

《2013 年中国互联网网络安全报告》

编 委 会

主 任 委 员	黄澄清				
副主任委员	云晓春	刘欣然			
执 行 委 员	王明华	严寒冰	李 佳	贺 敏	纪玉春
委 员	徐 娜	徐 原	何世平		
	温森浩	赵 慧	李志辉		
	姚 力	张 洪	朱芸茜		
	朱 天	高 胜	胡 俊		
	王小群	张 腾	何能强		
	摆 亮	陈 阳	李世淙		
	党向磊	徐晓燕	王适文		
	刘 婧	饶 毓	赵 宸		

前言 *PERFACE*

当前，互联网在我国政治、经济、文化以及社会生活中发挥着越来越重要的作用。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，英文缩写为 CNCERT 或 CNCERT/CC）作为我国非政府层面网络安全应急体系核心技术协调机构，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，在网络安全监测、预警、处置等方面积极开展工作，历经十余年的实践，形成多种渠道的网络攻击威胁和安全事件发现能力，与国内外数百个机构和部门建立网络安全信息通报和事件处置协作机制，依托所掌握的丰富数据资源和信息实现对网络安全威胁和宏观态势的分析预警，在维护我国公共互联网环境安全，保障基础信息网络和网上重要信息系统安全运行，保护互联网用户上网安全，宣传网络安全防护意识和知识等方面起到重要作用。

自 2004 年起，国家互联网应急中心根据工作中受理、监测和处置的网络攻击事件和安全威胁信息，每年撰写和发布《CNCERT 网络安全工作报告》，为相关部门和社会公众了解国家网络安全状况和发展趋势提供参考。2008 年，在收录、统计通信行业、网络安全企业相关部门网络安全工作情况和数据的基础上，《CNCERT 网络安全工作报告》正式更名为《中国互联网网络安全报告》。自 2010 年起，在工业和信息化部通信保障局的指导和互联网网络安全应急专家组的帮助下，国家互联网应急中心精心编制并公开发布年度互

联网网络安全态势报告，受到社会各界的广泛关注。

《2013 年中国互联网网络安全报告》汇总分析国家互联网应急中心自有网络安全监测数据和通信行业、网络安全企业相关单位报送的大量信息，具有鲜明的行业特色。报告涵盖互联网网络安全宏观形势判断，网络安全监测数据分析，网络安全事件案例详解，网络安全政策和技术动态等多个方面的内容。其中，报告对计算机恶意程序传播和活动，移动互联网恶意程序传播和活动，网站安全监测，安全漏洞预警与处置，网络安全事件接收与处理，网络安全信息通报等情况进行深入细致的分析。同时，报告对 2013 年开展的防范治理黑客地下产业链专项行动，对 DDoS 攻击的监测分析等进行专题介绍，并吸纳互联网行业单位针对典型网络安全事件的深入分析报告。接下来，报告对 2013 年国内外网络安全监管动态、国内网络安全组织发展情况、国内外网络安全重要活动做了阶段性总结。最后，针对当前网络安全的热点和难点问题，对 2014 年网络安全的威胁和形势做出判断。

国家互联网应急中心

2014 年 4 月

致 谢 *THANKS*

《2013 年中国互联网网络安全报告》的写作素材均来自国家互联网应急中心网络安全工作实践。国家互联网应急中心网络安全工作离不开政府主管部门长期以来的关心和指导，也离不开各互联网运营企业、网络安全企业、安全研究机构以及相关合作单位的大力支持。

在《2013 年中国互联网网络安全报告》撰写过程中，国家互联网应急中心向北京网秦天下科技有限公司、北京网御星云信息技术有限公司、哈尔滨安天信息技术有限公司、恒安嘉新（北京）科技有限公司、金山网络技术有限公司、卡巴斯基技术开发（北京）有限公司、奇虎 360 公司、洋浦科技有限公司等单位征集了专题和数据素材^[1]，在此一并致谢。

由于编者水平有限，《2013 年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，国家互联网应急中心诚挚地希望广大读者不吝赐教，多提意见，并继续关注和支持国家互联网应急中心的发展。国家互联网应急中心将更加努力地工作，不断提高技术和业务能力，为我国以及全球互联网的安全保障贡献力量。

[1] 《2013 年中国互联网网络安全报告》中其他单位所提供数据的真实性和准确性由报送单位负责，国家互联网应急中心未做验证。

关于国家计算机网络应急技术处理协调中心

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”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

2003 年，国家互联网应急中心在全国 31 个省（自治区、直辖市）成立分中心。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

国家互联网应急中心的主要业务能力如下。

事件发现。依托“863-917 公共互联网网络安全监测平台”，开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，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多种渠道发现网络攻击威胁和网络安全事件。

预警通报。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危害较大的事件报告，及时响应并积极协调处置，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。

测试评估。作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为

政府部门、企事业单位提供安全评测服务。CNCERT/CC 还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

同时，作为中国非政府层面开展网络安全事件跨境处置协助的重要窗口，CNCERT/CC 积极开展网络安全国际合作，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。CNCERT/CC 为国际著名网络安全合作组织 FIRST 的正式成员以及亚太应急组织 APCERT 的发起者之一。截至 2013 年，CNCERT/CC 已与 59 个国家和地区的 127 个组织建立了“CNCERT/CC 国际合作伙伴”关系。

联系方式

网址：<http://www.cert.org.cn/>

电子邮件：cncert@cert.org.cn

热线电话：+8610 82990999（中文），82991000（English）

传真：+8610 82990399

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

目 录 CONTENT

1	2013 年网络安全状况综述.	13
1.1	我国互联网网络安全总体状况	13
1.2	数据导读	22
2	网络安全专题分析	24
2.1	防范黑客地下产业链专项行动专题分析（来源：CNCERT/CC）	24
2.2	DDoS 攻击专题分析（来源：CNCERT/CC）	28
2.3	从“棱镜”看国内网络安全（来源：安天公司）	38
2.4	APT 攻击技术研究及防范（来源：网御星云）	41
2.5	网上交易服务安全风险分析（来源：奇虎 360 公司）	51
3	计算机恶意程序传播和活动情况	63
3.1	木马和僵尸网络监测情况	63
3.2	“飞客”蠕虫监测情况	73
3.3	恶意程序传播活动监测	75
3.4	通报成员单位报送情况	77
4	移动互联网恶意程序传播和活动情况	88
4.1	移动互联网恶意程序监测情况	88

4.2 移动互联网恶意程序传播活动监测	90
4.3 通报成员单位报送情况	92

5 网站安全监测情况 104

5.1 网页篡改情况	104
5.2 网页挂马情况	108
5.3 网页仿冒情况	113
5.4 网站后门情况	115

6 安全漏洞预警与处置 119

6.1 CNVD 漏洞收录情况	119
6.2 高危漏洞典型案例	123
6.3 CNVD 行业漏洞库	127
6.4 CNVD 漏洞处置情况	132

7 网络安全事件接收与处理 134

7.1 事件接收情况	134
7.2 事件处理情况	136
7.3 事件处理典型案例	139

8 网络安全信息通报情况 146

8.1 互联网网络安全信息通报	146
8.2 行业外互联网网络安全信息发布情况	149

9 国内外网络安全监管动态 151

9.1 2013 年国内网络安全监管动态	151
9.2 2013 年国外网络安全监管动态	154

10	国内网络安全组织发展情况	168
10.1	网络安全信息通报成员发展情况	168
10.2	CNVD 成员发展情况	171
10.3	ANVA 成员发展情况	173
10.4	CNCERT/CC 应急服务支撑单位	175
11	国内外网络安全重要活动	178
11.1	国内重要网络安全会议和活动	178
11.2	国际重要网络安全会议和活动	181
12	2014 年网络安全热点问题	186
13	网络安全术语解释	189



1 2013年网络安全状况综述

1.1 我国互联网网络安全总体状况

习近平总书记指出：“没有网络安全，就没有国家安全”。以互联网为核心的网络空间已成为继陆、海、空、天之后的第五大战略空间，各国均高度重视网络空间的安全问题。2013年，斯诺登披露的“棱镜门”事件如同重磅炸弹，更是引发了国际社会和公众对网络安全的空前关注。

在我国，随着“宽带中国”战略推进实施，互联网全面升级提速，用户规模快速增长，移动互联网新型应用层出不穷，4G网络正式启动商用，虚拟运营商牌照陆续发放，网络化和信息化水平显著提高，极大地促进了传统产业转型升级，带动了信息消费稳步增长。

维护互联网网络安全，是保障各领域信息化工作持续稳定发展的先决条件。我国政府相关部门、互联网服务机构、网络安全企业和广大网民对网络安全的重视程度日益提高，不断加强自身防护水平，加大网络安全威胁治理力度，积极参与网络安全国际合作，以期建立安全可信的网络环境，确保基础网络和重要信息系统安全运行，促进产业经济稳定发展。

在各方共同努力下，2013年我国互联网网络安全状况总体平稳。然而，根据CNCERT/CC监测数据和通信行业报送的信息，我国互联网仍然存在较多网络攻击和安全威胁，不仅影响广大网民利益，妨碍行业健康发展，甚至对社会经济和国家安全造成威胁和挑战。本综述着重分析和总结2013年我国互联网面临的安全形势和威胁。

（1）基础信息网络运行总体平稳，域名系统依然是影响安全的薄弱环节。2013年，我国基础网络安全防护水平有较大提升，但仍然发现较多信息系统安全风险，尤其是域名系统作为互联网运行的关键基础设施，面临安全漏洞和拒绝服务攻击等多种威胁，是影响网络稳定运行的薄弱环节。基础网络承载的互联网业务类型日益增多，

引发一些安全风险。

基础网络安全防护水平进一步提高。2013年，在工业和信息化部指导下，基础电信企业高度重视网络安全防护工作，在全网开展网络单元和业务系统的定级备案调整工作，对3000余个三级及以上网络单元开展符合性评测和风险评估，各企业符合性评测达标率均在97%以上，与2012年基本持平。在检测中还侧重加大对用户个人信息保护工作的检查力度，通过对安全隐患的测试和修复，有效降低了通信网络的安全风险。

基础网络信息系统仍存在较多安全风险。2013年，国家信息安全漏洞共享平台（CNVD^[2]）向基础电信企业通报漏洞风险事件518起，较2012年增长超过一倍。按漏洞风险类型分类，其中通用软硬件、信息泄露、权限绕过、SQL注入、弱口令等类型较多，分别占42.1%、15.3%、12.7%、12.0%和11.2%。这些漏洞风险事件涉及的信息系统达449个，其中基础电信企业省（子）公司所属信息系统占54.6%，集团公司所属信息系统占37.2%。对此，各企业均积极响应，及时进行修复加固处理。但是，2013年仍发现有部分企业的接入层网络设备被攻击控制，网络单元稳定运行以及用户数据安全受到威胁，我国基础网络整体防御国家级有组织攻击风险的能力仍较为薄弱。

域名系统依然是影响互联网稳定运行的薄弱环节。域名解析服务是互联网重要的基础应用服务，其安全问题直接影响网络的稳定运行。由于域名注册服务机构的域名管理系统存在漏洞，攻击者能随意篡改域名解析记录，2013年曾发生多起由此引发的政府部门网站和提供互联网服务的网站域名被劫持的事件，导致用户访问受到严重影响。此外，域名系统遭受拒绝服务攻击的现象日益严重。2013年8月25日，黑客为攻击一个以.CN结尾的网游私服网站，对我国.CN顶级域名系统发起大规模的拒绝服务攻击，导致大量政府网站、新浪微博等重要网站无法访问或访问缓慢。同年8月，域名注册服务机构爱民网（22.cn）的域名服务器在一周内连续遭受数十Gbit/s级的拒绝服务攻击，数万个域名受到影响。据CNCERT/CC监测，2013年针对我国域名系统较大规模的拒绝服务攻击事件日均约有58起。直接针对域名系统发起攻击，不仅能使目标网站瘫痪，还会导致大量无辜网站受到牵连，从而造成严重后果。

[2] CNVD是CNCERT/CC联合国内重要信息系统单位、基础电信企业、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。



对此，CNCERT/CC联合基础电信企业，积极配合政府部门，大力推进虚假源地址流量整治工作，将我国互联网虚假源地址流量占全部流量的比例控制在1%以内，有效提高了攻击源追溯能力，为国家.CN域名系统遭受攻击等重大事件查处提供了有力支撑。但与此同时，监测发现大量来自境外的虚假源地址攻击流量，给事件处置和攻击追溯带来很大困难。

2013年3月，国际反垃圾邮件组织Spamhaus遭受攻击，攻击峰值达300Gbit/s，堪称互联网史上最大流量的拒绝服务攻击。攻击者借助互联网庞大的开放域名解析服务器群，利用DNS反射技术发送大量伪造的DNS解析请求，使服务器向目标网站发送大量长字节应答包，从而对目标网站形成放大约100倍的攻击流量。互联网上大量存在的开放递归查询域名服务器，有可能成为黑客实施攻击的“军火库”。

基础信息网络承载的互联网业务频现安全问题。随着基础网络设施不断完善，其所承载的互联网业务类型日益增多，引入新的安全风险。2013年7月22日，腾讯微信业务出现故障，全国多地有6000多万用户无法正常使用，用户感知强烈。微信属于目前较为流行的OTT（Over The Top）业务模式，通过基础电信企业的网络发展自己的音视频和数据服务业务，但其安全保障水平和业务承载级别不匹配，一条线路的故障就能导致多家基础电信企业的用户受到影响。2013年，部分互联网公司的网站域名在某些地区被劫持，甚至被强行插入广告窗口，某些宽带接入商在小区路由器上对部分网站进行劫持跳转等事件，严重影响用户体验，损害互联网企业和网民利益。CNCERT/CC接到上述事件投诉后，及时协调相关单位进行处置。互联网业务的不断创新导致安全问题不断演化，如何及时、有效应对，需要互联网服务商和基础电信企业共同努力。

（2）公共互联网治理初见成效，打击黑客地下产业链任重道远。2013年工业和信息化部组织开展防范治理黑客地下产业链专项行动，及时处置木马僵尸等网络攻击威胁，取得一定成效。但网络设备后门、个人信息泄露等事件频繁出现，表明公共互联网环境仍然存在较多安全问题。

近年来我国境内感染木马僵尸网络主机数量首次下降。据CNCERT/CC监测，2013年我国境内感染木马僵尸网络的主机为1135万个，控制服务器为16万个，分别较2012年下降22.5%和44.1%，为近5年首次出现下降。这反映出我国持续开展木马僵尸网络专项治理行动和日常处置工作已初见成效。

2013年，在工业和信息化部组织开展的防范治理黑客地下产业链专项行动中，CNCERT/CC会同基础电信企业、域名注册服务机构共开展8次恶意程序专项打击工作，清理木马僵尸网络控制服务器3.4万余台，受控主机近72万台，重点处理控制规模较大的僵尸网络1455个，切断了黑客对375万余台感染主机的控制，有力地净化公共互联网环境。虽然我国境内感染的主机数量总体有所下降，但感染远程控制类木马的主机数量较2012年小幅上涨4.4%，这类木马能对用户主机实施远程控制、窃取重要文件和敏感信息或发起网络攻击，具有极大的危害性。

分析发现D-LINK等众多网络设备存在后门。2013年，CNVD共收录各类安全漏洞7854个，其中高危漏洞2607个，分别较2012年增长15.1%和6.8%。涉及通信网络设备的软硬件漏洞数量为505个，较2012年增长1.5倍，占CNVD收录漏洞总数的比例由2012年的2.9%增长至6.4%。同时，CNVD分析验证D-LINK、Cisco、Linksys、Netgear、Tenda等多家厂商的路由器产品存在后门，黑客可由此直接控制路由器，进一步发起DNS劫持、信息窃取、网络钓鱼等攻击，直接威胁用户网上交易和数据存储安全，使得相关产品变成随时可被引爆的安全“地雷”。以D-LINK部分路由器产品为例，攻击者利用后门可取得路由器的完全控制权，CNVD分析发现受该后门影响的D-LINK路由器在互联网上对应的IP地址至少有1.2万个，影响大量用户。CNVD及时向相关厂商通报威胁情况，向公众发布预警信息，但截至2014年1月底，仍有部分厂商尚未提供安全解决方案或升级补丁。路由器等网络设备作为网络公共出口，往往不引人注意，但其安全不仅影响网络正常运行，而且可能导致企业和个人信息泄露。

个人信息泄露问题挑战现有社会信任机制。云计算、移动互联网、社交网络等互联网新技术新业务正在改变个人信息的收集和使用方式，个人信息的可控性逐步削弱，姓名、住址、电话、身份证号、消费记录等重要生活信息越来越多地出现网络泄露问题。

2013年10月，“查开房”网站公开曝光2000万条客户酒店入住信息，据比对，该信息是往年泄露的，但其中涉及大量个人隐私信息，严重影响公众生活。该事件发生后，CNCERT/CC立即联系协调美国计算机应急响应组织（US-CERT）和相关域名注册服务机构对之进行处置，有效阻止了信息进一步泄露和扩散。2013年7月，Apache Struts 2被披露存在远程代码执行高危漏洞，可直接导致服务器被远程



控制或数据被窃取，多家大型电商和互联网企业以及大量政府、金融机构网站受到影响，上亿用户信息面临严重泄露风险。由于信息管理制度不完善，保险订单、航班订单、网购订单和快递物流单据等包含的用户个人信息被大量滥用，甚至公开售卖，也是个人信息泄露的重要原因之一。这些姓名、身份证号、电话等信息的真实性极高，被黑客广泛用来实施欺诈和社会工程学攻击，给现有社会信任机制带来严重挑战。

（3）移动互联网环境有所恶化，生态污染问题亟待解决。2013年，移动互联网恶意程序数量继续大幅增长，恶意程序的制作、发布、预装、传播等初步形成一条完整的利益链条，移动互联网生态系统环境呈恶化趋势，亟须加强管理。

针对安卓平台的恶意程序数量呈爆发式增长。2013年，CNCERT/CC通过自主监测和交换捕获的移动互联网恶意程序样本达70.3万个，较2012年增长3.3倍，其中针对安卓平台的恶意程序占99.5%。按照恶意程序行为属性统计，恶意扣费类数量仍居第一位，占71.5%，较2012年的39.8%有大幅增长；其次是资费消耗类（占15.1%）、系统破坏类（占3.2%）和隐私窃取类（占3.2%），与用户经济利益密切相关的恶意扣费类和资费消耗类恶意程序占总数的85%以上，表明黑客在制作恶意程序时带有明显的逐利倾向。按恶意程序的危害等级分类，高危占1.0%，中危占29.0%，低危占70.0%。其中，高危恶意程序所占比例较2012年大幅下降，反映出黑客为降低风险，从制作恶性性明显的木马或病毒转向制作恶意广告、恶意第三方插件等灰色应用，以达到既逃避监管又获取经济利益的目的。

手机恶意程序传播渠道多样化。2013年CNCERT/CC监测发现移动互联网恶意程序传播次数达到1296万余次，移动互联网恶意程序下载链接1207万个，用于传播移动互联网恶意程序的域名15247个、IP地址60976个，分别是2012年的23倍、33倍、32倍和11倍。这些域名包括移动应用商店、论坛、网盘、博客等众多类型，其中仅移动应用商店的数量就超过300家。移动应用商店的审核机制不完善、安全检测能力差等问题，使得恶意程序得以发布和扩散，仅“安丰市场”就有数千个流行的移动应用被植入木马程序，下载次数超过200万次。2013年发现某电商出售的行货手机，被第三方预置隐私窃取类手机病毒，能静默上传手机号、IMEI号、联网IP地址、位置信息、程序列表等，累计感染人数超过200万。移动应用商店、手机经销商等移动互联网生态系统的上

游环节被污染，导致下游用户感染恶意程序的速度加剧。

对此，CNCERT按照工业和信息化部发布的《移动互联网恶意程序监测与处置机制》，组织开展了8次移动互联网恶意程序治理行动，累计协调应用商店下架恶意应用软件37507个。2013年，中国反网络病毒联盟（ANVA）^[3]建立了“移动互联网应用自律白名单”机制，组织安全企业和应用商店成立白名单工作组和应用商店自律组，形成有序的白名单审核流程和执行机制，并公布了首批“移动互联网应用自律白名单”，以帮助应用商店、移动应用开发人员和广大用户推广或使用安全可信的“白应用”。

（4）经济信息安全威胁增加，信息消费面临跨平台风险。2013年，互联网与金融行业深度融合，以余额宝、现金宝、理财通等为代表的互联网金融产品市场火爆，在线经济活动日趋活跃。但与此同时，钓鱼攻击呈现跨平台发展趋势，在线交易系统防护稍有不慎即可能引发连锁效应，影响金融安全和信息消费。

跨平台钓鱼攻击出现并呈增长趋势。2013年，在传统互联网的钓鱼网站之外，黑客还结合移动互联网，利用仿冒移动应用、移动互联网恶意程序、伪基站等多种手段，实施跨平台的钓鱼欺诈攻击，危害用户经济利益。2013年，黑客利用安卓系统的“签名验证绕过”高危漏洞，制作散播大量仿冒国内主流银行等金融机构的移动应用，诱导用户安装，盗取用户银行账户信息。一些钓鱼网站在盗取用户银行账号和密码等信息时，还大量传播仿冒相应手机银行安全插件的恶意程序，劫持用户收到的短信验证码，从而使黑客进一步完成网银支付、转账等交易操作，牟取经济利益。此外，2013年利用伪基站进行欺诈的活动呈爆发趋势，一类是仿冒金融机构官方服务号码向周围用户发送钓鱼短信，致使一些大型银行被迫调整部分手机银行业务；另一类是冒充基础电信企业客服电话或手机充值号码联系用户，实施充值诈骗。此类事件不仅严重破坏企业形象，也对相关行业的健康发展造成不良影响。

2013年钓鱼网站数量继续迅速增长，CNCERT/CC共监测发现针对我国银行等境内网站的钓鱼页面30199个，涉及IP地址4240个，分别较2012年增长35.4%和64.6%。CNCERT/CC全年接收到网络钓鱼类事件举报10578起，处置事件10211起，分别较2012年增长11.8%和55.3%，为广大网民挽回数亿元损失。

[3] ANVA是由中国互联网协会信息安全工作委员会发起，CNCERT/CC具体组织运行的行业联盟。



在线交易系统安全问题易引发连锁效应。2013年，互联网金融市场火爆，互联网和移动通信技术降低了使用门槛，在带来便利的同时也引入新的安全风险。2013年12月，支付宝钱包客户端iOS版被披露存在手势密码漏洞，连续输错5次手势密码后可导致密码失效，使得攻击者可以任意进入手机支付宝账户，免密码进行小额支付。此后淘宝网被披露存在认证漏洞，可登录任意淘宝账户，给用户资金安全造成威胁。此类互联网公司通过所运营的在线交易信息系统，掌握大量用户资金、真实身份、经济状况、消费习惯等信息，系统出现安全问题后，风险随之传导至关联的银行、证券、电商等其他行业，产生连锁反应。2013年，CNCERT/CC监测发现银行、证券等行业联网信息系统的安全漏洞、网站后门、网页篡改等各类安全事件超过500起，存在交易信息被篡改、投资信息被泄露等诸多高危风险。此外，银行信息系统本身的故障可能对经济活动造成影响。2013年，国内两家主流银行的信息系统先后出现全国性大面积故障，导致柜面、ATM、网银、电话语音系统等瘫痪，相关业务受到严重影响。

（5）政府网站面临威胁依然严重，地方政府网站成为“重灾区”。政府网站因其公信力高、影响力大，容易成为黑客攻击目标。2013年，我国政府网站被篡改和植入后门的情况依然严重，相对部委网站而言，地方政府网站是遭受攻击的“重灾区”，影响政府形象及电子政务工作。

地方政府网站是黑客攻击的“重灾区”。据CNCERT/CC监测，2013年，我国境内被篡改网站数量为24034个，较2012年增长46.7%，其中政府网站被篡改数量为2430个，较2012年增长34.9%；我国境内被植入后门的网站数量为76160个，较2012年增长45.6%，其中政府网站2425个，较2012年下降19.6%。在被篡改和植入后门的政府网站中，超过90%是省市级以下的地方政府网站，超过75%的篡改方式是在网站首页植入广告黑链。由于地方政府网站存在技术和管理水平有限、网络安全防护能力薄弱、人员和资金投入不足等问题，其网站服务器成为黑客控制的资源节点。2013年，CNCERT/CC共通报和处置超过1600起涉及政府部门的网站漏洞事件。一些部门收到CNCERT/CC预警通报后置之不理，导致安全威胁长期存在；另一些部门则只针对安全事件简单清除，未对网站进行详细检测和加固处理，导致反复多次遭受攻击。相对于地方政府网站，国务院部委门户网站安全状况较好，未监测发现网页篡改和网站后门事件，不过部分子站和业务系统仍然存在较多安全漏洞和风险点，可能成为黑客进

一步实施攻击的跳板。

境外黑客组织频繁攻击我国政府网站。2013年，境外“匿名者”、“阿尔及利亚黑客”等多个黑客组织曾对我国政府网站发起攻击。其中，“反共黑客”组织较为活跃，持续发起针对我国境内党政机关、高校、企事业单位以及知名社会组织网站的攻击，2013年该组织对我国境内120余个政府网站实施篡改。据监测，该组织利用网站漏洞预先植入后门，对网站实施控制后遂发起攻击，目前至少入侵600余个境内网站，并平均每三天在其社交网站发布一起篡改事件。另有“匿名者”、“阿尔及利亚黑客”等组织先后篡改我国187个政府网站。此外，还出现黑客为报复国家出台的政策，对我国政府网站实施攻击的新苗头。2013年12月19日下午，继央行明确宣布不认可比特币，要求国内第三方支付机构停止为比特币交易平台提供充值和支付服务之后，央行官方网站和新浪官方微博遭到黑客网络攻击，出现间歇性访问困难和大量异常评论。

（6）国家级有组织攻击频发，我国面临大量境外地址攻击威胁。国家级有组织网络攻击行为显著增多，给国家关键基础设施和重要信息系统带来严重威胁和挑战。据CNCERT/CC监测，我国面临大量来自境外地址的网站后门、网络钓鱼、木马和僵尸网络等攻击。

具有国家背景的有组织攻击频发。2013年6月以来，斯诺登曝光“棱镜计划”等多项美国国家安全局网络监控项目，披露美国情报机构对多个国家和民众长期实施监听和网络渗透攻击，引起国际社会强烈反响。根据曝光信息，美国投入巨额资金，分别通过互联网、通信网、企业服务器等多种渠道以及采用网络入侵手段，实施信息监听和收集，监听内容包括互联网元数据、互联网通信内容、社交网络资料、电话和短信息等多种数据类型，监控对象包括多国政要、外交系统、媒体网络、大型企业网络和国际组织等。我国属于其重点监听和攻击目标，国家安全和互联网用户隐私安全面临严重威胁。

2013年，越来越多的有组织高级持续性威胁（APT）攻击事件浮出水面，APT攻击成为国家间网络对抗的新型有力武器。2013年3月20日，美、韩军事演习期间，韩国多家广播电视台和银行等金融机构遭受历史上最大规模的恶意代码攻击，导致系统瘫痪，一度引发韩国社会混乱。CNCERT/CC获知消息后，第一时间与韩国计算机应急响应组织（KrCERT）联系，并协助调查，及时消除攻击来自中国的误会。迈克菲公



司、卡巴斯基实验室等先后曝光持续多年、具有极强隐蔽性的“特洛伊行动”、“红色十月”、“Icefog”等一系列APT攻击，曾大量窃取政府部门、科研机构和重点行业单位的重要敏感信息。我国同样面临严重的APT攻击威胁，一些国家利用信息化技术优势，大力推动研发计算机病毒武器，破解互联网加密算法，或直接在标准算法中放置后门，持续对我国实施APT攻击。我国政府机构、基础电信企业、科研院所、大型商业机构的网络信息系统遭受攻击和渗透入侵。2013年，CNCERT/CC监测发现我国境内1.5万台主机被APT木马控制，对我国关键基础设施和重要信息系统安全造成严重威胁。

我国仍面临大量来自境外地址的攻击威胁。2013年，境外有3.1万台主机通过植入后门对境内6.1万个网站实施远程控制，虽然境外控制主机数量较2012年下降4.3%，但所控制的境内网站数量却大幅增长62.1%。从所控制的境内网站数量看，位于美国的主机居首位，共有6215台主机控制着境内15349个网站，平均每个主机控制2.5个境内网站，较2012年（约1.4个）增长78.6%。其次是中国香港，控制境内13116个网站，较2012年大幅增长179.5%。排名第三的是韩国，控制境内7052个网站，较2012年下降11.1%。

在网络钓鱼攻击方面，针对我国的钓鱼站点有90.2%位于境外，共有3823个境外IP地址承载29966个针对我国境内网站的仿冒页面，分别较2012年增长54.3%和27.8%。从承载的钓鱼页面数量看，美国仍居首位，共有2043台主机承载12573个钓鱼页面，中国香港和韩国列第二、三位，分别承载4500个和1093个钓鱼页面。

在木马僵尸网络方面，我国境内1090万余台主机被境外2.9万余个控制服务器控制，其中位于美国的8807个控制服务器控制了我国境内448.5万余台主机，控制主机数量占被境外控制主机总数的41.1%。从控制服务器占全部境外控制服务器的比例来看，美国占比由2012年的17.6%增长至30.2%，仍居首位；韩国和中国香港分列第二、三位，占比分别为7.8%和7.7%。就所控制的境内主机数量而言，美国居首位，葡萄牙和韩国分列第二、三位，分别控制我国境内398.8万和83.9万台主机。

CNCERT/CC不断加强与国际CERT组织间的网络安全合作，完善跨境网络安全事件处置协作机制。截至2013年年底，已与59个国家和地区、127个组织建立联系机制，全年共协调境外安全组织处理涉及境内的安全事件5498起，较2012年增长35.3%。

1.2 数据导读

多年来，CNCERT/CC对我国网络安全宏观状况进行持续监测，以下是2013年抽样监测获得的主要数据分析结果。

(1) 木马和僵尸程序监测

- 2013年木马或僵尸程序控制服务器IP总数为189369个，较2012年下降47.4%。其中，境内木马或僵尸程序控制服务器IP数量为160228个，较2012年下降44.1%；境外木马或僵尸程序控制服务器IP数量为29146个，较2012年大幅下降60.2%。
- 2013年木马或僵尸程序受控主机IP总数为18702202个，较2012年大幅下降64.5%。其中，境内木马或僵尸程序受控主机IP数量为11352817个，较2012年下降22.5%；境外木马或僵尸程序受控主机IP数量为7349385个，较2012年大幅下降80.7%。

(2) “飞客”蠕虫监测

2013年全球互联网月均约1723万个主机IP感染“飞客”蠕虫，其中，我国境内感染的主机IP数量月均超过175万个。

(3) 移动互联网安全监测

- 2013年CNCERT/CC捕获及通过厂商交换获得的移动互联网恶意程序样本数量为702861个，相比2012年大幅增长331.3%。
- 按行为属性统计，恶意扣费类的程序数量仍居首位，为502481个，占71.5%，资费消耗类（占15.1%）、系统破坏类（占3.3%）分列第二、三位。
- 按操作系统统计，针对Android平台的移动互联网恶意程序约占99.5%，仍居首位；其次是Symbian平台，约占0.5%。

(4) 网站安全监测情况

- 2013年我国境内被篡改网站数量为24034个，较2012年的16388个增长46.7%。其中，境内政府网站被篡改数量为2430个，较2012年的1802个增长34.9%，占境内全部被篡改网站数量的10.1%。
- 2013年，监测到仿冒我国境内网站的钓鱼页面30199个，涉及4240个IP地址，其



中有90.2%位于境外。在仿冒我国境内网站的境外IP地址中，美国占53.4%，位居第一，中国香港（占16.6%）和泰国（占1.4%）分列第二、三位。从钓鱼站点使用域名的顶级域分布来看，以.COM最多，占51.1%，其次是.TK和.NET，分别占16.8%和8.3%。

- 2013年，监测到境内76160个网站被植入后门，其中政府网站有2425个，占境内被植入后门网站的3.2%。向我国境内网站植入后门的IP地址有30824个位于境外，主要位于美国（20.2%）、印度尼西亚（11.4%）和韩国（6.5%）。

（5）安全漏洞预警与处置

- 2013年，CNVD收集新增漏洞7854个，包括高危漏洞2607个（占33.2%）、中危漏洞4467个（占56.9%）、低危漏洞780个（占9.9%）。

- 与2012年相比，2013年CNVD收录的漏洞总数增长15.1%，其中高危和中危漏洞分别增长6.8%和12.2%，低危漏洞大幅增长93.5%。

- 按漏洞影响对象类型统计，排名前三名的分别是应用程序漏洞（占64.8%）、Web应用漏洞（占18.1%）和操作系统漏洞（占7.3%）。

- 2013年，CNVD 共收录漏洞补丁5843个。

（6）网络安全事件接收与处理

- 2013年，CNCERT/CC共接收境内外报告的网络安全事件31655起，较2012年大幅增长65.5%。其中，境外报告的网络安全事件数量为971起，较2012年下降了19.1%。接收的网络安全事件中，排名前三位的分别是漏洞（占34.5%）、网页仿冒（33.4%）和网页篡改（14.4%）。

- 2013年，CNCERT/CC共成功处理各类网络安全事件31180件，较2012年的18805件大幅增长65.8%。其中，漏洞事件（占34.9%）、网页仿冒事件（占32.7%）、网页篡改类事件（占14.6%）等处理较多。

（7）网络安全信息发布情况

- 2013年，CNCERT/CC共收到通信行业各单位报送的月度信息556份，事件信息和预警信息509份，全年共编制并向各单位发送《互联网网络安全信息通报》45期。

- 2013年，CNCERT/CC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214份。

网络安全专题分析

2.1 防范黑客地下产业链专项行动专题分析 (来源: CNCERT/CC)

随着信息网络的快速发展和日益普及,公众日常工作、生活对网络的依赖程度越来越高。受经济利益驱动,以信息窃取、流量攻击、网络钓鱼为代表的黑客活动呈快速增长趋势,并形成黑客地下产业链,严重危害互联网用户和企业的切身利益。近年来通信和互联网行业采取了一系列措施,防范和治理黑客活动,取得一定成效,但有关问题依然十分突出。为控制黑客地下产业链蔓延的趋势,健全防范治理黑客地下产业链的长效机制,在工业和信息化部部署下,2013年8-12月CNCERT/CC围绕防范治理黑客地下产业链开展为期4个月的专项行动,在通信行业、网络安全企业的支持和参与下,专项行动取得了较好成效。

2.1.1 防范治理工作难点

黑客地下产业链涉及环节多、手段多样化、隐蔽性很强、执法难度大。近年来,通信和互联网行业围绕黑客地下产业链防范治理,从制度建设、网络安全防护、公共互联网环境治理及行业自律等方面开展了大量工作。同时,公检法机关惩治不少网络犯罪分子,发挥了法律的震慑作用,但黑客地下产业链活动仍屡禁不绝,主要还存在以下难点问题。

(1) 黑客地下产业链的技术性、虚拟性、隐蔽性强,并具有跨地域性甚至跨国性的特点,使得监测处置工作变得十分困难。同时,打击网络犯罪的执法成本高、技术难度大、量刑取证难,使得犯罪分子有隙可乘,防范治理黑客地下产业链仍是一个世界性难题。

(2) 信息类资产的法律界定和保护仍不完善,特别是对公民个人信息尚无明确的法律界定,缺乏一部综合性、操作性强的个人信息保护法律,不利于依法有效打击相关违法犯罪活动。



(3) 随着互联网特别是移动互联网的快速发展,我国网民数量大幅增长,但网民的安全意识和自我保护能力普遍不足,网络安全防范常识的普遍滞后,直接导致黑客地下产业链呈快速增长趋势。

2.1.2 工作内容和成效

专项行动开始后,CNCERT/CC组织人员制定详细的工作规范,指定专职工作人员和值班人员参与专项行动,同时还组织基础电信企业、12321网络不良与垃圾信息举报受理中心、域名注册管理和服务机构、网络安全企业等多家单位召开部署会,对各单位的工作进行梳理和细化,要求各单位严格落实有关部署内容,重视防范治理黑客地下产业链专项行动工作;此外,还要求互联网网络安全信息通报成员单位、CNVD成员单位、ANVA成员单位在治理黑客产业链专项行动期间,围绕防范治理黑客地下产业链内容开展信息通报工作,每月定期报送工作进展情况和监测的相关数据等。具体专项工作内容和成效如下。

(1) 木马和僵尸网络监测和处置方面,CNCERT/CC监测发现境内422.8万个IP地址对应的主机被木马或僵尸程序控制,境内木马或僵尸程序控制服务器IP地址有39946个,境外木马或僵尸程序控制服务器IP地址有14092个。其中,在监测发现的因感染木马或僵尸程序而形成的僵尸网络中,规模大于1万的僵尸网络有103个,规模在10万以上的有10个。CNCERT/CC组织基础电信企业、互联网接入企业、域名注册服务机构等共开展5次木马和僵尸网络专项处置行动。专项处置行动共成功关闭556个控制规模较大的僵尸网络,切断了黑客对123万余台感染主机的控制,处置了控制服务器和恶意程序传播所用IP地址及域名616个。处置工作中,CNCERT/CC加强对处置效果的验证,对验证发现仍从事恶意控制活动的木马和僵尸网络控制端,组织相关单位再次进行处置。日常处置工作中,协调各分中心清理木马或僵尸程序控制端10654个,受控端21.3万个,“飞客”蠕虫感染主机19.4万台。

(2) 移动互联网恶意程序监测和处置方面,CNCERT/CC共监测发现境内有609.5万户手机用户感染移动互联网恶意程序,协调35家手机应用商店删除移动互联网恶意程序传播URL链接7358条;组织开展5次移动互联网恶意程序专项处置行动,删除移动互联网恶意程序传播URL链接4280条,处置17个控制服务器所用域名,阻断移

移动互联网恶意程序控制端URL链接73条；协调向184.6万户感染移动互联网恶意程序的手机用户进行提醒处置。

(3) 网络钓鱼事件监测和处置方面，CNCERT/CC监测发现针对境内网站的仿冒页面10168个，涉及域名7128个，IP地址2074个。CNCERT/CC协调境内外域名注册机构、境外CERT等机构重点处理了5538起网络钓鱼事件，包含金融类网络钓鱼事件4448起、媒体传播类网络钓鱼事件708起、网络游戏类网络钓鱼事件41起、支付交易类网络钓鱼事件285起、即时通信类网络钓鱼事件20起以及其他网络钓鱼事件36起。

(4) 黑客行为主体分析方面，CNCERT/CC主要通过QQ群的监控对涉黑行为主体开展分析工作。成功加入到28个黑客产业链相关QQ群，基本掌握“黑客技术培训、实施网络攻击、贩卖用户个人信息”QQ群及主要活跃的20个QQ号信息。从监测信息来看，从事DDoS攻击类的QQ号数量最多，其次是贩卖肉鸡等，并进一步了解到网上涉黑信息的主要特点及其来源，以及涉黑产品的种类和价格等，并已将相关聊天消息进行记录整理，下一步可作为立案证据和线索。

(5) 广告黑链网站的监测和处置方面，CNCERT/CC监测发现上万个网站被恶意嵌入黑链，并从中提取出借黑链传播以提升搜索引擎排名的网站8127个，主要涉及博彩类、网游私服类、网站推广优化类、特定产品厂商类4类网站。其中，借助黑链传播15次以上的网站有53个，通过对以上网站进行排查，有备案号的网站达50%，在境外注册域名的网站为20%，服务器位于境外的网站为50%。传播数量最多的黑链网址为www.youhua5.com，该网站疑直接参与提供黑链服务，CNCERT/CC对其运行情况进行调查。此外，对于涉及地下博彩、网游私服、制贩国家违禁品内容的网站，CNCERT/CC对其进行处置，并进一步梳理调查线索，摸清“黑链广告联盟”可能存在的大规模入侵受害网站的攻击情况。

(6) 通信行业单位漏洞监测与处置方面，CNVD对基础电信企业、增值电信企业、域名机构的业务系统分别进行漏洞汇总，共发布漏洞通报12期。其中，收录308个基础电信企业相关的软硬件漏洞，并向基础电信企业通报漏洞风险事件171起，发现基础电信企业网上商城及相关业务系统的用户找回密码功能可暴力破解、订单系统权限绕过、订单逻辑校验等设计缺陷仍然较为突出，这些漏洞可被利用造成用户账户的



