# 7 “欢迎您参与网络安全信息共享工作”—网络安全信息通报情况

## 7.1互联网网络安全信息通报

2010 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。2010 年，我中心共收到各单位报送的月度信息 674 份，事件信息和预警信息 728 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了综合分析研判，全年共编制并向各单位发送《互联网网络安全信息通报》28 期，并通过网站向全社会发布《网络安全信息与动态周报》48 期。通报内容涵盖基础 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、互联网运营商、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，确保网络安全，提供了全面、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[1]，2010 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。

[1] 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。

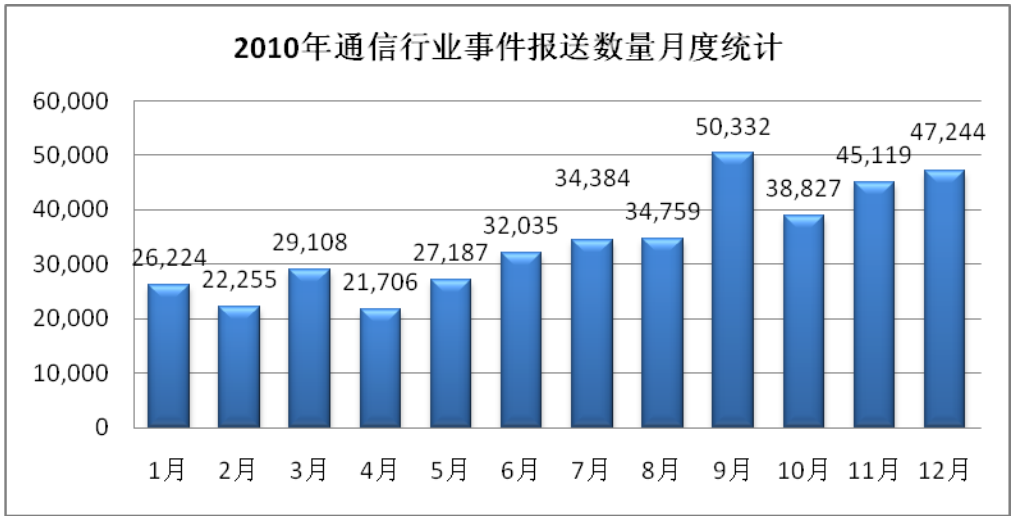


图 7-1　2010 年通信行业事件月度报送数量统计

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，2010 年报送的事件类型多为公共互联网环境以及基础 IP 网络中的网络安全事件，所占比例分别达到 66.4%和 33.5%。

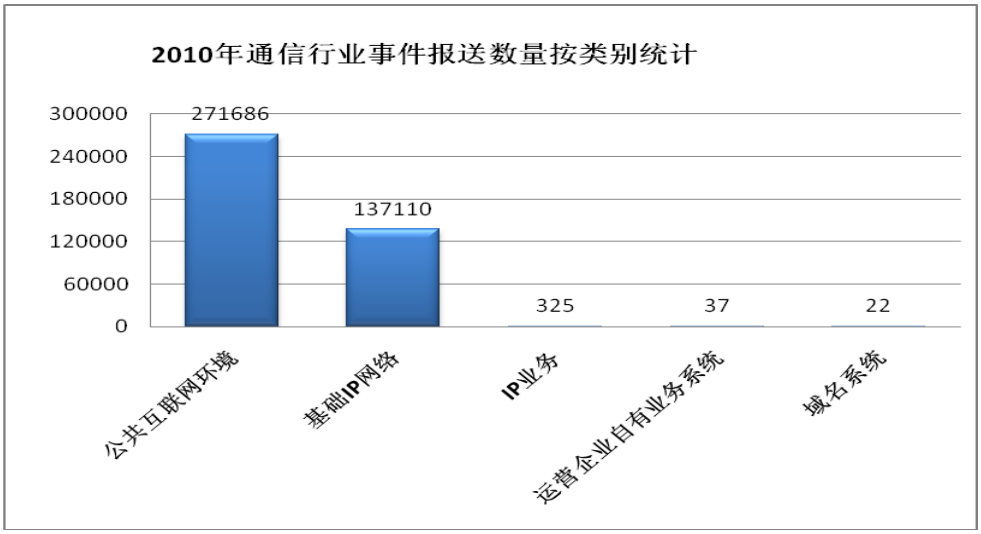


图 7-2　2010 年通信行业事件报送数量的分类统计

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、僵尸网络事件、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，垃圾邮件类型的事件数量最多，占公共互联网环境事件总数的比例为 56.2%；其他数量较多的事件类型还有：木马事件和僵尸网络事件，分别占 18.8%和 16.6%。

