

中国互联网网络安全报告

（ 2010 年上半年 ）

国 家 互 联 网 应 急 中 心



关于中国互联网网络安全报告（2010 年上半年）

本文档所包含的信息代表国家计算机网络应急技术处理协调中心(中文简称国家互联网应急中心；英文简称 CNCERT/CC 或 CNCERT) 对截至发布日期之前所讨论问题的当前观点。

本文档仅用于提供信息之目的。国家互联网应急中心（CNCERT）对于本文档中的信息不做任何明示、暗示或法定的担保。国家互联网应急中心（CNCERT）无法保证发布日期之后所提供的任何信息的准确性。

本文档版权为国家互联网应急中心（CNCERT）所有。非商业目的情况下，转载或引用其中的有关内容，包括数据及图表，请注明出处。

遵守所有适用的版权法是用户的责任。如未获得国家互联网应急中心（CNCERT）明确的书面许可，不得以任何形式将本档的任何部分或全部内容用于商业目的。

编者按：

感谢您阅读“中国互联网网络安全报告（2010 年上半年）”，如果您发现本报告存在任何问题，请您及时与我们联系，电子邮件地址为：cncert@cert.org.cn。我们对此深表感谢。

关于 CNCERT

国家互联网应急中心(全称为国家计算机网络应急技术处理协调中心, 英文简称为 CNCERT 或 CNCERT/CC) 成立于 1999 年 9 月, 是工业和信息化部领导下的国家级网络安全应急机构, 致力于建设国家级的网络安全监测中心、预警中心和应急中心, 以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能, 支持基础信息网络的安全防护和安全运行, 支援重要信息系统的网络安全监测、预警和处置。

2003 年, CNCERT 在全国 31 个省成立分中心, 完成了跨网络、跨系统、跨地域的公共互联网网络安全应急技术支撑体系建设, 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, 在协调国内网络安全应急组织(CERT) 共同处理公共互联网网络安全事件方面发挥着重要作用。

CNCERT 的业务能力主要包括:

- **监测发现**: 依托“863-917 网络安全监测系统”实现网络安全事件的监测发现。863-917 网络安全监测系统是一个全程全网、多层次、多渠道延伸的网络安全综合监测平台, 目前已具备木马和僵尸网络监测、网页篡改监测、网页挂马监测、恶意代码捕获、流量异常监测、域名服务监测等能力。
- **通报预警**: 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。此外, 按照 2009 年工业和信息化部颁布实施的《互联网网络安全信息通报实施办法》承担通信行业互联网网络安全信息通报工作。
- **应急处置**: 依托与运营商、域名注册商、安全服务厂商等相关部门的快速工作机制实现网络安全事件的应急处置。CNCERT 是接收国内网络安全事件报告的重要机构, 同时作为国际应急组织 FIRST 和亚太地区应急组织 APCERT 成员, 负责接收国际网络安全事件报告, 是中国处理网络安全事件的对外窗口。

CNCERT 的联系方式:

国家互联网应急中心 CNCERT

网址: <http://www.cert.org.cn/> 电子邮件: cncert@cert.org.cn

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

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

目 录

1. 2010 年上半年网络安全状况综述.....	5
2. 互联网业务流量监测分析.....	7
3. 网络安全事件接收与处置.....	11
3.1 事件接收情况	11
3.2 事件处理情况.....	12
3.3 事件处理部分案例介绍.....	13
4. 信息安全漏洞公告与处置.....	18
5. CNCERT 官方网站信息发布情况	19
6. 木马和僵尸网络监测情况.....	20
6.1 木马数据分析	20
6.2 僵尸网络数据分析	22
7. 被篡改网站监测分析.....	25
7.1 我国网站被篡改情况	25
7.2 中国大陆地区政府网站被篡改情况	25
7.3 黑客篡改我国网站活动情况	26
8. 网页仿冒事件情况.....	28
9. 通信行业网络安全信息通报情况.....	29

1. 2010 年上半年网络安全状况综述

根据 CNCERT 自主监测结果以及通信行业各单位报送的网络安全事件信息，2010 上半年，我国网络安全态势总体平稳，全国范围内或省级行政区域内未发生通信网络基础设施的重大网络安全事件，基础电信运营企业、国内域名注册管理和服务机构业务系统未发生重大网络安全事件，网络安全的主要威胁主要体现为来自公共互联网环境的安全威胁。根据 CNCERT 建立的网络安全评价指标体系，2010 年上半年指数评价为“中”的周数为 18 周，评价为“差”的周数为 2 周，评价为“良”的周数为 6 周，且第二季度总体状况要好于第一季度。

2010 年上半年，CNCERT 在网络安全事件监测、接收和处置等方面的主要数据如下：

■ 网络安全事件接收与处理情况

- 2010 年上半年 CNCERT 共接收 4780 次网络安全事件报告（不包括扫描和垃圾邮件类事件），与 2009 年上半年相比增长 105%。其中，恶意代码、漏洞和网页仿冒事件报告次数居前三位，所占比例分别为：57.57%，25.96%和 15.48%。
- 2010 年上半年 CNCERT 国家中心和各分中心处理各类网络安全事件共 784 件，与 2009 年上半年相比增长 92.2%。其中，恶意代码、网页仿冒、网页篡改是事件处理的重点，上述事件处理数量占事件处理总数的 98%以上。

■ 信息系统安全漏洞公告及处理情况

- 2010 年上半年国家信息安全漏洞共享平台（CNVD）共收录信息安全漏洞 1241 个，其中高危、中危、低危漏洞分别占 19.34%、23.93%和 56.73%。
- 2010 年上半年国家信息安全漏洞共享平台（CNVD）收录的信息安全漏洞中，可用于实施远程网络攻击的漏洞有 1076 个，占收录漏洞总数的 86.70%，0 day 漏洞 107 个。

■ 互联网业务流量监测情况

- 在 TCP 协议中，占用带宽最多的网络应用有四类：Web 浏览、网络多媒体（音频视频）、P2P 下载和网络代理。
- 在 UDP 协议中，占用带宽最多的是即时聊天工具和 P2P 软件下载。

■ 木马与僵尸网络监测情况

- 2010 年上半年中国大陆地区有近 124 万个 IP 地址对应的主机被木马程序控制；参与控制中国大陆计算机的境外木马控制服务器 IP 有 12.8 万个，主要来自美国、印度和中国台湾。
- 2010 年上半年中国大陆地区有 23.3 万个 IP 地址对应主机被僵尸程序控制，参与控制中国大陆计算机的境外僵尸网络控制服务器 IP 有 4584 个，主要来自美国、土耳其和印度。

■ 被篡改网站监测情况

- 2010 年上半年中国大陆被篡改网站总数为 14907 个，比 2009 年上半年下降 21.8%。
- 2010 年上半年中国大陆地区政府网站被篡改数量为 2574 个，比 2009 年上半年增长 222.56%。被篡改的政府网站占整个大陆地区被篡改网站的 17.27%。

■ 网页仿冒事件情况

- 2010 年上半年 CNCERT 共接到网页仿冒事件报告 740 次，经归类合并后具体成功处理了 308 件。被仿冒的网站大多是国外的著名金融交易机构。

2. 互联网业务流量监测分析

根据 CNCERT 在 2010 年上半年对互联网业务流量的抽样统计 ,在 TCP 协议中，占用带宽最多的网络应用主要是 Web 浏览、网络多媒体（音频视频）、P2P 下载和网络代理。

2010 年上半年 TCP 协议流量按源端口流量占 TCP 总流量比例居前十位的端口分布情况如图 2-1 和表 2-1 所示。

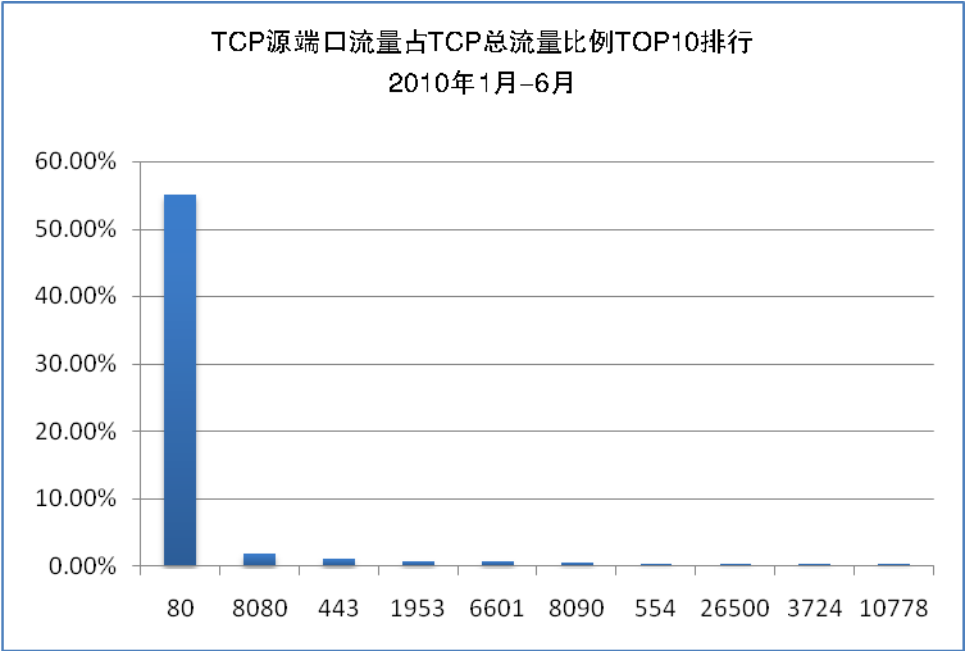


图 2-1 2010 年上半年 TCP 协议流量源端口排名 TOP 10

表 2-1 2010 年上半年 TCP 协议流量源端口排名 TOP 10

TCP 源端口	排名	占 TCP 总流量百分比	主要的业务种类
80	1	55.15%	网页服务端口
8080	2	1.75%	网页服务端口
443	3	1.00%	网页服务端口
1935	4	0.60%	RTMP 协议端口
6601	5	0.58%	未知端口
8090	6	0.46%	代理服务端口
554	7	0.35%	RTSP 默认端口
26500	8	0.32%	讯闪服务端口
3724	9	0.31%	网络游戏端口
10778	10	0.27%	未知端口