信息泄露或商城的经济损失；收录百度、京东、搜狐、阿里巴巴、腾讯、网易、新浪等增值电信企业的331起漏洞事件，漏洞风险主要存在于增值电信企业自营业务平台以及相关软件产品；收录域名系统软件的漏洞4起，该漏洞可被利用获得敏感信息、执行脚本代码或绕过安全限制，发现71起涉及境内域名机构的漏洞风险事件，从漏洞构成威胁看，上述漏洞可构成网站文件信息或用户敏感信息泄露。

（7）典型案例分析情况方面，根据互联网通报成员报送及CNCERT/CC自主监测情况，CNCERT/CC选取多起具有代表性的黑客产业链案例，从黑客采用的技术手段、事件影响范围和事件行为主体等方面对黑客地下产业链进行综合分析，并将上述案例报送给有关部门，作为立案调查的相关线索。

（8）跨境合作事件方面，CNCERT/CC共处理跨境网络安全事件3623起。其中，接收并协调处置国际应急组织和其他网络安全组织投诉拒绝服务攻击、恶意程序、网络钓鱼等事件524起，向国际应急组织和其他网络安全组织投诉事件3099起。

2.1.3 下一步工作建议

防范治理黑客地下产业链专项治理工作结束后，在一定程度上斩断黑客产业链条，有效净化公共网络环境，但随着防范治理黑客地下产业链工作的进一步推进，仍有诸多问题亟须解决。防范治理黑客地下产业链的工作任重道远，建议下一步围绕以下方面开展工作。

（1）防范打击黑客产业链工作的法律法规和相关规章仍需进一步健全

健全法律法规和相关规章，是从根本上治理黑客产业链蔓延态势的重要前提。一方面，我国仍缺少直接治理打击黑客活动的法律法规及解释条款，黑客的违法犯罪成本较低，建议推动出台相关法律法规，对黑客活动进行定罪和量刑，以形成有效震慑；另一方面，《木马和僵尸网络监测与处置机制》和《移动互联网恶意程序监测和处置机制》在一定程度上遏制黑客地下产业链的蔓延，但随着互联网快速发展，拒绝服务攻击、网络钓鱼、网站后门等均呈大幅增长态势。针对日趋多样的黑客地下产业链活动，上述文件已无法全面覆盖现有防范打击黑客产业链的监测和处置工作，同时也缺乏较强的执行力。因此，建议就打击黑客地下产业链行为、开展各类网络安全事件的监测和处置等工作整体出台统一规章，为防范打击黑客产业链

等工作进行指导和规范。

(2) 针对网络攻击、网络犯罪等仍缺乏有效应对手段

一方面，目前黑客攻击行为逐步采用匿名技术和分布式技术等手法，给追踪黑客活动的行为主体带来困难，导致黑客在实施破坏活动之余仍带有侥幸心理；另一方面，黑客的网络攻击行为更多地与移动互联网、云计算等新技术联系起来，面对黑客的攻击破坏行为仍缺乏有效的应对手段。建议加大资金和人才投入，加强对网络安全事件监测预警、应急响应、事件处置等方面的研究，进一步提高应对网络攻击的能力和水平。

(3) 专项治理工作仍需长效化和机制化

目前黑客地下产业链活动较为活跃，已形成一定规模，并具有产业化发展和迅速蔓延的趋势。从长期来看，阶段性的专项治理工作无法从根本上消除黑客地下产业链，建议政府部门、企业科研机构等多方力量广泛联合，将黑客产业链专项治理工作长效化和机制化。

(4) 网民安全防范意识仍需进一步提高

目前，网民虽有较高的网络安全意识，但却没有将其有效转化为安全防范意识和技能。建议政府、企业和社会组织等共同努力，提升网民的网络安全防范意识和技能。通过多种渠道提醒网民保护好个人隐私，谨慎进行电子交易等操作，及时修复安全漏洞，防范个人电脑或移动终端被黑客操控，确保网上个人信息和财产安全。

2.2 DDoS攻击专题分析（来源：CNCERT/CC）

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击指借助于远程控制技术，发动多台服务器或计算机终端对一个或多个目标机器同时开展拒绝服务攻击，从而成倍地提高拒绝服务攻击的并发请求数量和带宽，以达到快速有效地使目标机器无法提供服务的不法目的。一般来说，攻击者通过漏洞、挂马、社会工程等手段将DDoS代理程序安装在大量计算机（俗称“肉鸡”）上，在一个设定的时间由部署在控制服务



器上的主控程序向大量“肉鸡”的代理程序发送攻击指令，收到指令后“肉鸡”即开始对目标机器发动拒绝服务攻击。

DDoS攻击通常是不法分子为了攫取政治、经济利益而发动的，加上DDoS攻击技术要求不高，因此大量DDoS工具应运而生。2013年3月起，CNCERT/CC针对rejoice2013、darkness、darkshell、imddos、风云、猎鹰、脑残片制造机、雪花、幽幽、残壳、毁灭等典型DDoS工具开展抽样监测。监测数据显示，在利用上述典型DDoS工具进行的分布式拒绝服务攻击事件中，控制服务器IP地址数量11650个，被用于发起DDoS的“肉鸡”IP地址数量超过14万个，遭受DDoS攻击的目标主机IP地址数量1619个，总攻击次数达6823次，尤其是2013年10月中下旬攻击活动比较频繁。

2.2.1 2013年典型DDoS工具攻击事件监测数据^[4]

2013年，CNCERT/CC监测发现，典型DDoS工具攻击事件控制服务器IP地址数量为11650个，月均（3-12月）控制服务器IP地址数量超过1000个，具体如图2-1所示，其中6月、10月控制服务器比较活跃。

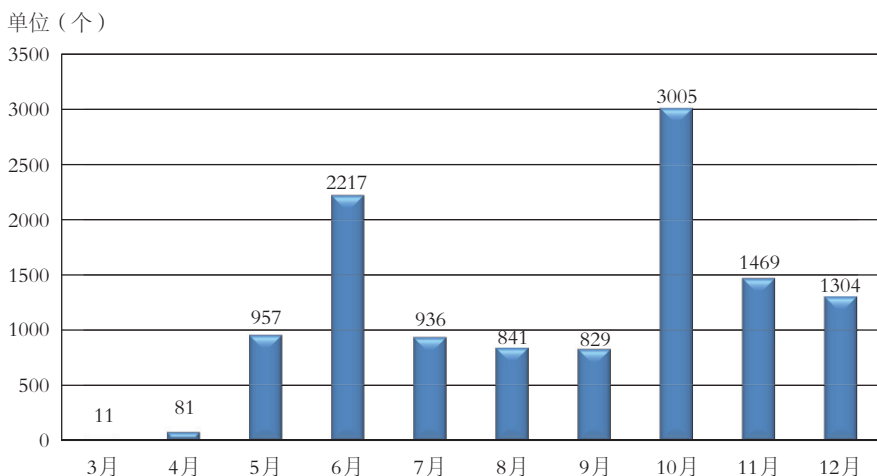


图2-1 2013年典型DDoS工具攻击控制服务器数量按月统计（来源：CNCERT/CC）

[4] 自2013年3月起，CNCERT/CC开展对典型DDoS工具攻击事件的监测。

2013年，CNCERT/CC监测发现，位于境内的典型DDoS工具攻击事件控制服务器IP地址数量6099个，境外的典型DDoS工具攻击事件控制服务器IP地址数量为5551个，分别占全部控制服务器的52.4%和47.6%。

境内典型DDoS工具攻击事件控制服务器IP地址数量按省份分布如图2-2所示，其中，北京市、广东省、江苏省居于境内控制服务器IP地址数量前3位，依次占境内控制服务器总数的20.9%、10.6%和8.7%。

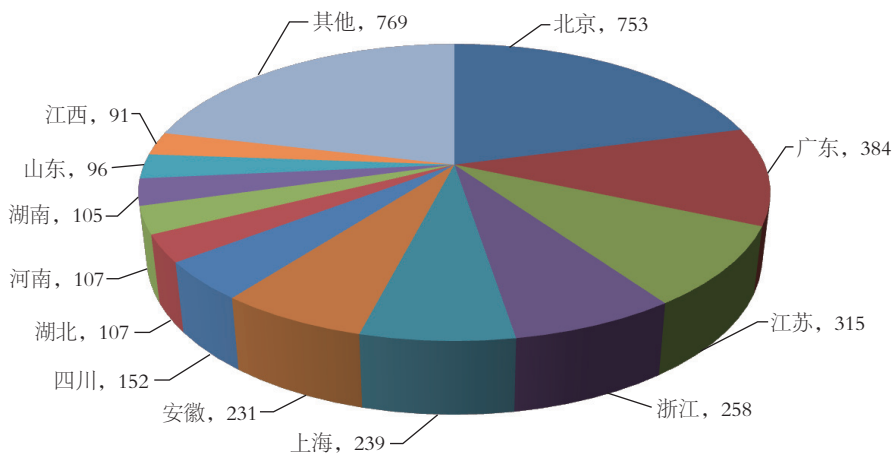


图2-2 2013年典型DDoS工具攻击控制服务器IP地址数量按省份分布
(来源: CNCERT/CC)

境外典型DDoS工具攻击事件控制服务器IP地址数量按国家和地区分布如图2-3所示，其中美国位居第一，占境外控制服务器数量的26.1%，韩国和中国香港分列第二、三位，占比分别为25.1%和13.4%。

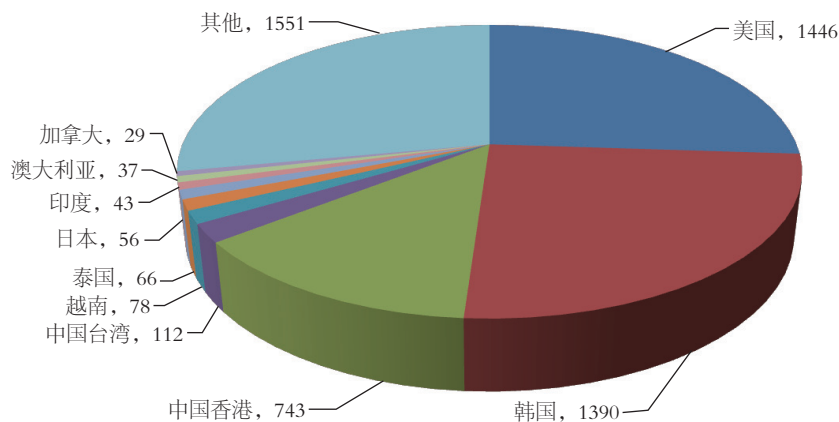


图2-3 2013年典型DDoS工具攻击控制服务器IP地址数量按国家和地区分布
(来源: CNCERT/CC)

2013年, CNCERT/CC监测发现, 典型DDoS工具攻击事件受控主机IP地址数量为140395个, 其中5月、10月、11月受控主机IP地址数量比较多, 具体如图2-4所示。

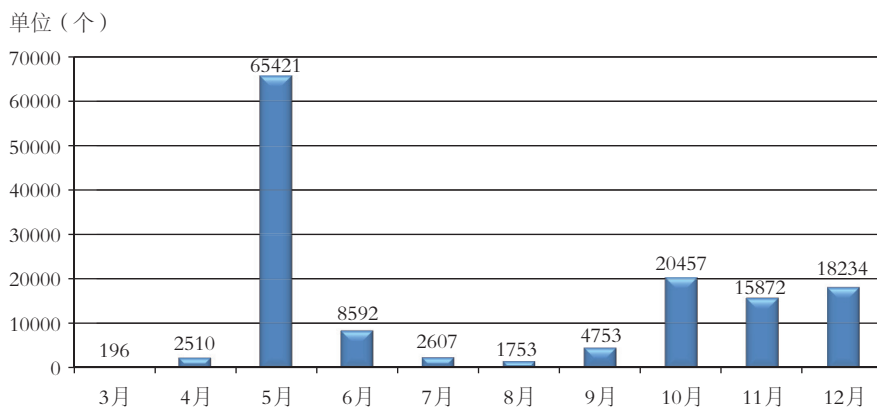


图2-4 2013年典型DDoS工具攻击受控主机IP地址数量按月份统计
(来源: CNCERT/CC)

2013年5月，DDoS控制服务器利用IMDDOS、脑残片制造机两种DDoS工具控制了6万余台受控主机，但5月实际发起的攻击次数为168次，远低于10月、11月。

2013年，境内典型DDoS工具攻击事件受控主机IP地址的数量为95031个，境外典型DDoS工具攻击事件受控主机IP地址的数量为45364个，分别占受控主机数量的67.7%和32.3%。

境内典型DDoS工具攻击事件受控主机IP地址数量地区分布如图2-5所示，其中，广东省、上海市、浙江省居于受控主机IP地址数量前3位，依次占境内受控主机总数的20.7%、7.6%和7.5%。

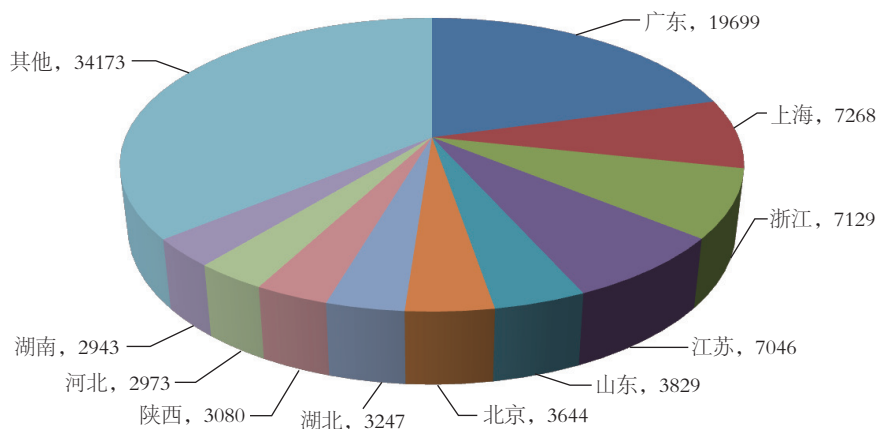


图2-5 2013年典型DDoS工具攻击受控主机IP地址数量按省份分布
(来源: CNCERT/CC)

受控主机IP地址位于境外的数量为38921个，其中位于印度、韩国和中国台湾的受控主机IP地址数量居境外受控地址数量前3位，依次占境外受控主机地址总数的19.3%、17.1%和10.2%。2013年典型DDoS工具攻击受控主机IP地址数量按国家和地区分布如图2-6所示。

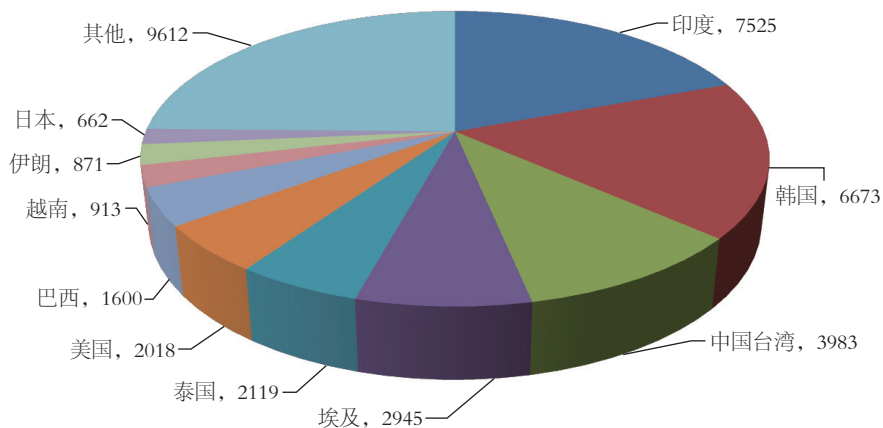


图2-6 2013年典型DDoS工具攻击受控主机IP地址数量按国家和地区分布
(来源: CNCERT/CC)

2013年,典型DDoS工具攻击事件中,受攻击的主机IP地址数量为1619个。其中,我国境内遭受攻击的主机IP地址数量达1035个,占受攻击主机总数的64.0%。从监测数据上看,受攻击目标大部分是位于我国境内的服务器IP地址。

2013年,典型DDoS工具攻击事件中,受攻击的主机IP地址按省份分布如图2-7所示,其中,广东省、浙江省、江苏省居于受攻击主机IP地址数量前3位,依次占境内受攻击主机总数的21.5%、11.9%、10.2%。

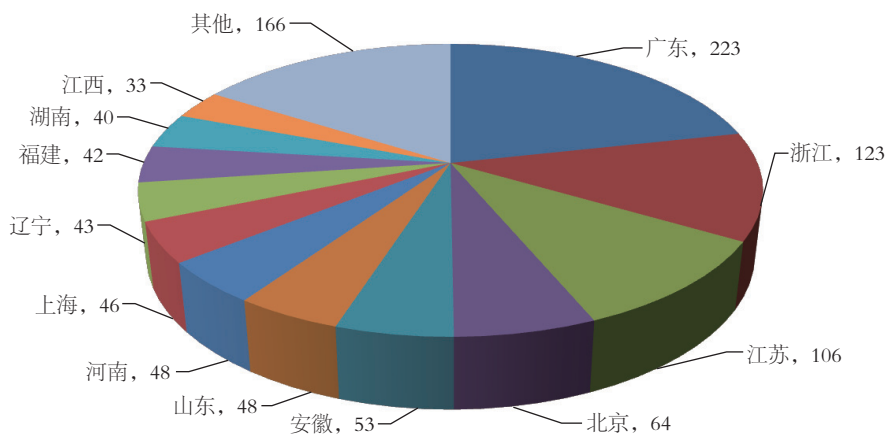


图2-7 2013年典型DDoS工具攻击的目标主机数量按省份分布（来源：CNCERT/CC）

境外受攻击IP主机数量是584个，其中位于美国、中国香港和韩国的受攻击主机数量居境外受攻击主机数量前3位，如图2-8所示。

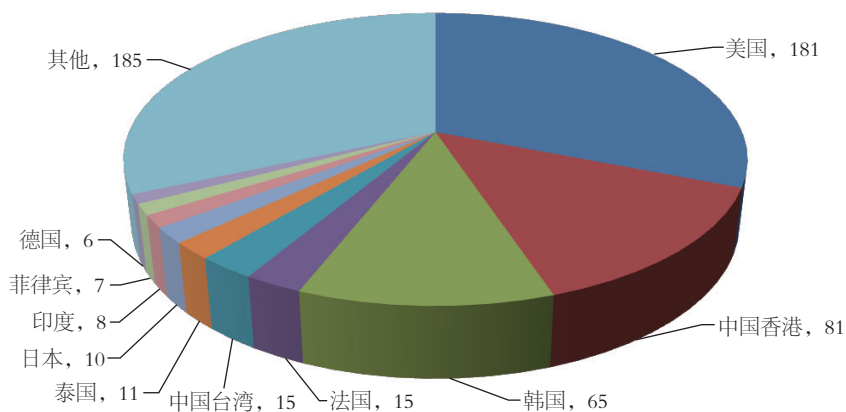


图2-8 2013年典型DDoS工具攻击的境外目标主机数量按国家和地区统计（来源：CNCERT/CC）



2.2.2 DDoS攻击的新特点

2013年,DDoS攻击依然是我国互联网基础设施和信息系统正常运转的主要威胁,且呈日益严重的趋势。根据CNCERT/CC抽样监测数据显示,我国平均每天发生攻击流量超过1Gbit/s的攻击事件1802起,较2012年增长76%,同时,2013年DDoS攻击呈现出一些新的特点,主要表现在以下几个方面。

(1) **攻击地址由原来的以虚假源地址为主逐渐转变为以真实地址为主。**2013年,在工业和信息化部的指导下,在各基础电信企业,尤其是中国联通集团的积极配合下,CNCERT/CC继续积极推进我国互联网虚假源地址流量整治工作并取得明显效果。由于攻击者构造的虚假源地址流量无法到达攻击目标,因此不得不采用真实地址发起攻击。此处的真实地址有以下几种可能。一种是攻击者通过技术手段控制的“肉鸡”,即感染木马病毒的普通网民的终端机器。普通网民接入带宽逐渐增加,一旦被攻击者控制用作攻击“肉鸡”,将导致更大的危害。例如8月25日,我国.CN顶级域名服务器遭受攻击事件中,攻击者就是通过控制数万台“肉鸡”发起规模流量攻击。第二种是攻击者租用服务器。这些服务器一般性能较高,且位于具有高带宽的IDC机房内,所以单台服务器就能够发起高达Gbit/s级的攻击流量,危害极为严重。但是如果只使用IDC服务器发起真实地址攻击容易被攻击目标防护系统阻断或被相关部门发现,因此“肉夹馍”的攻击方式,即IDC真实地址服务器作为主要攻击流量来源,混杂大量“肉鸡”作为掩护成为攻击者发起攻击的首选方式。2013年CNCERT/CC分析处置的典型攻击事件中,真实地址攻击占多数,且多数攻击流量都在数十Gbit/s,经分析追溯,基本都属于“肉夹馍”的攻击方式。

(2) **域名系统成为DDoS攻击的重点目标。**域名系统是网民访问网站的入口,由于域名解析系统自身存在的弱点,包括UDP协议、固定端口等,针对域名系统的攻击已经成为黑客对网站发起拒绝服务攻击的主要方式,且这类攻击事件一旦得逞往往会导致大量无辜网站受牵连,从而造成严重后果。2013年8月25日,黑客对我国的.CN国家顶级域名服务器发起大规模的拒绝服务攻击,导致我国大量.CN域名解析受到影响,我国大量政府网站、新浪微博等知名网站无法访问或访问缓慢。这也是我国近几年来首次出现的针对国家顶级域名服务器发起的攻击事件,对我国互联

网基础设施的安全提出更高的要求。此外，2013年8月31日和9月4日，爱民网（22.cn）域名服务器连续遭受数十Gbit/s的拒绝服务攻击，导致其负责解析的数十万个域名受到影响。据CNCERT/CC抽样监测数据，2013年我国平均每天约有58起针对域名系统的较大规模拒绝服务攻击事件，这进一步说明我国域名系统正面临日益严峻的拒绝服务攻击威胁。

（3）反射放大攻击逐渐增多，且规模巨大。所谓反射放大攻击，是指攻击者不是直接发起对攻击目标的攻击，而是利用互联网的某些网络服务以及对应开放的服务器，间接对攻击目标发起攻击。通常这些网络服务使用的都是无连接的UDP协议，常见的反射放大攻击包括DNS（Domain Name Service，域名系统）反射放大攻击以及NTP（Network Time Protocol，网络时间协议）反射放大攻击。

DNS反射放大攻击是指攻击者伪造攻击目标地址向互联网上开放的大量递归服务器发起域名请求，这些递归服务器收到请求后，将会把应答包返回给伪造的攻击目标地址，而且应答包往往比请求包大数十甚至数百倍，从而利用这些递归服务器对攻击目标地址发起反射放大攻击。2013年3月，国际反垃圾邮件组织Spamhaus遭受攻击，攻击者借助现网庞大开放的DNS群，利用DNS反射技术，将攻击流量轻松放大约100倍，峰值达300Gbit/s。据调查，目前互联网上存在2700余万个开放的递归查询域名服务器，这将可能成为黑客实施拒绝服务攻击的“军火库”，需要我们提高警惕和防护。

NTP反射放大攻击是指攻击者伪造攻击目标地址向互联网上开放的大量NTP服务器发起monlist 请求，这些NTP服务器收到请求后，将会把应答包返回给伪造的攻击目标地址，应答包中包含与NTP服务器进行过时间同步的最后600个客户端的IP地址，比请求包大出数百倍。利用这些NTP服务器可对攻击目标地址发起反射放大攻击。美国CDN服务商CloudFlare声称遭受过高达400Gbit/s流量的NTP反射放大攻击。

由于反射放大攻击的成本较低，且放大效果显著、追溯困难，且利用的相关服务本身具有开放式特点，因此难以有效地彻底杜绝，这将对DDoS攻击的防护带来更大的挑战。

（4）利用境外流量攻击境内目标的事件大量增加。2013年，CNCERT/CC抽样监测发现的日均1802起较大规模攻击事件中，有96.5%攻击目标位于境内。同时，抽样监测发现约19.5%攻击事件的攻击源地址中包含有境外地址。CNCERT/CC监测分析



的典型攻击事件中也发现多数攻击事件的攻击流量含有来自境外的攻击流量，这进一步说明我国是网络攻击的受害者。来自境外的攻击流量一方面难以判断其真实性，另一方面也难以进行进一步追溯，更增加了对网络安全事件的处置难度。

2.2.3 工作开展情况

针对2013年我国面临拒绝服务攻击日益严重的现象以及出现的新特点，下一步CNCERT/CC主要开展4方面的工作。

(1) 继续大力推进虚假源地址流量整治工作。由于虚假源地址攻击事件难以追溯和处置，因此CNCERT/CC自2012年以来一直在积极推进虚假源地址流量的整治工作，力争让虚假源地址流量成为“无源之水”、“无本之木”。据CNCERT/CC监测，2013年我国互联网虚假源地址流量占全部流量的比例控制在1%以内，较2012年下降2个百分点。CNCERT/CC监测分析的典型攻击事件中也发现攻击者逐渐以真实地址攻击为主。同时，由于大部分反射放大攻击首先需要伪造攻击目标地址发出请求包，因此虚假源流量整治工作将有效地遏制反射放大攻击事件的发生。

(2) 深入开展拒绝服务攻击事件的分析溯源工作，配合相关部门打击网络犯罪。CNCERT/CC充分利用技术和系统优势，对发生的攻击事件及时进行深入分析，追溯攻击来源，挖掘背后黑客。8月25日发生的针对.CN国家顶级域名的攻击事件中，CNCERT/CC经过细致分析，确定攻击者使用的主要攻击“肉鸡”，并对“肉鸡”背后的控制者进行追溯，最终确定黑客真实使用的控制端地址，为事件查处提供有力支撑。

(3) 持续开展攻击控制端IP地址和攻击源IP地址的清理工作。针对攻击中发起攻击的真实“肉鸡”以及控制端IP地址，CNCERT/CC积极协调基础电信企业开展清理工作，持续净化公共互联网网络环境。

(4) 积极为我国互联网基础设施和重要信息系统提供网络安全测评和监测服务。针对我国部分互联网基础设施和重要信息系统防护水平较弱的现状，CNCERT/CC一方面配合工业和信息化部对其开展网络安全防护检查，对发现的问题提出整改意见和建议，指导其加强安全防护措施；另外，积极提供网络安全监测服务，及时发现相关网络攻击事件，并针对不同的攻击事件提供具体处置建议和意见。



2.3.2 “棱镜”如此重要

从“棱镜”计划表面来看，似乎只与美国有关系，又为何能引起全球如此大的恐慌？其重要原因是全球信息流向长期不平衡，全球各国的信息都大量流向美国，如果美国对这些信息进行关注整理，将有能力控制全球各国的互联网。造成这一问题的原因有两方面：一是基于美国IT企业所提供的先进便捷的互联网服务，全球用户个人信息都向美国单方聚合；二是依托成熟价值观和法律机制打造出的优势地位和输出能力，美国持续而主动地深刻影响全球的政治与文化。

美国IT企业对其国家战略威慑力的推动，可以分为两个阶段。

第一阶段是以技术和产品的优势为主导，主要依靠IBM、苹果、微软、英特尔、思科、甲骨文等软硬结合的高科技产品企业。随着这些企业的发展，美国在全球的IT发展过程中，掌握大部分的关键产品和技术。在20世纪90年代信息高速公路建设完成之后，这种优势再次被放大，微软的Windows操作系统、英特尔的CPU和思科的路由器交换机等产品，基本统领全球信息化进程。全球用户对美国IT企业产品的高度依赖，导致对美国产品“预留”后门的恐慌和猜测，图2-10是部分代表性事件的传言，但这些传言缺乏证据支撑。

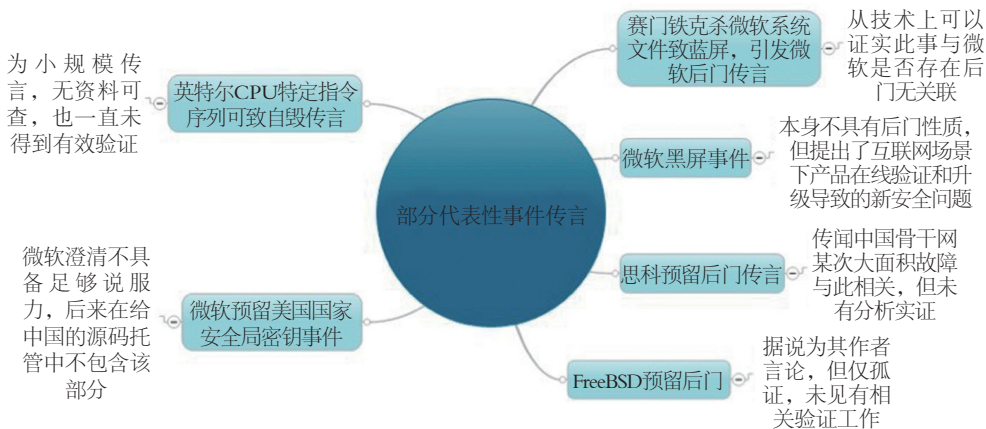


图2-10 美国预留后门的相关“传言”

第二阶段是以模式和资源为主导，主要依靠谷歌、亚马逊、Facebook、Twitter、转型后的苹果和微软，这些企业的产品在引领全球生活方式的改变，这种改变基于广

泛的信息收集和聚合的思想。互联网企业对海量用户的社会关系、个人习惯、喜好关注、行动轨迹等进行充分的聚合、分析和挖掘，并对用户体验给予前所未有的高度尊重，其优质服务和体验与普遍的免费方式相结合，开始改变全球网络用户的生活模式。人们为了获取高质量的免费信息服务，主动向云端提交个人信息，如苹果手机中 iCloud 备份功能（通讯录、照片、应用等）、手机找回功能。用户希望在手机丢失时数据仍可找回，就会开启这类功能。很显然，这部分信息就会流向美国，使得苹果公司能够了解用户，还可以很轻松地定位用户的地理位置、活动范围等。美国所拥有的这种优势基本是无可匹敌的。

因为全球信息大量流向美国，使得美国具有对全球互联网的管控能力，“棱镜”引发全球性的恐慌，已成为一个外交事件。此前，美国试图将自身宣传为网络正义者，炒作所谓的黑客威胁论，抹黑中国等国家的网络安全国际形象，由此在网络空间战中抢占话语主导权和道义制高点。棱镜事件爆发后，美国对包括中国在内的各国互联网目标的监控行为公之于众，让这个所谓制高点在一夜之间荡然无存，也促使世界各国更加重视网络安全问题。

2.3.3 从“棱镜”看IT基础设施安全现状

“棱镜”事件震动全球，同时引起网络安全界对国内IT基础设施的思考和担忧。2013年，腾达、TP-Link多款路由器被曝光存在后门漏洞。攻击者可以远程获取root权限，完全控制路由器，所有通过路由器的流量都可以被截取或被监听，攻击者还可以伪造DNS、设置钓鱼页面。由此可见，小小的路由器对用户是多么得重要。思科几乎参与了中国所有大型网络项目的建设，涉及政府、海关、邮政、金融、铁路、民航、医疗、军警等重要部门以及中国电信、中国联通等基础电信企业的网络基础建设。这些设备是否存在安全隐患，是否存在后门漏洞，值得我们思考研究。网络方面，我们使用谷歌搜索、微软MSN。操作系统方面，我们广泛使用美国产品，如PC端的Windows、MACOS，手机端的Android、IOS、Windows Phone。从以上几个方面来看，我们目前对美国是有严重依赖的，美国完全有能力对我们进行部分甚至是完全的网络控制。



2.3.4 如果没有“棱镜”

因为“棱镜”，我们认识到我国与美国的差距，更加意识到我国IT基础设施安全的重要性，网络安全警钟再次敲响。从这个角度来看，我们应该感谢“棱镜”事件，并以此为契机建设网络安全，应该看到网络带来的挑战和威胁，意识到我国应该在哪些方面加强自身实力。

美国近几年一直持续加强网络安全战备力量。美国在2006年、2008年、2010年举办三次网络战演习，演练其抵抗能力。白宫在2009年发布的《网络空间政策评估》和2011年发布的《网络空间国际战略》，清晰地通过国家战略的形式表达出这种决心和态度。震网病毒和火焰病毒，让我们见识到网络战争的攻击力和破坏力。我们不得不说，美国对网络安全的关注程度和实战能力超出常人的想象。

面对这样的局势，建议我国定期举行“国家级网络战防御演习”，参加机构包括政府部门和相关企业，特别要逐步加入关键基础设施相关单位，提高自身水平并发挥震慑力。从某种意义上说，“棱镜”事件可能成为中美在网络安全领域实现缓和并确定新规则的一个契机，也是中国对国家网络安全战略、政府能力与法制建设等多方面进行自我审视和反思的机遇。同时，应重视个人隐私安全，增加相应的法律法规对网站、论坛的约束和管理，使保护个人隐私安全有法可依，并加强对出售个人信息等不法行为的打击。

2.4 APT攻击技术研究及防范（来源：网御星云^[6]）

APT（Advanced Persistent Threat，高级持续性渗透攻击）是针对特定组织所做的复杂且多方位的网络攻击。APT可利用多种攻击手段，包括各种最先进的攻击技术和社会工程学方法，一步一步地获取进入组织内部的权限。APT攻击可能采用恶意软件、漏洞扫描、针对性入侵等多种攻击手段，甚至利用恶意的内部人员破坏安全措施。APT攻击典型过程包括：利用操作系统或应用软件漏洞发起入侵，在受害系统上安装恶意软件，发起与命令控制服务器的连接，绕过防火墙，搜寻网管主机，服务器

[6] 网御星云公司即北京网御星云信息技术有限公司，是通信行业互联网网络安全信息通报工作单位。

和数据库，提取数据等。

APT攻击的特点之一：出于经济利益或竞争优势的目的。企业所面临的信息安全威胁正在不断演变，其中最大的一项挑战来自APT攻击。企业和政府容易成为APT攻击目标的原因非常明显：企业拥有高价值的金融资产和知识产权；自有政府机构以来，政府机构就始终面临着来自外部的攻击。若这些新型的攻击重点针对关系到国计民生以及国家核心利益的国家基础设施，如涉及能源、电力、金融、国防等，则其攻击的后果将更为严重。尽管这些部门和单位可能已经部署相对完备且涵盖事前、事中和事后等各个阶段的纵深安全防御体系，拥有针对某个安全威胁的安全设备，以及将各单一安全设备串联起来的管理平台，然而，这样的防御体系仍然难以有效地防止来自互联网的入侵攻击和信息窃取，尤其是新型的APT攻击。

APT攻击的特点之二：长期且持续的攻击。APT攻击可能会持续几天、几周、几个月，甚至更长的时间。此类攻击往往以对后续攻击大有裨益的技术、人员情报的搜集开始。举例来说，如果攻击者试图窃取商业机密，可能就需要花几个月的时间执行有关安全协议、应用程序漏洞，以及文件存放位置的情报收集工作。当这些情报收集工作完成后，只需要一次持续几分钟的运行就可以完成商业机密的窃取。当然，在某些情况下，攻击的持续时间可以较长，例如，在将Rootkit成功部署到服务器上后，攻击者可定期传送有潜在价值的文件副本至命令控制服务器，以随时审查文件的价值。

APT攻击的特点之三：针对一个特定的公司、组织或平台。APT攻击是长期的过程导向性攻击，是攻击者动机和攻击手段进化的产物。不管是从攻击者所使用的技术，还是他们对组织内部的了解来看，APT攻击都是非常先进的。APT攻击往往利用组织内部的人员作为跳板进行攻击。在某些情况下，攻击者还会针对被攻击对象编写专门的攻击程序，而非使用通用的攻击代码。

2.4.1 APT攻击和传统安全威胁的区别

传统安全威胁包括蠕虫、木马、病毒、间谍软件、僵尸网络、钓鱼和诱饵（投放U盘或光盘）等社会工程学攻击、缓冲区溢出和SQL注入等。除以上安全威胁的新变种外，大部分传统安全威胁都可以被IPS、NGFW和AV等传统的基于特征的安全设备有效检测和防护。相较于传统的安全威胁，APT攻击是一支配备了精良武器的特种部



队，可让用户网络环境中的IPS/IDS、防火墙等传统安全网关失去应有的防御能力。无论是0day或者精心构造的恶意程序，基于特征库的传统被动防御体系都无法抵御定向攻击的入侵。

APT攻击主要有以下技术特点。

(1) 攻击者往往利用恶意网站作为诱骗手段，用钓鱼方式诱使目标上钩。目前企业和组织的安全防御体系对恶意网站的识别能力并不全面，缺乏权威、全面的恶意网址库，对内部员工访问恶意网站的行为无法及时发现。

(2) 攻击者往往将恶意邮件包装成拥有合法的发件人，采用恶意邮件的方式攻击受害者。企业和组织现有的邮件过滤系统大多基于垃圾邮件地址库，并不包含这些“合法”邮件。另外，邮件附件中隐含的恶意代码往往都是0day漏洞，对邮件内容的分析检测此时难以奏效。

(3) 一些攻击是直接通过对目标公网网站进行SQL注入而实现的。许多企业和组织的网站缺乏在SQL注入攻击方面的防范。

(4) 攻击者在网络渗透的初始阶段往往利用0day漏洞的恶意代码。目前企业和组织的安全防御/检测设备无法识别这些0day漏洞攻击。

(5) 攻击者在控制受害机器的过程中，往往使用SSL链接，使得目前大部分内容检测系统无法分析传输的内容，并且缺乏对可疑连接的分析能力。

(6) 攻击者在持续不断窃取目标企业和组织的重要数据时，一定会向外部传输数据，这些数据往往都是压缩和加密的，没有明显的指纹特征。这使得现有绝大部分基于特征库匹配的检测系统无法检测。

(7) 由于知识库的缺乏，客户无法从多个角度综合分析安全事件，无法从攻击行为的角度进行整合，从而发现攻击路径。尽管某些企业部署了内网审计系统、日志分析系统，或者SOC安全管理平台等，但这些系统主要是从内控与合规的角度来分析事件，并没有真正形成对外部入侵的综合分析。

(8) 攻击者往往不是直接攻击最终目标人，而是通过攻击外围人员进行层层渗透。例如，先攻击HR或者首轮受害人的网络好友，再以HR受害人的身份去欺骗（攻击）某个接近最终目标人的过渡目标，再透过过渡目标人去攻击最终目标人（例如掌握了某些机密材料的管理员、公司高管、财务负责人等）。

因此，在APT这样的新型攻击面前，大部分企业和组织的安全防御体系都将失灵，急需全新的思路和技术保障网络安全。

APT攻击行为和传统安全威胁的区别见表2-1。

表2-1 APT攻击行为和传统安全威胁的区别

说明	APT 攻击行为	传统安全威胁
是否破坏网络	否	带有目的性的破坏
是否有目标	明确的攻击目标	大面积扩展僵尸网络
目标用户	特殊机构或公司	个人
攻击频率	频繁	一次性
攻击途径	多种Oday、精心构造的远程控制工具（RAT）、各种后门程序	各种常见的攻击工具、构造恶意URL、全功能的木马软件
检测难度	通常存在较长时间的样本空白，检测率低于10%	成活时间短，容易被捕获，检测率95%

2.4.2 APT攻击案例分析

目前，披露的APT攻击案例相关细节基本由美国公布，但这并不代表APT攻击只针对欧美。其中最主要的原因在于美国IT技术发达，并且美国公司把安全事件发生后的调查和公布看作是公司的诚信行为。另一个可能的原因是，美国在APT攻击检测和防御技术上具备一定的先进性，可及时发现部分APT攻击，因此可在攻击开始时就及时取证从而了解完整的攻击过程与手法，而其他国家在这方面相对较为落后，发现攻击时即已处于攻击的后期阶段，只能清除而很难分析取证以掌握整个攻击过程。

APT攻击中比较著名的案例如下。

（1）针对Google等三十多个高科技公司的“极光攻击”

2010年针对Google公司的Aurora（极光）攻击是一个十分著名的APT攻击。Google的一名员工点击即时消息中的一条恶意链接，引发了导致此搜索引擎巨人的网络被渗透数月的一系列事件，造成各种系统的数据被窃取。此次攻击由一个有组织的网络犯罪团体精心策划，其目的是长时间地渗透这些企业的网络并窃取数据。