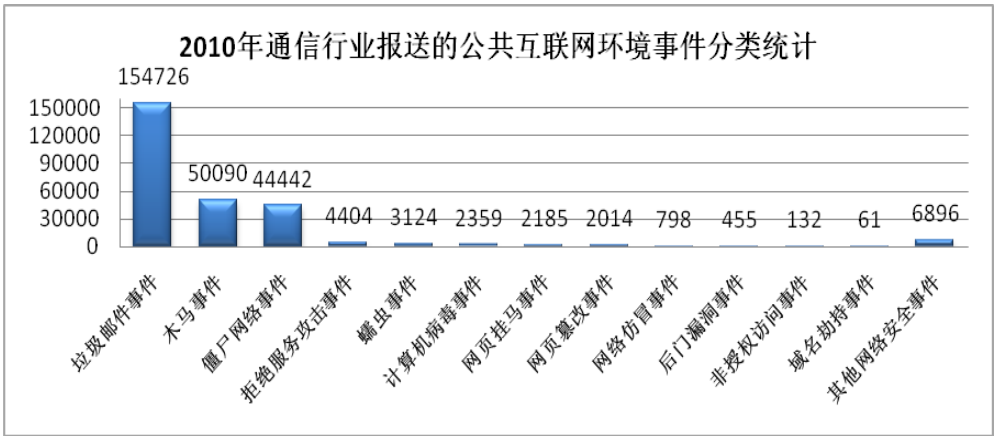


图 7-3　2010 年通信行业报送的公共互联网环境事件数量的分类统计

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。2010 年发布的重要通报增刊如表 7-1 所示。

表 7-1　2010 年 CNCERT 发布的通信行业重要通报增刊

| 2010 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 45 期)-关于流行论坛软件系统 Discuz!存在高危零日漏洞的情况通报 |
| 互联网网络安全信息通报(总第 46 期)-关于一月十二日百度公司网站无法访问事件处置情况的通报 |
| 互联网网络安全信息通报(总第 47 期)-关于微软 IE 浏览器存在对象重用远程攻击“0day”漏洞的公告 |
| 互联网网络安全信息通报(总第 50 期)-近期 CNCERT 打击仿冒央视“非常 6+1”栏目网站的情况通报 |
| 互联网网络安全信息通报(总第 51 期)-MySQL yaSSL 库存在证书解析远程溢出漏洞的情况通报 |
| 互联网网络安全信息通报(总第 54 期)-关于 IE 浏览器存在一个零日高危漏洞的情况通报 |
| 互联网网络安全信息通报(总第 63 期)-关于微软发布“不安全 DLL 加载”威胁的情况通报 |
| 互联网网络安全信息通报(总第 64 期)-关于近期中日黑客出现网络对抗倾向的情况通报 |
| 互联网网络安全信息通报(总第 66 期)-关于防范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 67 期)-关于 IBM 公司 Lotus Domino 群件平台存在密码散列泄露漏洞的情况通报 |
| 互联网网络安全信息通报(总第 68 期)-关于 9 月 10 日安徽电信 DNS 系统发生服务异常的情况通报 |
| 互联网网络安全信息通报(总第 70 期)-关于防范借广州亚运会名义实施网络钓鱼的情况通报 |

## 7.2 行业外互联网网络安全信息发布情况

2010 年 CNCERT 通过发布网络安全专报、周报、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 101 份。其中通过印刷品发布网络安全专报、简报各 12 期；通过邮件推送和 CNCERT 及工业和信息化部网站发布《网络安全信息与动态周报》48 期；发布网络安全数据分析文章 24 篇；发布网络安全简报增刊 2 篇；通过 CNCERT 网站发布了《2010 年上半年中国互联网网络安全报告》1 篇，出版发行了《2009 年中国互联网网络安全报告》1 篇，并首次与 CNNIC 联合完成并发布的《2009 中国网民网络信息安全状况调查报告》。其中《网络安全简报》增刊是在原有基础上为能及时将重要预警信息和事件信息向行业外有关单位进行通报而首次出现的通报形式。

2010 年 CNCERT 周报、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、中国新闻社等国内十余家主流媒体纷纷来我中心挖掘新闻类节目或新闻稿素材，并在 CCTV 新闻频道、新华社、中国新闻社播报，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《我国政府网站一周被篡改 178 个》、《.CN 恶意域名数量增加》、《手机“骷髅病毒”大肆传播》、《中国是黑客攻击的最大受害》、《中美欧业界联手打击 Waledac 僵尸网络，进一步深化在互联网网络安全领域的国际合作》、《亚运期间联网信息系统安全稳定运行》。此外，针对 2010 年外国媒体和报告多次刊登中国黑客发动网络攻击等不实报道，CNCERT 完成了多个公开新闻稿以澄清真实情况。