2010 年上半年 TCP 协议流量按目的端口流量占 TCP 总流量比例居前十位的端口分布情况如图 2-2 和表 2-2 所示：

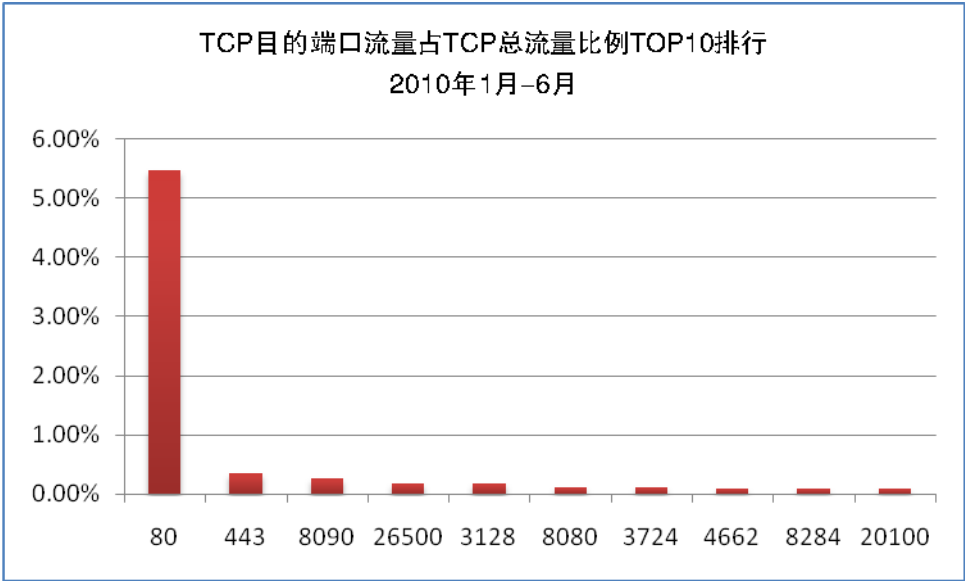


图 2-2 2010 年上半年 TCP 协议流量目的端口排名 TOP 10

表 2-2 2010 年上半年 TCP 协议流量目的端口排名 TOP 10

TCP 目的端口	排名	占 TCP 总流量百分比	主要的业务种类
80	1	5.46%	网页服务端口
443	2	0.35%	网页服务端口
8090	3	0.26%	代理服务端口
26500	4	0.18%	讯闪服务端口
3128	5	0.17%	代理服务端口
8080	6	0.11%	网页服务端口
3724	7	0.10%	网络游戏端口
4662	8	0.10%	eMule 服务端口
8284	9	0.09%	未知端口
20100	10	0.09%	QVOD 服务端口

而在 UDP 协议中，占用带宽最多的网络应用主要是各类即时通讯和 P2P 下载。

2010 年上半年 UDP 协议流量按源端口流量占 UDP 总流量比例居前十位的端口分布情况如图 2-3 和表 2-3 所示：

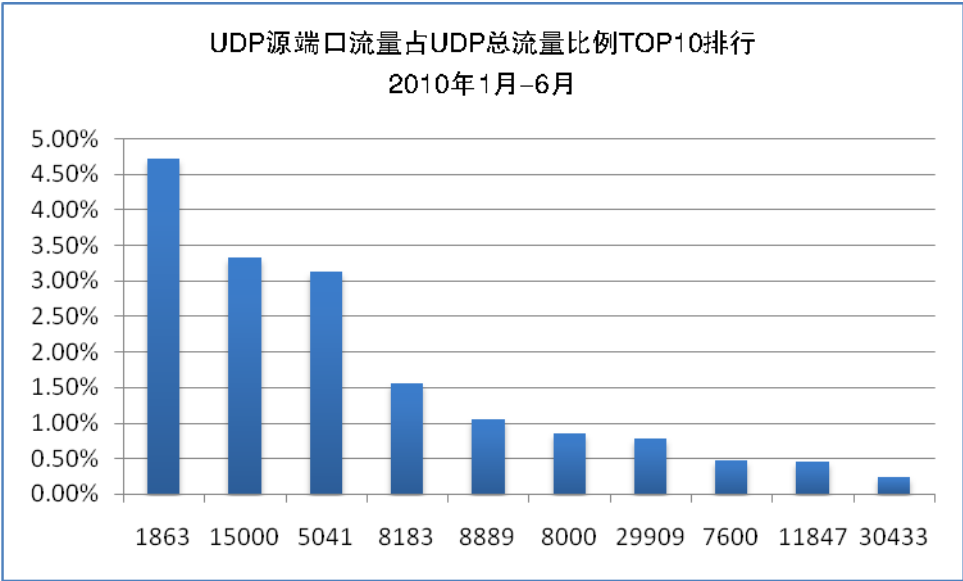


图 2-3 2010 年上半年 UDP 协议流量源端口排名 TOP 10

表 2-3 2010 年上半年 UDP 协议流量源端口排名 TOP 10

UDP 源端口	排名	占 UDP 总流量百分比	主要的业务种类
1863	1	4.73%	MSN 服务端口
15000	2	3.33%	迅雷下载工具默认端口
5041	3	3.13%	MTLS 协议端口
8183	4	1.56%	未知端口
8889	5	1.06%	未知端口
8000	6	0.86%	QQ 通讯端口
29909	7	0.79%	QQ 旋风下载工具端口
7600	8	0.48%	未知端口
11847	9	0.45%	未知端口
30433	10	0.23%	未知端口

2010 年上半年 UDP 协议流量按目的端口流量占 UDP 总流量比例居前十位的端口分布情况如图 2-4 和表 2-4 所示。

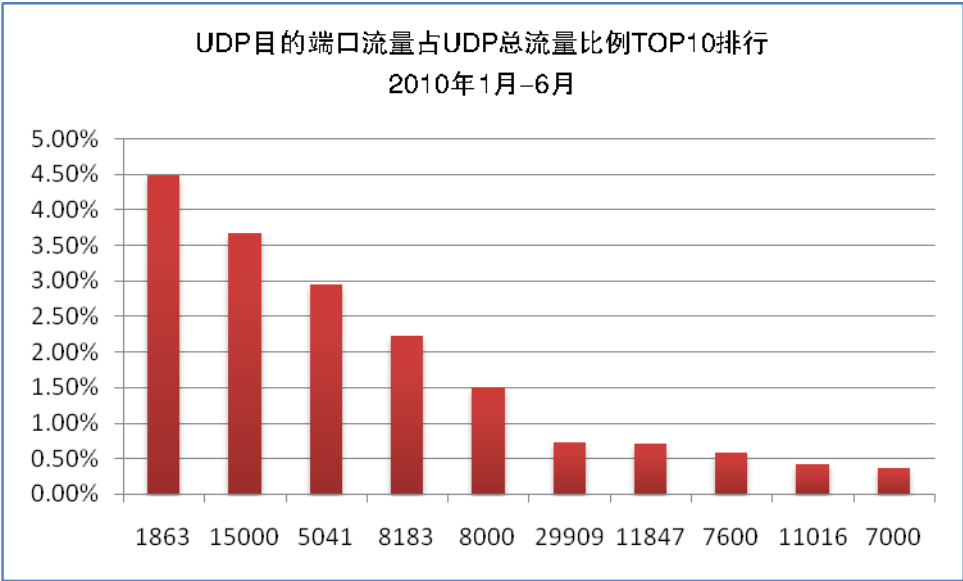


图 2-4 2010 年上半年 UDP 协议流量目的端口排名 TOP 10

表 2-4 2010 年上半年 UDP 协议流量目的端口排名 TOP 10

UDP 源端口	排名	占 UDP 总流量百分比	主要的业务种类
1863	1	4.49%	MSN 服务端口
15000	2	3.68%	迅雷下载工具默认端口
5041	3	2.96%	MTLS 协议端口
8183	4	2.23%	未知端口
8000	5	1.50%	QQ 通讯端口
29909	6	0.72%	QQ 旋风下载工具端口
11847	7	0.71%	未知端口
7600	8	0.58%	未知端口
11016	9	0.43%	未知端口
7000	10	0.36%	网络游戏端口

3. 网络安全事件接收与处置

为了能够及时了解和响应互联网上发生的安全事件，CNCERT 利用多种公开渠道接收公众的网络安全事件报告，如热线电话、传真、电子邮件、网站等。对于其中影响互联网运行安全的、波及较大范围互联网用户的、或涉及政府和重要信息部门的网络安全事件，CNCERT 积极协调基础电信运营企业、域名注册管理和服务机构以及应急服务支撑单位进行处理。

3.1 事件接收情况

2010 年上半年 CNCERT 接收 4780 次网络安全事件报告（不包括扫描和垃圾邮件类事件）¹，其中恶意代码事件和漏洞事件较多。上半年每月接收的网络安全事件报告具体数量如图 3-1 所示，月均接收到的事件报告数量为 797 次，与 2009 年上半年相比增加 105%