在此次攻击中，攻击者通过Facebook上的好友分析，锁定Google公司的一名员工和他一位喜欢摄影的电脑菜鸟好友。攻击者入侵并控制此电脑菜鸟好友的机器，伪造



一个放置IE Oday攻击代码的照片服务器，并以电脑菜鸟好友的身份邀请该Google员工来看其最新的照片。实际上，该邀请信息中的URL指向放置IE Oday攻击代码的页面，该Google员工打开这个页面之后便遭受攻击。攻击者利用这名Google员工的身份在内网持续渗透，最终获得Gmail邮件系统中许多敏感用户的访问权限。在窃取Gmail邮件系统中的敏感信息后，攻击者通过合法且加密的信道将窃密数据回传。事后调查，除Google之外，有30多家美国高科技公司都被此APT成功攻击，其中甚至包括赛门铁克这样的知名安全厂商。以上攻击过程大致如下。

- 首先，攻击者针对某Google员工进行刺探工作，攻击者尽可能地收集信息，包括此员工在Facebook、Twitter、LinkedIn和其他社交网站上发布的信息。
- 紧接着，攻击者通过动态DNS提供商建立一个托管伪造照片网站的Web服务器，该Google员工收到来自其信任的人所发来的网络链接，单击之后进入恶意网站。该恶意网站的页面上含有JavaScript程序代码，可造成IE浏览器溢出，执行FTP下载程序，进一步可从远端抓取更多的程序来执行（由于其中部分程序编译环境的路径名中带有Aurora字样，该攻击故此得名）。
- 接下来，攻击者通过SSL安全隧道与受害人的机器建立连接，持续监听并最终获得该员工访问Google服务器的账号、密码等信息。
- 最后，攻击者使用该员工的相关凭证信息成功地渗透到Google的邮件服务器，从而不断地获取特定Gmail账户的邮件内容信息。

（2）针对美国能源部的“夜龙攻击”

“夜龙攻击”是McAfee在2011年2月发现并命名的、针对全球主要能源公司的攻击行为。攻击者首先收集许多能源部门Web服务器的SQL注入漏洞，从而攻击并控制这些Web服务器，但这并不是攻击者的最终目的。攻击者在这些Web服务器供内部人员访问的页面上放置针对IE和Office应用的0day攻击代码。由于针对的是内部站点，这些攻击代码难以通过挂马检测发现，并且访问的站点基本都是其攻击目标。基于这种方式，攻击者很快通过一些个人终端，渗透进能源部门的内网，从而控制大量有价值的主机。

该攻击过程如下：

- 攻击者采用SQL注入方式对外网主机，如Web服务器进行攻击；

- 将被攻击的Web服务器作为跳板，对内网的其他服务器或PC进行扫描攻击；
- 攻击内网机器，如AD服务器或开发人员的电脑，多采用暴力破解获取密码；
- 对被攻击的机器植入恶意代码，安装远端控制工具，禁用被攻击机器的IE代理设置，通过建立的直连通道回传包括所有会议记录及组织人事架构图在内的大量机密文件（Word、PPT、PDF等）；
- 更多的内网机器被成功入侵，大部分发生在高级主管单击某看似正常却含有恶意代码的邮件附件之后。

“夜龙攻击”的攻击过程和危害如图2-11所示。

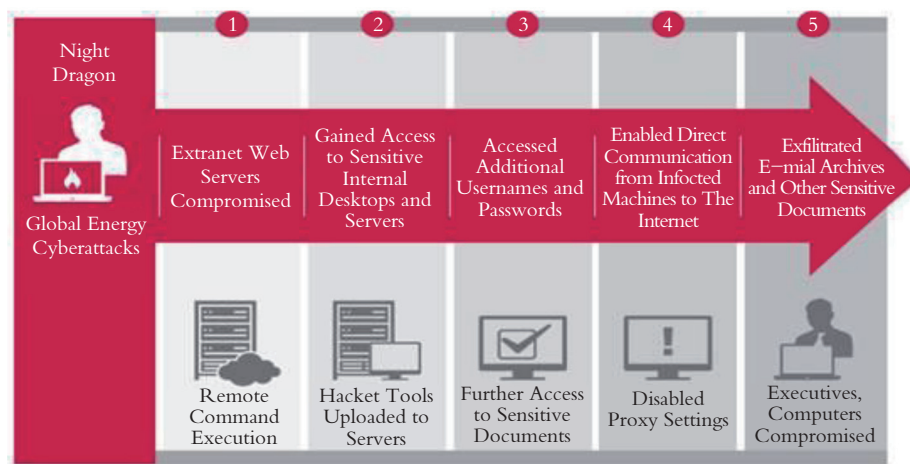


图2-11 “夜龙攻击”的攻击过程和危害

(3) 窃取RSA公司SecurID令牌种子的攻击

2011年3月，EMC公司下属的RSA公司遭到入侵，部分SecurID技术及客户资料被窃取，导致许多使用SecurID作为认证凭据建立VPN的公司，包括洛克希德马丁公司、诺斯罗普公司等美国国防承包商在内的公司，均受到攻击，被窃取重要资料。在此攻击中，攻击者首先获取RSA公司一个外地分支机构的工作人员邮箱，进而攻击其主机，然后以此工作人员的身份向RSA公司的财务主管发了一封财务预算的邮件，请求RSA的财务主管进行审核，并附上一份嵌入Flash的0day利用代码Excel附件。RSA的财务主管认为此邮件可信，基于自己的工作职责打开这个附件，随机使得攻击者成功控



制RSA财务主管的机器。随后，攻击者利用RSA财务主管的身份进行逐步渗透，最终成功窃取了SecurID令牌种子，并通过IE代理回传至控制端。在发现被入侵后，RSA公司一直不承认其SecurID令牌种子被窃取，直到攻击者利用窃取的SecurID令牌种子攻击美国多个军工企业之后，RSA公司才承认这一点。

在RSA SecurID攻击事件中，攻击者并没有大规模地使用SQL注入攻击，也没有使用网站挂马或钓鱼网站，而是采用最原始的网络通信方式——直接发送电子邮件至公司职员，并附带杀毒软件无法识别的恶意文件附件。具体攻击过程大体如下。

- 攻击者给RSA母公司EMC的4名员工发送两组恶意邮件。邮件标题为“2011年招聘计划”，寄件人是webmaster@Beyond.com。正文很简单，写着“我将此文件转发给你，请阅”，并附上一个名为“2011年招聘计划.xls”的Excel附件；

- 很不幸，有一位员工对此邮件感兴趣，并将其从垃圾邮件中取出来阅读，实际上在此电子表格中含有当时最新的Adobe Flash的0day漏洞(CVE-2011-0609)。打开这个Excel后，可以看到除了在表单的第一个格子中有个“X”之外，什么也没有，实际上，这个“X”就是内嵌的一个Flash。

- 于是，该名员工的主机被植入臭名昭著的Poison Ivy远端控制工具，并从BotNet的C&C服务器（位于good.mincesur.com）处下载指令并执行任务。

- 首批攻击受害者并非“位高权重”的关键人物，很快相关人士包括IT与非IT等服务器管理员相继被攻击。

- 随后，RSA公司发现其开发用服务器遭到入侵，攻击者随即撤离，并将所有资料加密压缩(都为.rar格式)，并以FTP方式传送至远端主机，之后迅速搬离该远端主机，清除所有踪迹。

- 在拿到了SecurID令牌种子后，攻击者开始对使用SecurID的公司（例如上述防务公司等）进行攻击。

另一个与此攻击类似的事件是针对Comodo公司数字证书颁发系统的攻击，攻击者成功生成多个伪造的Comodo公司签发的数字证书。

（4）针对伊朗核电站的“震网”攻击

遭遇“震网”病毒攻击的核电站计算机系统是与外界物理隔离的，理论上不会遭

遇来自外界的攻击，只能从其内部攻破。“震网”病毒充分地利用这一点，攻击者并没有广泛的传播病毒，而是针对核电站工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击，以此为第一道攻击跳板，进一步感染相关人员的U盘。随即，病毒以U盘为桥梁进入“堡垒”内部潜伏下来，耐心地逐步扩散，利用多种漏洞逐步地实施破坏。这是一次十分成功的APT攻击，其最为可怕的地方在于极为巧妙地控制攻击范围，攻击十分精准。“震网病毒”攻击原理图2-12所示。具体攻击过程如下。

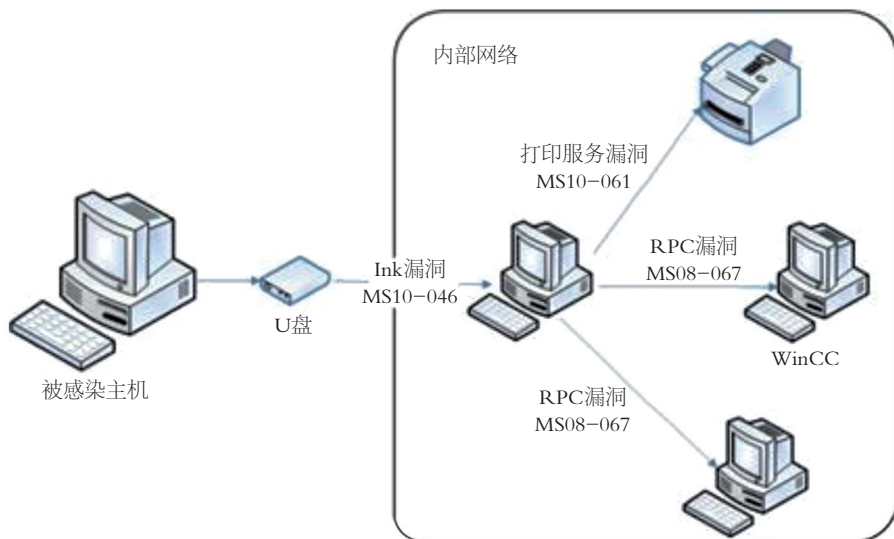


图2-12 “震网病毒”攻击原理

攻击者首先获得一些核电站工作人员及其家庭成员的信息，并针对这些家庭成员的主机发起攻击，最终成功控制这些家用主机。随后，攻击者利用4个Windows的0day漏洞，感染所有接入的USB移动介质，并通过USB移动介质攻击其后续接入的主机。最终，靠这种方式攻击者成功攻击、渗透进防护森严并且物理隔离的伊朗核电站内网，再利用3个西门子工业控制系统的0day漏洞，成功控制离心机的控制系统，修改离心机参数，使该核电站正常发电却生产不出任何制造核武器的物质，并且通过人为检测不能发现任何异常，从而成功地将伊朗制造核



武器的进程拖后若干年。

(5) Shady RAT攻击

2011年8月，McAfee/Symantec发现并报告Shady RAT攻击。在长达数年的持续攻击过程中，该攻击渗透并攻击全球多达70个公司和组织的网络，包括美国政府、联合国、红十字会、武器制造商、能源公司、金融公司等。其攻击过程如下：

- 攻击者首先通过社会工程学的方法收集被攻击目标的信息；
- 攻击者给目标公司的某人发送一系列极具诱惑性的、带有附件的邮件，例如邀请他参加某个所在行业的会议，以其同事或者HR部门的名义告知其更新通讯录，或请他审阅某个真实存在项目的预算等；
- 当受害人打开邮件并查看附件（大部分为.xls格式的表格）后，受害人使用的Excel程序的FEATHEADER远程代码执行漏洞（Bloodhound.Exploit.306）即被利用，从而被植入木马，实际上，该漏洞并不是0day漏洞，但受害人没有及时打补丁，并且该漏洞只针对某些版本的Excel有效，可见被害人所使用的Excel版本信息已为攻击者所知；
- 木马开始与远程的服务器进行连接，下载恶意代码，这些恶意代码被精心伪装（例如被伪装为图片或者HTML文件），安全设备难以识别；
- 借助恶意代码，受害人的机器与远程的控制计算机建立远程Shell连接，导致攻击者可以随意控制受害人的机器。

(6) 其他案例

以下为属于APT攻击范畴但细节相对较少或者在攻击时就被发现的案例。

- 洛克-马丁：攻击者将PDF 0day代码嵌入到邮件中发起攻击，但该攻击被检测出来，但洛克-马丁公司并未公布是如何检测到这个攻击的。
- VERISIGN：VERISIGN承认其公司内部被黑客成功攻击，但当时在任的高管人员都不知道此事。虽然没有证据证明，但VERISIGN公司仍然坚信其用于可信站点签名的根证书依旧安全。如果VERISIGN公司的根证书与RSA公司的SecurID令牌种子一样已被窃取，这意味着攻击者可以假扮成任何一个可信站点针对加密链路发起中间人攻击而不被察觉。
- NASA承认其在2013年至少有13次被黑客成功入侵的经历，许多核心机密被窃

取，但具体的攻击细节并没有披露。

- 韩国农协银行：据披露，攻击者首先利用社会工程学方法，将一张免费的网络电影观看券（在韩国网上看电影需要付费）给了负责韩国农协银行内部系统开发的IBM外包团队的项目经理，该名项目经理使用工作用笔记本访问该电影的URL，由此遭受攻击。进一步，攻击者利用此台笔记本作为跳板，成功控制韩国农协银行所有重要系统并窃走机密信息。之后，攻击者长期潜伏在银行系统内，在银行进行数据备份时进行恶意破坏，最后将所有数据删除后撤离。韩国农协银行试图使用其备份系统恢复数据时才发现近期的备份都遭到破坏，导致大量数据无法同步，损失惨重。

2.4.3 APT攻击防范思路

目前业界讨论的APT检测和防御思路主要分为以下几种。

（1）主机应用控制思路

这种思路认为APT攻击的一般落脚点为员工的个人电脑或者开放服务器，恶意代码必须在主机上执行。不管攻击者通过何种渠道将恶意代码发送至员工，恶意代码都必须在员工的个人电脑上执行，因此，如果能够确保员工个人电脑的安全，则可以有效地防止APT攻击。具体思路是采用白名单方法控制个人主机上应用程序的加载和执行，从而防止恶意代码在员工个人电脑上执行。许多从事终端安全的厂商就是从这个角度制定APT攻击的防御方案。一般过程包括：采用白名单方式加载应用程序，对运行中的应用进行行为建模和监控，对于可疑应用采用安全沙盒的方式运行。

（2）恶意代码检测思路

由于绝大多数APT攻击都是采用恶意代码来攻击员工的个人电脑以进入目标网络，因此，恶意代码的检测至关重要。此类APT解决方案是检测APT攻击过程中恶意代码的传播过程，许多从事恶意代码检测的安全厂商都是从这方面入手制定APT攻击检测和防御方案。对于Web、E-mail和共享文件三种恶意代码的可能来源，可采取传统特征匹配（解决已知攻击）和虚拟执行引擎（解决未知攻击）相结合的方法来检测。



（3）网络入侵检测思路

网络入侵检测思路认为，在APT攻击过程中，受害者主机上的后门程序会经常连接至特定的C&C服务器，以接收指令或传输数据。虽然APT攻击中的恶意代码变种多样，但恶意代码网络通信的命令和控制模式并不会经常变化。因此，可以采用传统入侵检测的方法来检测APT攻击的通信通道。

（4）大数据分析和检测思路

通过全面采集网络中的各种数据包括原始的网络数据包、业务和安全日志等形成大数据，再通过大数据分析技术和智能分析算法来检测APT攻击。此思路覆盖APT攻击的各个阶段，易于重现整个攻击过程。该类APT攻击检测方案并不重点检测APT攻击中的某个步骤，而是全面收集重要终端和服务端上的日志信息以及采集网络设备上的原始流量，并进行集中的分析和数据挖掘。这实际上是网络取证思路，可以在发现APT攻击的蛛丝马迹后，通过全面地分析海量数据还原整个APT攻击场景。大多数拥有大数据分析技术的厂商采用这种思路检测APT攻击。

2.5 网上交易服务安全风险（来源：奇虎360公司^[7]）

2.5.1 客户端安全环境交易风险

2.5.1.1 PC木马威胁

2013年第三季度，360互联网安全中心共截获新增恶意程序样本5.40亿个，较2013年第二季度的5.27亿个环比增长2.5%，平均每天截获新增恶意程序样本587万个。

2013年第三季度，360互联网安全中心统计的恶意程序云查询拦截量为151.1亿次，较2013年第二季度的90.7亿次环比增长66.6%，平均每天为用户拦截恶意程序攻击约1.64亿次。

从恶意程序的攻击目的来看，盗号木马和网购木马接近半数，而这两类木马对网上交易的安全威胁最大。在盗号木马中，针对网银账号、支付宝账号、游戏账号和QQ账号的盗号木马最为常见。网购木马主要特点是在支付过程中，劫持商品的名

[7] 奇虎360公司即奇虎360软件（北京）有限公司，是通信行业互联网网络安全信息通报工作单位，同时也是CNCERT/CC国家级应急服务支撑单位。

目、价格和交易对象等信息，从而实现资金的盗窃。最新出现的网购木马，还能直接将用户通过支付宝支付的货款转账给指定的网银账户，从而省去以往的洗钱过程。虽然木马程序的新增数量很大，但大多数很难通过安全软件的查杀和拦截。

2.5.1.2 钓鱼网站威胁

2013年第三季度，360互联网安全中心共截获新增钓鱼网站43.9万个，较2013年第二季度的51.4万个环比下降15.0%，平均每天截获新增钓鱼网站约4772个。

2013年第三季度，360互联网安全中心共拦截钓鱼网站访问量10.8亿次，较2013年第二季度的5.9亿次环比增加了83.1%，平均每天拦截钓鱼网站访问量约1174万次。

从新增钓鱼网站的类型分布上看，虚假购物、虚假中奖和模仿登录仍然位居三甲。最近一年来，虚假购物始终是新增钓鱼网站中数量最多的类型。图2-13给出2013年第三季度各类新增钓鱼网站的比例分布情况。

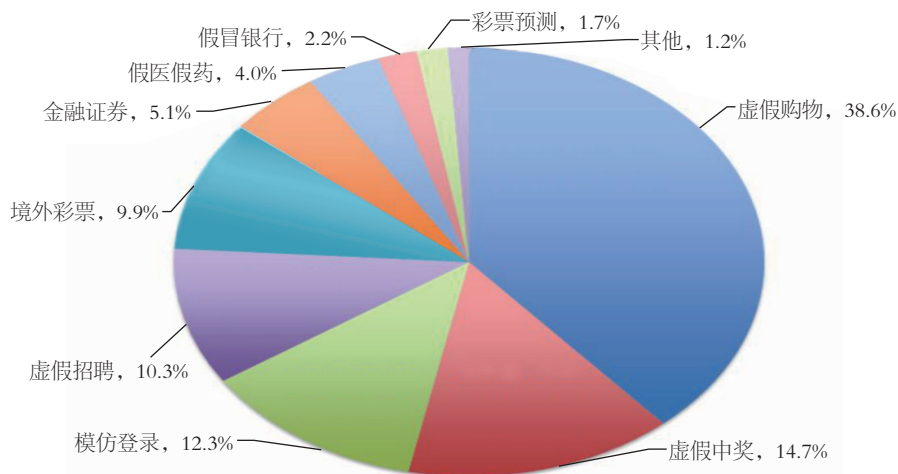


图2-13 2013年第三季度新增钓鱼网站类型分布（来自：奇虎360公司）

从钓鱼网站服务器的地域分布上看，88.1%的钓鱼网站分布在境外地区，美国是国内钓鱼网站的第一源头，占比高达55.4%。由于绝大多数钓鱼网站的服务器设在国外，使得有关部门的监管工作变得异常困难。具体如图2-14所示。

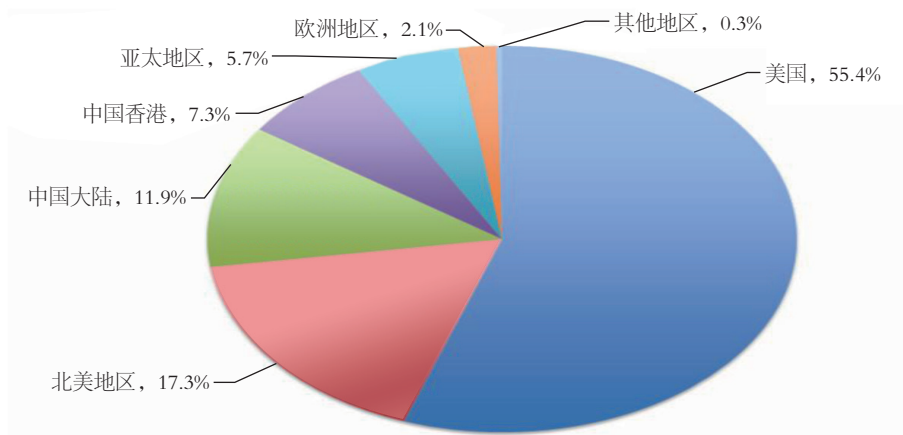


图2-14 2013年第三季度新增钓鱼网站地域分布（来自：奇虎360公司）

从攻击手法上，最近几个月，钓鱼网站在信息窃取方面明显加强。钓鱼网站不仅会骗取用户身份证号码、手机号码等敏感信息，而且出现很多专门骗取手机验证码的钓鱼网站。这类钓鱼网站要求用户同时输入相关账号、密码以及手机验证码，一旦用户填写相关信息，就将遭受不可挽回的损失。

钓鱼网站不会无缘无故地进入用户电脑之中。调查显示，搜索引擎正是绝大多数钓鱼网站进行推广的主要方式。2013年11月6日至11月8日，360安全中心连续三天在某搜索引擎中搜索“天天分红”，对其首页含搜索词的14条“推广链接”进行统计后发现，投资理财类钓鱼网站占到所有推广链接的71.4%。实际情况是，不法分子会通过多个相近关键词同时推广某个钓鱼网站，除“天天分红”外，“投资理财”、“理财项目”、“理财产品”、“网上理财”等关键词的搜索结果中，暗藏不少恶意欺诈网站。

2.5.1.3 手机安全威胁

在传统支付领域，手机主要承担交易信息告知、接收验证码和回复信息确认功能，但在智能手机系统中，这三个以短信息为核心的支付功能正在受到严峻威胁和挑战。除了传统支付领域外，移动支付本身逐渐成为网上交易新的流行方式，但各种手机安全漏洞和木马病毒正在挑战移动支付的安全性。

广泛存在的手机安全漏洞，使得手机恶意程序有可能劫持手机的通信功能，特别是短信信息，从而使基于手机验证码体系的各种支付认证方式都被轻易攻破。

2013年第三季度，360互联网安全中心特别针对市面上比较流行的9个品牌，18个典型型号的安卓手机进行测试分析。结果显示：安卓2.x版本的9款手机平均有20个已知的安全漏洞，最少的有8个漏洞，最多的有40个漏洞；而安卓4.x版本的9款手机平均有19个已知的安全漏洞，最少的有3个漏洞，最多的有40个漏洞。漏洞数目纵向比较如图2-15所示。

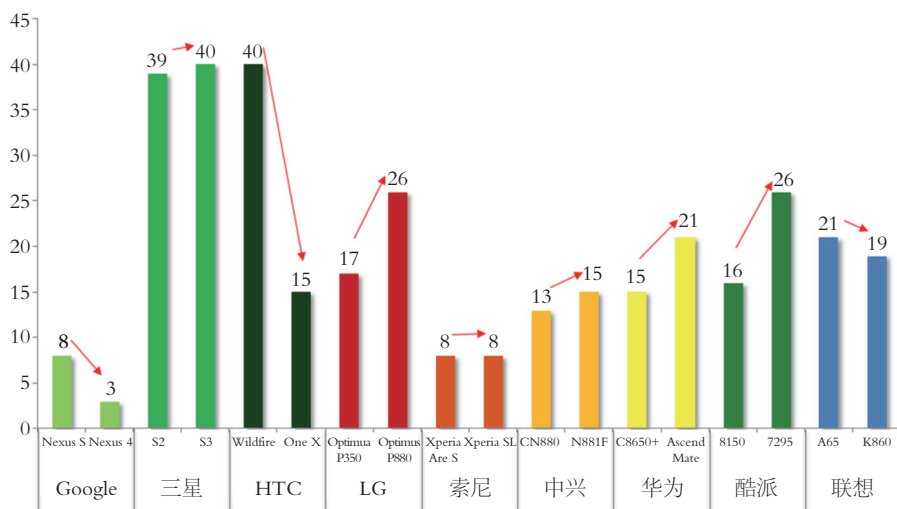


图2-15 漏洞数目纵向比较

在针对上述机型进行安全检测过程中，360互联网安全中心还专门针对6种危害较大或比较常见的漏洞类型进行统计。这些漏洞类型分别是：后台电话、后台消息、静默安装、短信欺诈、清除数据和签名漏洞。表2-2给出具体的统计结果。



表2-2 移动互联网终端漏洞漏洞类型及统计情况

漏洞类型	漏洞危害	涉及机型数 (个)	涉及机型比例	检出漏洞数 (个)
后台消息	恶意程序可以在用户不知情的情况下在后台向指定号码发送消息	18	100%	70
签名漏洞	恶意程序可以在不改变正常程序签名的情况下篡改这些程序	18	100%	18
短信欺诈	恶意程序可以向机主手机发送欺诈短信	17	94%	57
后台电话	恶意程序可以在用户不知情的情况下在后台向指定号码拨打电话	17	94%	29
清除数据	恶意程序可以恶意删除手机中的文件或信息	5	28%	8
静默安装	恶意程序可以在后台静默安装,用户不知情	4	22%	7

从表2-2中可以看出,后台电话、后台消息、签名漏洞和短信欺诈这4类漏洞几乎是所有手机共有的漏洞,而后台消息和短信欺诈漏洞的检出数量更是达到惊人的70个和57个。后台消息和后台电话漏洞很可能被用于恶意扣费,短信欺诈漏洞则更是严重威胁每个用户的财产安全。

正是由于这些漏洞,特别是各种短信漏洞的存在,使得所有基于手机验证码的安全措施都可能遭到严重威胁。另外,检测分析发现,由厂商定制而产生的手机安全漏洞,约占这些被测试手机中已知漏洞总数的70%。

根据360互联网安全中心的监测,2013年第三季度,在安卓系统平台中,资费消耗和恶意扣费类恶意程序的感染量最高,分别占到感染人次总数量的52%和24%,二者之和为76%,即对于已经感染恶意程序的手机用户来说,面临直接经济损失的可能性超过7成。如果将手机资费视为一种支付方式,那么恶意程序的威胁不可小视。2013年第三季度Android平台恶意程序感染量分布如图2-16所示。

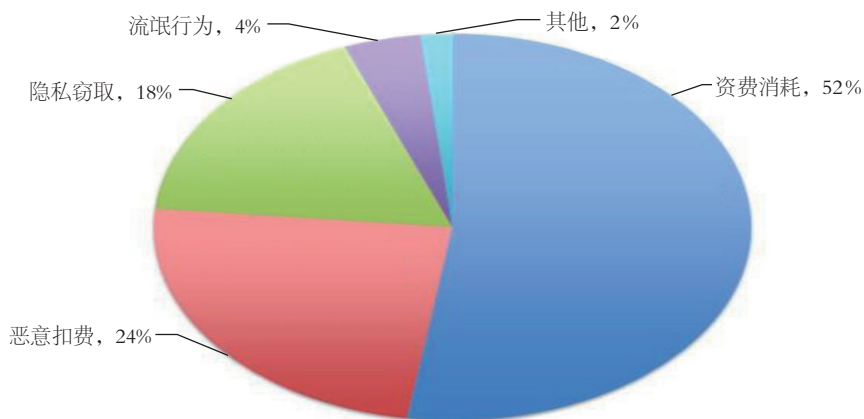


图2-16 2013年第三季度Android平台恶意程序感染量分布

进入2013年第三季度以来，以伪基站为代表的新型金融诈骗最值得关注。伪基站问题的出现，事实上是由于传统的通信系统缺乏必要的安全性验证机制所导致的。

2.5.2 电商网站安全环境与信息泄露

根据360网站安全检测平台数据，中国每个电商网站平均存在3.9个网站漏洞。在电商网站的安全漏洞中，高危漏洞占32%，严重漏洞占8%，警告漏洞占43%，轻微漏洞占17%。中国电商网站漏洞级别分布情况如图2-17所示。

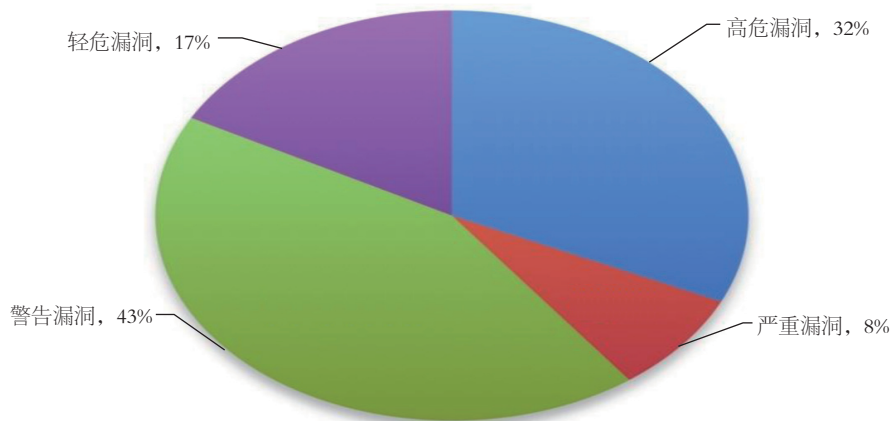


图2-17 中国电商网站漏洞级别分布情况

也就是说，每个电商网上平均存在一个以上的高危安全漏洞。黑客可利用这些高危漏洞直接获取核心数据或者完全控制业务，包括用来获取服务器权限、获取数据库任意数据甚至拖库、盗取管理员在内的合法用户身份等。

在数量排名前10的网站安全漏洞中，跨站脚本漏洞、SVN/CVS信息泄露漏洞和列目录漏洞最为多见，分别占54.2%、11.48%和11.1%。三类漏洞占有所有漏洞的7成以上，其余安全漏洞占比相对很小，为SQL注入漏洞、本地路径泄露、IIS短文件名漏洞、源代码泄露、URL跳转漏洞、文件备份漏洞和ECShop支付插件漏洞。中国电商网站安全漏洞类型情况如图2-18所示。

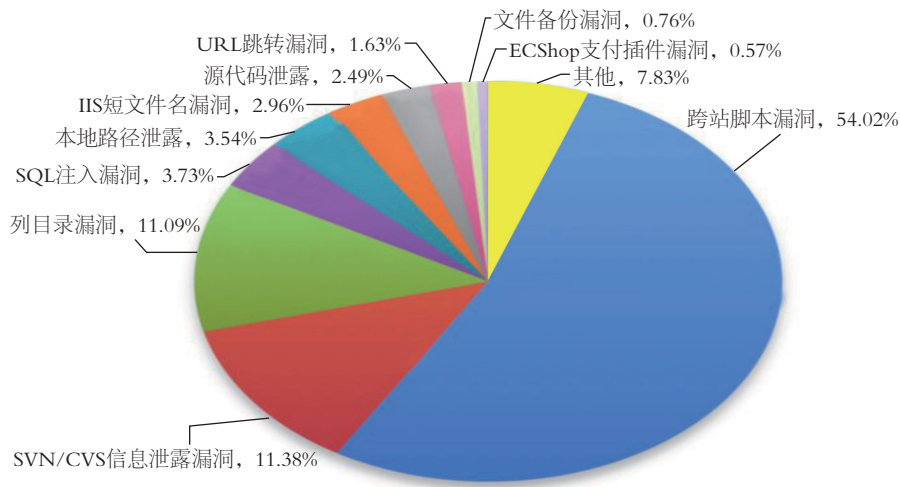


图2-18 中国电商网站安全漏洞类型情况（来自：奇虎360公司）

研究显示，黑客针对电商网站进行攻击，主要有以下几种方式。

篡改支付链接，进行钓鱼欺诈。2013年1-5月，360互联网安全中心接到多起利用电商网站进行钓鱼欺诈的案例报告。犯罪分子利用电商网站安全漏洞入侵网站，篡改网站代码，使消费者进行购物支付时其支付链接直接跳转到钓鱼网站，从而导致消费者的款项直接打到骗子账户中，对消费者财产和电商网站都造成极大损失，而且这种来自合法网站的非法跳转，很难被消费者察觉。

盗取用户账户，进行恶意消费。2013年6月，国内多家知名电商被爆用户账号和密码泄露，大量用户账户内资金被犯罪分子恶意购买充值卡等虚拟物品进行转移，给用户和网站造成巨大的经济损失。

盗取电商数据，形成黑色产业。如今盗卖网站数据库已经成为一个黑色产业：黑客入侵网站后会盗取网站整个数据库（拖库），特别是用户的账户信息和个人资料，用于黑市出售、广告推送或网络欺诈等不法行为，不仅危害用户本人的财产安全，而且还会给其亲朋好友的财产安全带来隐患。恶意竞争盛行，导致行业混乱。电商网站受到的流量攻击很多来自竞争对手的行为。这样的恶意攻击不仅会导致被攻击网站无



法正常运营，影响消费者使用，而且还会导致恶性竞争的泛滥，造成整个行业混乱，整体竞争力下降。

2.5.3 新兴安全威胁与交易风险

2.5.3.1 路由器DNS篡改

路由器攻击，特别是CSRF（Cross-Site Request Forgery，跨站请求伪造）攻击，是2013年5月曝光的一种新型网络攻击方式。用户点击网页上的某些特定信息后，其家用无线路由器就会被入侵，并遭到篡改。从篡改结果上来看，篡改路由器DNS设置是攻击的主要目的。当路由器的DNS设置被篡改后，用户访问正常的网站就可能被劫持到钓鱼网站，安全的云查询服务会被关闭，从而使用户电脑处于一种极为不安全的状态。

根据360 Wi-Fi体检的检测结果反馈显示：2013年第三季度，全国4.7%用户的家用路由器DNS遭到篡改。篡改能够成功的主要原因是路由器存在CSRF漏洞，以及用户使用弱密码作为路由器管理账号。360互联网安全中心针对市面上主流的344款路由器进行检测分析发现，共有104个型号的路由器容易被常见的CSRF攻击或DNS、DHCP等设置被篡改，占总数的30.2%。另外，统计显示，全国98.6%的家用无线路由器存在弱密码风险。

在DNS设置被篡改的用户中：70%以上指向境外恶意DNS服务器，其中韩国（52.0%）最多，美国（11.1%）和日本（10.0%）次之；境内，广东湛江（4.9%）、浙江绍兴（4.2%）和安徽铜陵（4.0%）则是恶意DNS服务器的三大源头。

从篡改DNS设置的目的来看：49.5%的篡改是为了向用户推送色情网页和游戏广告；28.0%的篡改是为了将淘宝等电商网站劫持到付费推广页面，从而骗取推广佣金，还有22.5%的其他各类劫持，如将正规网站的访问请求劫持到钓鱼网站或挂马网站，将360导航页劫持到其他导航页等。除此之外，很多DNS篡改还会封堵安全软件的云查询服务和软件升级，从而将用户电脑置于无法获得联网安全服务的极其危险的状态。

关于“推广佣金”：很多网店会通过搜索引擎、网页广告或软件广告等方式进行

推广。如果消费者单击了这些推广信息进入网店，并在一定时间内在该网店消费，那么店家就需要将消费款中的一部分作为佣金支付给推广信息提供者，如果用户是通过非推广渠道进入网店并消费，店家则无须向任何人支付佣金。

如果路由器的DNS遭到恶意篡改，当用户通过普通途径打开网店时，地址解析的结果就会将用户的访问请求强制引导到某个推广链接，之后再跳转到这家网店。这样一来，用户本应直接进入的网店，就变成了从推广链接打开的网店，店家因此就要向虚假的推广者支付本不必要的佣金。这是路由器对网上支付的一种隐蔽性极强的攻击。

2.5.3.2 恶意利用金融规则

由于现代网上交易系统非常复杂，用户对很多复杂的交易规则并不熟悉。黑客或骗子往往会利用人们对这些规则的不熟悉，曲解或误导用户进行相关操作，从而给用户造成财产损失。

从实际情况看，超级网银的授权支付、网上代付和淘宝红包，是被恶意利用频率最高的三个金融规则。

超级网银允许不同银行的账户之间进行相互授权，从而实现被授权账户可以不经过授权账户的同意，对该账户进行“任意”转账和支付操作。由于超级网银通常是默认开启的，在授权过程中不会验证双方身份，因此，骗子往往会制造交易异常的假象，并以解冻账户或解除交易异常为由，诱骗受害者在自己的网银上进行授权支付操作，授权骗子可以用其他账户来操作自己的网银账户。一旦受害者中招，账户余额就会被骗子迅速洗劫一空。根据现有的银行交易规则，通常情况下，受害人除了挂失银行卡外，完全无法自救。

网上代付允许商品购买人将商品信息发给付款人，之后由付款人来代替自己进行支付。付款人付款后，商品归商品购买人所有，购买人账户中有交易记录，而付款人账户中只有支出记录，没有商品的交易信息和交易记录，这就是代为付款的模式。网上代付用于诈骗主要有两种形式：一是骗子冒称商家将代付链接作为商品链接发送给受害人，让受害人代替自己购买商品；二是骗子在受害人完成代付操作后，利用受害人账户中没有交易记录的特点，谎称其商品交易发生异常，再以解除异常为由，把受



害人诱骗到更为危险的骗局中。

淘宝红包诈骗是2013年二季度开始流行的诈骗方式。淘宝红包是商家发送给消费者的一种现金礼品，获得红包的消费者可以使用红包中的资金购买其他商品。但很多新手买家并不了解红包的存在和使用规则，因此，骗子就谎称红包是“消费者保障金”，诱骗买家向自己派发红包。

2.5.3.3 物流信息泄露

网上实物交易大多以快递的形式实现最终兑付，但物流环节的安全性几乎完全无法掌控。快递公司员工批量盗卖用户信息的事件从2012年年底开始就不断被各路媒体曝光。由于快递单中包含用户的真实姓名、联系电话和详细地址等非常敏感的个人信息，这些信息的泄露将使受害者极易遭遇各种欺诈犯罪，特殊情况下，还可能遭遇人身安全等方面的威胁。

2.5.4 对策建议

(1) 建立路由器产品的安全准入机制

类似于前述的手机安全准入机制，对路由器产品采取新品安全准入机制。组织路由器厂商和具有路由器安全检测能力的互联网安全公司共同组成路由器安全检测机构，对即将上市的新品路由器进行安全鉴定。鉴定合格者方可入市销售。

(2) 建议金融机构全面排查网上交易规则

很多金融机构的网上交易规则还是很多年之前制定的，面对新型的手机安全威胁和钓鱼、社工等不断翻新变化的网络犯罪手法，其中某些规则，如超级网银授权支付规则等已经显得非常脆弱，非常容易被攻击或恶意利用。因此，金融机构有必要对自身网站及各种在线交易规则进行系统性排查，对于风险较高，存在安全隐患的交易规则，应当及时进行修订或修补。

(3) 在全国高校展开网上兼职安全教育活动

网站兼职诈骗基本上是一种纯粹的社会工程学诈骗，通常不需要配合使用木马钓鱼等专业的计算机手段，因此防范难度非常之大。根据《2013年一季度360网购先赔典

型案例》报告显示，近80%的网上兼职受害者为在校大学生。另外，90后在所有网购受害者中的占比高达49.2%。因此，在高校大学生中集中开展以防范网上兼职诈骗为主的上网安全教育活动，将十分有助于打击网络欺诈犯罪，可以大大减少网上兼职诈骗的案发率。

（4）金融机构建立24h响应机制

银行等金融机构应当设立24h无差别的电话服务或网上服务。根据360互联网安全中心的统计，每天23:00到次日凌晨1:00是网购用户被骗比例最高的时段。骗子在这个时段发动攻击，正是看中银行系统在这个时段基本不提供任何安全保障服务的特点。建议银行在该时段加强相关保障服务。

（5）制作以网上犯罪为主题法制情景剧

从犯罪分子和受害人等不同角度出发，制作一系列的以防范网络犯罪、防范网上欺诈为主要目的的法制科普片或安全情景剧，从而更好地向普通百姓解释网络犯罪的手法，提高网民防范网络欺诈的意识和能力。



