互联网环境事件数量的分类统计

除每月汇总和发布月度情况通报外，对于报送的重要事件信息和预警信息，CNCERT 会通过通报增刊和漏洞通报专刊的方式向信息通报工作单位发布。对于一些涉及政府和重要信息系统部门以及威胁广大互联网用户的信息，CNCERT 还会定向通报给有关单位或通过广播电视、新闻媒体、官方网站等多种形式广而告之。2011 年发布的重要通报增刊如表 7-1 所示。

表 7-1　2011 年 CNCERT 发布的通信行业重要通报增刊

2011 年发布的重要通报增刊列表
互联网网络安全信息通报(总第 73 期)-关于北京亚控科技有限公司工业系统监控软件存在高危漏洞的通报
互联网网络安全信息通报（总第 74 期）-关于厦门易名 DNS 遭受攻击事件的通报
互联网网络安全信息通报（总第 75 期）-工业和信息化部奚国华副部长勉励通信行业继续做好通信网络安全防护工作
互联网网络安全信息通报（总第 77 期）-关于域名系统软件 BIND 9 存在远程拒绝服务漏洞的情况通报
互联网网络安全信息通报（总第 79 期）-2010 年互联网网络安全态势综述
互联网网络安全信息通报（总第 82 期）-关于域名系统软件 BIND 9 存在递归服务器对.com 域名解析异常漏洞的情况通报
互联网网络安全信息通报（总第 83 期）-关于紧急防范无线网络控制器安全漏洞威胁有关情况的通报
互联网网络安全信息通报（总第 85 期）-关于大量现网设备存在 VxWorks WDB 高危漏洞的情况通报
互联网网络安全信息通报（总第 86 期）-关于傲天动联无线网络控制器安全漏洞处置情况的通报
互联网网络安全信息通报（总第 87 期）-关于手机病毒导致某运营商分公司网站受攻击事件的通报
互联网网络安全信息通报（总第 88 期）-关于域名系统软件 BIND 存在安全漏洞的情况通报
互联网网络安全信息通报（总第 89 期）-关于 Microsoft HTML Help 缓冲区溢出 0 day 漏洞的情况通报
互联网网络安全信息通报（总第 90 期）-关于勤云科技远程稿件处理系统存在文件上传高危漏洞的情况通报
互联网网络安全信息通报（总第 93 期）-关于域名系统软件 BIND 9 存在安全漏洞的情况通报
互联网网络安全信息通报（总第 94 期）-关于网站内容管理系统软件 TurboCMS 存在安全漏洞的情况通报
互联网网络安全信息通报（总第 95 期）-关于 H3C ER 系列路由器存在安全漏洞的情况通报

互联网网络安全信息通报（总第 96 期）-关于新浪微博跨站漏洞被利用大量传播恶意链接事件的情况通报

互联网网络安全信息通报（总第 97 期）-关于网赢企业网络营销平台存在高危安全漏洞的情况通报

互联网网络安全信息通报（总第 98 期）-关于图派 kingtop 网站内容安全管理系统存在高危安全漏洞的情况通报

互联网网络安全信息通报（总第 99 期）-关于万户公司 ezEIP 2.0 网站内容安全管理系统存在高危安全漏洞的情况通报

互联网网络安全信息通报（总第 101 期）-关于苹果公司产品 IOS 操作系统存在特权提升漏洞的情况通报

互联网网络安全信息通报（总第 102 期）-关于颖源公司 E3 CMS 软件存在多个安全漏洞的情况通报

互联网网络安全信息通报（总第 103 期）-关于信达证券“牵牛花”网上交易系统存在多个安全漏洞的情况通报

互联网网络安全信息通报（总第 105 期）-关于 Apache HTTP Server 存在拒绝服务 0day 漏洞的情况通报

互联网网络安全信息通报（总第 106 期）- 关于 8.18 和 8.19 新疆某运营商域名系统攻击事件情况通报

互联网网络安全信息通报（总第 107 期）-关于 2011 年 9 月 5 日全网 DNS 单向流量异常监测情况的通报

互联网网络安全信息通报（总第 109 期）-关于域名系统软件 BIND 9 存在安全漏洞的情况通报

互联网网络安全信息通报（总第 110 期）-关于心海心理管理系统软件存在多个安全漏洞的情况通报

互联网网络安全信息通报（总第 112 期）-关于防范新一轮针对工业控制系统的网络攻击的情况通报

互联网网络安全信息通报（总第 114 期）-关于防范 Carrier IQ 软件收集手机用户隐私信息行为的通报

互联网网络安全信息通报（总第 115 期）-关于相关网站用户信息泄露事件的通报

互联网网络安全信息通报（总第 116 期）-关于国产无线网络控制器(AC 设备)存在安全漏洞的通报

互联网网络安全信息通报（总第 117 期）-关于 RSA1024 算法存在可能被破译风险的通报

7.2 行业外互联网网络安全信息发布情况

2011 年，CNCERT 通过发布网络安全专报、周报、月报、年报和在期刊杂志上发表文章等多种形式面向行业外发布报告 139 份。其中通过印刷品向有关部门发布月度网络安全专报和简报各 12 期、简报增刊 2 期 通过邮件推送、CNCERT

网站发布《网络安全信息与动态周报》52 期、英文版《网络安全信息与动态周报》18 期、《CNCERT 互联网安全威胁报告》12 期、《2011 年互联网网络安全态势报告》1 份；通过期刊杂志发布网络安全数据分析文章 29 篇；出版发行了《2010 年中国互联网网络安全报告》。其中，英文版《网络安全信息与动态周报》自 2011 年 8 月起开始公开发布，主要面向国际组织机构和用户，以进一步促进国内外网络安全信息共享与交流。

2011 年，CNCERT 周报、月报、年报等公开信息被多家权威媒体转载，相关数据被大量论文引用。中央电视台、新华社、中国日报等国内主流媒体纷纷来我中心挖掘新闻类节目或新闻稿素材，在 CCTV 新闻频道、CCTV 财经频道、新华网、人民网、中国日报英文版、参考消息、凤凰网、腾讯网、新浪网等二十余家媒体栏目或频道上播报，引起各级政府部门及公众的高度重视。代表性的文章主要有：《国家互联网应急中心发布网络安全态势报告》、《国家互联网应急中心：手机恶意程序正在快速蔓延》、《中国网络安全形势严峻 政府网站隐患多》、《2.78 亿数据泄露 CNCERT 发布信息泄露事件的通报》、《中美网络安全对话机制重点探讨反垃圾邮件》、《部分跨境网络安全事件回顾》、《反网络病毒联盟制定我国首个手机病毒技术规范》等。