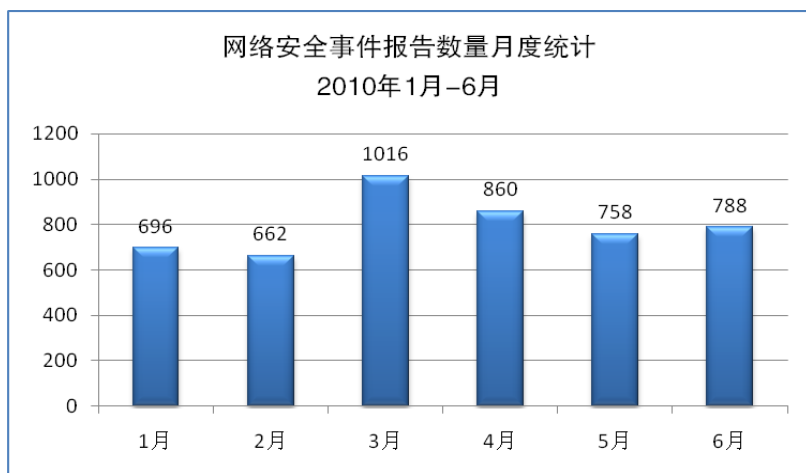


图 3-1 2010 年上半年 CNCERT 接收到的网络安全事件报告数量统计

所报告的网络安全事件主要集中在恶意代码事件、漏洞事件、网页仿冒事件等。根据报告的网络安全事件类型统计，如图 3-2 所示，恶意代码事件比例最大，为 2725 次，占报告事件总数的 57.57%。其次是漏洞事件，为 1241 次，占 25.96%。网页仿冒数量为 740 次，占 15.48%。拒绝服务攻击事件为 47 次，占 0.98%。

总的来看，2010 年上半年所接收的网络安全事件报告数量与去年同期相比大量增加，恶意代码事件、漏洞事件仍然是影响企业和用户网络安全的主要威胁。

¹ 因 CNCERT 一般不对扫描类事件和垃圾邮件类事件报告进行处置，故未做统计。对于垃圾邮件事件报告，CNCERT 直接转中国互联网协会反垃圾邮件中心处置。

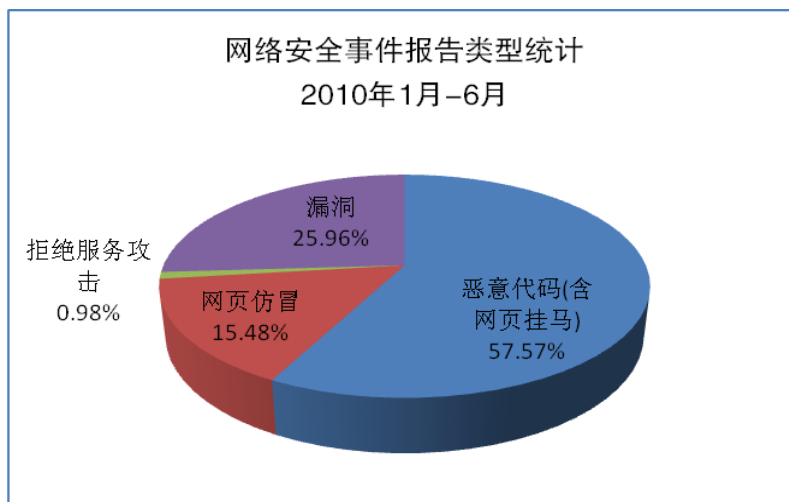


图 3-2 2010 年上半年 CNCERT 接收的网络安全事件按类型分布

3.2 事件处理情况

2010 年上半年，CNCERT 共处理各类网络安全事件 784 件，比去年同期增长了 92.16%。CNCERT 处理的事件类型主要有恶意代码、网页仿冒、网页篡改等。各类事件处理数量分布如图 3-3 所示。在 CNCERT 处理的网络安全事件中，针对金融企业、重要商业机构的网页仿冒类事件最多，网页挂马和网页篡改事件也较多，尤其是涉及国内政府机构和重要信息系统部门的挂马和篡改事件。

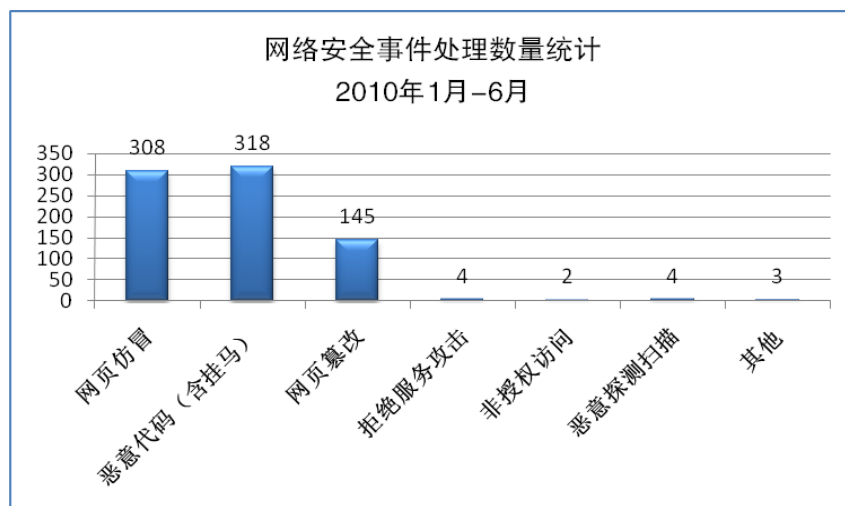


图 3-3 2010 年上半年 CNCERT 处理的网络安全事件数量统计

CNCERT 在中国大陆各省、自治区、直辖市设立了分中心，协助 CNCERT 国家中心处理各类网络安全事件。2010 年上半年各分中心共参与处理事件 328 件，各分中心处理的事件数量和比例如图 3-4 所示。

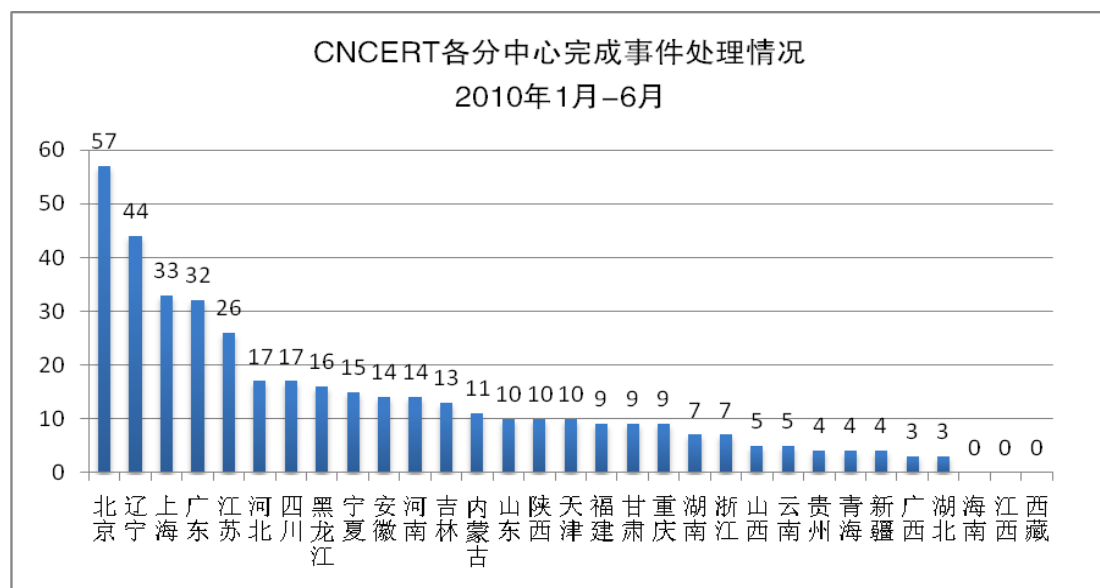


图 3-4 2010 年上半年 CNCERT 各分中心完成事件处理情况

3.3 事件处理部分案例介绍

■ 协调处置百度公司网站无法访问事件

1 月 12 日上午 7 时左右，百度公司网站（baidu.com）突然无法访问。鉴于此事引起互联网用户的广泛关注，造成一定影响，工业和信息化部立即要求百度公司采取有效措施，尽快恢复网站的正常访问。在工业和信息化部的领导下，CNCERT 积极协调百度公司、CNNIC 和基础电信运营企业采取应急处置措施。12 日上午 11 时左右，百度公司网站访问逐步恢复正常。12 日下午 1 时，工业和信息化部召集百度公司、基础电信运营企业、CNCERT 以及 CNNIC 召开专家研判会，对事件相关情况进行汇总研判。经查，百度公司的域名 baidu.com 是在美国域名注册服务商 register.com 公司注册的。综合各方提供的技术报告，与会专家分析认为，造成本次事件的原因是 baidu.com 域名的注册信息被非法篡改，致使 baidu.com 域名在全球的解析被错误指向，最终导致全球互联网用户无法正常访问 baidu.com 网站。

■ 出现一类使得域名解析服务器间接受害的网络攻击事件

2010 年上半年，CNCERT 获知多起针对域名企业域名解析服务器的网络攻击事件，其中一类事件需引起相关单位重视，加强防范。

1 月 25 日凌晨 0 时至上午 11 时 30 分，北京新网数码公司一台主 DNS 服务器受到大流量攻击影响，具体现象为：网上出现大量以 880sf.com（某游戏私服站点）为目标的攻击包，但攻击者在攻击包中指定了由新网数码公司的 DNS 负

责对目标域名进行解析，从而使得这台 DNS 服务器以及所在网络都遭受较大影响。众多域名注册用户在互联网上讨论、抱怨服务异常情况。

2 月 9 日 16 时左右北京新网互联公司遭遇类似攻击事件。网上出现大量以 haofg.com（某游戏私服站点）为目标的攻击包，攻击包中指定由新网互联的 DNS 负责对该目标域名进行解析，导致新网互联受到严重影响。16 时 30 分左右，随着 haofg.com 被停用，攻击流量逐步消失。期间，新网互联的托管机房因流量策略限制，屏蔽了服务器的网络连接，造成其提供服务的数万域名无法正常解析。