计算机恶意程序传播和活动情况

恶意程序主要包括计算机病毒、蠕虫、木马、僵尸程序等。近年来，不同类别的恶意程序之间的界限逐渐模糊，木马和僵尸程序成为黑客最常利用的攻击手段。通过对恶意程序的监测、捕获和分析，可以评估互联网及信息系统所面临的安全威胁情况，掌握黑客最新攻击技术和手段，从而进一步深入研究维护用户计算机和信息系统安全必需的防护措施。

3.1 木马和僵尸网络监测情况

木马是以盗取用户个人信息和文件数据，甚至是以远程控制用户计算机为主要目的并尽可能隐藏自身的恶意程序。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”。按照功能分类，木马程序可进一步分为：盗号木马、网银木马、窃密木马、远程控制木马、流量劫持木马、下载者木马等类型木马。随着木马程序编写技术的发展和网络攻击技术的演进，一个木马程序往往同时包含上述多种功能。

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来操纵感染僵尸程序的主机执行相同的恶意行为，如可同时对其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。

2013年CNCERT/CC抽样监测结果显示，在利用木马或僵尸程序控制服务器对主机进行控制的事件中，控制服务器IP地址总数为18.9万个，较2012年下降47.4%。木马或僵尸程序受控主机IP地址总数为1870.2万个，较2012年大幅下降64.5%。其中，境内受控主机IP地址数量达1135.3万个，较2012年下降22.5%。这是近4年来我国境内感染木马或僵尸网络主机数量首次出现下降，反映出我国持续开展木马和僵尸网络专项治理行动和日常处置工作初见成效。

3.1.1 木马或僵尸程序控制服务器分析

2013年，境内木马或僵尸程序控制服务器IP地址数量为160228个，境外木马或僵

尸程序控制服务器IP地址数量为29146个，较2012年均有一定程度的下降，降幅分别为44.2%和60.2%，具体如图3-1所示。

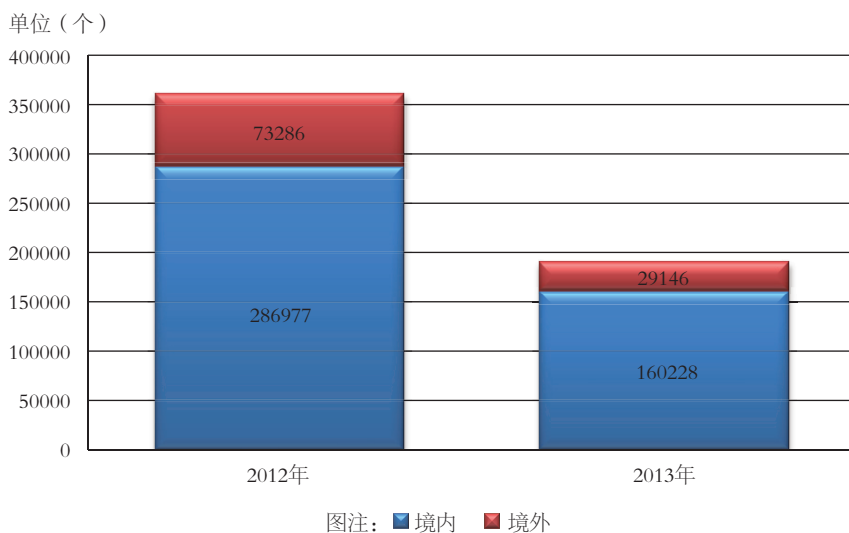


图3-1 2013年与2012年木马或僵尸程序控制服务器数量对比（来源：CNCERT/CC）

2013年，在发现的因感染木马或僵尸程序而形成的僵尸网络^[8]中，规模在100~1000的僵尸网络数量占73.7%以上。控制规模在100~1000、1000~5000、5000~20000、2万~5万、10万以上的主机IP地址的僵尸网络数量与2012年相比分别减少2255个、88个、61个、8个、50个，控制规模在5万~10万的僵尸网络数量与2012年相比增加9个。分布情况如图3-2所示。

[8] 僵尸网络刚刚出现时，黑客往往通过IRC协议来控制。随着恶意代码的发展，越来越多的僵尸网络被通过木马来控制，因此从广义上可把感染木马并由同一组控制端控制的联网计算机称为僵尸网络。

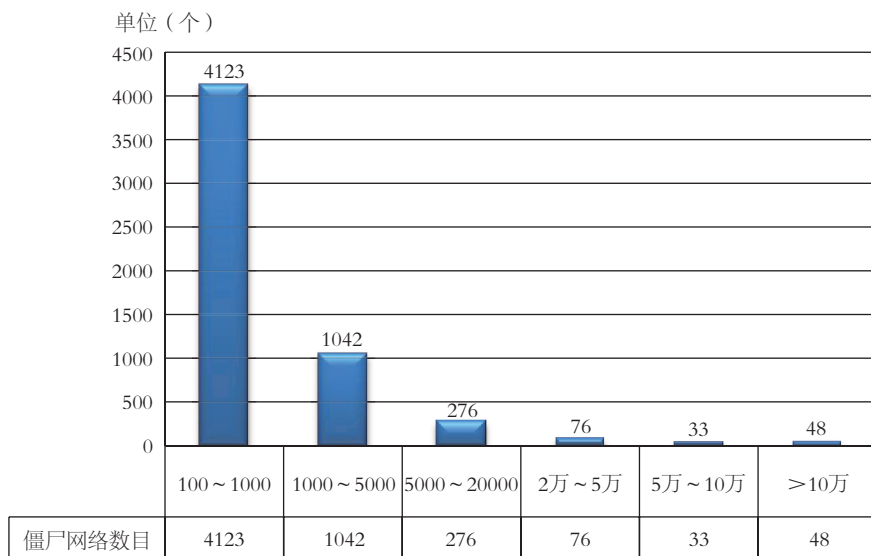


图3-2 2013年僵尸网络规模分布（来源：CNCERT/CC）

2013年木马或僵尸程序控制服务器IP地址数量的月度统计分布如图3-3所示。1月控制服务器数量近6万个，在2月开展的木马僵尸专项处置行动中CNCERT/CC对一批活跃恶意控制域名和控制服务器IP地址进行处置，2月开始控制服务器IP地址数量大幅下降，3-12月呈总体下降态势。

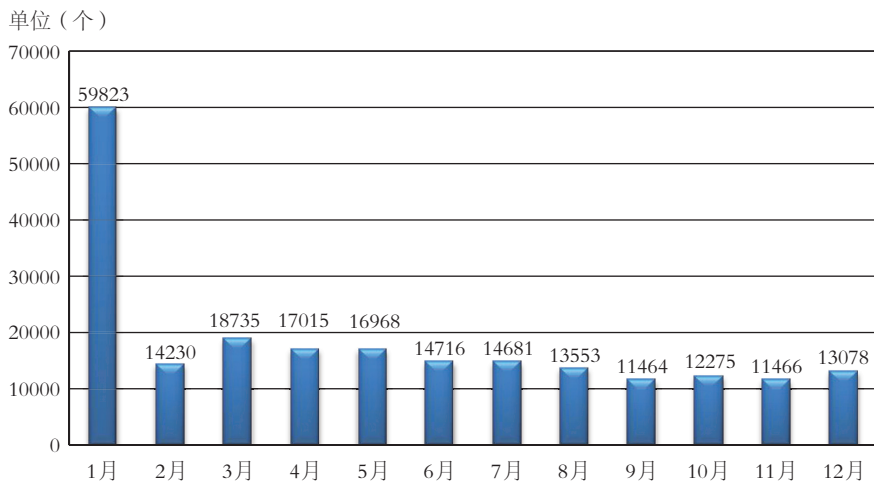


图3-3 2013年木马或僵尸程序控制服务器IP地址数量月度统计（来源：CNCERT/CC）

境内木马或僵尸程序控制服务器IP地址绝对数量和相对数量（即各地区木马或僵尸程序控制服务器IP地址绝对数量占其活跃IP地址数量的比例）前10位地区分布如图3-4和图3-5所示，其中，广东省、江苏省、浙江省居于木马或僵尸程序控制服务器IP地址绝对数量前3位，广西壮族自治区、广东省、新疆维吾尔自治区居于木马或僵尸程序控制服务器IP地址相对数量的前3位。

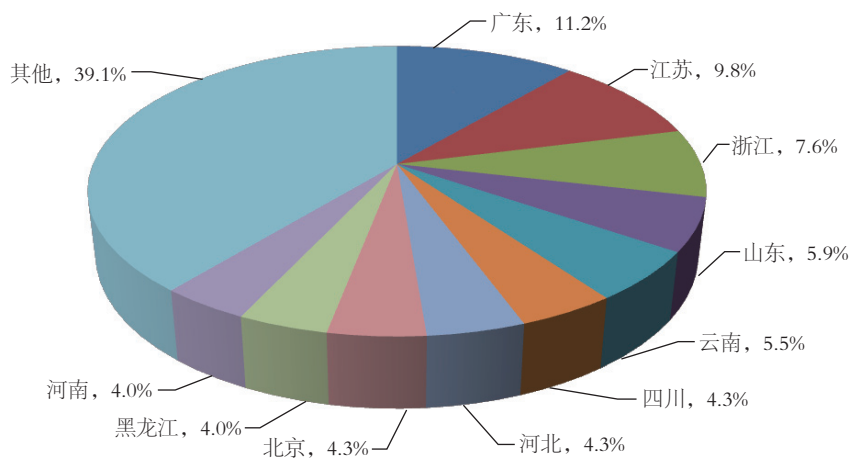


图3-4 2013年境内木马或僵尸程序控制服务器IP地址按省份分布（来源：CNCERT/CC）

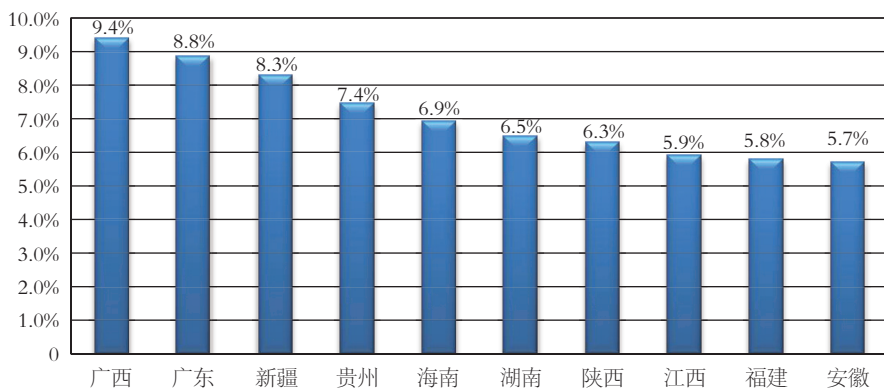


图3-5 2013年境内木马或僵尸程序控制服务器IP地址占所在省份活跃IP地址比例TOP10（来源：CNCERT/CC）

图3-6、图3-7为2012年境内木马或僵尸程序控制服务器IP地址数量按基础电信企业分布及所占比例，木马或僵尸程序控制服务器IP地址数量无论是绝对数量，还是相对数量（即各基础电信企业网内木马或僵尸程序控制服务器IP地址绝对数量占其活跃IP地址数量的比例），位于中国电信网内的数量均排名第一。其中位于中国电信网内的木马或僵尸程序控制服务器IP地址数量占据全部境内控制服务器IP地址数量的2/3以上。

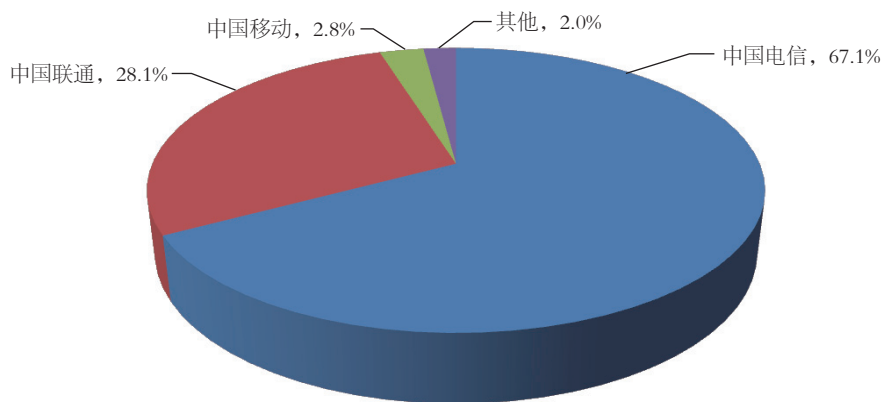


图3-6 2013年境内木马或僵尸程序控制服务器IP地址按基础电信企业分布
(来源: CNCERT/CC)

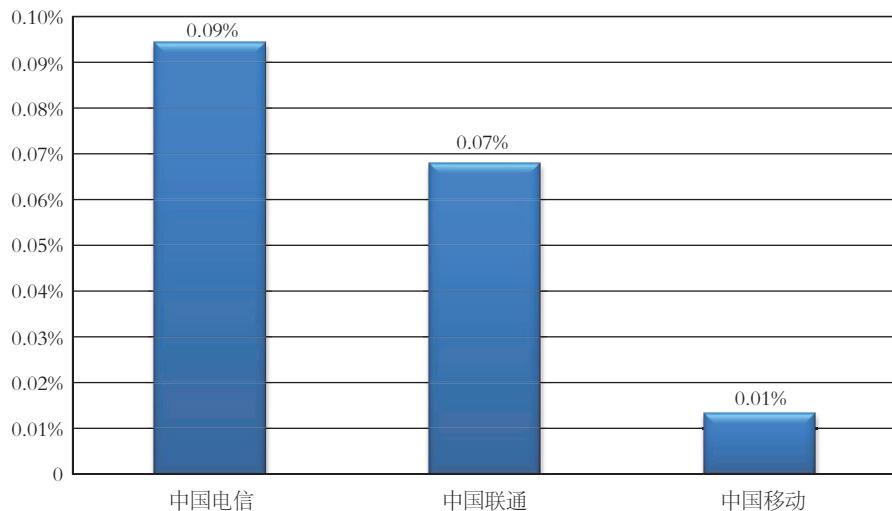


图3-7 2013年境内木马或僵尸程序控制服务器IP地址占所属基础电信企业活跃IP地址比例
(来源: CNCERT/CC)

境外木马或僵尸程序控制服务器IP地址数量前10位按国家和地区分布如图3-8所示, 其中美国位居第一, 占境外控制服务器的30.2%, 韩国和中国香港分列第二、三



位，占比分别为7.8%和7.7%。

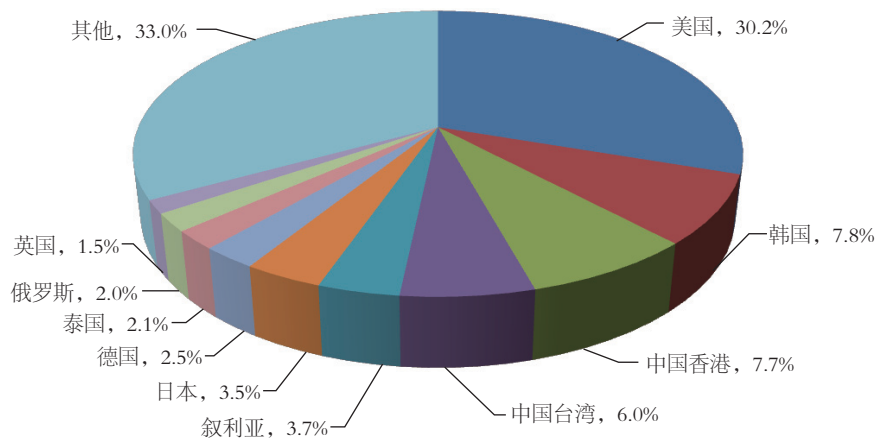


图3-8 2013年境外木马或僵尸程序控制服务器IP地址按国家和地区分布
(来源: CNCERT/CC)

3.1.2 木马或僵尸程序受控主机分析

2013年,境内共有11352817个IP地址的主机被植入木马或僵尸程序,数量较2012年减少22.5%。境外共有7349385个IP地址的主机被植入木马或僵尸程序,数量较2012年大幅减少80.7%。

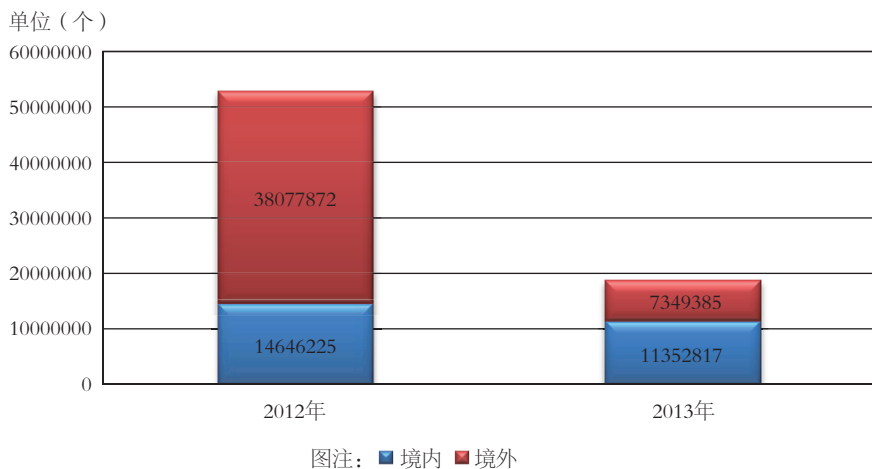


图3-9 2013年和2012年木马或僵尸程序受控主机数量对比(来源: CNCERT/CC)

2013年，CNCERT/CC持续加大对木马或僵尸网络的治理力度，木马或僵尸程序受控主机IP地址数量全年总体呈现下降态势，其中1月达到最高值303.1万个，10月为最低值93.2万个。2013年木马或僵尸程序受控主机IP地址数量月度统计如图3-10所示。

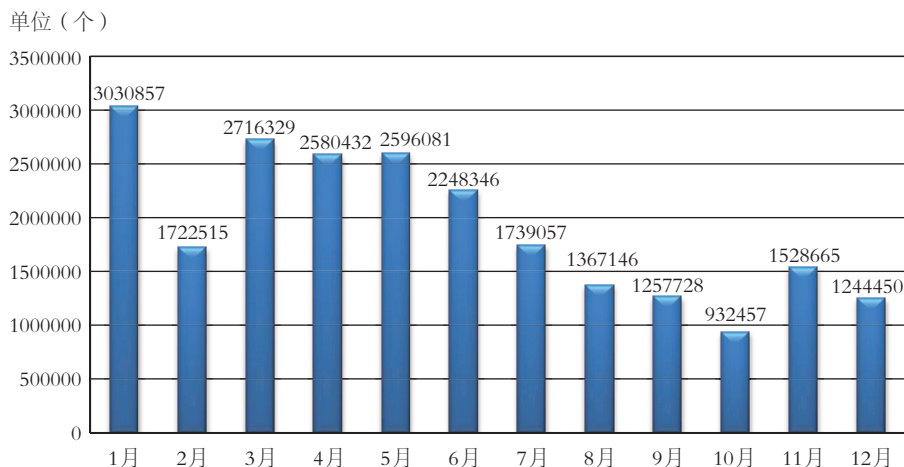


图3-10 2013年木马或僵尸程序受控主机IP地址数量月度统计（来源：CNCERT/CC）

境内木马或僵尸程序受控主机IP地址绝对数量和相对数量（即各地区木马或僵尸程序受控主机IP地址绝对数量占其活跃IP地址数量的比例）前10位地区分布如图3-11和图3-12所示，其中，广东省、江苏省、浙江省连续3年木马或僵尸程序受控主机IP地址绝对数量分别位于前3位，广西壮族自治区、广东省、新疆维吾尔自治区居于木马或僵尸程序受控主机IP地址相对数量的前3位。这在一定程度上反映出经济较为发达、互联网较为普及的东部地区因网民多、计算机数量多，该地区的木马或僵尸程序受控主机IP地址绝对数量处于全国前列。

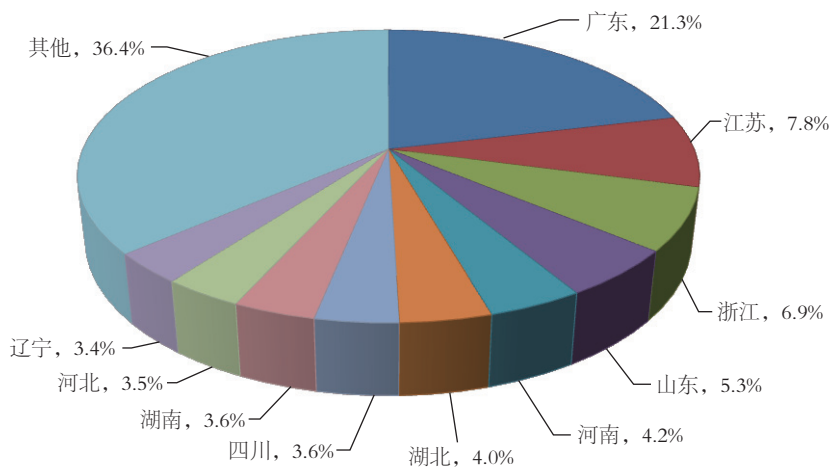


图3-11 2013年境内木马或僵尸程序受控主机IP地址按地区分布
(来源: CNCERT/CC)

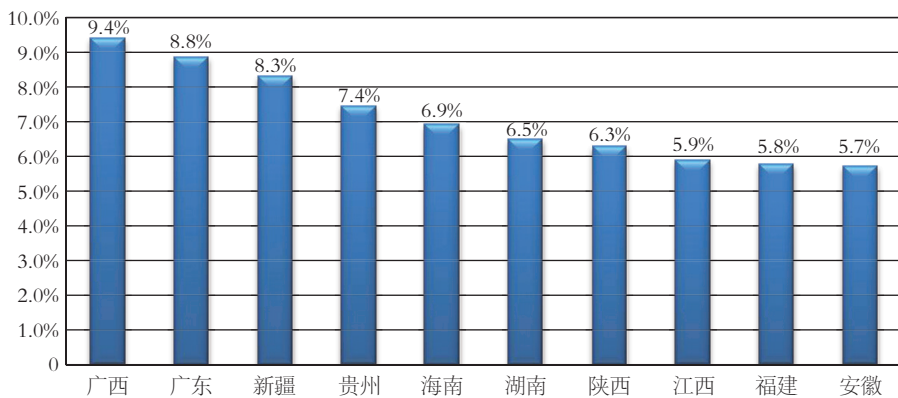


图3-12 2013年境内木马或僵尸程序受控主机IP地址占所在地区活跃IP地址比例
(来源: CNCERT/CC)

图3-13和图3-14为2013年境内木马或僵尸程序受控主机IP地址数量按基础电信企业分布及所占比例, 木马或僵尸程序受控主机IP地址位于中国电信网内的数量占据总数的2/3以上。从相对数量(即各基础电信企业网内木马或僵尸程序受控主机IP地址绝

对数量占其活跃IP地址数量的比例)上看,中国电信、中国联通网内感染木马或僵尸程序的主机IP地址数量占其活跃IP地址数量的比例均超过4%。

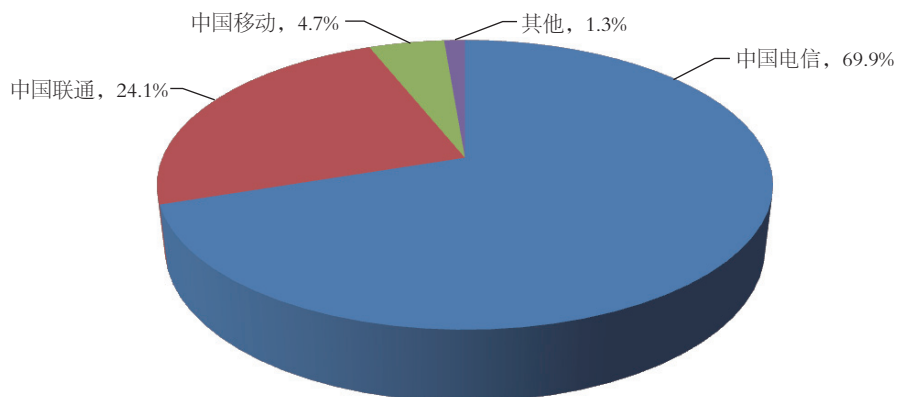


图3-13 2013年境内木马或僵尸程序受控主机IP地址按基础电信企业分布
(来源: CNCERT/CC)

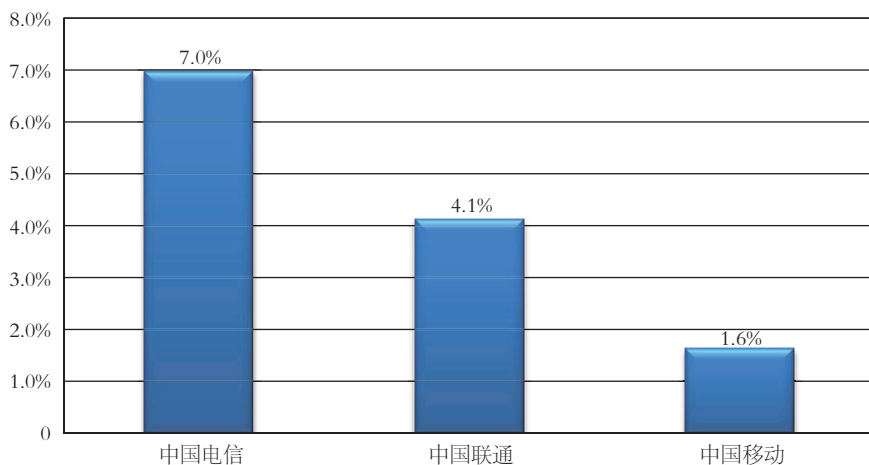


图3-14 2013年境内木马或僵尸程序受控主机IP地址数量占所属基础电信企业
活跃IP地址数量比例(来源: CNCERT/CC)

境外木马或僵尸程序受控主机IP地址数量按国家和地区分布前10位如图3-15所



示, 其中, 伊朗、日本、印度木马或僵尸程序受控主机IP地址数量居前3位。

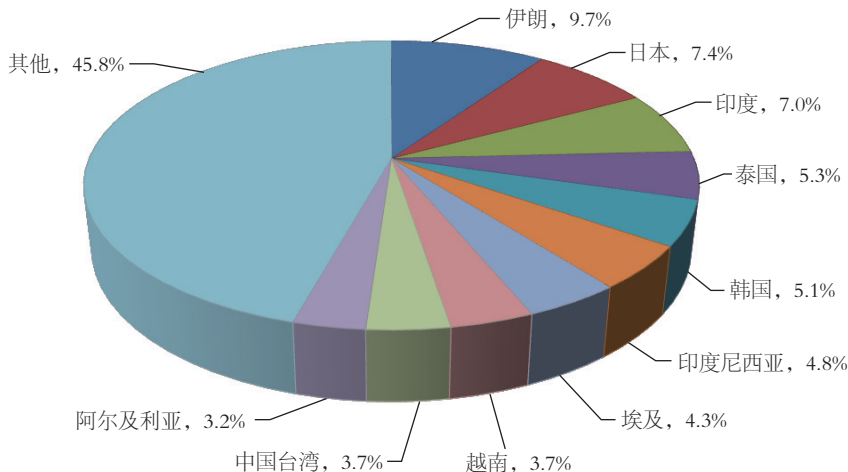


图3-15 2013年境外木马或僵尸程序受控主机IP地址按国家和地区分布
(来源: CNCERT/CC)

3.2 “飞客”蠕虫监测情况

“飞客”(英文名称Conficker、Downup、Downandup、Conflicker或Kido)是一种针对Windows操作系统的蠕虫病毒,最早在2008年11月21日出现。“飞客”蠕虫利用Windows RPC远程连接调用服务存在的高危漏洞(MS08-067)入侵互联网上未进行有效防护的主机,通过局域网、U盘等方式快速传播,并且会停用感染主机的一系列Windows服务。自2008年以来,“飞客”蠕虫衍生了多个变种,这些变种感染了上亿台主机,构建了一个庞大的攻击平台,不仅能够用于大范围的网络欺诈和信息窃取,而且能够被利用发动无法阻挡的大规模拒绝服务攻击,甚至可能成为有力的网络战工具。

CNCERT/CC自2009年起对“飞客”蠕虫感染情况进行持续监测。监测数据显示,全球互联网月均感染“飞客”蠕虫的主机数量持续减少,从2010年12月超过6000万台主机,到2011年月均3500万台主机,到2012年月均2800万台主机,再到2013年月均有1722万台主机。根据CNCERT/CC抽样监测显示,2013年,排名前三的国家或地

区分别是中国大陆（13.7%）、巴西（10.0%）和印度（6.5%），具体分布情况如图3-16所示。其中，中国大陆感染的主机IP地址数量月均超过175万个，图3-17所示为2013年我国大陆主机感染“飞客”蠕虫的IP地址数量月度统计。

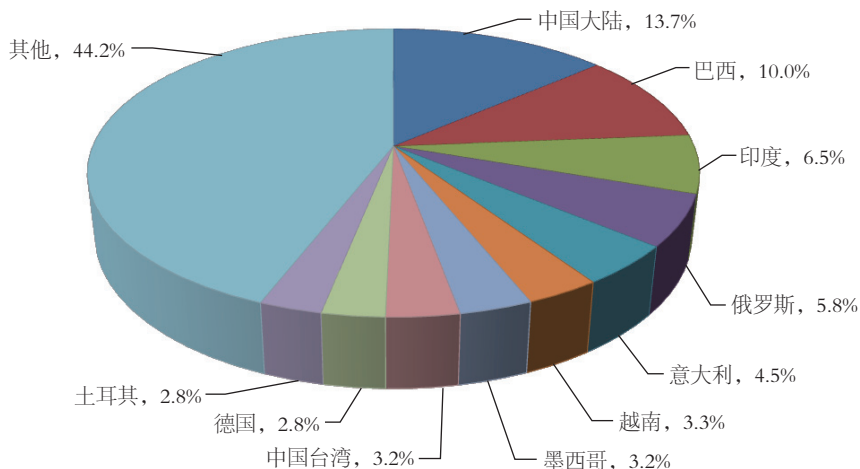


图3-16 2013年全球互联网感染“飞客”蠕虫的主机IP地址数量按国家和地区分布
(来源: CNCERT/CC)

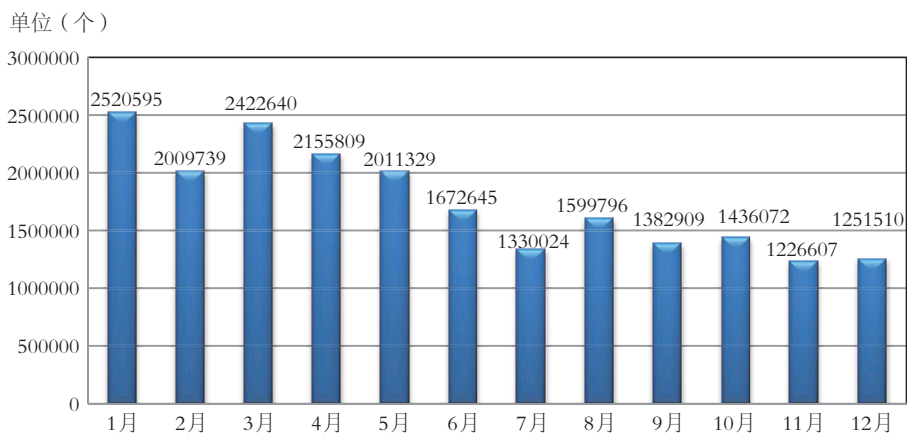


图3-17 2013年中国大陆感染“飞客”蠕虫的主机IP地址数量月度统计
(来源: CNCERT/CC)



3.3 恶意程序传播活动监测

2013年，CNCERT/CC监测发现已知恶意程序^[9]的传播事件近398.1万次，其中涉及已知恶意程序的下载链接17608个，“放马站点”（指存放恶意程序的网络地址）使用的域名2648个，“放马站点”使用的IP地址4788个。

已知恶意程序传播事件的月度统计如图3-18所示，2013年前10个月的恶意程序传播活动频次一直维持在比较低的水平，11月的恶意程序传播事件数量较前10个月出现暴增，12月的恶意程序传播事件数量仍然保持增长的态势。频繁的恶意程序传播活动将使用户上网面临的感染恶意程序风险加大，除需进一步加大对恶意程序传播源的清理工作外，提高广大用户的安全意识十分重要。

单位（个）

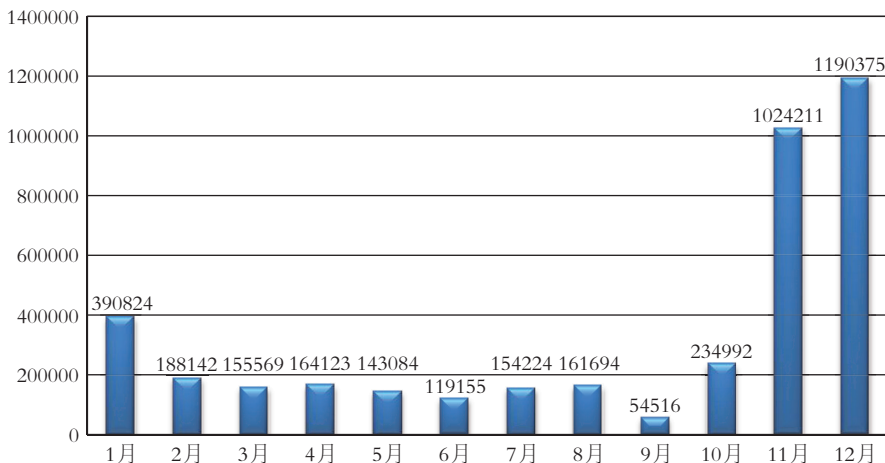


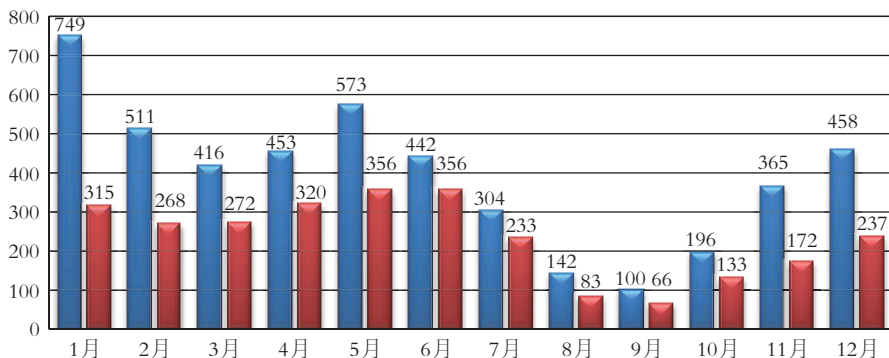
图3-18 2013年已知恶意程序传播事件次数月度统计（来源：CNCERT/CC）

“放马站点”使用的域名和IP地址数量的月度统计如图3-19所示。可以看出，2013年上半年的恶意域名数量总体较为稳定，但从7月开始有了较为明显的下降，下降趋势一直保持到9月，从10月开始恶意域名数量又开始上升，可直接访问“放马站点”的IP地址数量分布与恶意域名数量的分布相似。对恶意域名和IP地址的清理力度

[9] “已知恶意程序”是指被主流病毒扫描引擎识别和命名的恶意程序，而“未知恶意程序”是指虽有恶意行为但尚未被主流扫描引擎识别和命名的恶意程序。

应继续保持逐年加大的态势，为广大上网用户营造一个安全有序的互联网环境。

单位（个）



图注：■ 域名数量（通过域名访问） ■ IP数量（通过IP直接访问）

图3-19 2013年“放马站点”使用的域名和IP地址数量月度统计（来源：CNCERT/CC）

监测还发现，恶意程序传播绝大部分都是使用“8”开头的端口，其中以HTTP协议端口，即80端口为最多。用户上网一般都会在本机开放对远程主机80端口的访问权限，这样恶意程序的下载传播过程就不会受到防火墙设备的阻断，对用户来说防范的难度更高。2013年CNCERT/CC监测到的“放马站点”使用的端口分布统计如图3-20所示。

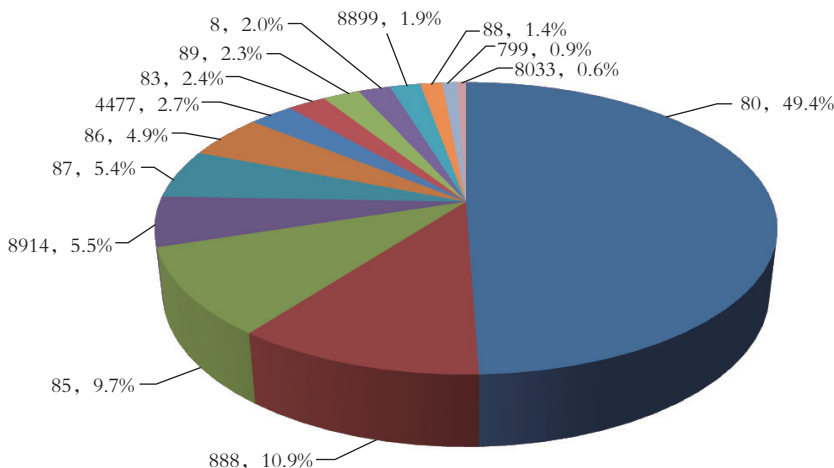


图3-20 2013年“放马站点”使用的端口分布统计（来源：CNCERT/CC）



3.4 通报成员单位报送情况

3.4.1 安天公司恶意程序捕获情况

根据安天公司监测结果，2013年全年捕获恶意程序样本总量为10887753个，比2012年的9473523个上升14.9%，具体如图3-21所示。

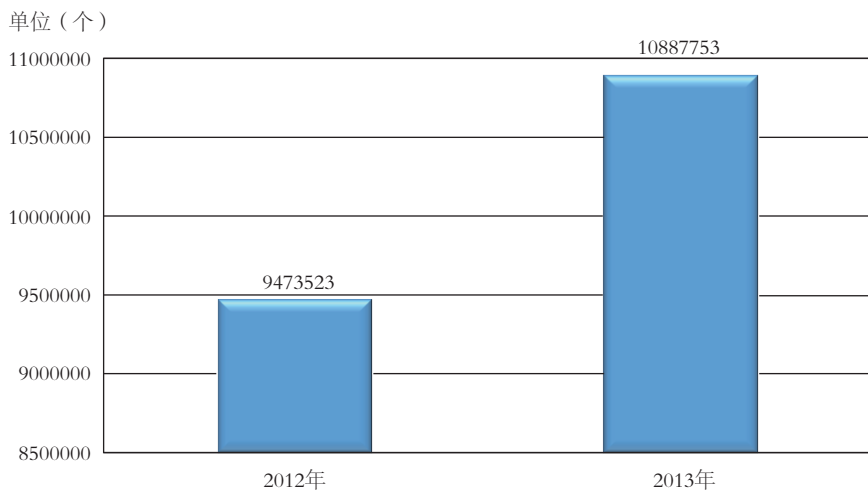


图3-21 2013年与2012年捕获恶意程序样本数量对比（来源：安天公司）

2007-2013年捕获恶意程序样本数量走势如图3-22所示。

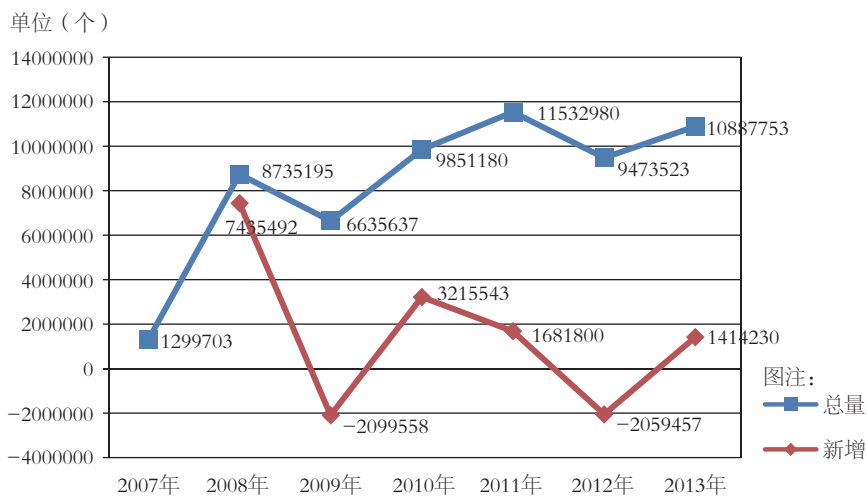


图3-22 2007-2013年捕获恶意程序样本数量走势图(来源:安天公司)