上述两起事件中，网游私服争斗是事件起因，但由于攻击者对攻击包进行特殊技术处理，使得域名企业成了受害者。应对此类事件，CNCERT 建议域名企业一方面要进一步优化域名系统架构，加大域名冗余安全方面的投入，提高域名系统的抗攻击能力；另一方面，要在发生安全事件后及时上报，借助全行业的应急机制寻求快速处理。

■ 发现微软 IE 浏览器存在零日高危漏洞

3 月初，国家信息安全漏洞共享平台（CNVD）发现 IE 浏览器存在一个新的零日高危漏洞。依据 CNVD 工作流程，CNCERT 立即组织 CNVD 成员单位完成对漏洞的测试验证，并向微软公司通报了有关情况；3 月 10 日 CNVD 和微软公司同步发布了安全公告。根据 CNCERT 联合相关信息通报工作成员单位对与漏洞相关的黑客网页挂马活动进行的持续跟踪监测结果显示，该漏洞被大量利用来传播恶意代码。微软公司已于 3 月 31 日发布了 IE 累积性更新（MS10-018），修补了包括该漏洞在内的十个 IE 漏洞。

■ 处理手机骷髅病毒

3 月份，一个名为“手机骷髅”的手机病毒迅速传播，该病毒主要针对拥有大量用户的 Symbian S60 3 系列版本操作系统的智能手机，这当中包括市面上常见的数十款诺基亚手机和十余款三星手机。感染该病毒的手机会在用户不知情的情况下暗中联网且向手机通信录中的联系人大量群发带有病毒链接的彩信和短信，直接后果是导致用户手机因大量发送短信、彩信而被收取高额费用。仅根据 CNCERT 一周内的抽样监测结果，就发现有 13 万余手机用户感染了此病毒。3 月 21 日，CNCERT 在官方网站发布了关于该病毒危害严重的安全公告。为扩大公告的知晓范围，CNCERT 还联系中央电视台在 CCTV 新闻频道多个时段播出了公告信息。建议各单位做好安全防范和宣传工作，提醒智能手机用户要提高警惕，避免打开带有诱惑性标题的彩信或用手机访问短信中不明来源的链接。

■ 与美欧联手打击 Waledac 僵尸网络

CNCERT 与美国微软公司以及欧美一些网络安全机构联手，成功打击一个名为 Waledac 的全球大型僵尸网络。Waledac 僵尸网络所使用的控制服务器大多位于德国、荷兰、瑞典和俄罗斯等欧洲国家，控制了全球数十万台计算机，每天能发出超过 15 亿封的垃圾邮件。打击 Waledac 僵尸网络行动成功后，微软公司在第 37 届 ICANN 会议上发表演讲，感谢包括 CNCERT 在内的所有合作伙伴在打击 Waledac 僵尸网络中采取的快速及时的行动，并于 3 月 17 日向 CNCERT 致函以示谢意。

■ 与韩国 KrCERT 联手处置针对我运营业务系统恶意扫描事件

5 月 25 日，某运营商向 CNCERT 宁夏分中心投诉称，其业务系统近期遭受持续的恶意扫描。在短短一周内，针对目标系统的扫描次数就高达百万余次，对业务系统运营造成一定影响。

CNCERT 在对攻击事件进行技术验证和数据分析后，发现恶意扫描数据包中大多数源 IP 地址位于韩国。对此，CNCERT 利用近年来建立的国际网络安全事件应急处置工作机制，紧急联系韩国 KrCERT，请其协助处置此次攻击事件。韩国 KrCERT 迅速响应，很快就协调其国内互联网运行单位对三个危害较大的攻击源 IP 进行了处置。5 月 26 日下午，针对该运营业务系统的攻击呈趋缓态势，至 5 月 27 日攻击完全停止，系统业务运行恢复正常。

本次事件的成功处置再次表明，各国各地区安全组织加强网络安全协作，建立通畅的应急处置渠道，有助于应对当前日益严峻的网络安全威胁。

■ 处理针对 Symbian S60 系统的手机短信木马

6 月中旬，CNCERT 分别收到诺基亚和芬兰 CERT-FI 的报告称，发现针对 Symbian S60 系统的手机短信木马及相关恶意链接。该木马会在用户不知情的情況下执行一些非法操作，如发送用户手机信息至一些不明网址。

据 F-Secure 和卡巴斯基公司确认，该木马为 SymbOS/MerogoSMS 木马的变种，会影响 Symbian 60 系列第 3 版和第 5 版操作系统的手机。该木马通过中文手机短信传播，其中包括一个恶意链接。一旦用户点此链接，会立即安装一个应用。该木马会在手机启动时启动，并通过 GPRS 或 3G 尝试连接另外的恶意网址 [http://rec\[...\].rzwxdsu.com](http://rec[...].rzwxdsu.com)，从而达到感染手机和重启短信服务的目的。此木马尚

仅在中国境内传播。

CNCERT 对相关恶意网址进行了处理，并发布安全公告建议用户不要轻信所谓绿色软件和轻易下载不明手机应用程序，如需各类手机应用程序和安全工具，请到手机官方网站进行下载。

■ 处理多起针对我国用户的网页仿冒事件

1、集中打击假冒央视“非常 6+1 栏目”钓鱼网站

1 月下旬 CNCERT 接到举报，一些不法分子通过飞信、聊天工具以及垃圾邮件大量传播假冒央视“非常 6+1 栏目”的数十个钓鱼网站信息，极易使用户受到蒙骗，造成经济损失。对此，CNCERT 及时组织协调万网志成和新网数码等国内域名注册商对监测发现的钓鱼网站域名开展专项治理行动，共关闭钓鱼网站 27 个，有效地打击了不法分子进行网络钓鱼的猖獗势头。此事件发生时正值春节临近，不法分子选择此时借用“中奖”、“送礼品”等幌子进行网络欺诈的活动更具迷惑性。

2、处理借捐助赈灾名义的网络钓鱼事件

4 月 13 日，CNCERT 接收到事件报告：有部分雅虎邮箱用户收到主题为“伸出你们的援手，救助灾区人民！”的邮件，邮件中含有一个钓鱼网站网址 <http://sygongyi.com>，仿冒中国思源工程扶贫基金会“思源-甘泉”活动页面（<http://gongyi.sina.com.cn/z/siyuan/index.shtml>），骗取用户捐款。思源工程扶贫基金委发布了紧急公告，提醒互联网用户注意防范，并提供真实的赈灾活动相关页面供鉴别。该钓鱼网站很快被清除，CNCERT 未接收到有用户遭受经济损失的事件报告。

3、提醒防范利用博客的网络钓鱼事件

5 月，CNCERT 监测发现，一些不法分子通过在博客中插入网络钓鱼链接对用户进行欺诈，并多以“世博会门票”、“2010 虎年运势测算”等字样作为此类博客搜索的关键字。这些博客多通过骗取用户手机费等方式损害用户利益，网易博客、新浪博客和百度空间等知名博客网站均存在此类型的钓鱼博客。此类推广钓鱼页面的方式简便、成本低、浏览群体大，更容易诱使互联网用户上当受骗。对此，CNCERT 发布安全公告建议各博客网站及时过滤此类信息，维护个人博客健康发展，共同净化互联网环境。同时也提醒广大网民在浏览网页时提高警惕，避免

利益受损。

4. 信息安全漏洞公告与处置

2010 年上半年，国家信息安全漏洞共享平台（CNVD）共收录信息安全漏洞 1241 个。其中，收录高危漏洞 240 个（占 19.34%）、中危漏洞 297 个（占 23.93%）、低危漏洞 704 个（占 56.73%）。各级别漏洞的数量及比例分布如图 4-1、图 4-2 所示。在上述收录的漏洞中，可用于实施远程网络攻击的漏洞有 1076 个，占收录漏洞总数的 86.70%，0 day 漏洞²107 个。

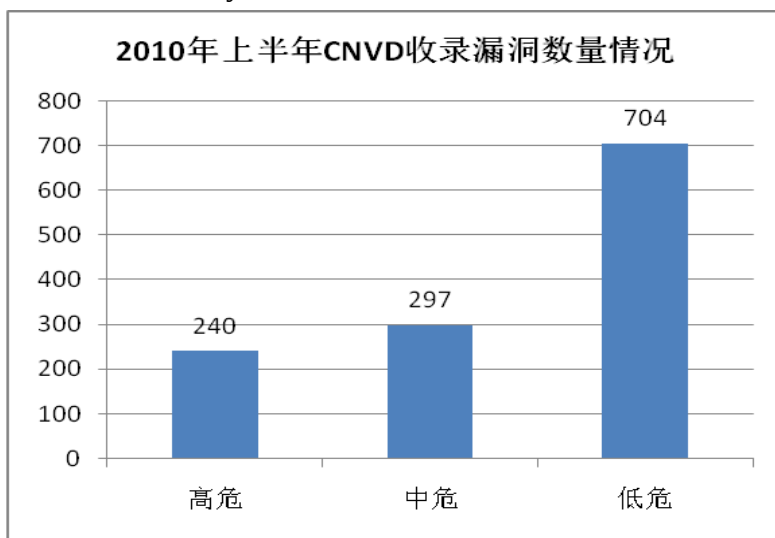


图 4-1 2010 年 CNVD 收录漏洞数量情况

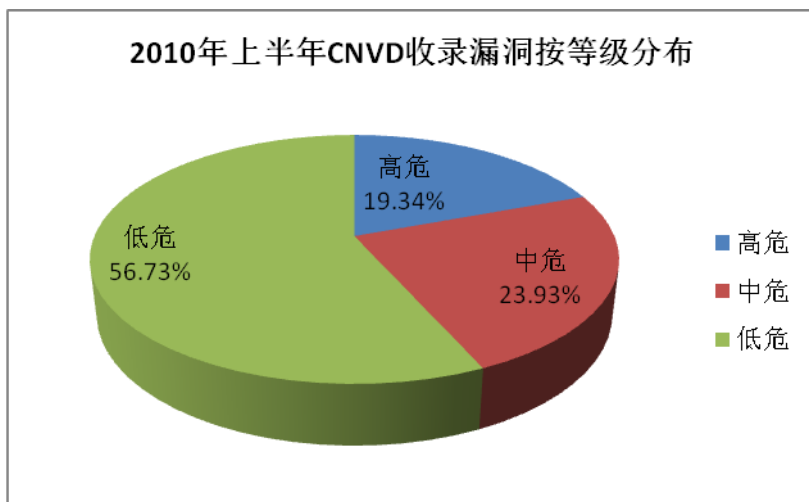


图 4-2 2010 年 CNVD 收录漏洞按等级分布

² 0day 漏洞一般指那些被公开或秘密披露之时还未能有安全补丁或安全解决方案的漏洞，攻击者在知晓漏洞信息的时刻即可发动用户无法防范的攻击。这种攻击又称 0day 攻击。

5. CNCERT 官方网站信息发布情况

2010 年上半年，CNCERT 在官方网站上整理发布与我国用户密切相关的安全公告 79 个，发布数量与 2009 年上半年相比增加 41%。其中有 72 个国家信息安全漏洞共享平台（CNVD）漏洞公告，3 个中国反网络病毒联盟（ANVA）安全公告和 4 个其他威胁公告。此外，CNCERT 还通过官方网站发布了其他各类消息共 230 条，其中包括 109 条全球要文、44 篇资料与文档、6 份活动及日程、71 份安全状况图表等。CNCERT 网站已成为国内外安全组织和网站参考或转载权威信息的重要来源。CNCERT 官方网站发布的各类公告消息分布情况如图 5-1 所示。

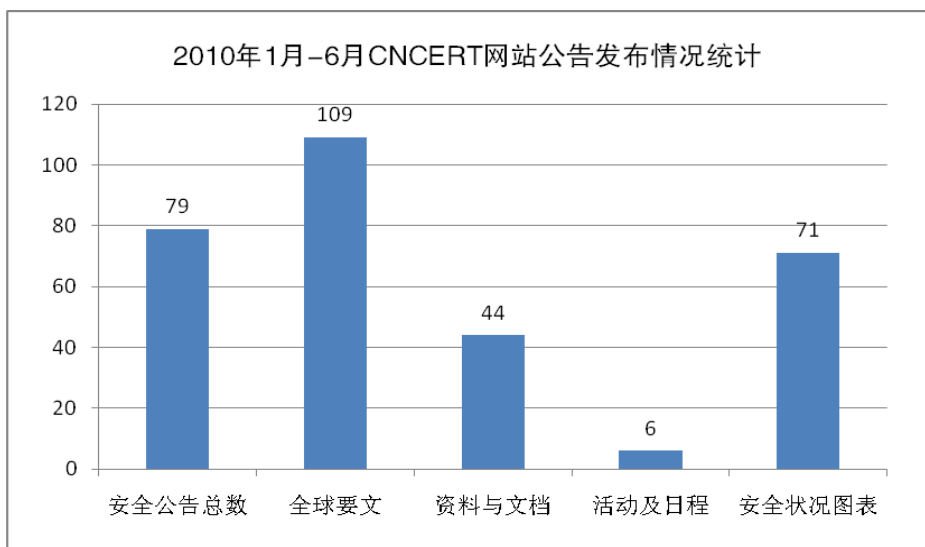


图 5-1 2010 年上半年 CNCERT 官方网站信息发布情况

6. 木马和僵尸网络监测情况

木马和僵尸网络两者都是非常有效的远程监听和控制手段，尤其是在网络失窃密和发动 DDoS 攻击方面对政府部门、商业机构以及普通用户造成了严重危害，因此 CNCERT 对此两类事件进行了重点监测。

6.1 木马数据分析

CNCERT 2010 年上半年抽样监测结果显示，中国大陆地区有 1239538 个 IP 地址对应的主机被木马程序控制，月度统计情况见图 6-1 所示。中国大陆地区木马受控主机数量比去年同期有大幅增长，这主要是因为 CNCERT 在 6 月份新增了对下载者木马和盗号木马的监测，而这两类木马的受控主机数量巨大。不过，2010 年上半年中国大陆地区传统远程控制类木马受控主机 IP 数量其实是呈缩减态势，这主要得益于 CNCERT 组织通信行业持续开展的木马和僵尸网络专项打击行动以及常态化治理活动。

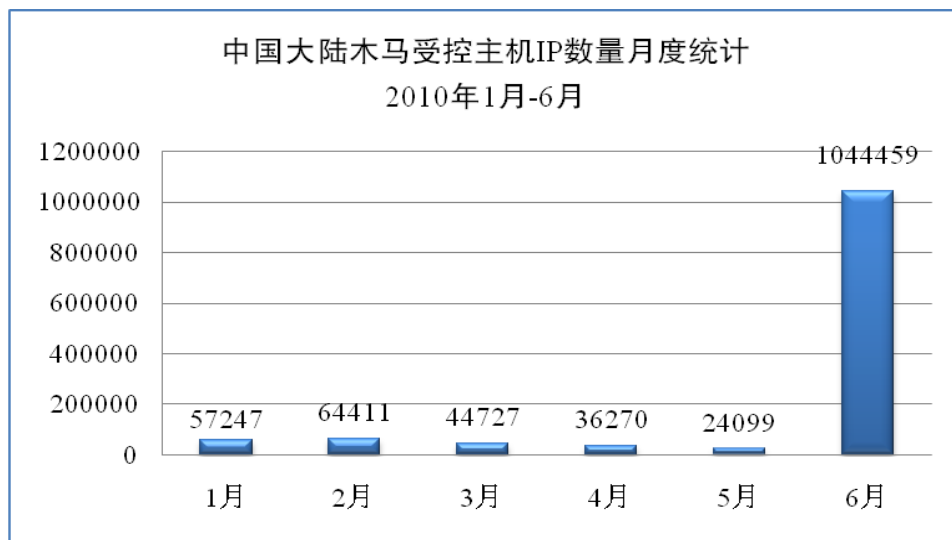


图 6-1 2010 年上半年境内木马受控主机 IP 月度统计

■ 中国大陆地区木马受控主机分布统计

根据 CNCERT 抽样监测结果，中国大陆木马受控主机最多的地区分别为广东省（15.12%）、江苏省（7.25%）、浙江省（7.18%）、山东省（6.67%）和河南省（5.81%），如图 6-2 所示。

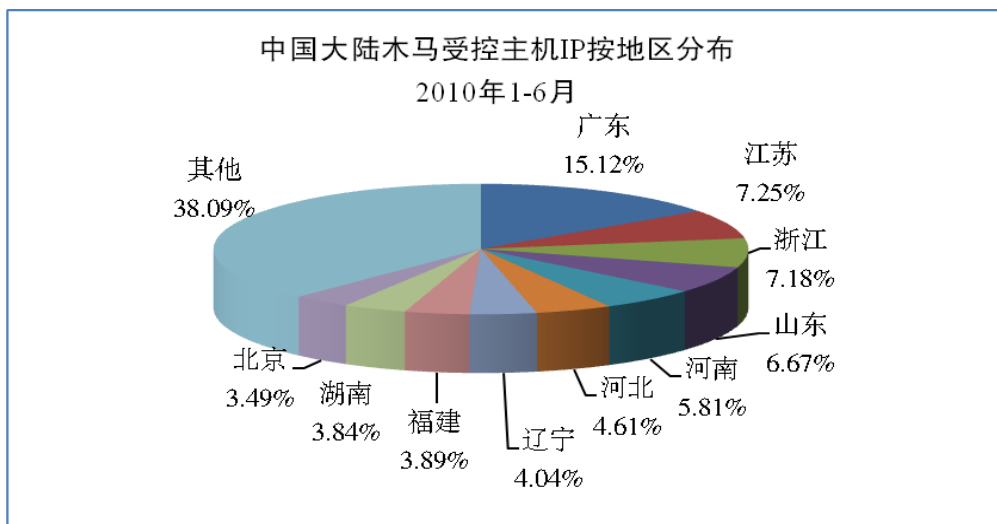


图 6-2 2010 年上半年中国大陆木马受控主机 IP 按地区分布

图 6-3 所示为 2010 年上半年中国大陆木马受控主机在各运营商中的分布。其中，电信网内木马被控端占 61.03%，联通占 33.9%，移动占 0.34%。

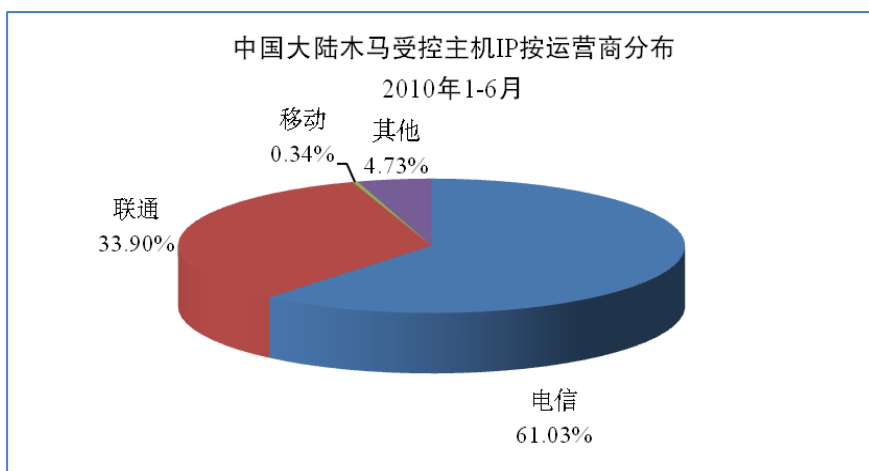


图 6-4 2010 年上半年中国大陆木马受控主机 IP 按运营商分布

■ 境外木马控制服务器分布统计

CNCERT 同时监测发现境外有 127559 个 IP 地址作为木马控制服务器参与控制中国大陆地区的木马受控主机。木马控制服务器 IP 按国家和地区分布如图 6-5 所示，其中位于美国（17.38%）、印度（8.64%）、中国台湾（5.39%）、巴西（4.71%）和韩国（4.42%）的木马控制服务器 IP 数量居前五位。