2013年全年捕获恶意程序样本数量总体呈现波动态势,如图3-23所示。其中6月达到全年最高值2128458个,2月为全年最低值319921个。

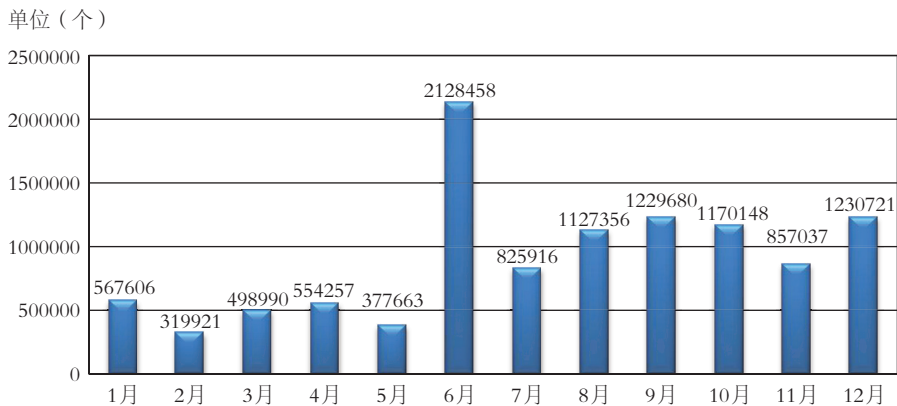


图3-23 2013年捕获恶意程序样本月度统计(来源:安天公司)

安天公司将捕获的恶意程序类型分为五大类,分别是病毒、蠕虫、木马、后门和



其他，每类恶意程序捕获数量月度统计如图3-24所示。其中，木马是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获木马数量共5480463个，占有所有恶意程序的50%，具体如图3-24所示。

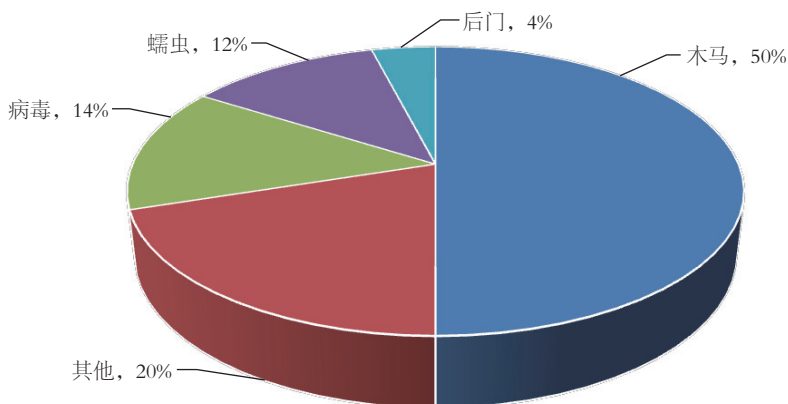


图3-24 2013年各类恶意程序捕获数量月度统计（来源：安天公司）

根据2013年和2012年监测结果对比，在捕获的各类恶意程序中，病毒和后门分别下降22.8%和30.0%，而木马、蠕虫和其他类型恶意程序的数量分别增长16.1%、59.3%和58.5%，如图3-25所示。

单位（个）

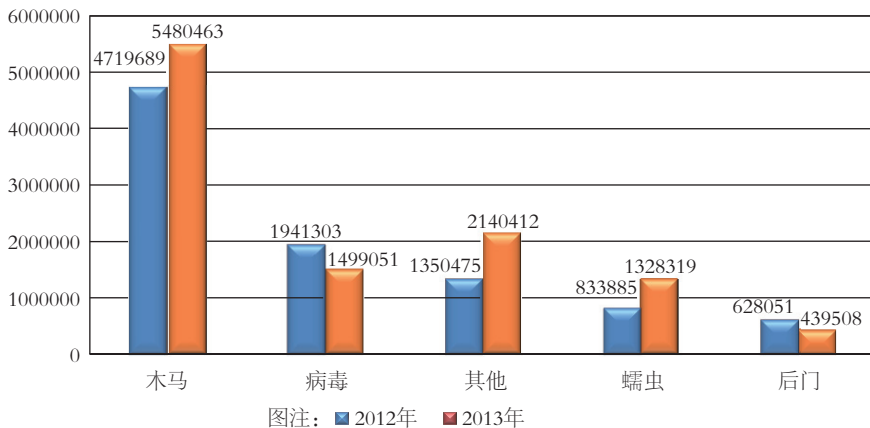


图3-25 2012年与2013年捕获恶意程序数量分类对比（来源：安天公司）

此外，从恶意程序的行为特征分析，用于恶意程序下载（Downloader）、间谍类（Spy）和捆绑类（Dropper）行为的恶意程序占据前三位，如图3-26所示。其中，捆绑类（Dropper）的数量较2012年下降41.4%，由第二位降至第三位，而间谍类（Spy）和偷窃类（Stealer）的数量比2012年分别增加16.3%和18.9%，排名较2012年分别上升2位和1位。

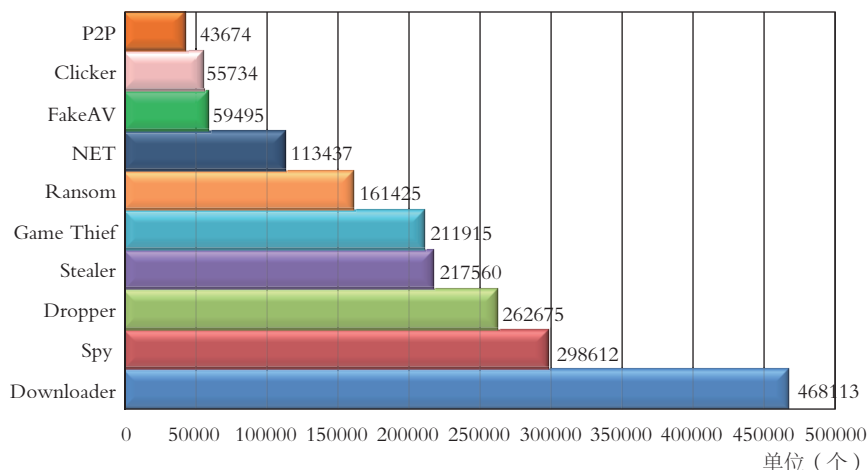


图3-26 2013年恶意程序样本按行为特征分类统计（来源：安天公司）

安天公司对恶意程序样本家族按捕获数量进行统计，2013年共有样本家族32920个，比2012年新增家族6818个。2013年恶意程序家族前10位见表3-1。

表3-1 2013年捕获恶意程序样本家族数量TOP10（来源：安天公司）

序号	家族名称	数量（个）
1	Downloader[:not_virus]/Win32.AdLoad	332570
2	Virus/Win32.Expiro	266726
3	Trojan/Win32.Jorik	264480
4	Worm/Win32.Debris	243478
5	Trojan[Spy]/Win32.Zbot	239524
6	Virus/Win32.Virut	231255
7	Virus/Win32.Sality	227446
8	Hoax[:not_virus]/Win32.ArchSMS	202622
9	Virus/Win32.Nimnul	192129
10	Virus/Win32.Parite	189375



2013年，恶意程序样本加壳的比例由2012年的8.6%上升至2013年的17.6%，如图3-27所示。2013年恶意程序所使用的主要壳类型TOP10见表3-2。

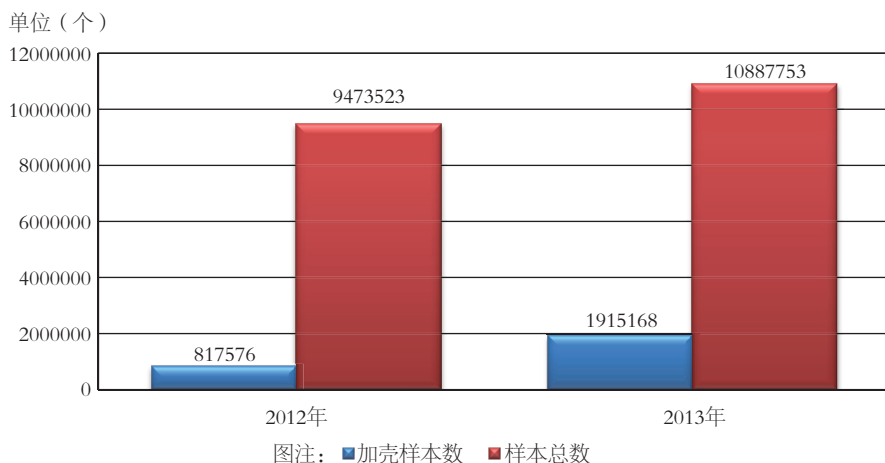


图3-27 2012年与2013年加壳样本数与样本总数统计对比（来源：安天公司）

表3-2 2013年恶意程序所使用的壳类型TOP10（来源：安天公司）

序号	壳名称	数量（个）
1	UPX	863840
2	PE_Patch	424160
3	ASPACK	91802
4	PECOMPACT	69346
5	ASPROTECT	64679
6	UPACK	45332
7	ZPROTECT	28454
8	Com100	27452
9	MPRESS	26108
10	NSPACK	21239

3.4.2 金山网络公司^[10]报送的恶意程序情况

根据金山网络公司监测结果，2013年全年捕获恶意程序样本总量为67619099个（去重后数量），比2012年的42905082个增长36.5%。2013年各月捕获数量如图3-28所

[10] 金山网络公司即金山网络技术有限公司，是通信行业互联网网络安全信息通报工作单位。

示，其中2月达到全年最低值3155866个，6月达到全年最高值9039568个。

单位（个）

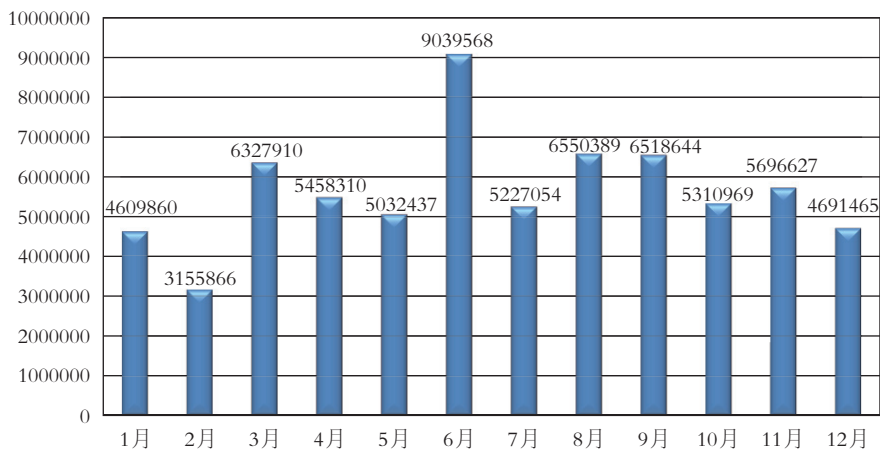


图3-28 2013年捕获恶意程序样本数量月度统计（来源：金山网络公司）

2003-2013年捕获恶意程序数量走势如图3-29所示。

单位（个）

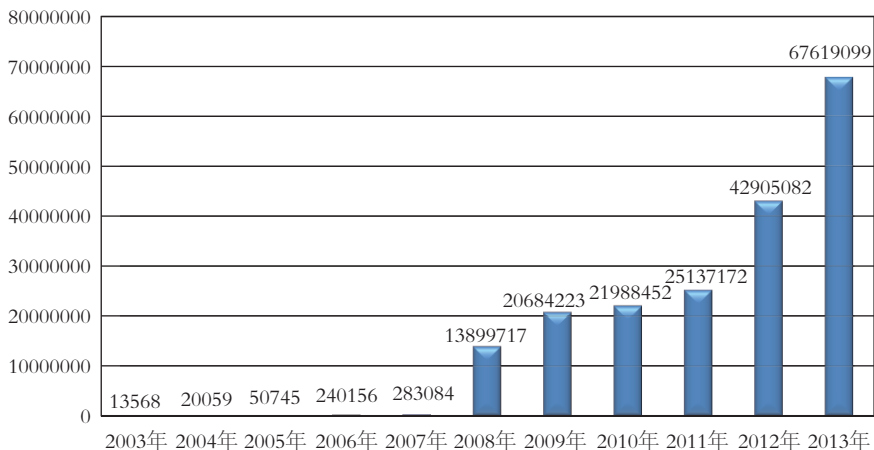


图3-29 2003-2013年捕获恶意程序数量走势图（来源：金山网络公司）

2013年全年捕获新增恶意程序特征总量为42501293个（去重后数量），各月捕获数



量如图3-30所示,其中2月为全年最低值1798850个,11月达到全年最高值5779044个。

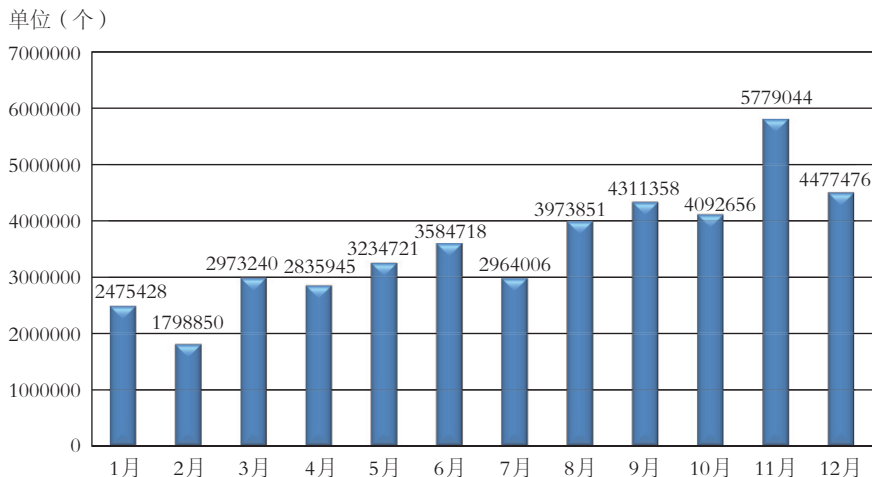


图3-30 2013年捕获新增恶意程序特征月度统计(来源:金山网络公司)

2013年全年监测到感染恶意程序的主机210335555台,比2012年的236277086台下降12.3%,感染恶意程序的主机数量为下降趋势。其中感染主机数量2月为全年最低值11647302台,10月达到全年最高值20209795台,如图3-31所示。

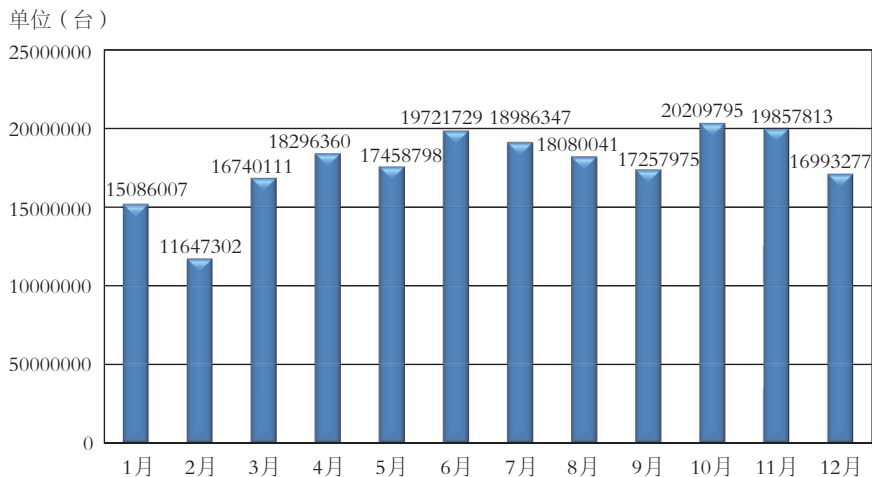


图3-31 2013年感染恶意程序主机数量月度统计(来源:金山网络公司)

3.4.3 奇虎360公司报送的恶意程序情况

根据奇虎360公司监测结果，2013年全年捕获恶意程序样本总量为18.85亿个（MD5值不同），比2012年的13.68亿个增长37.8%。2013年各月捕获数量如图3-32所示，其中2月达到全年最低值9977万个，12月达到全年最高值2.1亿个。2009-2013年捕获恶意程序数量趋势如图3-33所示。

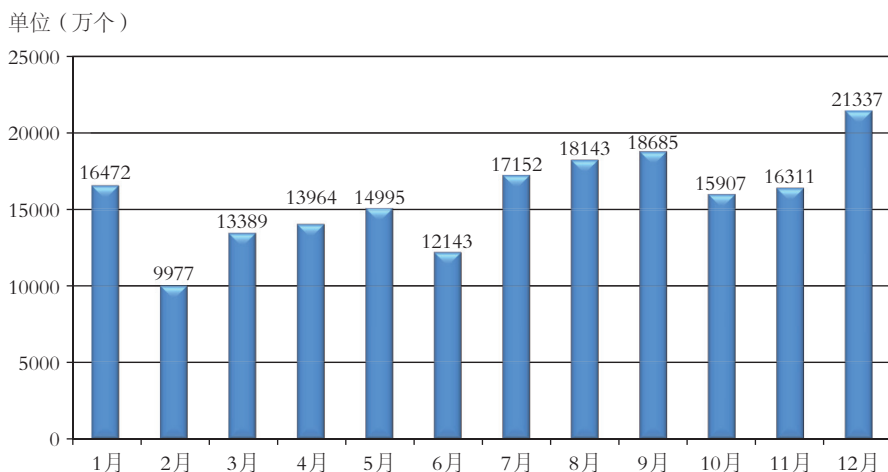


图3-32 2013年捕获恶意程序样本月度统计（来源：奇虎360公司）

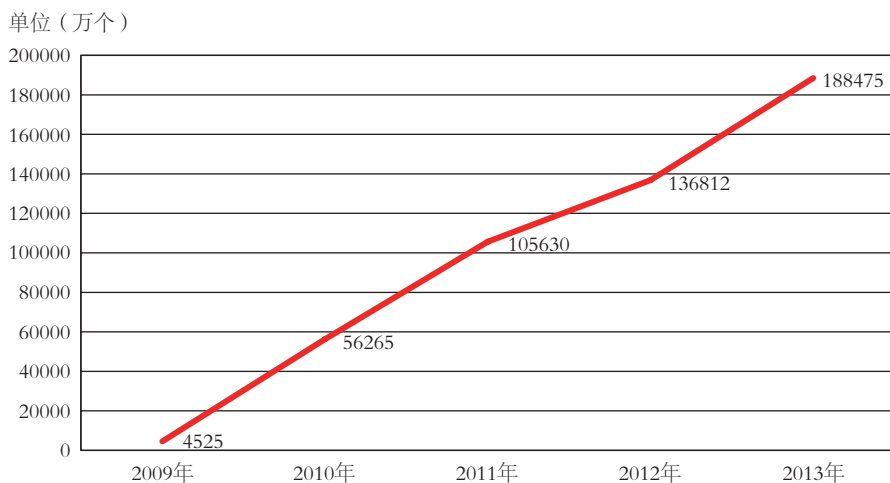


图3-33 2009-2013年捕获恶意程序数量走势（来源：奇虎360公司）



3.4.4 卡巴斯基公司^[11]恶意程序捕获情况

根据卡巴斯基公司监测结果,2013年全年捕获恶意程序总量约为1388343个(按恶意程序名称统计),比2012年1125888个增长24%。2013年各月捕获数量如图3-34所示,其中1月为全年最低值69487个,9月达到全年最高值145406个。

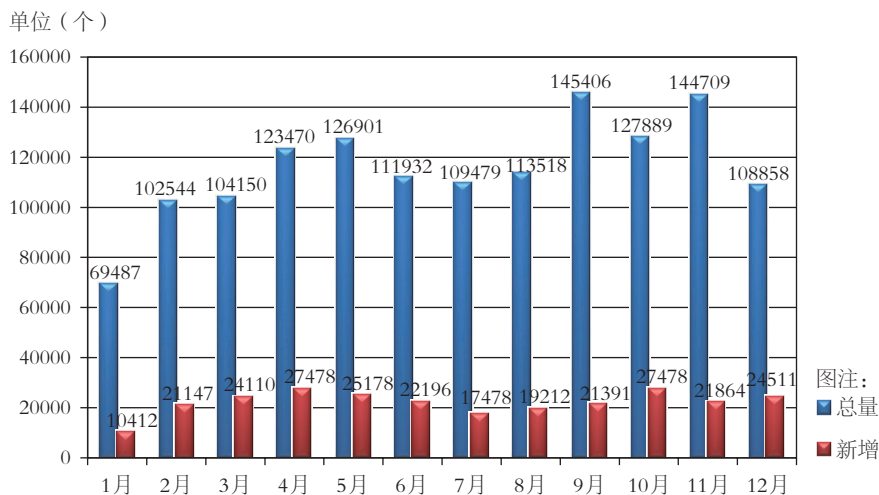


图3-34 2013年捕获恶意程序数量月度统计(来源:卡巴斯基公司)

2013年全年捕获恶意程序样本总量为19025479个(MD5值不同),比2012年的12871056个增长47%。2013年各月捕获数量如图3-35所示,其中12月达到全年最低值307672个,2月达到全年最高值764815个。

[11] 卡巴斯基公司即卡巴斯基技术开发(北京)有限公司。

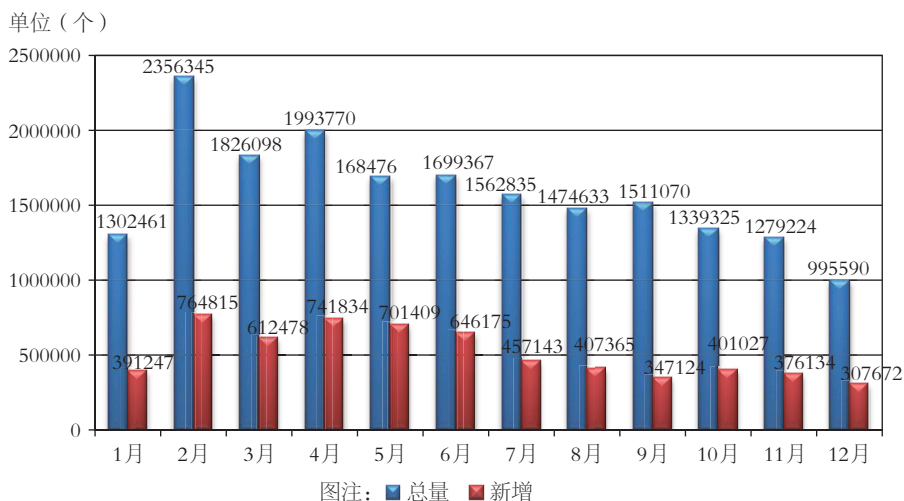


图3-35 2013年捕获恶意程序样本数量月度统计（来源：卡巴斯基公司）

2013年全年监测到感染恶意程序的主机4605147台，比2012年的4251920台增长8%。感染恶意程序的主机数量呈上升趋势，其中感染主机数量8月为全年最低值331478台，11月达到全年最高值419457台，如图3-36所示。

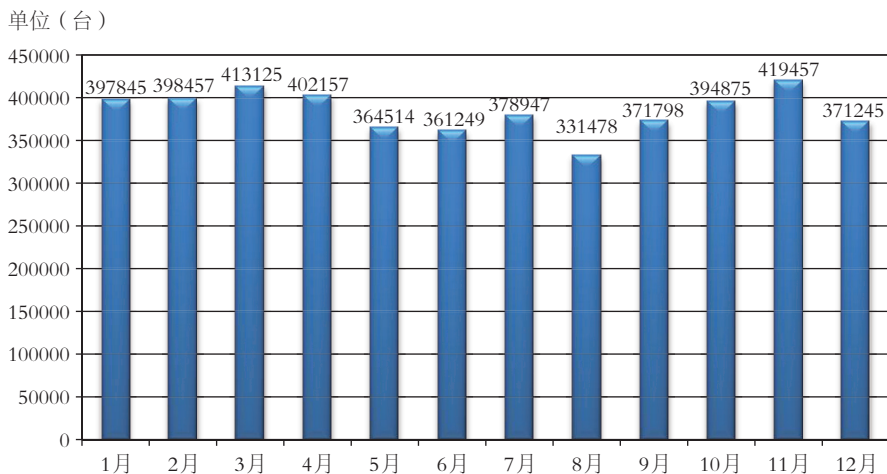


图3-36 2013年感染恶意程序主机数量月度统计（来源：卡巴斯基公司）



卡巴斯基公司将捕获的恶意程序类型分为六大类，分别是病毒、木马、恶意软件、广告软件、风险软件和色情软件。其中，木马是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获木马数量约897万个。各类恶意程序数量增幅位居前三位的是木马、病毒和蠕虫，增幅分别为13.3%、7.7%和6.1%。

卡巴斯基公司对恶意程序样本家族按捕获数量进行统计，2013年比2012年新增家族11478个。2013年恶意程序家族前10位见表3-3。

表3-3 2013年恶意程序样本家族捕获数量TOP10（来源：卡巴斯基公司）

序号	家族名称	数量（个）
1	DangerousObject.Multi.Generic	1952336
2	Trojan.Win32.Generic	1928122
3	Trojan.Win32.AutoRun.gen	996954
4	Virus.Win32.Sality.gen	863392
5	Exploit.Win32.CVE-2010-2568.gen	601752
6	AdWare.Win32.DelBar.a	340733
7	Trojan.Win32.Starter.lgb	397182
8	Virus.Win32.Nimnul.a	201747
9	Worm.Win32.Debris.a	101033
10	Virus.Win32.Generic	71768

4 移动互联网恶意程序传播和活动情况

2013年，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》（工业和信息化部保[2011]545号）文件规定和要求，CNCERT/CC持续加强对移动互联网恶意程序的监测、样本分析和验证处置工作。根据监测结果，2013年移动互联网恶意程序的数量继续呈爆发式增长趋势。

4.1 移动互联网恶意程序监测情况

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。移动互联网恶意程序一般存在以下一种或多种恶意行为，包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。2013年CNCERT/CC捕获及通过厂商交换获得的移动互联网恶意程序样本数量为702861个。

2013年CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序按行为属性统计如图4-1所示。其中，恶意扣费类的恶意程序数量仍居首位，为502481个，占71.5%，资费消耗类104069个（占15.1%）、系统破坏类22805个（占3.3%）分列第二、三位。结果显示与用户经济利益密切相关的恶意扣费类和资费消耗类恶意程序已占到恶意程序总数的85%以上，显示了黑客制作恶意程序带有明显的趋利性。2013年，CNCERT/CC组织通信行业开展了8次移动互联网恶意程序专项治理行动。

按操作系统分布统计，2013年CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序主要针对Android平台，共有699514个，占总数99%以上，位居第一。其次是Symbian平台，共有3341个，占0.48%，此外仍有6个针对J2ME平台的恶意程序。2013年，随着Nokia对Symbian操作系统停止开发，Symbian手机的市场逐渐萎缩，另外，Android手机的市场不断扩大，Symbian手机市场和Android手机市场的此消彼长，



使2013年Android恶意程序数量占比较2012年增加17%，Symbian恶意程序数量占比较2012年减少17%。2013年移动互联网恶意程序数量按操作系统分布如图4-2所示。

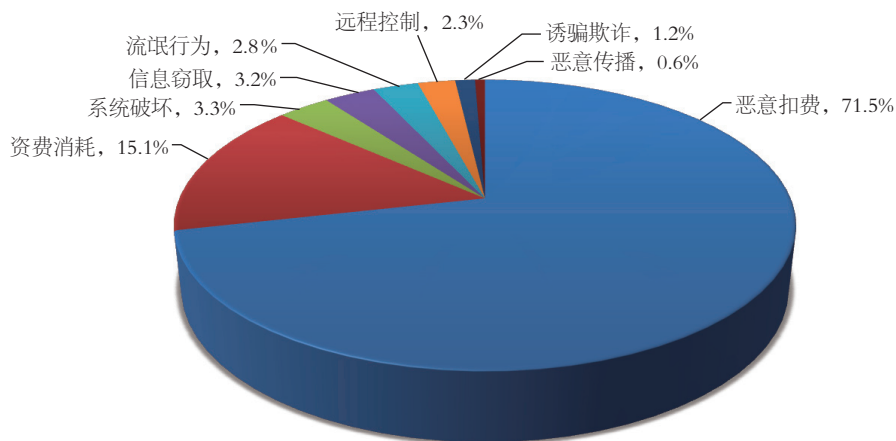


图4-1 2013年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

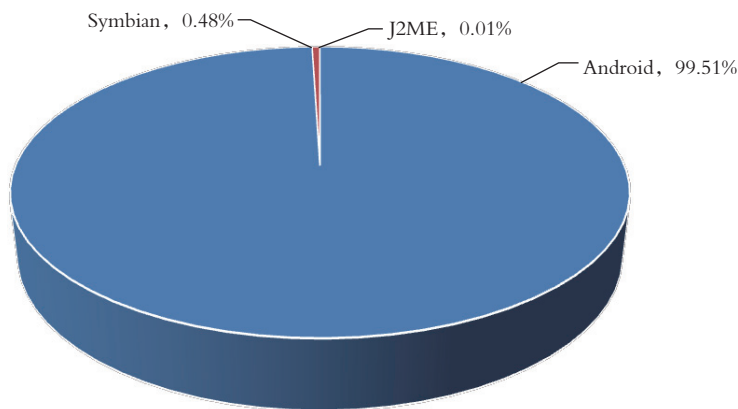


图4-2 2013年移动互联网恶意程序数量按操作系统统计（来源：CNCERT/CC）

如图4-3所示，按危害等级统计，2013年CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序中，高危的为7028个，占1.0%；中危的为203830个，占29.0%；低危的为492003个，占70.0%。相对于2012年，高危移动互联网恶意程序所占比例有所下降，这反映了黑客为逃避监管逐渐向灰色地带发展，不再制作恶意性明显的手机木

马等病毒，开始制作恶意广告、恶意第三方插件等灰色应用，达到既逃避监管又获取经济利益的目的。

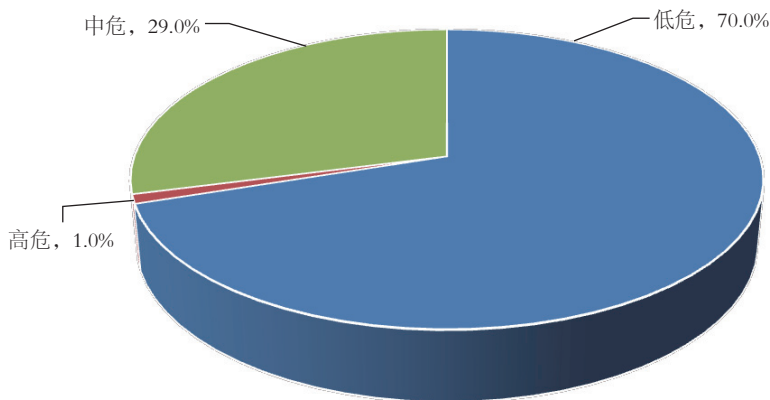


图4-3 2013年移动互联网恶意程序数量按危害等级统计（来源：CNCERT/CC）

4.2 移动互联网恶意程序传播活动监测

与传统互联网恶意程序通过“放马站点”传播不同的是，大量移动互联网恶意程序主要通过手机应用商店、论坛、下载站点等进行传播。由于当前管理机制尚不完善，安全检测手段有所欠缺，对开发者上传的移动互联网应用程序审核不严格等原因，造成种类繁多的手机应用商店、论坛和下载站点成为移动互联网恶意程序传播的重灾区。

2013年，CNCERT/CC监测发现移动互联网恶意程序传播事件12956836次，是2012年同期562019次的23倍。移动互联网恶意程序URL下载链接1206798个，是2012年同期36192个的33倍，进行移动互联网恶意程序传播的域名15427个、IP地址60976个，分别是2012年同期的32倍和11倍，其中.com域名占78.8%，.cn域名占15.1%。以上15427个恶意域名包含了应用软件商店、论坛、网盘、博客等众多网站类型，其中应用软件商店数量超过300家。

移动互联网恶意程序传播事件的月度统计如图4-4所示，2012年1-7月移动恶意程序传播活动频次相对较低，8月后传播事件数量有所增长，并维持在较高水平。

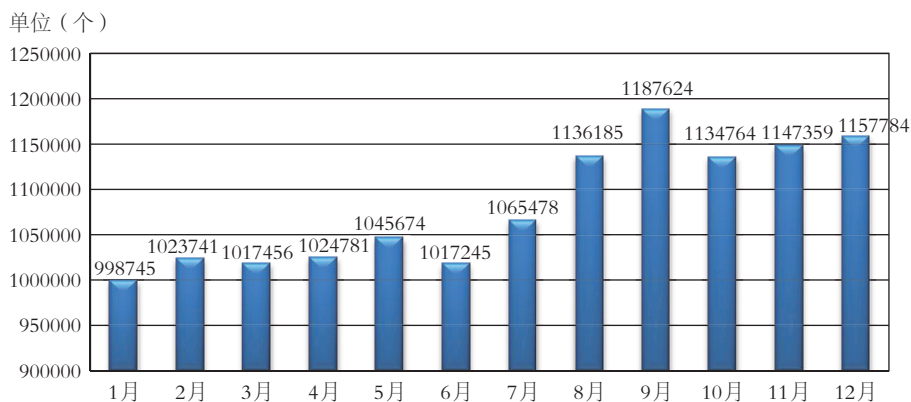


图4-4 2013年移动互联网恶意程序传播事件数量月度统计（来源：CNCERT/CC）

移动互联网恶意程序传播所使用的域名和IP地址数量的月度统计如图4-5所示，可以看出全年呈波动趋势。在每次开展专项治理工作后，传播移动互联网恶意程序的域名和IP地址数量便有所下降。

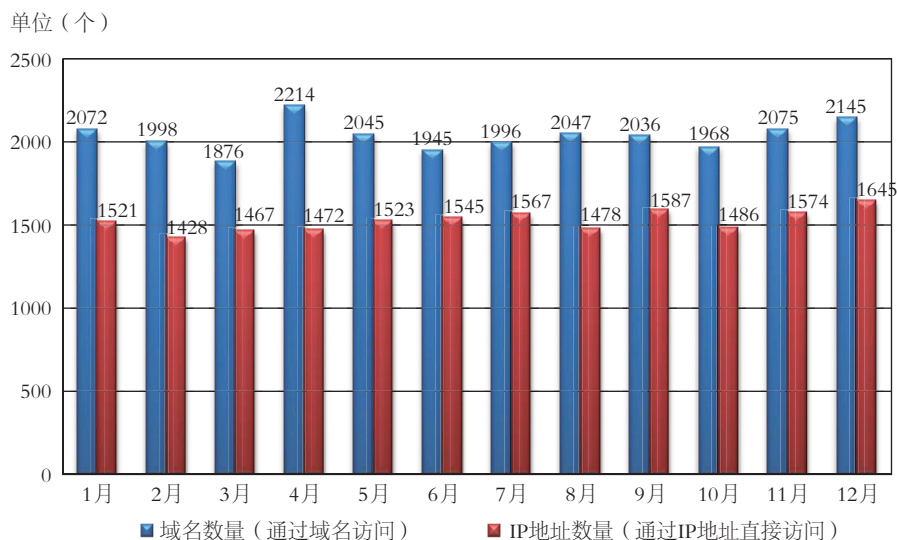


图4-5 2013年移动互联网恶意程序传播源域名和IP地址数量月度统计（来源：CNCERT/CC）

4.3 通报成员单位报送情况

4.3.1 网秦公司^[12]移动互联网恶意程序捕获情况

根据网秦公司监测结果，截至2013年年底，累计发现移动互联网恶意程序（按恶意程序名称统计）11266个，其中2013年新发现1094个。截至2013年年底，累计捕获移动互联网恶意程序样本（MD5值不同）1181589个，其中2013年新捕获样本798942个。按照《移动互联网恶意程序描述格式》的八大分类标准，2013年发现的移动互联网恶意程序分类统计数据为：恶意扣费323203个；资费消耗244585个；流氓行为120379个；远程控制55325个；信息窃取41244个；系统破坏8487个；诱骗欺诈5211个；恶意传播509个。

2013年各月捕获移动互联网恶意程序数量（按恶意程序名称统计）如图4-6所示，其中2月为全年最低值40个，11月达到全年最高值167个。

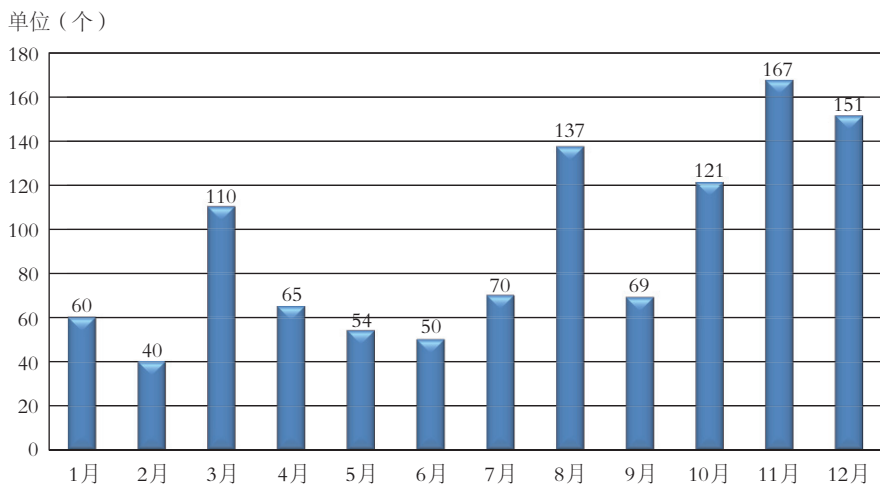


图4-6 2013年捕获移动互联网恶意程序月度统计（来源：网秦公司）

2013年各月捕获移动互联网恶意程序样本数量（MD5值不同）如图4-7所示，其中2月达到全年最低值425个，8月达到全年最高值174028个。

[12] 网秦公司即北京网秦天下科技有限公司，是通信行业互联网网络安全信息通报工作单位。

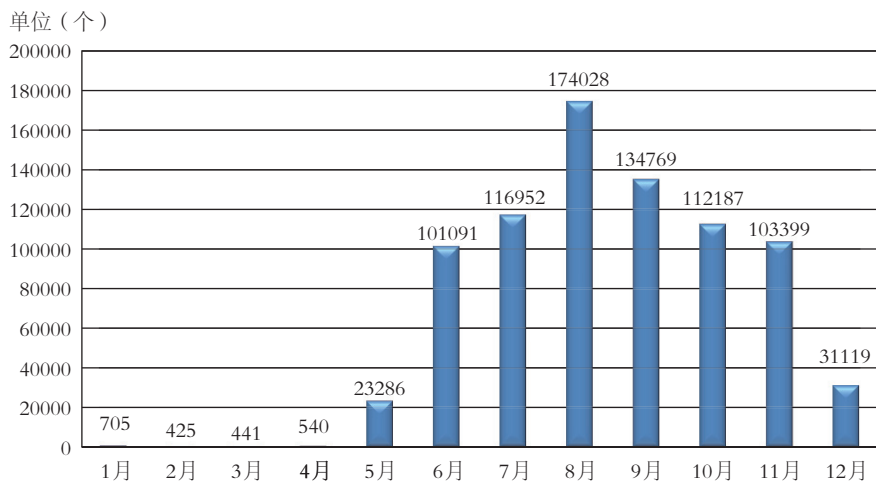


图4-7 2013年捕获移动互联网恶意程序样本月度统计（来源：网秦公司）

4.3.2 安天公司移动互联网恶意程序捕获情况

根据安天公司监测结果，2013年，捕获移动互联网恶意程序样本604541个，比2012年的177761个大幅增长240%，2013年移动互联网安全呈现越发严峻的形势。从2013年新增恶意样本数量的月统计数量来看，7月达到最高值73783个，1月为最低值23748个。具体如图4-8所示。