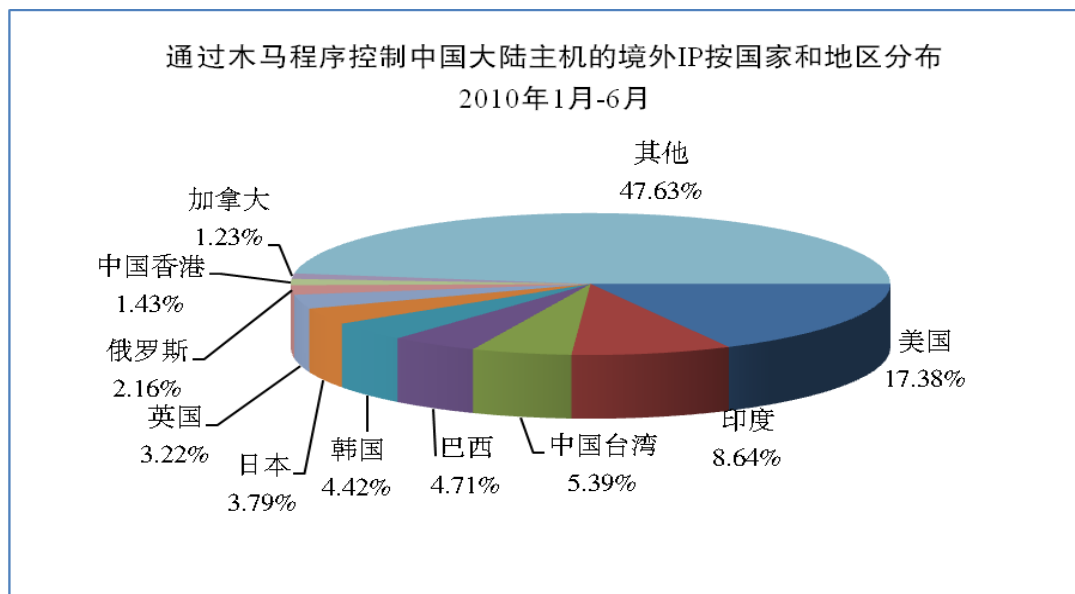


图 6-5 2010 年上半年通过木马控制我国计算机的境外 IP 按国家和地区分布

6.2 僵尸网络数据分析

CNCERT 2010 年上半年抽样监测结果显示，中国大陆地区有 233335 个 IP 地址对应主机被僵尸程序控制，与去年上半年相比下降 47%。中国大陆地区僵尸网络受控主机数量的大幅下降同样得益于 CNCERT 组织通信行业持续开展的木马和僵尸网络专项打击行动以及常态化治理活动。从月度统计情况看，2010 年上半年 1 月至 3 月境内僵尸网络受控主机数量维持在较高水平，从 4 月份开始急剧下降，如图 6-6 所示。

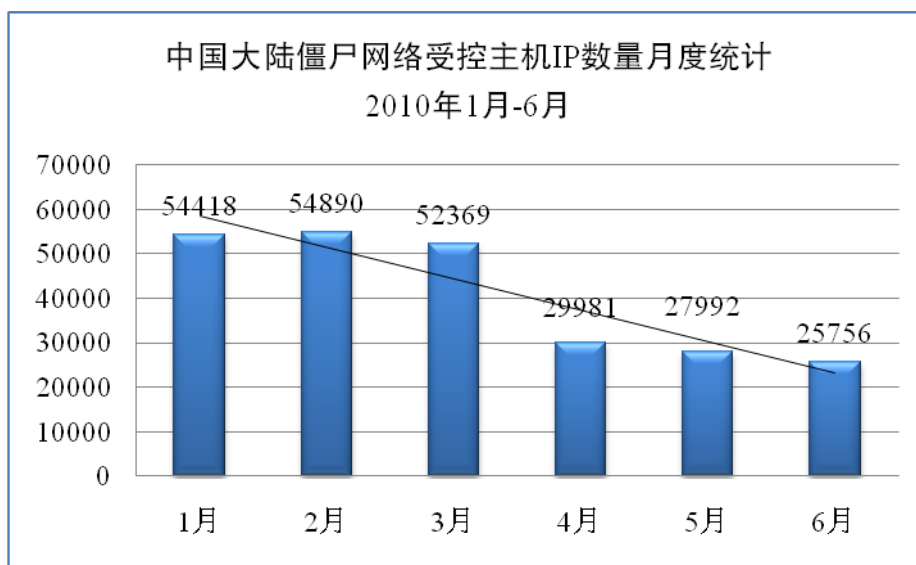


图 6-6 2010 年上半年中国大陆僵尸网络受控主机 IP 数量月度统计

2010年上半年CNCERT监测到僵尸网络按规模分布如图6-7所示，1千以内规模的僵尸网络约占总数的99%，僵尸网络规模继续呈现小型化。

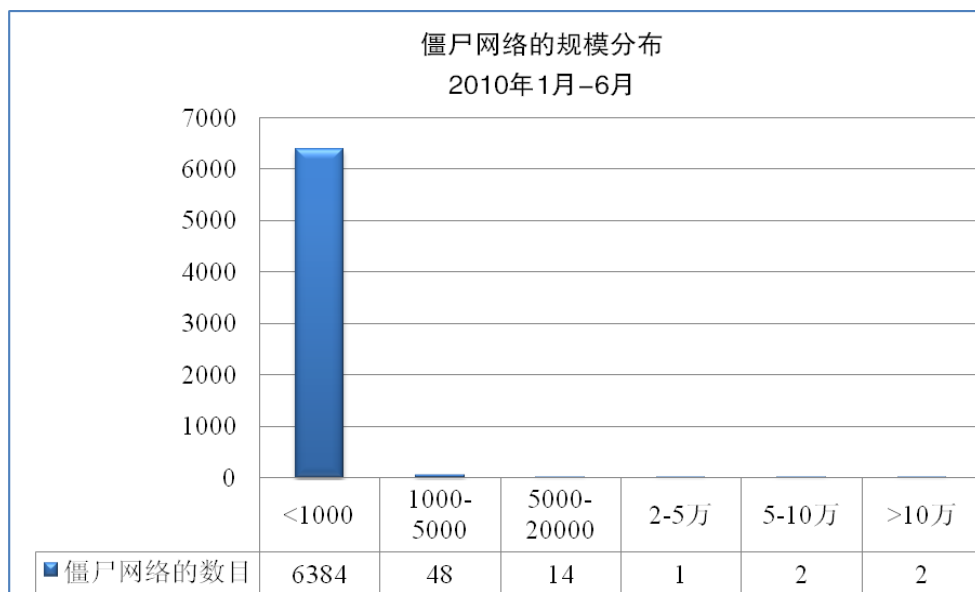


图 6-7 2010 年上半年僵尸网络规模分布图

■ 中国大陆地区僵尸网络受控主机分布统计

根据CNCERT抽样监测结果，2010年上半年中国大陆有233335个IP地址的主机感染僵尸程序。中国大陆僵尸网络受控主机IP分布情况如图6-8所示，僵尸网络受控主机最多的地区分别为广东省（11.28%）、上海市（9.08%）、浙江省（7.93%）、北京市（6.62%）和河南省（5.80%）。