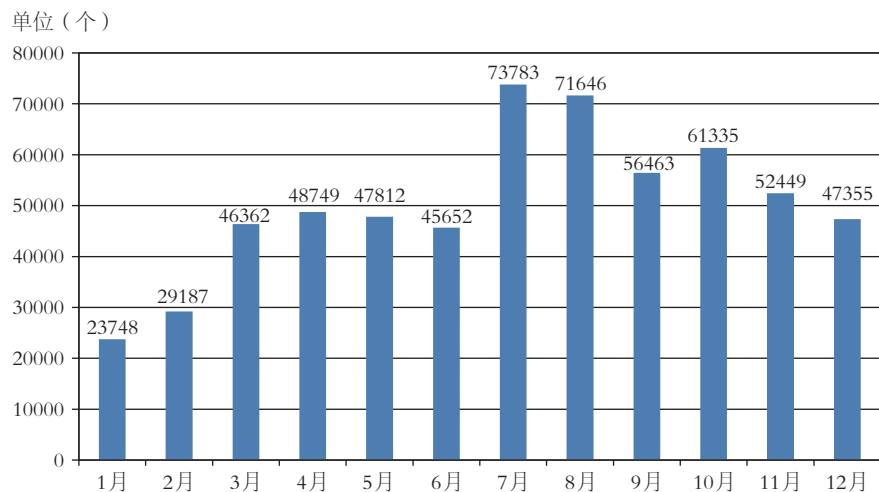


图4-8 2013年新增移动互联网恶意程序样本数量月度统计（来源：安天公司）

按照《移动互联网恶意程序描述格式》的八大分类标准，2013年发现的移动互联网恶意程序分类统计数据为：恶意扣费类432043个，数量仍位居第一，其次是资费消耗类和系统破坏类，数量为91034个和19782个，分别居第二、三位。2013年捕获移动互联网恶意程序数量分类统计如图4-9所示。

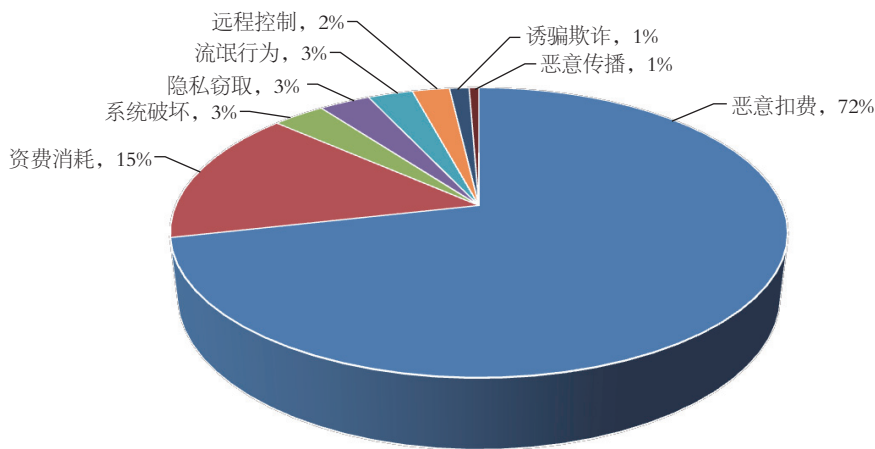


图4-9 2013年捕获移动互联网恶意程序数量分类统计（来源：安天公司）

4.3.3 金山公司移动互联网恶意程序捕获情况

根据金山网络监测结果，截至2013年年底，累计捕获移动互联网恶意程序样本11082815个（MD5值不同），其中2013年新捕获恶意程序样本656029个，2月新捕获恶意程序数量达到全年最高值156486个，3月为全年最低值27268个。具体如图4-10所示。

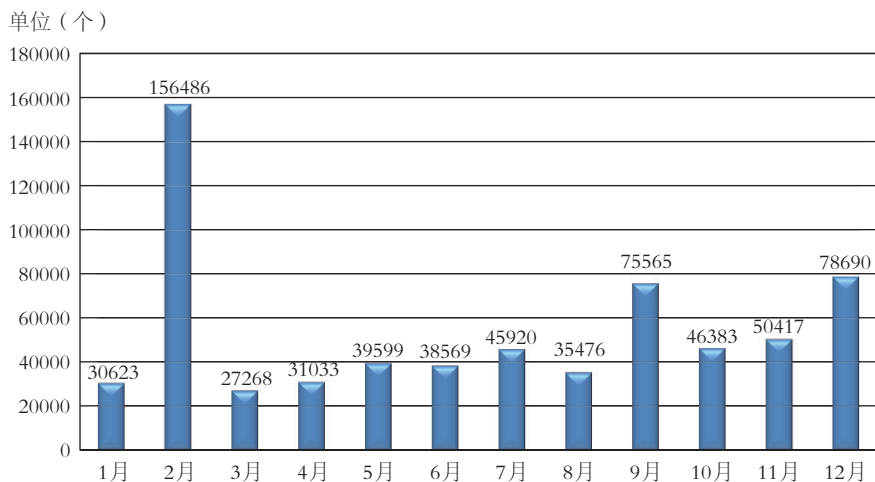


图4-10 2013年捕获新增移动互联网恶意程序样本数量月度统计（来源：金山网络公司）

2013年发现的移动互联网恶意程序分类统计数据为：资费消耗类8117054个，数量位居第一；恶意传播类和恶意扣费类，分别居第二、三位。2013年捕获移动互联网恶意程序数量分类统计如图4-11所示。

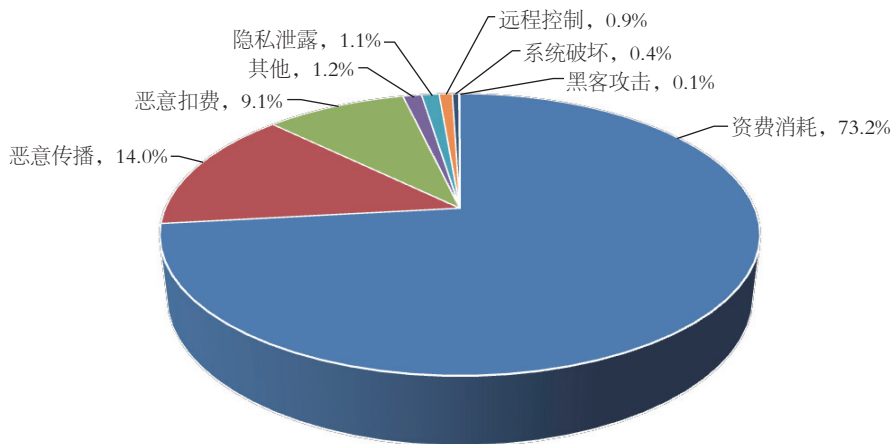


图4-11 2013年捕获移动互联网恶意程序数量分类统计（来源：金山网络公司）

4.3.4 恒安嘉新公司^[13]移动互联网恶意程序捕获情况

根据恒安嘉新公司监测结果，截至2013年年底，累计发现移动互联网恶意程序（按恶意程序名称统计）3053个，其中2013年新发现411个。截至2013年年底，累计捕获移动互联网恶意程序样本159282个（MD5值不同），其中2013年新捕获样本145925个。按照《移动互联网恶意程序描述格式》的八大分类标准，2013年发现的移动互联网恶意程序样本分类统计数据为：恶意扣费88306个；资费消耗23450个；流氓行为11228个；隐私窃取7239个；远程控制7069个；系统破坏3859个；诱骗欺诈3551个；恶意传播1223个。

2013年各月捕获新增移动互联网恶意程序数量（按恶意程序名称统计）如图4-12所示，其中2月为全年最低值19个，9月达到全年最高值48个。

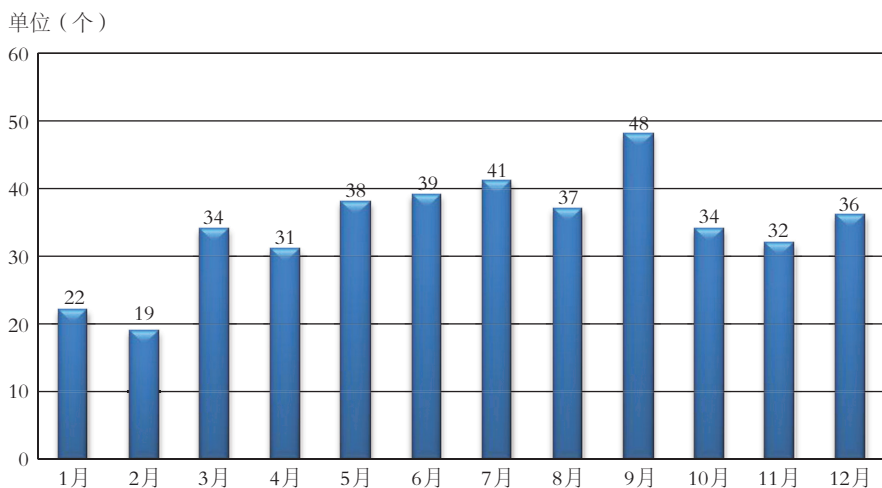


图4-12 2013年捕获新增移动互联网恶意程序数量月度统计（来源：恒安嘉新公司）

2013年各月捕获移动互联网恶意程序样本数量（MD5值不同）如图4-13所示，其中2月为全年最低值7786个，8月达到全年最高值15719个。

[13] 恒安嘉新公司即恒安嘉新（北京）科技有限公司，是CNCERT/CC国家级应急服务支撑单位。

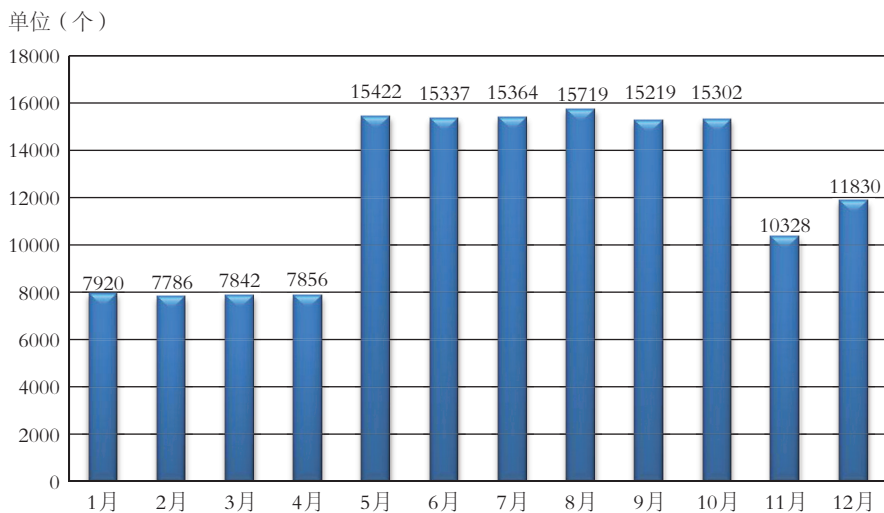


图4-13 2013年捕获移动互联网恶意程序样本数量月度统计（来源：恒安嘉新公司）

2008-2013年发现移动互联网恶意程序数量（按恶意程序名称统计）走势如图4-14所示。

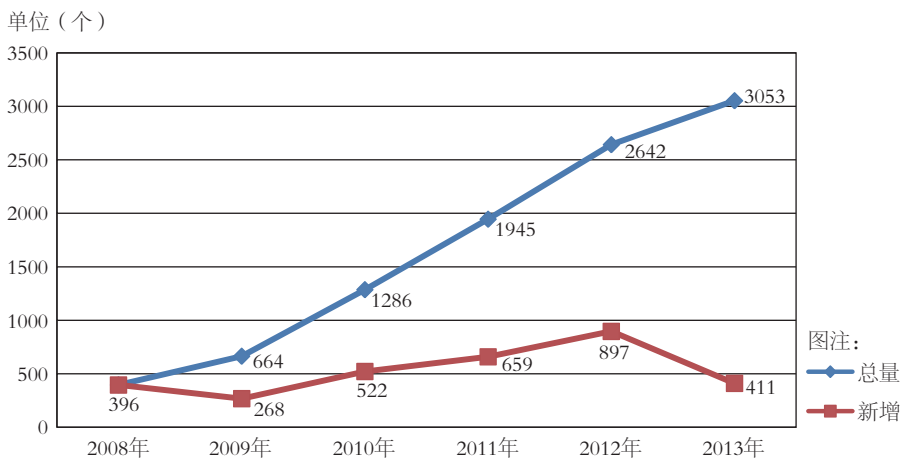


图4-14 2008-2013年捕获移动互联网恶意程序数量走势（来源：恒安嘉新公司）

2008-2013年捕获移动互联网恶意程序样本数量（MD5值不同）走势如图4-15所示。

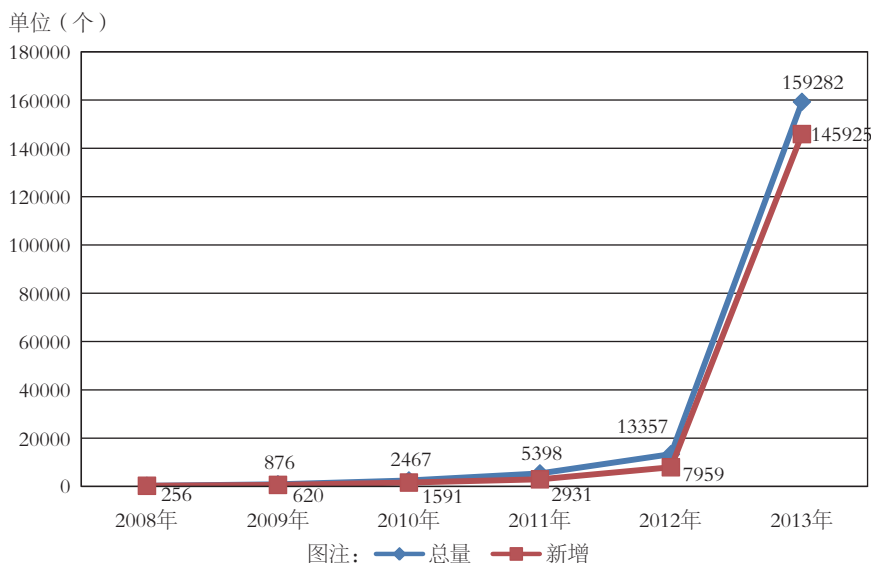


图4-15 2008-2013年捕获移动互联网恶意程序样本数量走势（来源：恒安嘉新公司）

截至2013年年底，累计发现移动互联网恶意程序下载链接37643条。其中，2013年共发现移动互联网恶意程序下载链接36603条，涉及209个手机应用商店，按恶意程序下载链接数排行前10的手机应用商店见表4-1。

表4-1 手机应用商店域名按恶意程序下载链接数排行TOP10（来源：恒安嘉新公司）

手机应用商店域名	恶意程序下载链接数
izhuti.com	88
paojiao.cn	20
liqucn.com	13
anzhi.com	10
gamedog.cn	8
ruan8.com	8
goapk.com	8
1000chi.com	8
gfan.com	6
hiapk.com	4

4.3.5 卡巴斯基公司移动互联网恶意程序捕获情况

根据卡巴斯基公司监测结果，截至2013年年底，累计发现移动互联网恶意程序（按



恶意程序名称统计)约11万个,其中2013年新发现约4.8万个。截至2013年年底,累计捕获移动互联网恶意程序样本(MD5值不同)约1801.8万个,其中2013年新捕获样本约701.5万个。按照《移动互联网恶意程序描述格式》的八大分类标准,2013年发现的移动互联网恶意程序分类统计数据为:恶意扣费6928330个;诱骗欺诈10478个;信息窃取9124个;资费消耗3012个;远程控制2401个;恶意传播2034个;流氓行为534个;系统破坏107个。

2013年各月捕获移动互联网恶意程序数量(按恶意程序名称统计)如图4-16所示,其中9月为全年最低值3263个,3月达到全年最高值5280个。

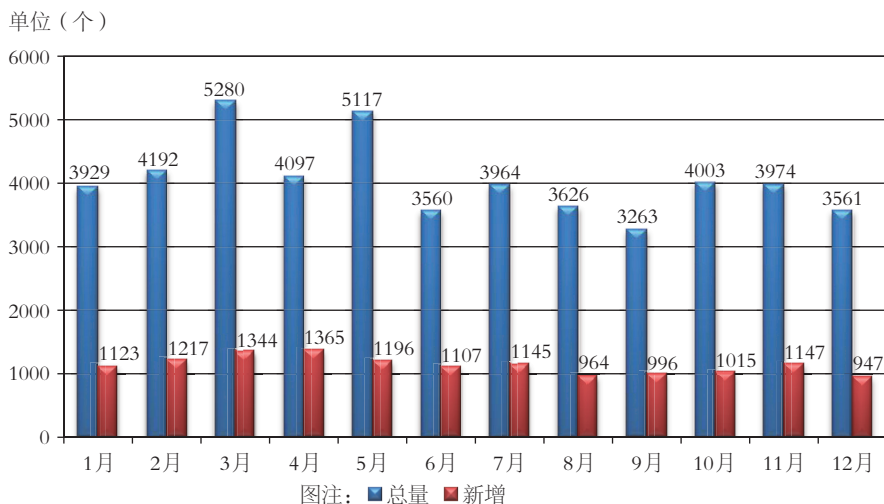


图4-16 2013年移动互联网恶意程序捕获月度统计(来源:卡巴斯基公司)

2013年各月捕获移动互联网恶意程序样本数量(MD5值不同)如图4-17所示,其中6月为全年最低值505660个,2月达到全年最高值1250644个。

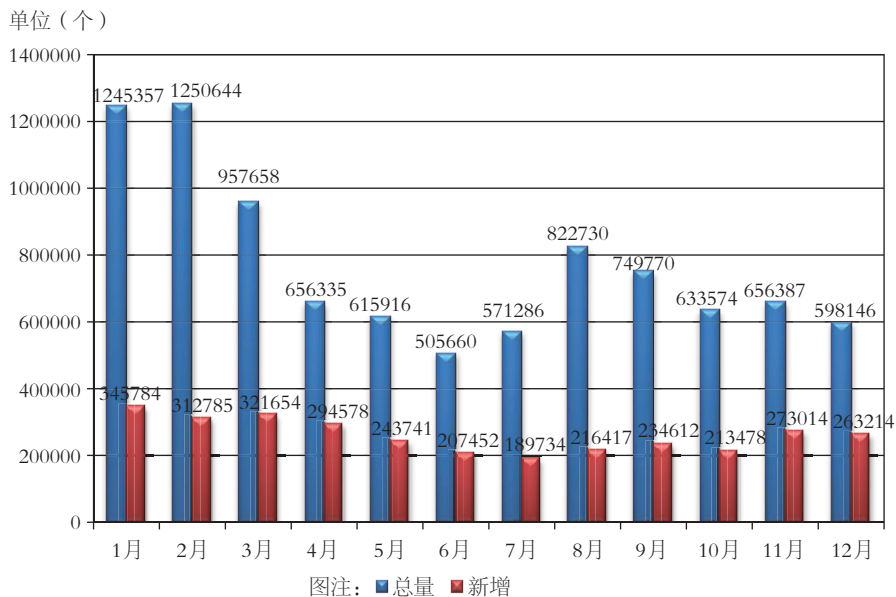


图4-17 2013年移动互联网恶意程序样本捕获月度统计（来源：卡巴斯基公司）

4.3.6 奇虎360公司移动互联网恶意程序捕获情况

根据奇虎360公司监测结果，截至2013年年底，累计捕获移动互联网恶意程序样本（MD5值不同）839998个，其中2013年新增捕获样本670393个。按照《移动互联网恶意程序描述格式》的八大分类标准，2013年新增发现的移动互联网恶意程序样本分类统计数据为：资费消耗461731个；信息窃取158202个；恶意扣费类45660个；诱骗欺诈2645个；流氓行为1162个；系统破坏526个；恶意传播257个；远程控制210个。

2013年各月捕获移动互联网恶意程序样本数量如图4-18所示，其中2月为全年最低值10698个，7月达到全年最高值198602个。

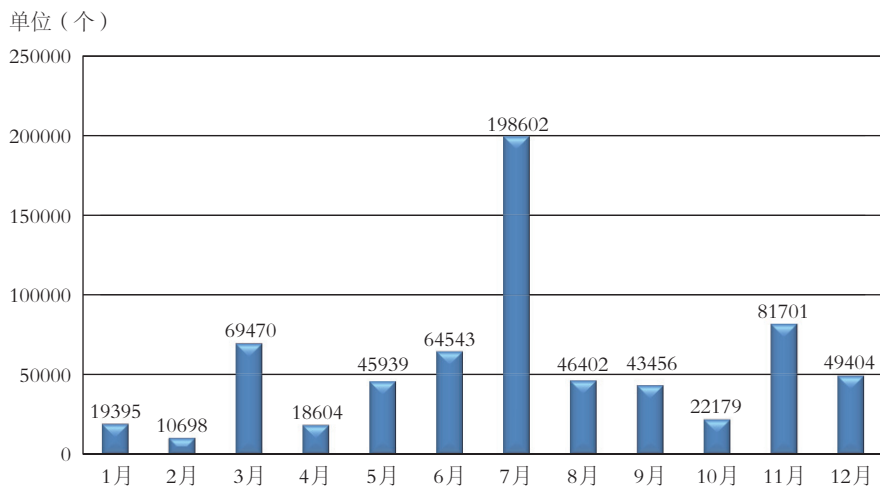


图4-18 2013年移动互联网恶意程序样本捕获月度统计（来源：奇虎360公司）

2010–2013年捕获的移动互联网恶意程序样本走势数量如图4-19所示。

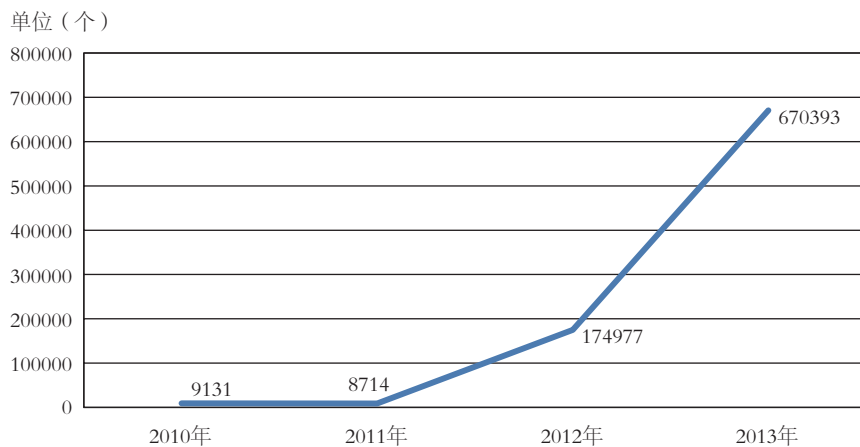


图4-19 2010–2013年移动互联网恶意程序样本数量走势（来源：奇虎360公司）

4.3.7 洋浦科技^[14]移动互联网恶意程序捕获情况

根据洋浦科技公司监测结果，截至2013年年底，累计发现移动互联网恶意程序（按恶意程序名称统计）30133个，其中2013年新发现28861个。截至2013年年底，累计捕获移动互联网恶意程序样本300495个（MD5值不同），其中2013年新捕获样本241567个。按照《移动互联网恶意程序描述格式》的八大分类标准，2013年发现的移动互联网恶意程序分类统计数据为：流氓行为136467个；远程控制29625个；恶意扣费24159个；信息窃取23832个；系统破坏16479个；资费消耗8204个；诱骗欺诈2675个；恶意传播126个。

2013年各月捕获移动互联网恶意程序数量（按恶意程序名称统计）如图4-20所示，其中2月为全年最低值385个，4月达到全年最高值4242个。

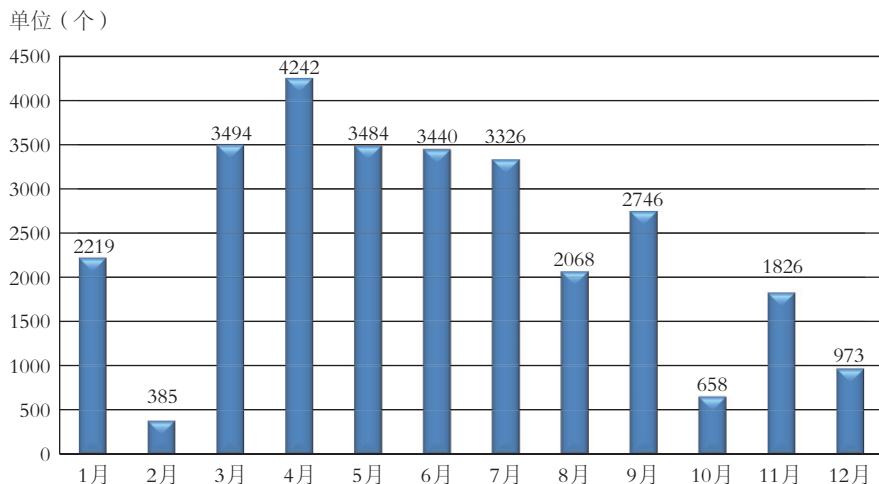


图4-20 2013年捕获移动互联网恶意程序数量月度统计（来源：洋浦科技）

2013年各月捕获移动互联网恶意程序样本数量（MD5值不同）如图4-21所示，其中2月为全年最低值1624个，9月达到全年最高值32392个。

[14] 洋浦科技公司即北京洋浦伟业科技发展有限公司。

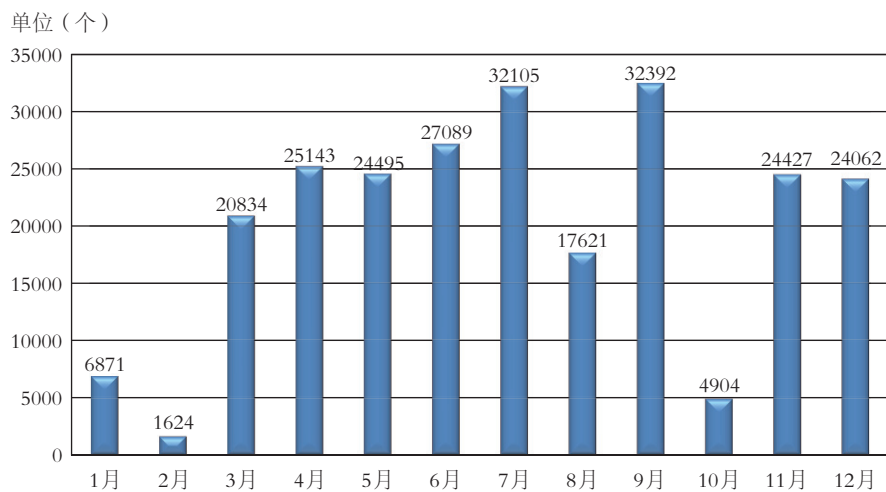


图4-21 2013年捕获移动互联网恶意程序样本数量月度统计（来源：洋浦科技）

网络安全监测情况

5.1 网页篡改情况

在众多的网络攻击方式中，网页篡改是比较浅层的攻击手段，而我国相对滞后的网站建设却使之成为攻击网站的主要手段之一。

依照攻击方式，网页篡改可以分成显式篡改和隐式篡改。通过显式网页篡改，黑客可炫耀自己的技术和技巧，或达到声明自己主张的目的；隐式篡改则一般是在被攻击网站的网页中植入暗链，这些暗链往往被链接到色情、诈骗等非法信息，可帮助黑客谋取非法经济利益。为了篡改网页，黑客一般需提前知晓网站的漏洞，提前在网页中植入后门，并最终获取网站的控制权。

2003年起，CNCERT/CC每日跟踪监测我国境内被篡改的网页情况，发现被篡改的网站后及时通知相关分中心或网站负责人进行协调解决，以争取在第一时间恢复网站，减少攻击事件带来的影响。此外，CNCERT/CC也会跟踪被植入后门的网页情况，及时对将发生的网页篡改行为进行预警。

5.1.1 我国境内网站被篡改总体情况

2013年，我国境内被篡改的网站数量为24034个，较2012年的16388个大幅增长46.7%。我国境内被篡改网站的月度统计情况如图5-1所示。2012年11月开始，CNCERT/CC加大了对我国境内网站被植入暗链情况的监测范围，导致2013年全年较2012年被篡改网站的总数有大幅度增长。



单位(个)

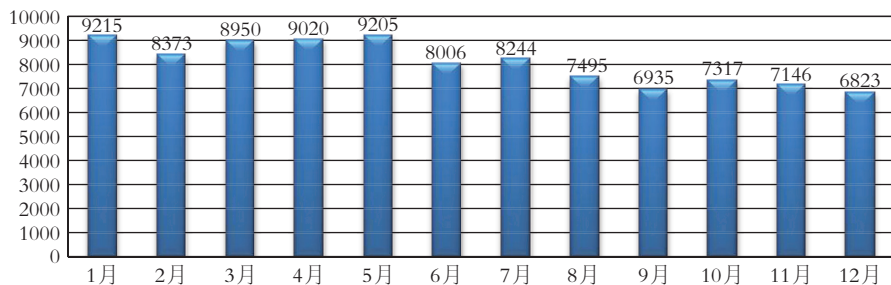


图5-1 2013年我国境内被篡改网站数量月度统计(来源: CNCERT/CC)

从域名类型来看,2013年我国境内被篡改网站中,代表商业机构(.COM)的网站最多,占67.2%,其次是政府类(.GOV)网站和网络组织类(.NET)网站,分别占10.1%和6.4%,非营利组织类(.ORG)网站和教育机构类(.EDU)网站分别占1.9%和0.4%。对比2012年,我国商业机构类网站被篡改情况有小幅度上升,从2012年的64.5%,上升至2013年的67.2%。2013年我国境内被篡改网站按域名类型分布情况如图5-2所示。

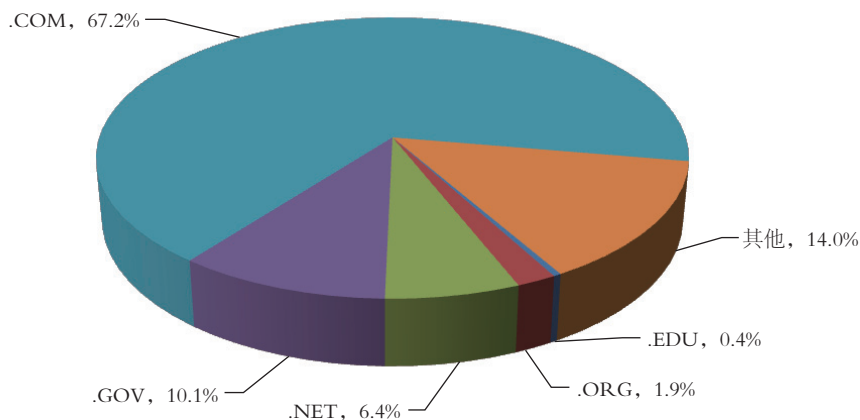


图5-2 2013年我国境内被篡改网站按域名类型分布(来源: CNCERT/CC)

如图5-3所示, 2013年我国境内被篡改网站数量按地域进行统计, 排名前10位的地区分别是北京市、江苏省、上海市、浙江省、广东省、福建省、河南省、四川省、山东省、安徽省。2013年的情况与2012年类似, 仅安徽省代替湖北省。以上地区均为我国互联网发展状况较好的地区, 互联网资源较为丰富, 总体上发生网页篡改的事件次数较多。

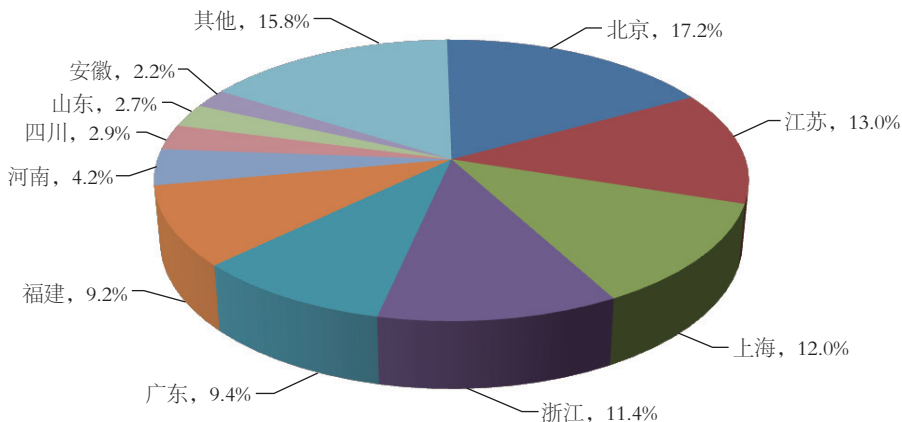


图5-3 2013年我国境内被篡改网站按地区分布 (来源: CNCERT/CC)

5.1.2 我国境内政府网站被篡改情况

近年来, 各级政府更加重视信息化建设, 许多政府机构都建立了自己的网站。然而目前政府网站还缺乏足够的防护措施, 已成为我国网络安全中最薄弱的一环。同时, 由于政府网站有着不可替代的权威性, 对它的攻击严重影响着我国的网络信息安全。

2013年, 我国境内政府网站被篡改数量为2430个, 较2012年的1802个大幅度增长34.9%, 占CNCERT/CC监测的政府网站列表总数的4.0%, 即平均每1000个政府网站中就有40个网站遭到了篡改。2013年我国境内政府网站被篡改数量和其占被篡改网站总数比例按月度统计如图5-4所示。

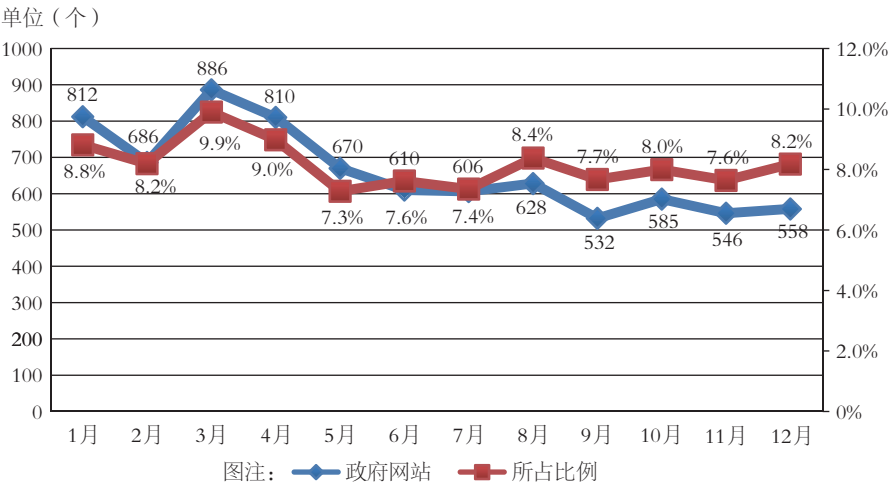


图5-4 2013年我国境内政府网站被篡改数量及所占比例月度统计
(来源：CNCERT/CC)

2013年，CNCERT/CC监测发现的部分被篡改的省市级政府网站见表5-1。2013年，我国省市级政府网站维护保障水平提升，未发现2012年间多个省市级网站被同时篡改的现象。另外，在我国被篡改的政府网站中，以植入暗链方式被攻击的网站占57%，对比我国被篡改的境内网站总数中以植入暗链方式被攻击的占41.8%的差异来看，境内政府网站更容易以被植入暗链的方式攻击。

表5-1 2013年CNCERT/CC监测发现被篡改的部分省市级政府网站

网站所属部门	被篡改后的URL	监测时间
安徽省交通厅	http://chaxun.ahjt.gov.cn/index.htm	2013/1/2
陕西省新闻出版局	http://www.sxxwcb.gov.cn	2013/1/21
四川省民政厅	http://www.scmz.gov.cn/images	2013/1/23
内蒙古自治区煤炭工业局官方网站	http://www.nmgmt.gov.cn	2013/1/24
北京平谷区组织部	http://zzb.bjpg.gov.cn/m3.htm	2013/1/30
天津出入境检验检疫信息网	http://tjciq.gov.cn	2013/1/31
湖北省知识产权局	http://www.hbipo.gov.cn/learner.htm	2013/2/17
广东法院网	http://www.gdcourts.gov.cn/gdcourt/front/index.jsp	2013/3/6
天津市发展改革委员会	http://www.tjztb.gov.cn/s.txt	2013/3/28

(续表)

网站所属部门	被篡改后的URL	监测时间
吉林省中医药管理局	http://www.jltcm.gov.cn	2013/4/24
中华人民共和国民政部中益老龄事业发展中心	http://zyac.mca.gov.cn/article/lxwm/	2013/5/7
湖南省发展和改革委员会网站	http://www.hnfgw.gov.cn/	2013/8/8
黑龙江省中医药管理局	http://www.hljtcn.gov.cn	2013/10/25
黑龙江省审计厅	http://www.hljaudit.gov.cn	2013/10/27

5.2 网页挂马情况

网页挂马是通过在网页中嵌入恶意程序或链接，致使用户计算机在访问该页面时被植入恶意程序，是黑客传播恶意程序的常用手段。通信行业、网络安全企业相关单位在监测网页挂马和恶意程序传播方面开展了大量工作，并与CNCERT/CC建立良好的协作关系。

5.2.1 挂马网站监测情况

图5-5至图5-7分别为奇虎360公司、网御星云公司^[15]、卡巴斯基公司监测发现的中国大陆地区挂马网站数量月度统计情况，可以看到2013年网页挂马活动整体呈现出下降的波动态势。随着政府主管部门和通信行业相关单位对恶意程序传播行为不断加强治理，实施网页挂马的成本逐渐提高，其生存空间逐渐缩小。

[15] 网御星云公司即北京网御星云信息技术有限公司，是通信行业互联网网络安全信息通报工作单位。

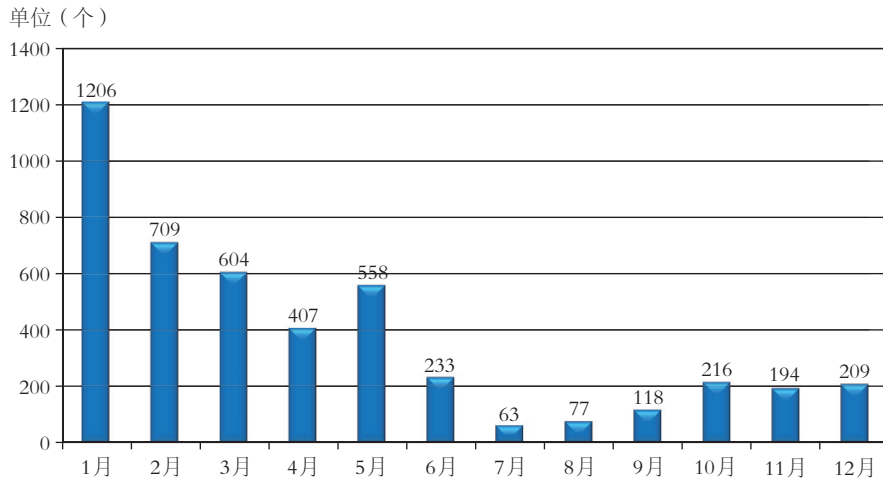


图5-5 2013年中国大陆挂马网站数量月度统计（来源：奇虎360公司）

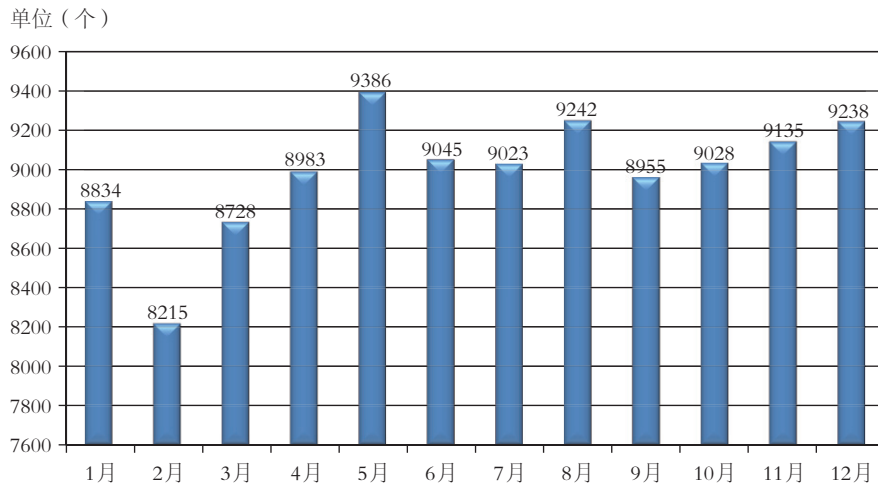


图5-6 2013年中国大陆地区挂马网站数量月度统计（来源：网御星云）

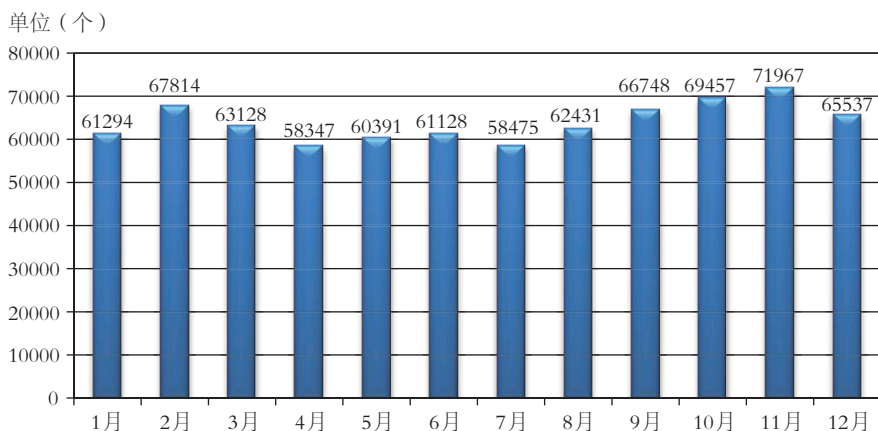


图5-7 2013年中国大陆地区挂马网站数量月度统计（来源：卡巴斯基公司）

此外，根据奇虎360公司、网御星云公司、卡巴斯基公司的监测结果（各公司监测节点分布和检测方式有所不同），中国大陆地区挂马网站较多地集中在浙江、北京、江苏、广东、上海、四川、辽宁、河南、湖北、福建、湖南、吉林、山东等省市，如图5-8至图5-10所示。

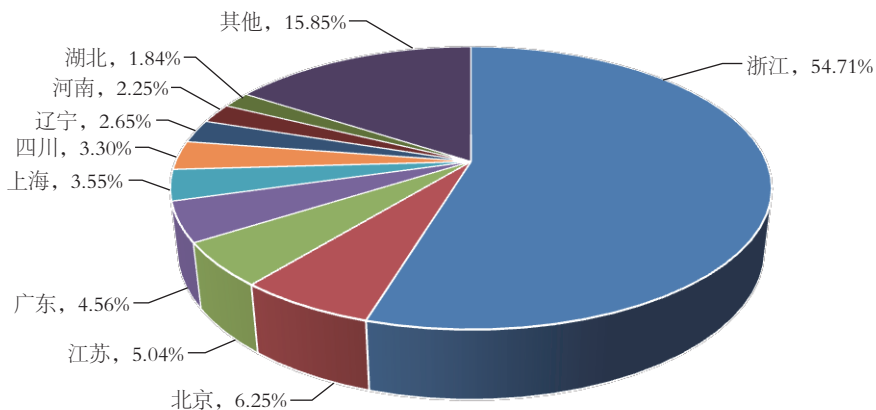


图5-8 2013年中国大陆地区挂马网站按地区分布（来源：奇虎360公司）

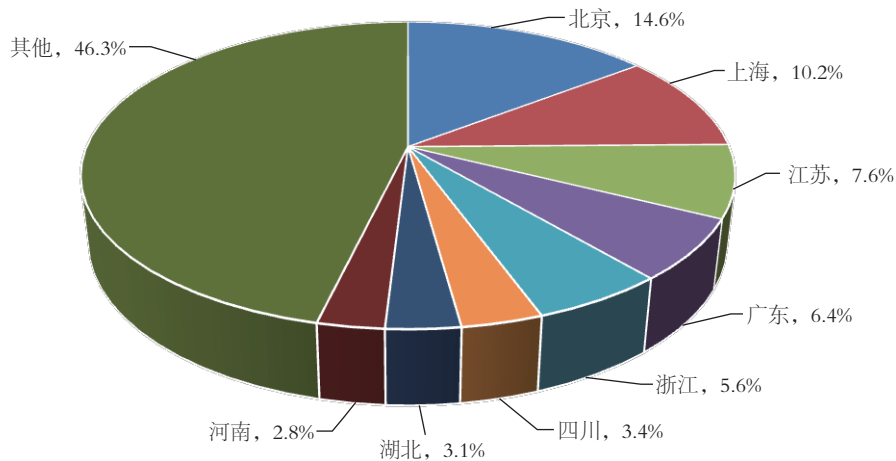


图5-9 2013年中国大陆地区挂马网站按地区分布（来源：网御星云）

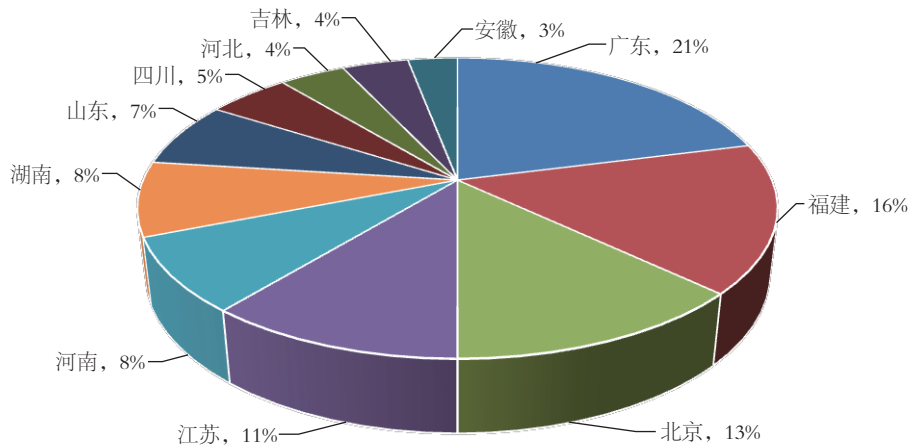


图5-10 2013年中国大陆地区挂马网站按地区分布（来源：卡巴斯基公司）

5.2.2 恶意域名监测情况

挂马网站数量反映了黑客对网站的入侵和对用户可能带来的威胁情况，而恶意域

名的活跃情况反映了黑客实施网页挂马攻击的频繁度和能力。奇虎360公司监测结果显示（见表5-2），黑客使用大量动态域名来传播恶意程序，且大部分为境外注册域名，加大了监测处置的难度。

表5-2 用于网页挂马的恶意域名TOP10（来源：奇虎360公司）

挂马网站域名	相关挂马子域名数（个）	部分挂马子域名举例
snda5188.com	1683	www.snda5188.com:88 msfvt.snda5188.com mvfvttu.snda5188.com
jkub.com	147	gy.jkub.com dferfdrf12jkub.com dcfeffr567.jkub.com
findhere.org	110	360cd.findhere.org cvsv72v.findhere.org klpm-.findhere.org
12e.asia	5	zx.12e.asia tl.12e.asia xy.12e.asia
12a.asia	3	wd.12a.asia 9yin.12a.asia xy.12a.asia
0412game.com	3	qq.0412game.com mm.0412game.com 2012.0412game.com
100ecg.com	3	xy.100ecg.com wd.100ecg.com zx.100ecg.com
230x.net	3	dd.230x.net 1b.230x.net c.230x.net
1dd.asia	2	a.1dd.asia s.1dd.asia
8lungu.com	2	test.8lungu.com 2012.8lungu.com

5.2.3 网页挂马攻击常见步骤

目前，黑客在互联网上主要以两种方式快速传播恶意代码，一是通过下载网站捆



绑带病毒软件，二是通过网页挂马。近年来，网页挂马随漏洞技术、网页代码变形、免杀等技术的不断发展呈现出许多新的特点，这也为防治网页挂马以及清除放马网站提出新的挑战。表5-3为2013年网页挂马事件中极具代表性的案例。

表5-3 典型网页挂马案例（来源：奇虎360公司）

步骤	说明
第一步	利用网站漏洞取得相关权限，嵌入恶意跳转链接 [wide]http://www.8lungu.com（被挂马网站） [script]2012.8lungu.com（恶意跳转链接）
第二步	通过恶意跳转链接，再次跳转至集成挂马页面 [iframe] http://2012.8lungu.com:83/dn/dn.html?house.longhoo.net (暴雷漏洞)
第三步	漏洞触发条件执行成功，取得用户主机权限，自动下载带有远程控制或窃取信息等功能的恶意代码 http://xz.8lungu.com:70/dn/dn.exe
第四步	在用户主机上执行下载的恶意代码

5.3 网页仿冒情况

网页仿冒俗称网络钓鱼（Phishing），是将社会工程学欺骗原理与网络技术相结合的典型应用。2013年，CNCERT/CC共监测发现仿冒境内网站的仿冒页面30199个，涉及域名18011个，这些域名分别解析到境内外4240个IP地址，平均每个IP地址承载4.2个仿冒网站域名。在这4240个IP地址中，有90.2%位于境外，美国（53.4%）、中国香港（16.6%）和泰国（1.4%）数量居前三位，分别承载12573个、4500个和934个针对我国境内网站的钓鱼页面，其分布比例如图5-11和图5-12所示。

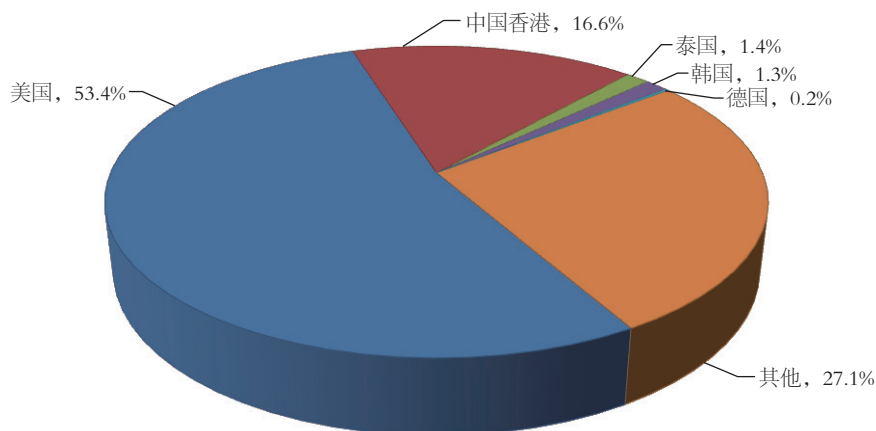


图5-11 2013年仿冒我国境内网站的境外IP地址按国家和地区分布（来源：CNCERT/CC）

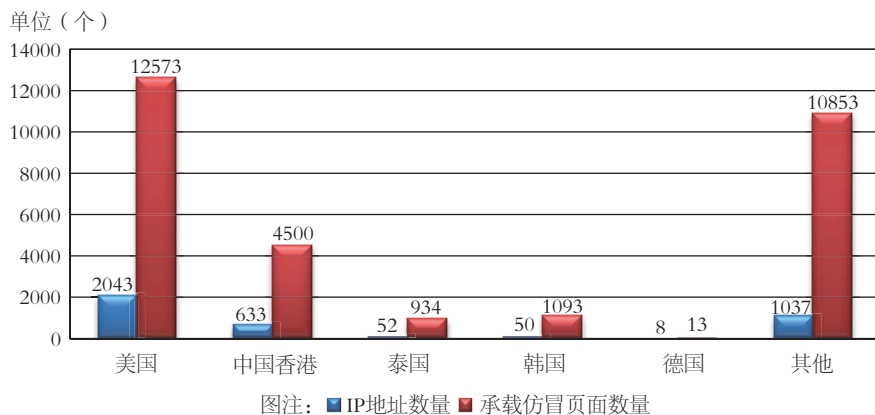


图5-12 2013年仿冒我国境内网站的境外IP地址及其承载的仿冒页面数量按国家和地区分布TOP5（来源：CNCERT/CC）

从钓鱼站点使用域名的顶级域分布来看，以.COM最多，占51.1%，其次是.TK和.NET，分别占16.8%和8.3%。2013年，CNCERT/CC监测发现的钓鱼站点所用域名按顶级域分布如图5-13所示。

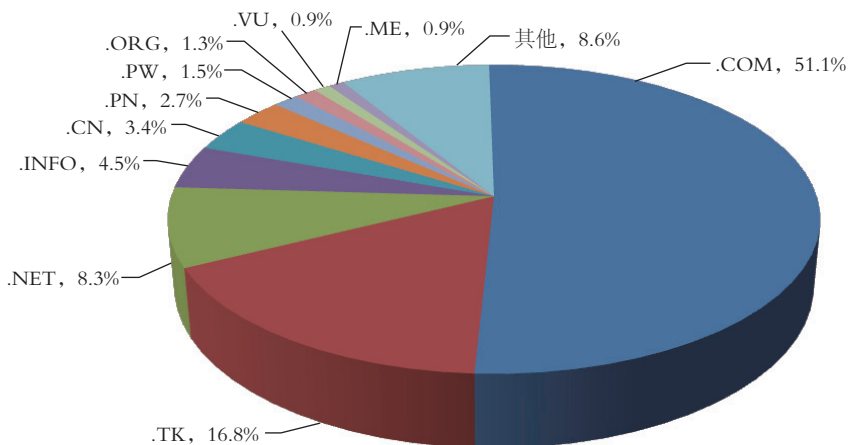


图5-13 2013年CNCERT/CC监测发现的钓鱼站点所用域名按顶级域分布
(来源: CNCERT/CC)

5.4 网站后门情况

网站后门是黑客成功入侵网站服务器后留下的后门程序。通过在网站的特定目录中上传远程控制页面, 黑客可以暗中对网站服务器进行远程控制, 上传、查看、修改、删除网站服务器上的文件, 读取并修改网站数据库的数据, 甚至可以直接在网站服务器上运行系统命令。

2013年CNCERT/CC共监测到境内76160个网站被植入网站后门, 其中政府网站2425个。我国境内被植入后门网站数量月度统计情况如图5-14所示。

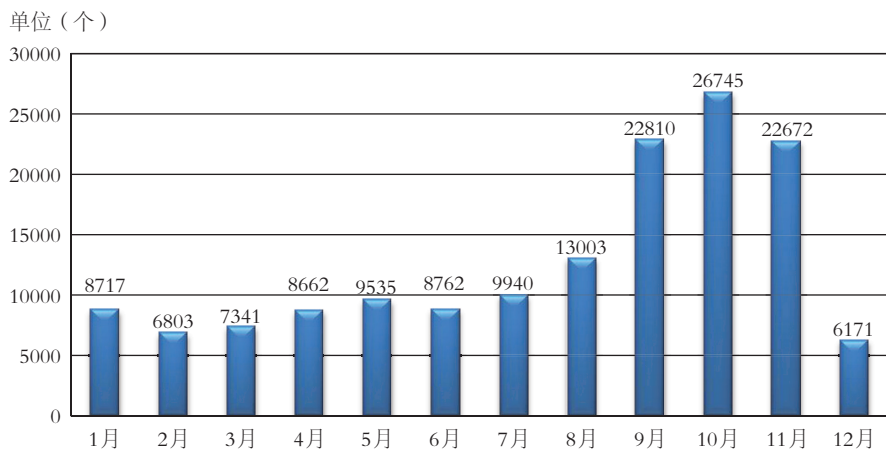


图5-14 2013年我国境内被植入后门网站数量月度统计（来源：CNCERT/CC）

从域名类型来看，2013年我国境内被植入后门的网站中，代表商业机构的网站（.COM）最多，占58.3%，其次是网络组织类（.NET）和政府类（.GOV）网站，分别占7.0%和3.2%。2013年我国境内被植入后门的网站数量按域名类型分布情况如图5-15所示。

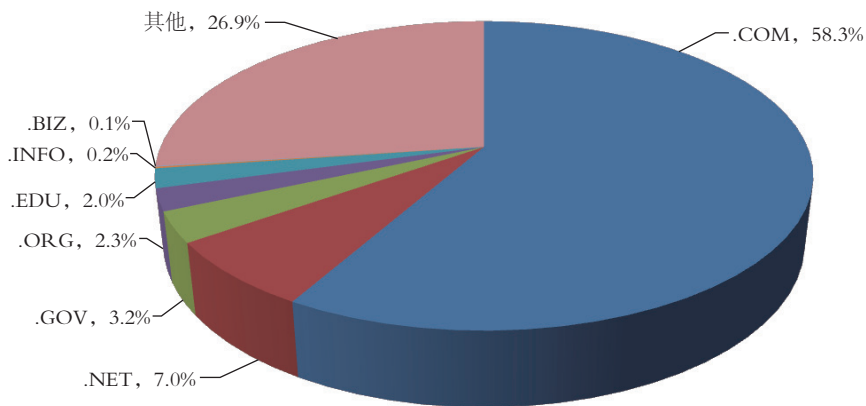


图5-15 2013年我国境内被植入后门网站数量按域名类型分布（来源：CNCERT/CC）



如图5-16所示，2013年我国境内被植入后门的网站数量按地域进行统计，排名前10位的地区分别是北京市、广东省、浙江省、江苏省、上海市、河南省、福建省、四川省、湖北省、山东省。

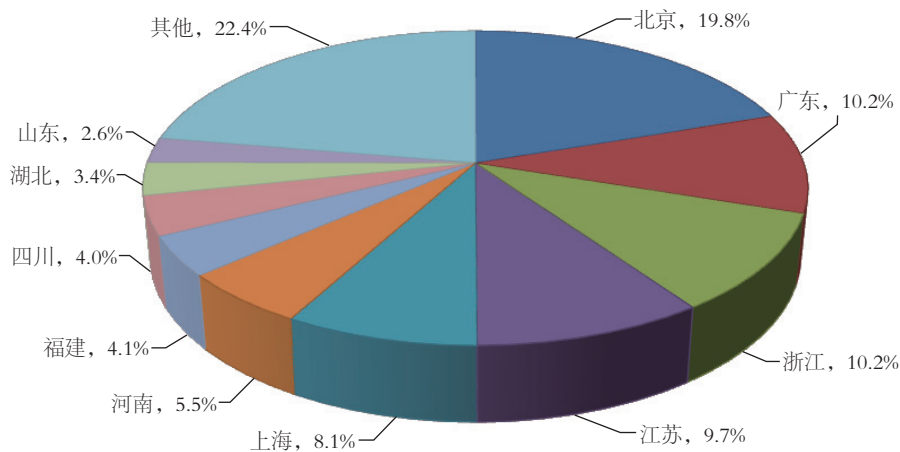


图5-16 2013年我国境内被植入后门网站数量按地区分布（来源：CNCERT/CC）

向我国境内网站实施植入后门攻击的IP地址中，有30824个位于境外，主要位于美国（20.2%）、印度尼西亚（11.4%）和韩国（6.5%）等国家和地区，如图5-17所示。

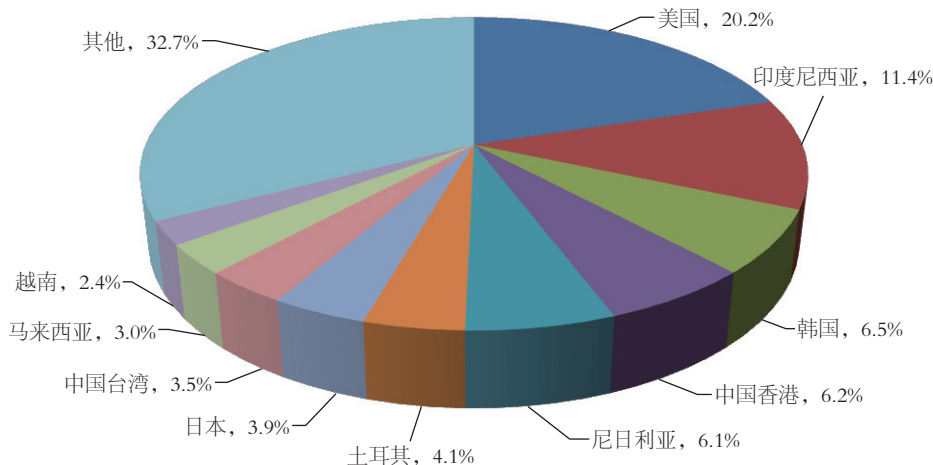


图5-17 2013年向我国境内网站植入后门的境外IP地址按国家和地区分布
(来源: CNCERT/CC)

其中，位于美国的6215个IP地址共向我国境内15349个网站植入后门程序，侵入网站数量居首位，其次是位于中国香港和韩国的IP地址，分别向我国境内13116个和7052个网站植入后门程序，如图5-18所示。

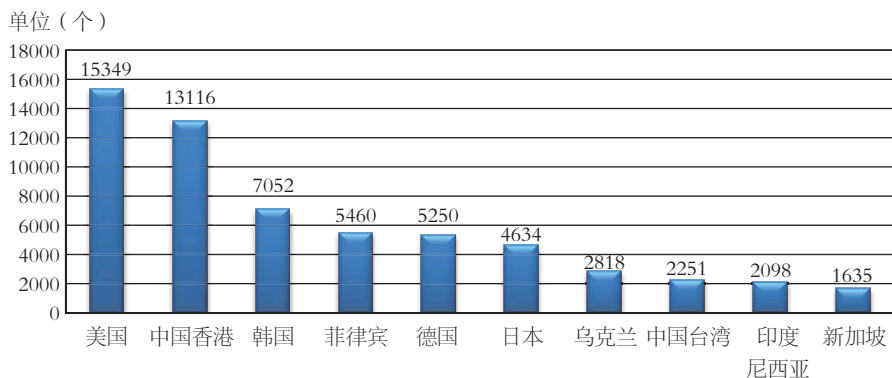


图5-18 2013年境外通过植入后门控制我国境内网站数量TOP10
(来源: CNCERT/CC)



安全漏洞预警与处置

CNCERT/CC高度重视对安全威胁信息的预警通报工作。由于大部分严重的网络安全威胁都是由信息系统所存在的安全漏洞诱发的，所以及时发现和处理漏洞是网络安全防范工作的重中之重。

6.1 CNVD漏洞收录情况

自2009年成立以来，CNVD共收集整理漏洞信息59822个（含补录漏洞10112个）。其中，2013年新增漏洞7854个，包括高危漏洞2607个（占33.2%）、中危漏洞4467个（占56.9%）、低危漏洞780个（占9.9%）。各级别比例分布与月度数量统计如图6-1、图6-2所示。在所收录的上述漏洞中，可用于实施远程网络攻击的漏洞有6962个，可用于实施本地攻击的漏洞有892个。

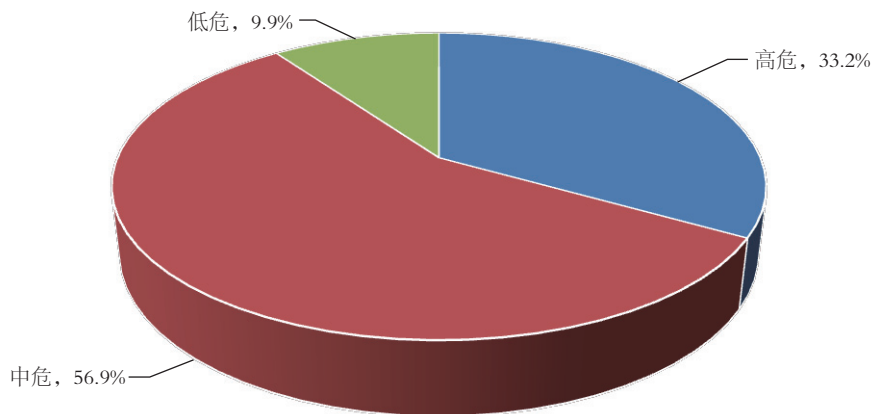


图6-1 2013年CNVD收录漏洞数量按威胁级别统计（来源：CNVD）

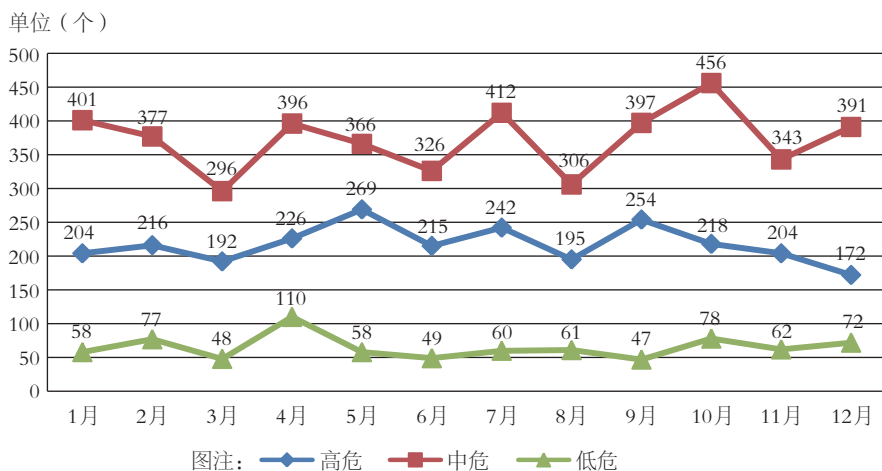


图6-2 2013年CNVD收录漏洞威胁级别数量按月度统计（来源：CNVD）

2013年，CNVD共收集、整理了2607个高危漏洞，涵盖Microsoft、IBM、Apple、WordPress、Adobe、Cisco、Mozilla、Novell、Google、Oracle等厂商的产品。各厂商产品中高危漏洞的分布情况如图6-3所示，可以看出，涉及Oracle产品的高危漏洞最多，占全部高危漏洞的6.9%。

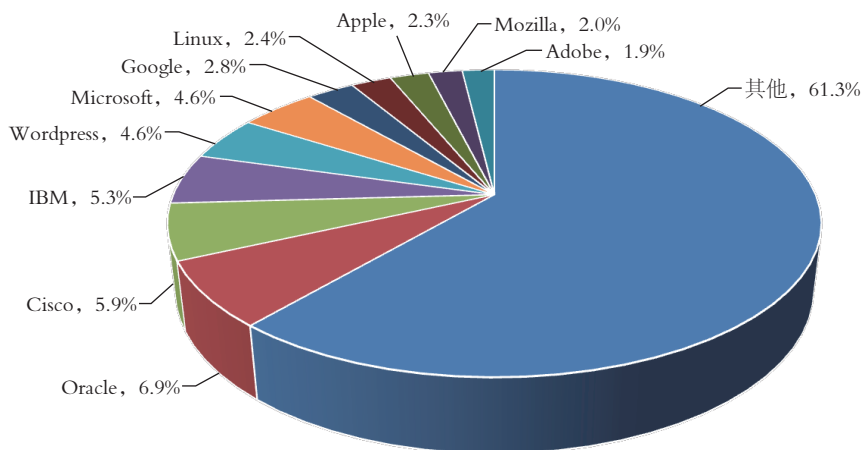


图6-3 2013年CNVD收录高危漏洞按厂商分布（来源：CNVD）



根据影响对象的类型，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）。如图6-4所示，在CNVD 2013年度收集整理的漏洞信息中，操作系统漏洞占7.4%，应用程序漏洞占64.8%，Web应用漏洞占18.1%，数据库漏洞占1.7%，网络设备漏洞占6.4%，安全产品漏洞占1.6%。

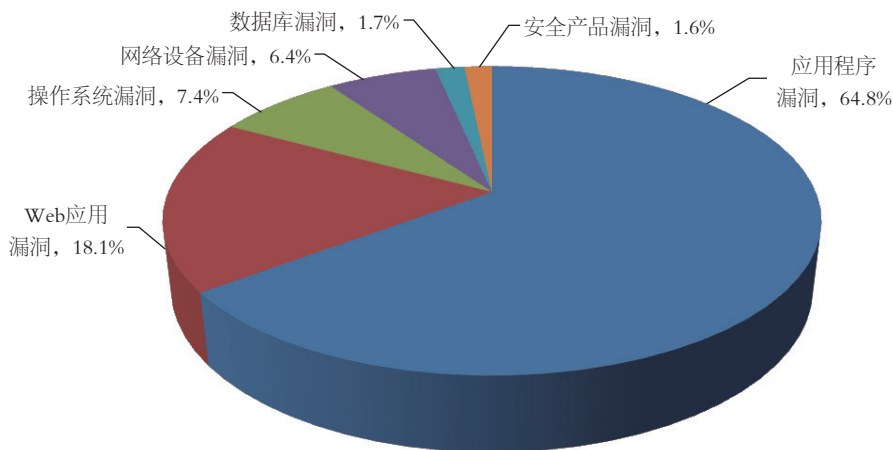


图6-4 2013年CNVD收录漏洞按影响对象类型分类统计（来源：CNVD）

CNVD对收录的漏洞进行验证，并掌握一些仅在CNVD成员单位中知晓、未通过互联网公开披露的攻击代码。CNVD通过验证和测试攻击代码，对漏洞带来的危害进行较为全面的分析研判。2013年，CNVD共进行1246次验证，其中比较重要的包括：eYou电子邮件系统网关远程代码执行漏洞，We7CMS文件存在多个文件上传漏洞，多个网站Apache Struts远程命令执行漏洞，Zimbra邮件系统存在文件包含高危漏洞，Nginx空格解析安全绕过漏洞，多款D-Link路由器产品存在后门漏洞，Microsoft IE浏览器存在远程代码执行漏洞，Android系统存在签名验证绕过漏洞，快客邮件系统（QuarkMail）存在远程代码执行漏洞，TP-Link部分路由器存在后门漏洞，UPnP（即插即用）设备相关应用协议存在多个漏洞，Java7存在远程代码执行零日漏洞，通达OA 2011-2013存在多处远程代码执行漏洞，多个网站JBoss权限绕过/文件上传漏

洞，多家单位所属深信服SSLVPN设备存在应用软件漏洞，国内外多家VPN设备文件上传/文件包含漏洞，Foosun（风讯）CMS SQL注入漏洞，metinfo企业网站管理系统存在SQL注入漏洞等。

漏洞中较危险的是零日漏洞，一旦针对这些漏洞的攻击代码在补丁发布之前被公开或被不法分子知晓，就可能被用来发动大规模网络攻击。2013年CNVD共收录了2011个零日漏洞，主要涉及服务器系统、操作系统、数据库系统以及应用软件等。

2013年，CNVD共收录漏洞补丁5843个，并为大部分漏洞提供了可参考的解决方案，提醒相关用户注意做好系统加固和安全防范工作。CNVD发布的漏洞补丁数量按月度统计如图6-5所示。

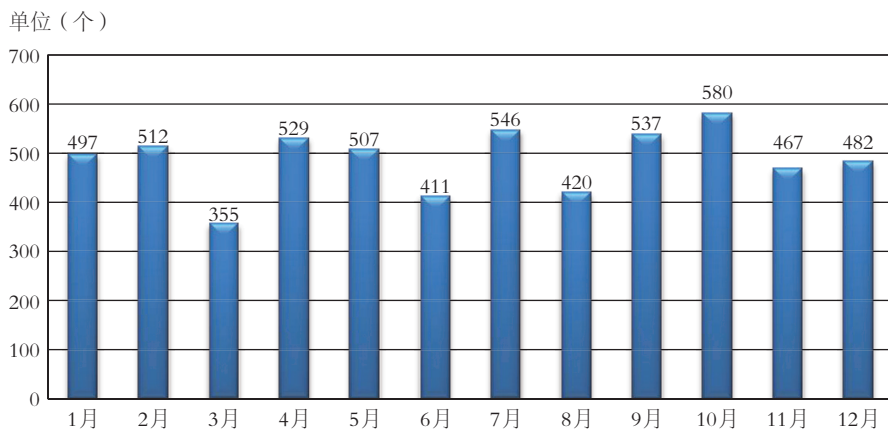


图6-5 2013年CNVD收录的漏洞补丁数量月度统计（来源：CNVD）

2013年，CNVD各成员单位积极报送安全漏洞信息，全年共计报送漏洞19639个（未去重），为CNVD的发展做出积极贡献。各成员单位报送的漏洞数量如图6-6所示。

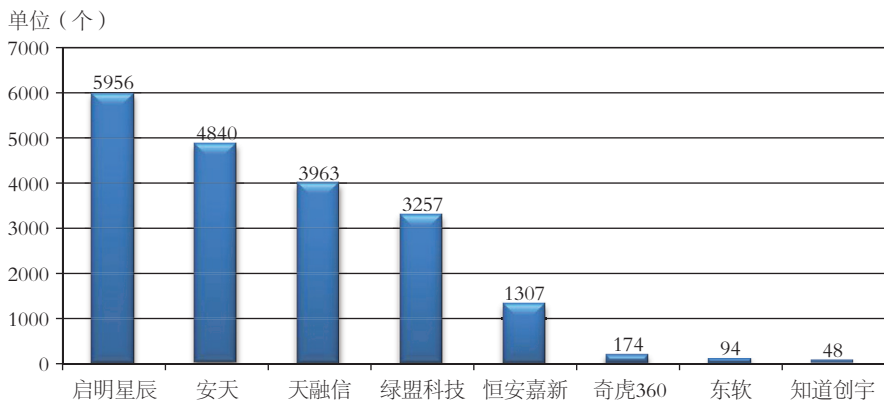


图6-6 2013年CNVD各成员单位报送漏洞数量统计(来源:CNVD)

6.2 高危漏洞典型案例

(1) Zimbra邮件系统存在文件包含高危漏洞

2013年12月,CNVD收录了关于Zimbra邮件系统存在的一个文件包含高危漏洞(收录编号:CNVD-2013-14944)。Zimbra是一款企业级邮件系统软件,在国内外应用较为广泛。由于页面中存在文件包含漏洞,攻击者可以利用漏洞绕过限制读取未经授权的主机操作系统文件或网站其他目录配置文件,如Zimbar默认配置文件/opt/zimbra/conf/localconfig.xml。

测试结果表明,从上述配置文件中可获得Zimbra用户名和LDAP口令。若Zimbra服务器集成开放SOAP服务和7071后台管理端口,则可通过SOAP服务直接添加新的管理权限用户,取得邮件服务器后台控制权。

12月6日,exploit-db.com网站披露了攻击代码。根据CNCERT/CC和上海交通大学网络信息中心的监测情况,从当天下午开始,出现了大量利用该漏洞对境内政府和高校用户发起的攻击。

CNVD对互联网上使用Zimbra的邮件服务器进行了检测。截至12月13日9时,共

检测发现互联网上有1814个IP地址主机为Zimbra邮件服务器。按国家和地区统计，IP地址数量位于前5位的是巴西（252个）、美国（233个）、中国大陆（181个）、法国（148个）和中国香港（105个）。此外，根据抽样测试结果，约有50.0%的Zimbra邮件服务器存在所述高危漏洞。

（2）Nginx空格解析安全绕过漏洞

Nginx是一款轻量级的Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。2013年11月，Nginx被披露存在空格解析安全绕过漏洞。技术成因是由于Nginx对HTTP协议解析时，库文件ngx_http_parse.c存在字符串回溯的设计缺陷。攻击者通过构造一些包含未经过转义的空格字符的URL，有可能绕过网站服务器访问权限，执行读取、新增页面操作。CNVD后续分析认为，该漏洞使用条件存在一定的限制，与管理员设置网站路径与目录名称相关。此外，若管理员在服务器端做好URL转义处理，也可以较好地防范向网站服务器植入网页后门（WebShell）的攻击请求。

CNVD对漏洞的综合评级为“中危”。目前受影响的版本为Nginx 0.8.41-1.5.6。经CNVD评估，目前尚未构成利用漏洞发起大规模网站攻击的条件。

（3）多款D-Link路由器产品存在后门漏洞

2013年10月，CNVD收录了友讯（D-Link）多款路由器产品存在的后门漏洞（收录编号：CNVD-2013-13777）。D-Link系列路由器是友讯集团推出的宽带路由器产品。根据漏洞研究者提交的情况，D-Link部分路由器使用的固件版本中存在一个人为设置的后门漏洞，攻击者通过修改User-Agent值为xmlset_roodkcableoj28840ybtide即可绕过路由器Web认证机制取得后台管理权限。取得后台管理权限后攻击者可以通过升级固件的方式植入后门，取得路由器的完全控制权。

CNVD对漏洞的综合评级为“高危”。根据目前安全研究者及相关组织的测试结果，受影响的D-Link路由器固件版本涉及DIR-100、DI-524、DI-524UP、DI-604S、DI-604UP、DI-604+、TM-G5240、TM-G5240、BRL-04R、BRL-04UR、BRL-04CW、BRL-04FWU等。上述固件版本对应的路由器产品在国内外企业和个人用户中应用极为广泛。

CNVD已组织开展对漏洞风险的情况监测。至2013年10月24日，共检测发现对应



有62000多个IP地址采用D-Link网络设备产品。根据固件型号匹配,研判受漏洞影响的D-Link路由器设备共对应12000多个IP地址,其中位于中国大陆境内的有102个IP地址。较少一部分IP地址对应的设备由于自身NAT防护策略不够完善,可通过互联网进行渗透。

(4) Microsoft IE浏览器存在远程代码执行0day漏洞

2013年9月18日,CNVD收录Microsoft IE浏览器被披露的一个远程代码执行Oday漏洞(漏洞编号:CNVD-2013-13095)。Microsoft IE是微软公司推出的一款网页浏览器。IE的MSHTML.DLL组件存在一个远程代码执行漏洞。使用IE访问已经被删除或未正确分配的内存对象,会触发此漏洞,导致内存破坏,从而以当前运行环境用户权限执行任意指令(包括操作系统指令)。远程攻击者可能利用此漏洞通过诱使用户访问恶意网页,发起大规模挂马攻击,窃取用户信息或组建大规模僵尸网络。

CNVD对该漏洞的评级为“高危”。该漏洞影响范围较广,从IE6到IE11的所有版本均受到漏洞影响。微软公司的安全公告称,已经发现有攻击者在利用此漏洞攻击IE8和IE9用户。

(5) Apache Struts2远程命令执行漏洞和开放重定向漏洞

2013年7月,Apache Struts被披露存在一个远程命令执行漏洞和一个开放重定向漏洞(编号:CNVD-2013-09777,对应CVE-2013-2251;CNVD-2013-09784,对应CVE-2013-2248)。Struts2是第二代基于Model-View-Controller(MVC)模型的Java企业级Web应用框架。它是WebWork和Struts社区合并后的产物。

Apache Struts远程命令执行漏洞:由于Apache Struts2的action:、redirect:和redirectAction:前缀参数在实现其功能的过程中使用OGNL表达式,并将用户通过URL提交的内容拼接入OGNL表达式中,从而造成攻击者可以通过构造恶意URL来执行任意Java代码,进而可执行任意命令。

Apache Struts开放重定向漏洞:Apache Struts2 DefaultActionMapper在处理短路径重定向参数前缀redirect:或redirectAction:时存在开放重定向漏洞,允许远程攻击者利用漏洞操作redirect:或redirectAction:后的信息,重定向URL到任意位置。

CNVD对上述两个漏洞的评级为“高危”,由于redirect:和redirectAction:此两项前缀为Struts默认开启功能,因此Apache Struts2.3.15.1以下版本受到漏洞影响。该漏洞与

在2012年对我国境内政府和重要信息系统部门、企事业单位网站造成严重威胁的漏洞（编号：CNVD-2013-05924，对应CVE-2013-1966）相比，技术评级相同且受影响版本更多。

（6）Android系统存在签名验证绕过高危漏洞

2013年7月，CNVD收录了Android操作系统存在一个签名绕过的高危漏洞（编号：CNVD-2013-08957）。Android操作系统对应用程序安装文件（APK文件）采用一套数字签名校验机制来确认安装文件的有效性和完整性，用于防范应用程序的篡改和伪造。根据测试情况，该套校验机制存在不完全校验设计缺陷，对应用程序安装包内相同文件名的多个文件仅执行一次数字签名验证，验证成功后继续执行后续文件安装操作。攻击者可以精心构造同名恶意代码文件，使得应用程序既可通过Android系统的验证又可将恶意代码文件在安装过程中替换原有正常文件。

CNVD对该漏洞的综合评级为“高危”。受该漏洞影响的Android系统版本包括Android1.6至Android4.2.2之间相关版本。CNCERT/CC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。