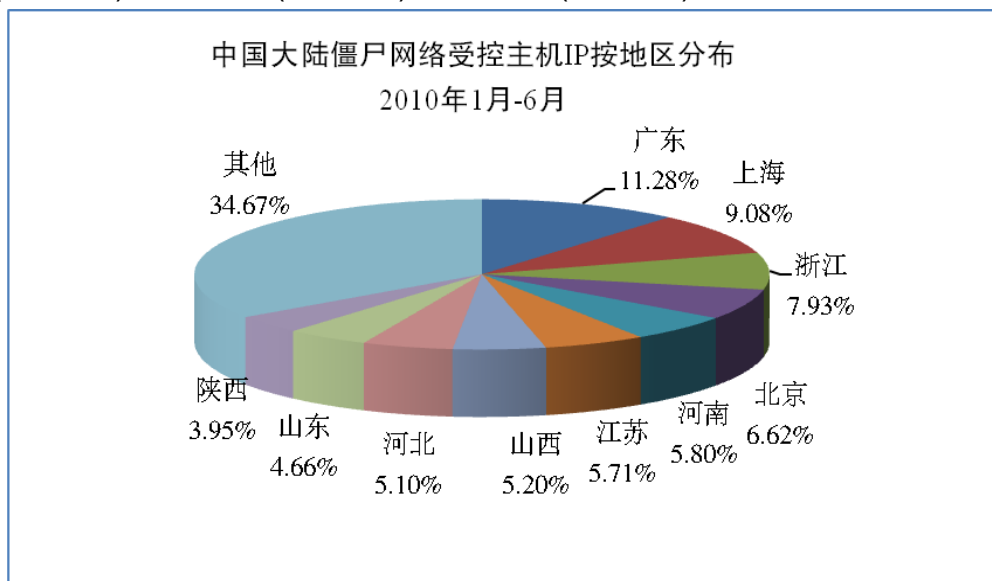


图 6-8 2010 年上半年中国大陆僵尸网络受控主机按地区分布

图6-9所示为2010年上半年中国大陆僵尸网络受控主机在各运营商中的分布。其中，电信网占60.49%，联通占28.09%，移动占0.34%。

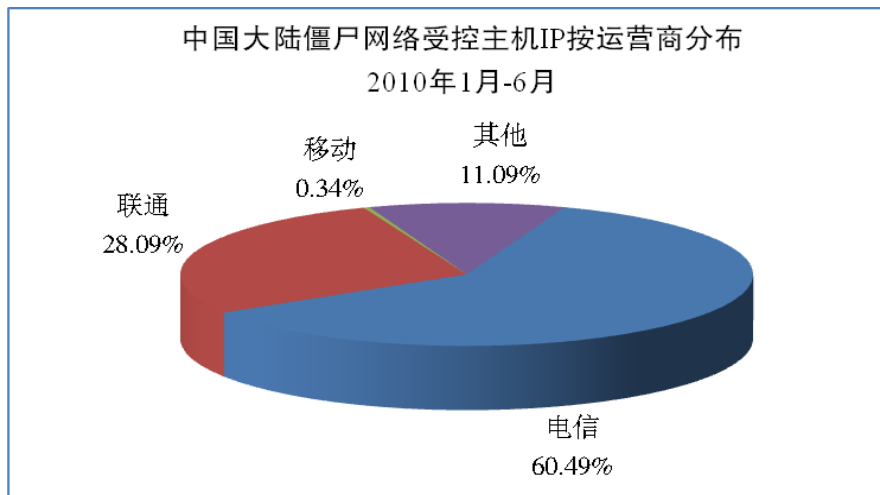


图 6-9 2010 年上半年中国大陆僵尸网络受控主机 IP 按运营商分布

■ 境外僵尸网络控制服务器分布统计

CNCERT同时发现境外有4584个主机IP作为僵尸网络控制服务器参与控制我国境内僵尸网络受控主机。僵尸网络控制服务器IP按国家和地区分布如图6-10所示，其中位于美国(24.21%)、土耳其(7.98%)、印度(6.94%)、英国(5.08%)和巴西 (2.84%) 的僵尸网络控制服务器IP数量居前五位。

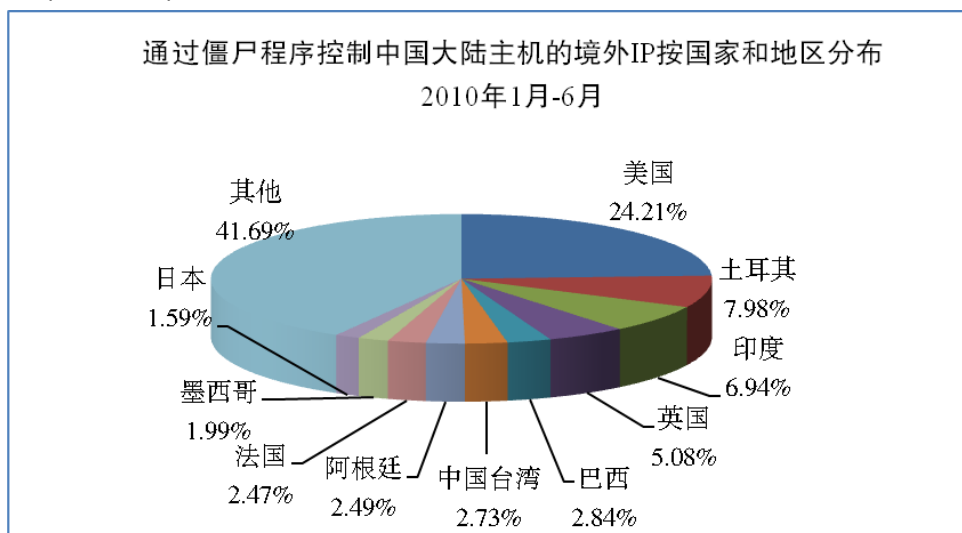


图 6-10 2010 年上半年通过僵尸程序控制我国计算机的境外 IP 按国家和地区分布

7. 被篡改网站监测分析

自 2003 年 CNCERT 便开始监测中国大陆地区网站被篡改情况，并在发现被篡改网站后及时通知网站所在省份的分中心协助解决，争取被篡改网站快速恢复。

7.1 我国网站被篡改情况

2010 年上半年，CNCERT 的监测结果显示，中国大陆地区被篡改网站数量为 14907 个，较 2009 年上半年下降 21.8%。中国大陆地区网页篡改数量月度统计情况如图 7-1 所示，网页篡改数量在 4 月达到峰值 2889 个，第二季度较第一季度总体呈上升趋势。

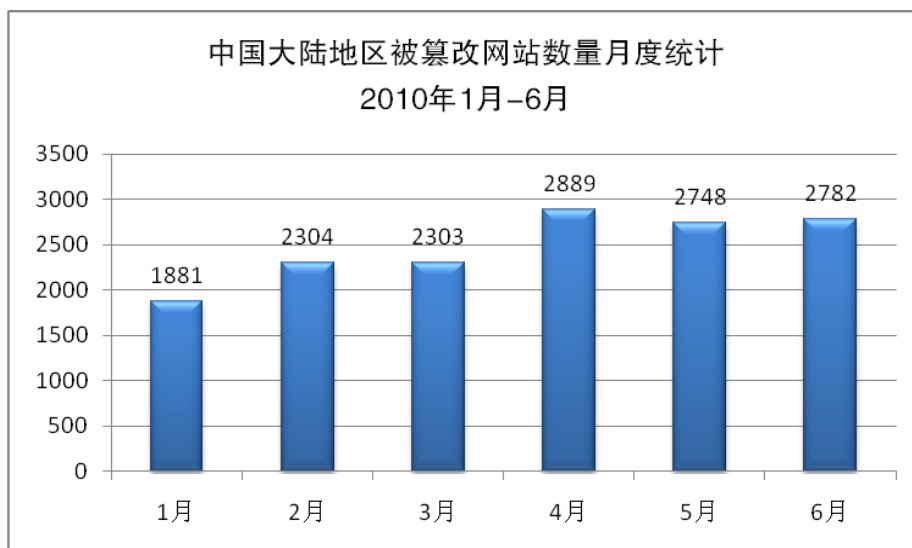


图 7-1 2010 年上半年中国大陆地区网页篡改数量月度统计

7.2 中国大陆地区政府网站被篡改情况

2010 年上半年，中国大陆政府网站被篡改数量为 2574 个，较 2009 年上半年的 798 个增长 222.6%。中国大陆被篡改的网站中政府网站的数量如图 7-2 所示。经统计，每月被篡改的 gov.cn 域名网站约占整个大陆地区被篡改网站的 17.27%，而 gov.cn 域名网站仅占大陆地区总网站数的 0.3%，由此可以看出政府网站是黑客攻击的重要目标。

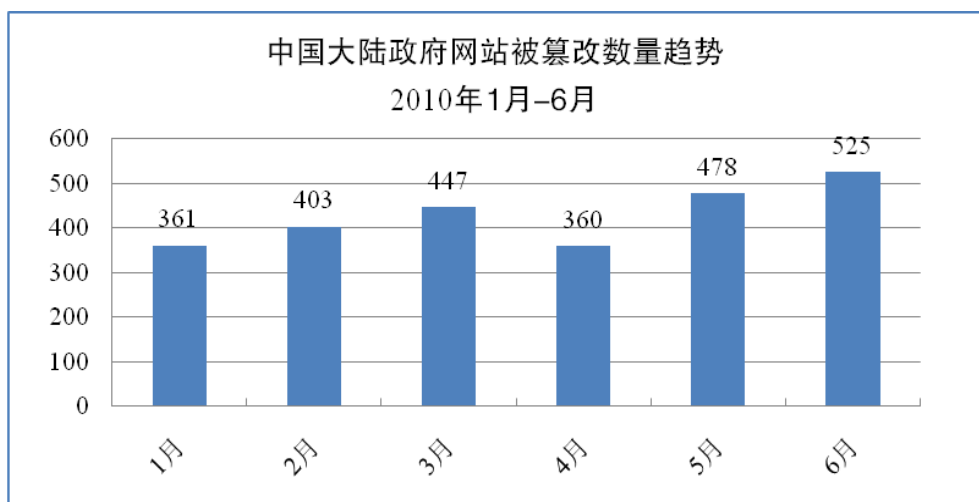


图 7-2 2010 年上半年中国大陆被篡改的网站中政府网站的数量和比例

政府网站易被篡改的主要原因是网站整体安全性差，缺乏必要的经常性维护，某些政府网站被篡改后长期无人过问，还有些网站虽然在接到报告后能够恢复，但并没有根除安全隐患，从而遭到多次篡改。政府网站作为行政事务公开和政务信息发布平台，其安全防护意识仍旧比较淡薄。

7.3 黑客篡改我国网站活动情况

2010 年上半年，国内外黑客（组织）对中国大陆网站进行攻击的活动比较猖獗。表 7-1 列出了排名前 20 位篡改中国大陆网站的黑客信息，这些黑客篡改的网站数量大多都在 100 个以上。大量网站被篡改说明中国大陆很多网站存在较为严重的安全漏洞，特别是一些安全漏洞可能影响采用同一网站架构或建站系统的一批网站，以至于黑客可以在短时间内批量对网站实施篡改。

表 7-1 2010 年上半年篡改中国大陆网站的黑客按数量排名前 20 位

2010 年上半年篡改中国大陆网站的黑客按攻击次数排名前 20 位		
排名	黑客名称	数量
1	Timeless	454
2	By_aGReSiF	352
3	Joker	242
4	iskorpitx	205
5	Link	196

6	Hmei7	176
7	冰鱼	155
8	aGResiF	148
9	HEXB00T3R	145
10	Cracker-Mr.X	140
11	qq1281232825	137
12	X7-HaCker	123
13	ZoRRoKiN	117
14	用幸福触摸忧伤@W.S.H	103
15	DATA ir Security Group	99
16	Trotou	95
17	TeaM HITMAN HaCkEr	91
18	ck	88
19	Dirk	84
20	树枝	81

8. 网页仿冒事件情况

2010 年上半年 CNCERT 共接到网页仿冒（俗称网络钓鱼）事件报告 740 次，经归类合并后 CNCERT 成功处理了 308 件，处理数量超过 2009 年全年，较 2009 年上半年增长 140.6%。在 CNCERT 接收到的这些网页仿冒事件中，被仿冒的大都是大型电子商务网站、大型金融机构网站、第三方在线支付站点、大型社区交友网站。表 8-1 列出了前 10 名的被仿冒网站。

表 8-1 2010 年上半年被仿冒网站按次数排行 TOP10

2010 年上半年 CNCERT 接收到的被仿冒网站按事件次数排序前 10 名	
被仿冒网站	次数
BANCO BRADESCO S.A. (巴西布拉德斯科银行)	72
BBVA (毕尔巴鄂比斯开银行)	72
ALLIANCE LEICESTER BANK (英国联合莱斯特银行)	49
HSBC (中国香港汇丰银行)	49
CCTV (中国中央电视台)	41
Ebay (美国网上交易站)	32
PNC (美国 PNC 金融服务集团)	25
Internal Revenue Service (美国国家税务局)	22
CECA (西班牙储蓄银行联盟)	17
Twitter (美国社交及微博服务网站)	12

9. 通信行业网络安全信息通报情况

2009 年 6 月 1 日起工业和信息化部颁布的《互联网网络安全信息通报实施办法》正式实施。一年来，在各有关单位的共同努力下，CNCERT 与各省通信管理局、基础电信运营企业、增值电信业务经营者、域名注册管理和服务机构、互联网协会等单位建立了顺畅的通报工作机制，并制定了规范的工作流程。同时，CNCERT 积极拓展安全企业、增值电信业务经营者等纳入信息通报工作成员单位。截至 2010 年上半年，全国已有 262 家信息通报工作单位。通报工作单位列表详见：<http://www.cert.org.cn/isir.shtml>。通信行业各单位报送的网络安全事件信息对于掌握基础网络设施安全状况以及公共互联网环境安全状况具有重要的参考意义。

2010 年上半年，CNCERT 共接收各地通信管理局、基础电信运营企业集团公司汇总的各类网络安全事件共 158515 件，图 9-1 所示为 2010 年上半年各月报送情况统计。

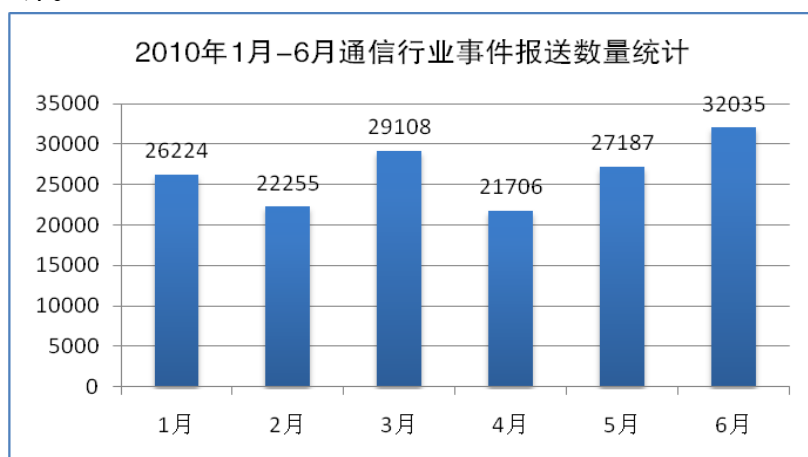


图 9-1 2010 年上半年通信行业报送的网络安全事件数量月度统计

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。如图 9-2、9-3 所示，2010 年上半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，其所占比例分别达到 63.8%和 36.0%。这当中，公共互联网安全事件又以垃圾邮件、僵尸网络事件和木马居多。另外，基础 IP 网络中多为基础电信运营企业报送的针对 IDC 或相关增值业务系统的流量事件。

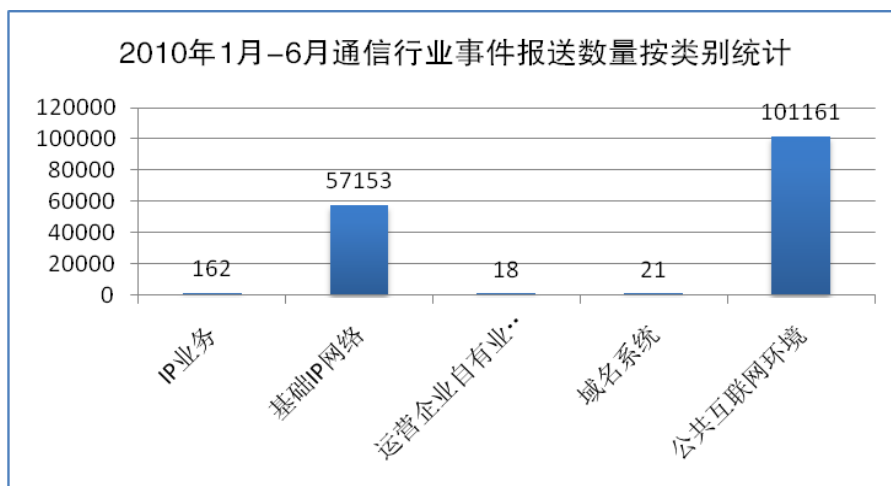


图 9-2 2010 年上半年通信行业报送的网络安全事件数量按类别统计

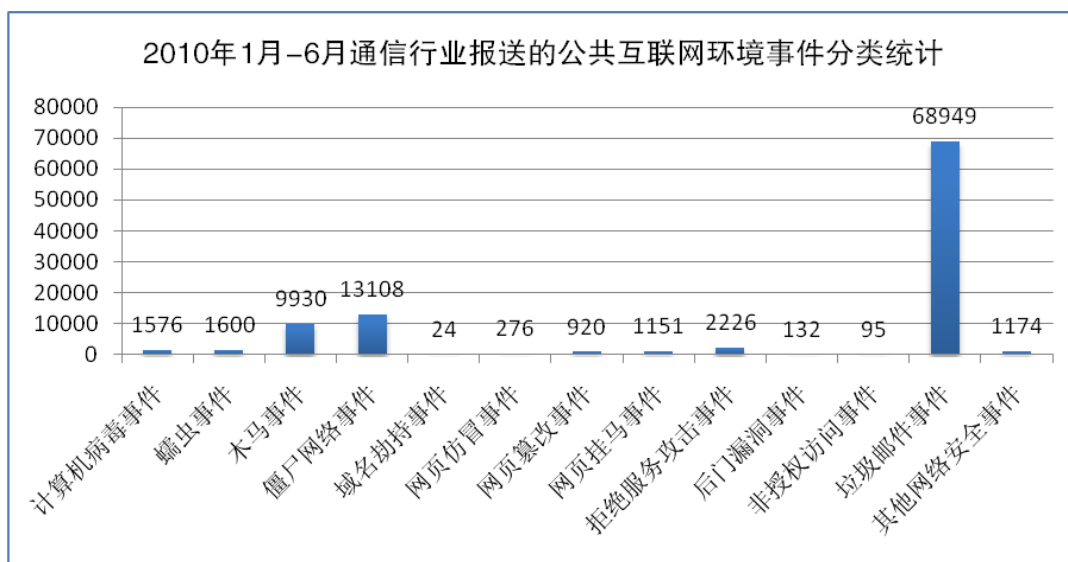


图 9-3 2010 年上半年通信行业报送的公共互联网环境事件数量分类统计

安全企业在网络安全事件监测以及网络安全信息收集方面具备较强的技术和业务能力，其报送信息已成为基础运营商等单位报送数据的重要补充。2010 年上半年，在信息通报、国家信息安全漏洞共享平台（CNVD）和中国反网络病毒联盟（ANVA）组织框架下，积极向 CNCERT 国家中心报送和研判漏洞信息的企业有：启明星辰、东软、绿盟、安氏领信、知道创宇、安天；每周或每月报送网页挂马信息的企业有：微软、华为、奇虎 360、知道创宇、绿盟、金山、联想网御、安天、启明星辰、东软、浪潮；每周或每月报送和分析恶意代码样本信息的企业有：奇虎 360、瑞星、金山、启明星辰、安天、绿盟；每月报送典型事件处理案例的企业有：安氏领信、网御神州；此外，积极报送其他事件信息和预警信息的企业有：启明星辰、东软、绿盟、安天、华为、天融信、金山、奇虎

360、瑞星、浪潮、安氏、联想网御、网御神州、知道创宇。

2010 年 3 月份起，根据安全企业报送的恶意域名及恶意 URL 信息，CNCERT 重点跟踪并积极处置如下几组侵害中国大陆地区网站的用于网页挂马的恶意域名。

表 9-3 2010 年上半年侵害中国大陆地区网站较为活跃的恶意域名组

2010 年上半年侵害中国大陆地区网站较为活跃的恶意域名组	
组别	恶意域名组特征和数量描述
第一组	注册在 inc.0rg.fr、conna.dtdns.net、officea.ze.tc 等域上的恶意域名，主要用于构建恶意跳转链接，每周监测发现的三级域名数量以数十、数百计
第二组	注册在 2288.org、3322.org、8800.org、8866.org、9966.org 上的恶意域名，被发现用于网页挂马的各个环节，如：恶意跳转链接、网页木马集成页面、漏洞触发页面以及恶意代码下载服务器，每周监测发现的三级域名数量以数百计
第三组	注册在 xorg.pl 域上的恶意域名，主要用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计，6 月份活跃程度有所下降
第四组	注册在 wwwv.us 域上的恶意域名，三级域名前缀经常采用国内外知名站点，特征明显，每周监测发现的三级域名数量约为 10 余个，但活跃周期长，侵害的网站数量均较大。
第五组	注册在 isgre.at、rr.nu 域上的恶意域名，三级域名命名呈现有规律的按字母顺序变换，用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计
第六组	注册在.info 域上的恶意域名，三级域名命名为“单字母+含 2012 字符串+.info”形式，用于构建恶意跳转链接，每周监测发现的三级域名数量以数十计甚至上百。