（7）JBoss网站蠕虫利用漏洞再次大规模爆发

2013年2月，CNCERT/CC抽样监测发现，JBoss网站蠕虫在继2012年第三季度大规模爆发后，2月26日凌晨1:50左右再次出现大规模的攻击情况。抽样检测结果显示，从2月26日1:50左右开始，JBoss网站蠕虫再次活跃，仅截止到27日12:00已感染网站服务器203个，其中境内网站58个。这些被JBoss网站蠕虫成功入侵的服务器，还会自动扫描其他网站服务器，利用JBoss漏洞对之进行攻击从而传播自身。截至27日12:00，被扫描攻击的网站数量高达90.7万个，其中境内网站有35.7万，涉及大量政府网站、金融行业网站、新闻类网站及科研院所网站等重要网站。

JBoss网站蠕虫主要攻击存在“JBoss企业应用平台JMX控制台安全绕过漏洞”（编号：CNVD-2010-00821）的网站服务器，并通过服务器开放的JMXInvokeServlet服务，在网站上植入JSP类型的网站后门文件以及相关恶意程序，常见后门文件有：zecmd.jsp、idssvc.jsp、iesvc.jsp、wstats.jsp、invoker.jsp。由于感染JBoss网站蠕虫的都是



网站服务器，而并非普通的用户个人计算机，且受感染的大量网站能够形成一个受到黑客远程集中控制的僵尸网络，所以JBoss网站蠕虫危害十分严重，需引起高度重视。

(8) 快客邮件系统存在远程代码执行高危漏洞

2013年3月，CNVD收录了快客邮件系统存在的一个远程代码执行漏洞（CNVD编号：CNVD-2013-02240）。快客邮件系统是北京雄智伟业有限公司开发的邮件系统软件。根据CNVD测试结果，相关版本的快客电邮产品采用CGI脚本，存在一处远程代码执行漏洞。攻击者可利用漏洞直接发起恶意URL请求，远程执行操作系统指令。通过当前邮件服务器运行用户已有权限，攻击者可逐步渗透并控制邮件服务器主机操作系统。该产品广泛应用于我国政府和重要信息系统部门以及军队、电信、新闻、教育机构和科研院所等多个领域。

(9) Java7存在远程代码执行零日漏洞

2013年1月，CNVD收录了Java7存在的一个远程代码执行零日漏洞（CNVD编号：CNVD-2013-00216）。Oracle Java7（1.7、1.7.0）是Oracle公司发布的、为Java应用程序提供运行环境的产品，相关产品包括：Java SE 7、JDK7、JRE7，并支持当前主流浏览器插件扩展。由于Java7对代码执行权限机制存在处理异常，一些未经信任的Java程序通过调用setSecurityManager（）函数可以实现权限提升，进而执行任意代码。攻击者通常利用漏洞构建挂马页面，诱使用户解析，在用户主机上执行木马程序，取得用户主机操作系统的控制权。

CNVD对该漏洞的综合评级为“高危”。受影响的Oracle Java7（1.7、1.7.0）产品包括Java 7 update 10之前的版本，并且集成Java7扩展插件的软件产品也会受到影响，如当前主流的网页浏览器软件。互联网上已经出现针对该漏洞的网页挂马和恶意邮件攻击。

6.3 CNVD行业漏洞库

2013年7月，CNVD对现有漏洞进一步深化建设，建立起基于重点行业的子漏洞库，目前涉及的行业包括电信、移动互联网、工业控制系统和电子政务。面向的重

点行业客户包括政府部门、基础电信运营商、工控行业客户等，提供量身定制的漏洞信息发布服务，从而提高重点行业客户的安全事件预警、响应和处理能力。

CNVD行业漏洞通过资产和关键字匹配。目前行业漏洞库资产总数为：电信1512类，移动互联网135类，工控系统174类，电子政务95类。关键词总数为：电信84个，移动互联网42个，工控系统59个，电子政务11个。

2011年至今，CNVD共收录移动互联网行业漏洞603个，电信行业漏洞1802个，工控行业漏洞442个，电子政务漏洞592个。近3年各行业漏洞统计数如图6-7所示。

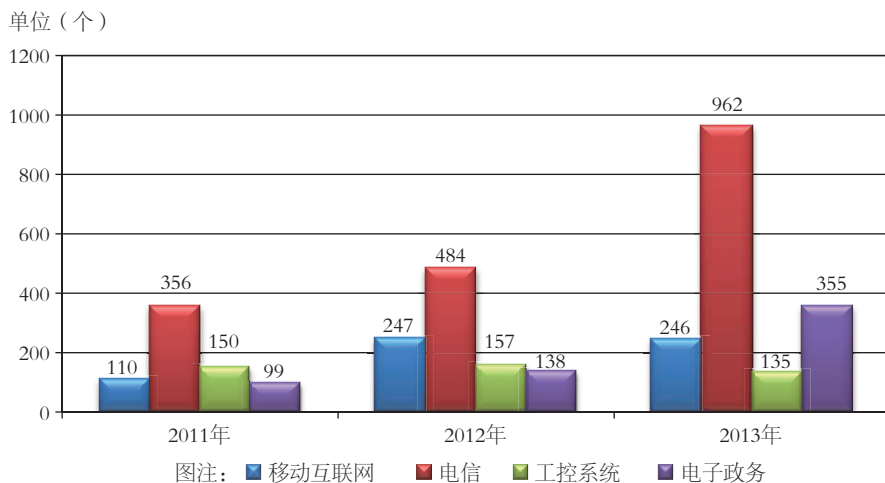


图6-7 2011-2013年CNVD收录行业漏洞对比（来源：CNVD）

移动互联网行业漏洞最为相关的厂商包括Apple、Adobe、Google、HTC、Research In Motion。厂商分布如图6-8所示。

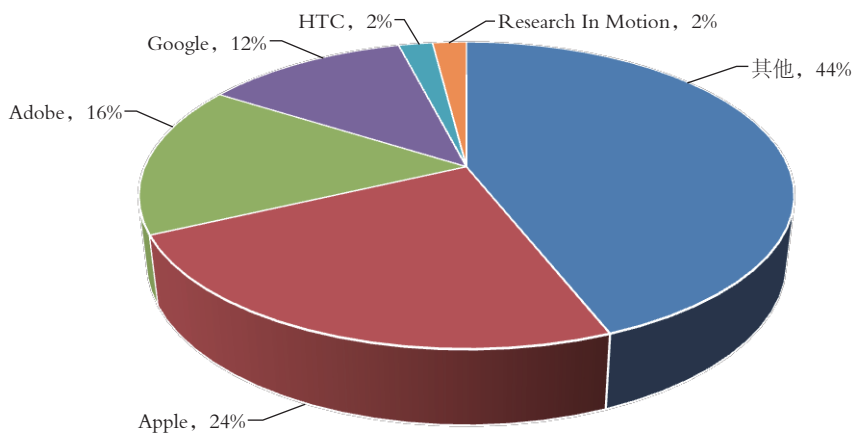


图6-8 2011-2013年CNVD收录移动互联网行业漏洞厂商分布（来源：CNVD）

电信行业漏洞最为相关的厂商包括Cisco、IBM、Oracle、D-Link、Apache。厂商分布如图6-9所示。

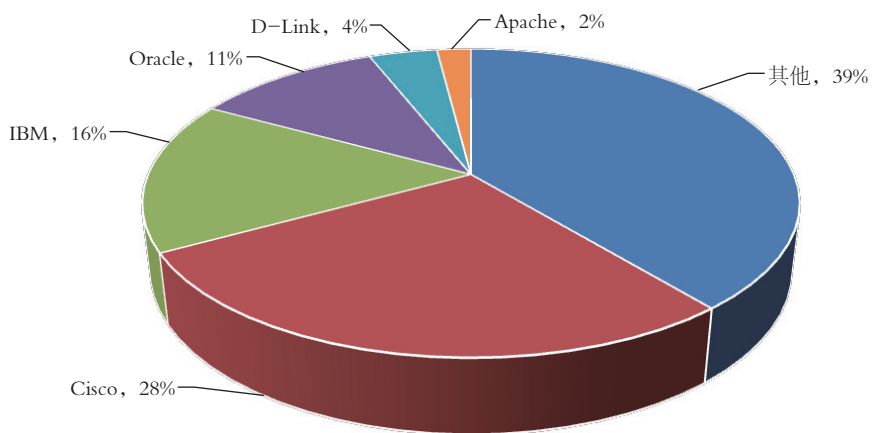


图6-9 2011-2013年CNVD收录电信行业漏洞厂商分布（来源：CNVD）

工控行业漏洞最为相关的厂商包括Siemens、Advantech、Rockwell Automation、Invensys、Schneider Electric。厂商分布如图6-10所示。

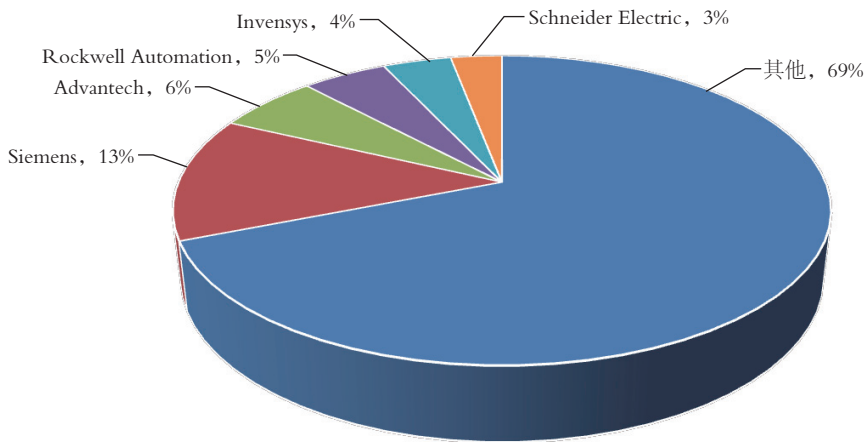


图6-10 2011-2013年CNVD收录工控行业漏洞厂商分布（来源：CNVD）

电子政务行业漏洞最为相关的厂商包括Phpcms、Aspcms、DedeCMS、Phpmyadmin、Comsenz。厂商分布如图6-11所示。

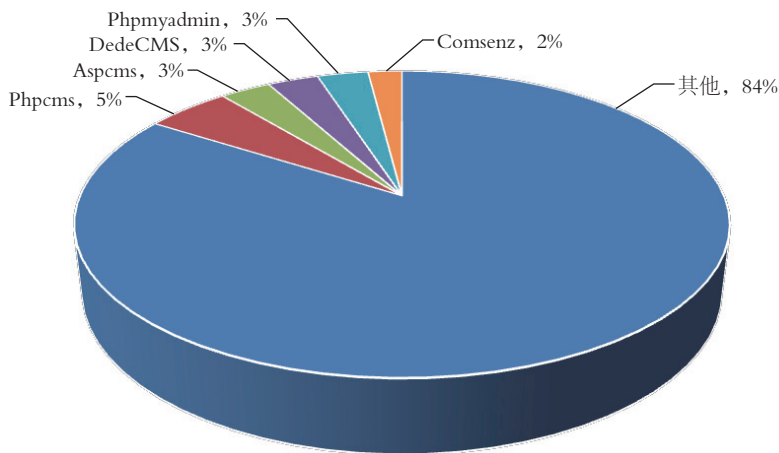


图6-11 2011-2013年CNVD收录电子政务行业漏洞厂商分布（来源：CNVD）



2013年，CNVD收录的漏洞中影响移动互联网行业的重大漏洞包括：Android操作系统存在一个签名绕过的高危漏洞（编号：CNVD-2013-08957）和Android WebView组件存在远程代码执行漏洞（编号：CNVD-2013-12829）。

（1）Android是基于Linux开放性内核的操作系统。攻击者利用Android签名绕过漏洞可修改APK代码，不破坏应用的加密签名，将合法应用转变为恶意代码的程序。

（2）Android WebView组件存在远程代码执行漏洞是由于Android的SDK中封装WebView控件。这个控件主要用开控制网页浏览，其中WebView下有一个非常特殊的接口函数addJavascriptInterface，能实现本地Java和JS的交互。利用addJavascriptInterface接口函数可实现穿透Webkit控制Android本机。攻击者可以构建恶意Web页，诱使用户解析，可以应用程序上下文执行任意命令。

影响电信行业的重大漏洞包括：友讯（D-Link）多款路由器产品存在后门漏洞（编号：CNVD-2013-13777），TP-LINK路由器存在的一个后门漏洞（编号：CNVD-2013-01769）。

（1）D-Link系列路由器是友讯集团推出的宽带路由器产品。根据漏洞研究者提交的情况，D-Link部分路由器使用的固件版本中存在一个人为设置的后门漏洞，攻击者通过修改User-Agent值为xmlset_roodkcableoj28840ybtide即可绕过路由器Web认证机制取得后台管理权限。取得后台管理权限后攻击者可以通过升级固件的方式植入后门，取得路由器的完全控制权。

（2）TP-Link部分型号的路由器存在某个无需授权认证的特定功能页面（start_art.html），攻击者访问页面之后可引导路由器自动从攻击者控制的TFTP服务器下载恶意程序并以root权限执行。攻击者利用这个漏洞可以在路由器上以root身份执行任意命令，从而可完全控制路由器。目前已知受影响的路由器型号包括：TL-WDR4300，TL-WR743ND（v1.2、v2.0），TL-WR941N，其他型号也可能受到影响。这些产品主要应用于企业或家庭局域网的组建。

影响电子政务行业的重大漏洞包括：Zimbra邮件系统存在文件包含高危漏洞（编号：CNVD-2013-14944），快客邮件系统存在远程代码执行高危漏洞（编号：CNVD-2013-02240），Apache Struts2 远程命令执行高危漏洞（编号：CNVD-2013-09777）。

(1) Zimbra是一款企业级邮件系统软件，在国内外应用较为广泛。由于在某处页面中存在文件包含漏洞，攻击者可以利用漏洞绕过限制读取未授权的主机操作系统文件或网站其他目录配置文件，如Zimbar默认配置文件/opt/zimbra/conf/localconfig.xml。测试结果表明，从上述配置文件中可获得Zimbra用户名和LDAP口令。若Zimbra服务器集成开放SOAP服务和7071后台管理端口，则可通过SOAP服务直接添加新的管理权限用户，取得邮件服务器后台控制权。

(2) 快客电邮是北京雄智伟业有限公司开发的邮件系统软件。相关版本的快客电邮产品采用CGI脚本，存在一处远程代码执行漏洞。攻击者可利用漏洞直接发起恶意URL请求，远程执行操作系统指令。通过当前邮件服务器运行用户已有权限，攻击者可逐步渗透并控制邮件服务器主机操作系统。

(3) Struts2是第二代基于Model-View-Controller (MVC) 模型的Java企业级Web应用框架。由于ApacheStruts2的action:、redirect:和redirectAction:前缀参数在实现其功能的过程中使用OGNL表达式，并将用户通过URL提交的内容拼接入OGNL表达式中，从而造成攻击者可以通过构造恶意URL来执行任意Java代码，进而执行任意命令。

6.4 CNVD漏洞处置情况

2013年，CNVD协助CNCERT/CC处置漏洞365次，涉及国内外软件厂商306家，联系次数较多的厂商见表6-1。

表6-1 2013年协调软件厂商处置漏洞情况（来源：CNVD）

厂商	漏洞数
正方软件股份有限公司	12
中国地震局（中国地震台网6个）	9
长城宽带网络服务有限公司	8
万科集团（万科企业股份有限公司）	7
吉祥航空（上海吉祥航空有限公司）	7

其中，正方软件股份有限公司、中国邮政集团、河南紫光容盾信息系统有限公司、上海泛微网络科技股份有限公司、南京大汉网络有限公司、浙江慧达驿站网络有



限公司等多家单位对CNVD的处置积极响应，并能及时回复漏洞修复方案，也有部分厂商未给予配合，如友讯电子设备（上海）有限公司、深圳市益光实业有限公司等。

此外，CNVD合作伙伴上海交通大学、赛尔网络公司配合CNVD进行漏洞检测和协调处置。其中上海交通大学处置漏洞49次，验证漏洞6次，主要包括：whatycms建站系统存在远程代码执行漏洞，多个高校网站存在IIS写权限高危安全漏洞，多个育软教育电子政务平台存在JBoss未授权访问漏洞，集思鹏jpcms系统存在SQL注入漏洞，人民大学多个分站存在SQL注入，弱口令漏洞等。赛尔网络处置漏洞13次，验证2次，主要事件包括：多个网站所属webtextbox存在cookie权限绕过漏洞，合肥工业大学网站存在通用软件SQL注入漏洞，人民大学汉青经济与金融研究院和劳动人事学院网站存在SQL注入漏洞的情况通报，四川化工职业技术学院泸州市普通话测试网上报名成绩查询系统存在多个漏洞，多个大学教育机构网站远程代码执行漏洞等。

网络安全事件接收与处理

为了能够及时响应、处置互联网上发生的攻击事件，CNCERT/CC通过热线电话、传真、电子邮件、网站等多种公开渠道接收公众的网络安全事件报告，对于其中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或涉及政府部门和重要信息系统的事件，CNCERT/CC积极协调基础电信企业、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。

7.1 事件接收情况

2013年，CNCERT/CC共接收境内外报告的网络安全事件31655起，较2012年增长65.5%。其中，境内报告的网络安全事件30684起，较2012年增长71.2%，境外报告的网络安全事件数量为971起，较2012年下降19.1%。2013年CNCERT/CC接收的网络安全事件数量月度统计情况如图7-1所示。

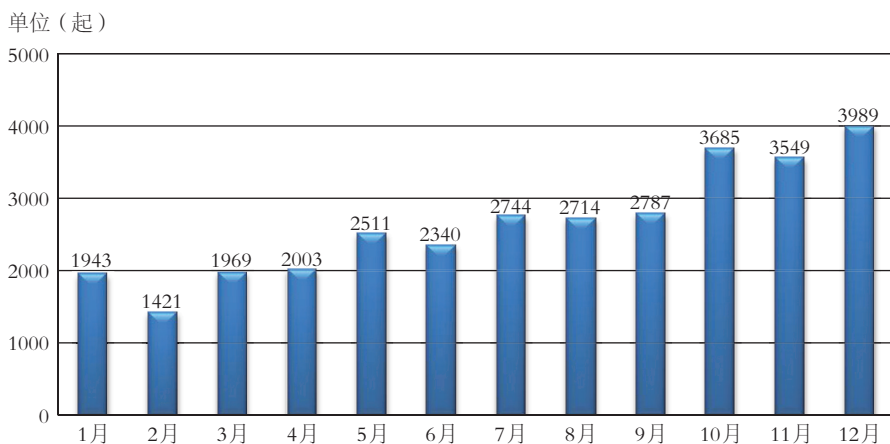


图7-1 2013年CNCERT/CC网络安全事件接收数量月度统计（来源：CNCERT/CC）



2013年，CNCERT/CC接收到的网络安全事件报告主要来自于政府部门、金融机构、基础电信企业、互联网企业、域名服务机构、IDC、安全厂商、网络安全组织以及普通网民等。事件类型主要包括网页仿冒、漏洞、恶意程序、网页篡改、网站后门、拒绝服务攻击、网页挂马等，具体分布如图7-2所示。

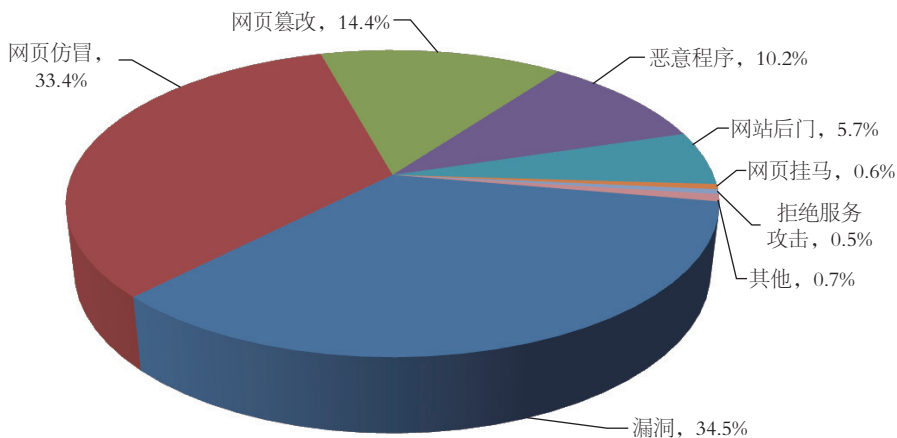


图7-2 2013年CNCERT/CC接收到的网络安全事件按类型分布
(来源: CNCERT/CC)

2012年，CNCERT/CC接收的网络安全事件数量排在前三位的依次是网页仿冒、漏洞和恶意程序。2013年，CNCERT/CC接收的网络安全事件数量排名发生了变化，前三位为漏洞、网页仿冒和网页篡改。具体情况如下。

漏洞事件数量为10936起，较2012年的7537起增加45.1%，超过网页仿冒事件数量，重新居于首位，占有所有接收事件的比例为34.5%。这主要是由于在CNVD成员单位以及互联网安全从业人员的大力协助下，CNVD漏洞库新增信息安全漏洞数量较2012年继续保持增长态势。

网页仿冒事件数量为10578起，紧随漏洞事件之后，排名降为第二，占有所有接收事件的比例为33.4%。由于电子商务和在线支付的日益普及、在线经济活动的日益频繁，网页仿冒事件虽排名第二，但其数量较2012年的9463起依然增加11.8%，保持增长态势。

网页篡改事件数量为4552起，较2012年的680起成倍增加了569.4%，超过恶意程序

事件数量，跃居第三位，占有接收事件的比例为14.4%。这一方面是由于黑客地下产业链蔓延发展，黑客通过对大量网页进行篡改，暗中植入黑链推广游戏、广告、色情网站，从而牟取经济利益。另一方面是由于网站漏洞频发，网页篡改成本较低，使得进行网页篡改活动的黑客越来越多。

7.2 事件处理情况

对上述投诉事件以及CNCERT/CC自主监测发现的危害大、影响范围广的事件，CNCERT/CC积极进行协调处理，以消除其威胁。2013年，CNCERT/CC共成功处理各类网络安全事件31180件，较2012年的18805件增长65.8%。2013年CNCERT/CC网络安全事件处置数量的月度统计如图7-3所示。针对公共互联网恶意程序日益猖獗、黑客地下产业链蔓延发展的现状，2013年CNCERT/CC共开展8次公共互联网恶意程序的专项清理行动，并继续加强针对网页仿冒事件的处置工作。在事件处置工作中，基础电信企业、域名注册服务机构和手机应用商店的积极配合有效提高了事件处置的效率。

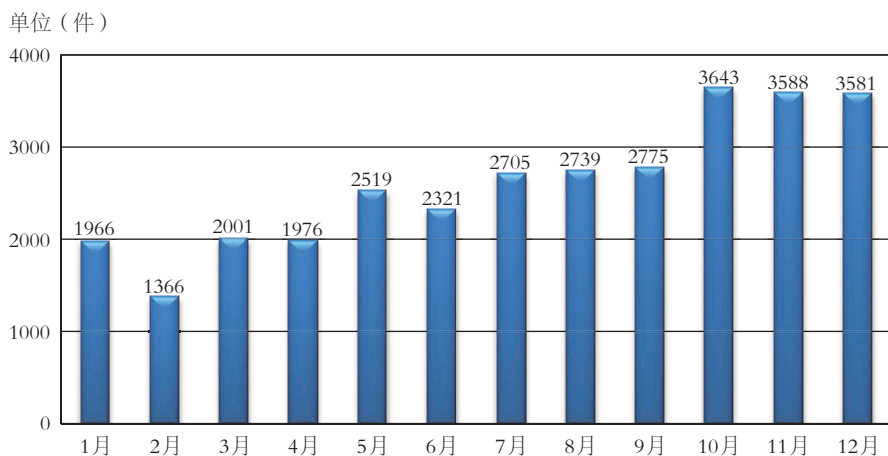


图7-3 2013年CNCERT/CC网络安全事件处置数量月度统计（来源：CNCERT/CC）



CNCERT/CC处理的网络安全事件的类型分布如图7-4所示，其中漏洞事件最多，共10884件，占34.9%，主要来源于CNVD收录并处理的漏洞事件。

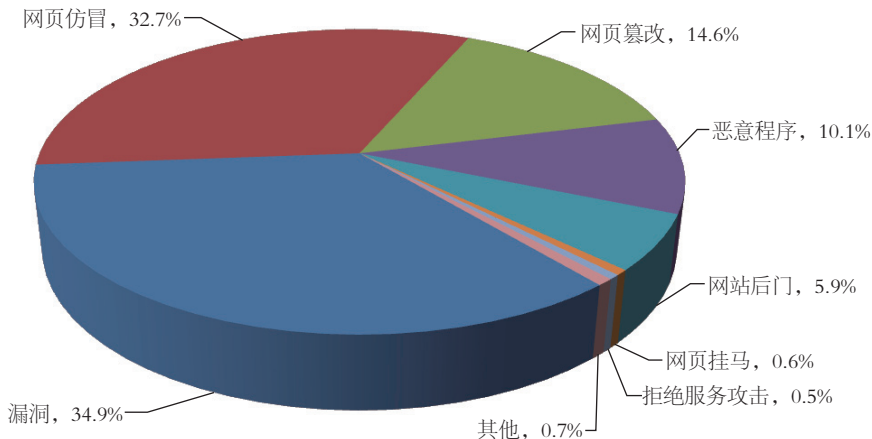


图7-4 2013年CNCERT/CC处理的网络安全事件按类型分布
(来源: CNCERT/CC)

网页仿冒事件处置数量排名第二，全年共处置10211件，占32.7%，较2012年的6575件大幅增长55.3%。CNCERT/CC处理的网页仿冒事件主要来源于自主监测发现和接收用户报告（包括中国互联网协会12321举报中心提供的事件信息）的网页仿冒事件。在处理的针对境内网站的仿冒事件中，有大量网页是仿冒中国农业银行、中国建设银行、中国工商银行、中国银行、淘宝等境内著名金融机构和大型电子商务网站的，黑客通过仿冒页面骗取用户的银行账号、密码、短信验证码等网上交易所需信息，进而窃取其钱财。同时，也有大量是仿冒央视网、湖南卫视、浙江卫视、东方卫视、腾讯、去哪儿网等知名媒体和互联网企业的，这类事件通过发布虚假中奖信息、新奇特商品低价销售信息等开展网络欺诈活动。CNCERT/CC通过及时处理这类事件，有效避免普通互联网用户由于防范意识薄弱而导致的经济损失。值得注意的是，除骗取用户经济利益外，一些仿冒页面还会套取用户的个人身份、地址、电话等信息，导致用户个人信息泄露。

居第三位的是网页篡改类事件。2013年，CNCERT/CC处理网页篡改类事件4551起，占14.6%，较2012年的2204件增长106.5%。对政府部门、重要信息系统或大型企事业单位来说，网页篡改是严重影响其形象、威胁其网站安全的重要事件类型之一。CNCERT/CC持续对我国境内网站被篡改情况进行跟踪监测，并将涉及政府机构和重要信息系统部门的网页篡改事件列为日常处置工作重点，力争使被篡改网站快速恢复。

此外，影响范围较大或涉及政府部门、重要信息系统的恶意程序、网站后门、网页挂马、拒绝服务攻击等事件也是2013年CNCERT/CC事件处理工作的重点。

2013年，CNCERT/CC加大公共互联网恶意程序治理力度。在工业和信息化部的指导下，CNCERT/CC及各地分中心积极开展公共互联网恶意程序的专项打击和常态治理，加强对木马和僵尸网络等传统互联网恶意程序、移动互联网恶意程序的处置，以打击黑客地下产业链，维护公共互联网安全。

专项打击工作方面，CNCERT/CC组织基础电信企业、互联网接入企业、域名注册服务机构和手机应用商店先后开展8次公共互联网恶意程序专项打击行动。在传统互联网方面，共成功关闭境内外1455个控制规模较大的僵尸网络，累计处置恶意程序控制服务器和传播所用IP地址及域名1916个，成功切断黑客对近375万台感染主机的控制。在移动互联网方面，下架6474个恶意APP程序，处置17个控制规模较大的恶意程序控制服务器所用域名，在全国大面积阻断73条恶意程序传播所用URL链接的访问。

常态治理工作方面，2013年，CNCERT/CC协调基础电信企业、域名注册服务机构等及时处置涉及传播源或重要单位的传统互联网恶意程序事件2822起，协调手机应用商店以每周一次的频率处置移动互联网恶意程序传播源，下架恶意APP程序3.1万个。此外，CNCERT/CC协调清理木马和僵尸网络控制服务器3.3万个、受控主机近72万个，向299万个感染移动互联网恶意程序的手机用户进行提醒处置。

2013年，CNCERT/CC协调各分中心持续开展的恶意程序专项打击和常态治理行动初见成效，我国境内感染木马僵尸网络主机数量近4年来首次下降，公共互联网安全环境有所好转。



7.3 事件处理典型案例

(1) CNCERT/CC监测发现JBoss网站蠕虫再次大规模爆发

根据CNCERT/CC抽样监测发现,从2013年2月26日1:50左右开始,JBoss网站蠕虫再次活跃,仅截止到27日12:00已感染网站服务器203个,其中境内网站有58个。这些被JBoss网站蠕虫成功入侵的服务器,还会自动扫描其他网站服务器,利用JBoss漏洞对其进行攻击从而传播自身。截至27日12:00,被扫描攻击的网站数量高达90.7万个,其中境内网站有35.7万,涉及大量政府网站、金融行业网站、新闻类网站及科研院所网站等重要网站。

JBoss网站蠕虫主要攻击存在“JBoss企业应用平台JMX控制台安全绕过漏洞”(编号:CNVD-2010-00821)的网站服务器,并通过服务器开放的JMXInvokeServlet服务,在网站上植入JSP类型的网站后门文件以及相关恶意程序,常见后门文件有zecmd.jsp、idssvc.jsp、iesvc.jsp、wstats.jsp、invoker.jsp。由于感染JBoss网站蠕虫的都是网站服务器,并非普通的用户个人计算机,且受感染的大量网站能够形成一个受到黑客远程集中控制的僵尸网络,所以JBoss网站蠕虫危害十分严重,应引起高度重视。

(2) CNCERT/CC协助调查发现韩国多家广播电视台及银行遭受的攻击并非来自中国

2013年3月20日,CNCERT/CC从互联网、事件响应与安全组织论坛FIRST和亚太地区计算机应急响应组APCERT了解到韩国主要广播电视台KBS、MBC、YTN,以及韩国新韩银行(ShinNan Bank)、农协银行(NongHyup Bank)等部分金融机构疑似遭受黑客攻击,相关网络与信息系统突然出现瘫痪。CNCERT/CC立即联系韩国国家级应急响应组织KrCERT了解具体情况。3月21日,CNCERT/CC从互联网得知,韩国民官军联合应对小组证实,向韩国多家广播电视台及银行等金融机构植入恶意代码的IP地址来自中国。CNCERT/CC迅速联系KrCERT。据KrCERT称,通过对农协银行的计算机系统进行分析后发现,黑客经由我国的IP地址(101.106.25.105)攻击韩国部分电视台和金融公司的杀毒软件管理服务器,并植入恶意程序。

经CNCERT/CC的深入调查和分析,发现此IP地址自2012年8月起已停用。

CNCERT/CC立即于2013年3月22日向KrCERT进行反馈，并要求韩方提供攻击分析报告及相关证据线索。韩国民官军联合应对小组经过再次调查发现，农协银行一直使用私自设立的IP地址，而这恰好与中国的IP地址一致。参加此次调查的相关负责人在对遭到黑客攻击的农协银行内部电脑进行分析时，误认为这是国际公认的中国IP地址。韩国民官军联合应对小组于3月22日16:00在韩新社正式发布消息称，3月20日导致韩国部分电视台和金融公司计算机网络全面瘫痪的恶意代码来自韩国境内电脑，而不是中国。

(3) CNCERT/CC协调处置美国谷歌公司投诉其产品遭受恶意攻击事件

2013年3月22日，CNCERT/CC接到美国谷歌公司投诉，称其广告产品在中国某接入网络商网内遭到恶意攻击，其广告被恶意替换成其他网络广告商的广告。CNCERT/CC在进行技术验证后，确认因部分用户的DNS解析请求遭到劫持和篡改，导致谷歌广告遭到恶意篡改攻击。依据中国应急处置体系的工作机制和有关管理办法，CNCERT/CC迅速采取行动，分别协调北京和天津两个分中心，对该事件中涉及的恶意DNS服务器和恶意广告服务器IP地址进行处理，使得谷歌广告服务恢复正常，有效地保障了用户的权益。

(4) CNCERT/CC协调处置多起针对美国重要信息系统的拒绝服务攻击事件

2013年3月，CNCERT/CC陆续接收到美国计算机应急响应组织US-CERT投诉拒绝服务攻击事件12起，称美国多家银行和大型企业网站、系统遭到拒绝服务攻击，其中有部分攻击来源于中国境内的262个IP地址，具体网站域名或链接1595个。

针对US-CERT提供的信息，CNCERT/CC协调基础电信企业及相关分中心进行处理，向相关用户及时预警，采取的措施包括：通知用户及时杀毒，切断攻击来源，同时对网站进行漏洞扫描和修补，防范再次被控成为发起拒绝服务攻击的僵尸肉鸡。同时，CNCERT/CC向US-CERT及时反馈处置情况。

(5) CNCERT/CC发现一系列具有欺诈行为的手机木马

2013年6月，CNCERT/CC发现一种假借机主名义发送诈骗短信的Android平台手机木马。当用户手机被感染后，木马会遍历读取用户通讯录、SIM卡内联系人，在用



户不知情的状态下，向手机中的所有联系人私自发送欺诈短信，短信内容涉及“银行账号”、“汇款”等金融欺诈内容，诱骗联系人进行转账汇款，并且不会在被感染手机的短信记录中显示。依据YD/T 2439-2012《移动互联网恶意程序描述格式》，CNCERT/CC对该手机木马进行全面分析，鉴定此类手机木马属于“诱骗欺诈”类恶意程序，将其归入a.fraud.SMSfraud恶意代码家族中。目前，CNCERT/CC已掌握77个被植入该木马的恶意APP程序，并公布其名单。经CNCERT/CC检测分析，该木马的植入时间最早可追溯至2012年12月，同时在2013年6月仍然活跃。这些恶意APP以工具类为主，例如，视频播放器类（新视频播放器、万能播放器、3D播放器）、GPS追踪类（GPS Tracker）、阅读器类（PDF阅读器、NFC阅读器）等，已感染数万名手机用户，造成一定的危害。CNCERT/CC提醒手机用户及时借助手机安全工具进行恶意APP程序的查杀，以消除隐患。

（6）CNCERT/CC发现针对TP-Link路由器的域名劫持攻击

2013年6月中旬，CNCERT/CC从信息通报成员单位报送信息获知，近期出现了针对TP-Link路由器的域名劫持攻击。黑客利用宽带路由器的缺陷对用户上网所使用的域名解析服务器IP地址进行篡改，导致大量用户被钓鱼欺骗。使用TP-Link路由器admin/admin等默认账号和密码的用户只要浏览黑客所掌控的Web页面，其宽带路由器的域名解析服务器IP地址就会被黑客篡改。CNCERT/CC建议用户检查使用的TP-Link路由器设置的域名解析服务器IP地址，如发现可疑的不明地址，应立即复位路由器的出厂设置，并更改默认账号和密码；未发现可疑地址的用户，也应及时修改默认的账号和密码，避免遭受攻击。

（7）CNVD收录和通报Android系统存在签名验证绕过高危漏洞

2013年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/CC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。

根据互联网的公开报道称，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/CC在获知漏洞情况后询问国内部分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。建议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；建议应用商店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/CC做好应用程序的鉴定和处置相关工作；建议Android智能终端用户提高警惕，避免下载来源不明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。

(8) CNVD收录和通报Apache Struts2远程命令执行高危漏洞和开放重定向高危漏洞

2013年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（编号：CNVD-2013-28972，对应CVE-2013-2251；CNVD-2013-28979，对应CVE-2013-2248）。利用漏洞可发起远程攻击，轻的窃取网站数据信息，严重的可取得网站服务器控制权，构成信息泄露和安全运行威胁。

CNVD对远程命令执行漏洞（编号：CNVD-2013-28972）和开放重定向漏洞（编号：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及时发布漏洞预警通报，跟踪监测国内相关用户受影响情况，指导国内相关单位进行信息系统应用情况排查及漏洞修补。

(9) 安卓签名漏洞疯狂爆发 正版应用遭遇“寄生虫”

2013年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/CC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/CC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/CC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ANVA向全社会进行黑名单发布。

(10) CNCERT/CC处置.CN国家顶级域名服务器遭受DDoS攻击事件并提供有力支撑

8月25日凌晨0:06起，中国互联网络信息中心（CNNIC）管理运行国家.CN顶级域名服务器遭受大规模拒绝服务攻击，对一些用户正常访问部分.CN网站造成短时间影响，凌晨2:00，.CN域名解析服务逐步恢复正常。

CNCERT/CC对事件进行研判。发现此次攻击系黑客利用僵尸网络向.CN顶级域名系统持续发起大量针对游戏私服网站域名rfinfo.cn的查询请求，造成.CN顶级域名系统的互联网出口带宽短期内严重拥塞。此外，CNCERT/CC通过此次攻击事件的监测数据分析，追溯此次事件的攻击源头，为相关部门进行事件查处提供有力支撑。目前，公安机关已在山东青岛逮捕犯罪嫌疑人，该案件正在进一步审理中。

(11) CNCERT/CC发现和处置一种利用短信方式进行传播的手机木马病毒

2013年9月22日，CNCERT/CC监测发现一个Android平台手机木马病毒。该病毒具有隐私窃取、远程控制、恶意传播、系统破坏等一系列高危恶意行为，通过短信方式向联系人传播该木马病毒，并通过后台下载更为复杂的手机银行盗号病毒，可窃取用户的银行账户、密码等隐私信息。9月22日，中国电信、中国移动紧急对该病毒涉及的传播源地址和控制端地址进行网内处置，及时遏制该病毒的蔓延。截至9月23日上午，CNCERT/CC在全网范围内监测仍发现有数千名用户感染该病毒。

同时，CNCERT/CC第一时间从网络侧和终端侧两大方面开展处置工作。网络

侧处置方面，通知手机病毒涉及域名所在的域名注册商（成都西部数码）对相关域名进行关停；通知运营商在网内对该恶意程序所涉及的URL链接进行处置；协调运营商严查是否存在短信群发机用于传播该恶意短信；由于该病毒的控制端IP地址位于中国香港和美国，并协调中国香港计算机应急响应组织HKCERT和美国计算机应急响应组织US-CERT核查该病毒所涉及的IP地址信息。终端侧处置方面，将该病毒信息在ANVA移动互联网恶意程序报送平台的黑名单中进行发布；将病毒样本在ANVA成员中进行共享，通知360、腾讯、金山等终端安全厂商更新病毒特征库，在终端侧查杀该病毒。

（12）CNCERT/CC发现和处理一类新型移动互联网恶意程序事件

2013年10月，CNCERT/CC监测发现一类新型的移动互联网恶意程序。首先，攻击者利用该程序，仿冒银行网站，诱骗用户输入手机号和登录密码，攻击者进一步利用窃取的用户信息登录用户网上银行，获取更多用户的账户信息。其次，攻击者在仿冒银行网页的同时，也仿冒手机银行安全插件，在安全插件中植入恶意程序，并在仿冒网站上设立恶意插件的下载链接，诱骗用户下载，攻击者可将用户接收到的网银短信验证码转发到其预先设定的手机号中，结合仿冒网站所得到的用户信息，完成网银支付、转账等交易行为，达到直接获取经济利益的目的。目前，CNCERT/CC共监测发现3个仿冒该银行网站的域名以及恶意手机银行安全插件的3个变种。

针对仿冒网站，CNCERT/CC已协调相关域名注册商对网站域名进行关停处理，相关的仿冒网站已无法访问；针对恶意手机银行安全插件所涉及的控制端手机号，CNCERT/CC已分别协调中国电信、中国移动和中国联通进行处置。

（13）CNCERT/CC成功协调美国US-CERT关闭查开房网站

2013年11月21日，CNCERT/CC与美国计算机应急响应组织US-CERT紧密协作，成功关闭了严重泄露中国公民个人信息、侵犯公民隐私的“查开房信息”网站。

CNCERT/CC通过网民投诉获知一个名为“查开房信息”的网站（<http://chakaifang.info/index.php>）提供在线查询酒店住客信息的服务，只要提供住客姓名或身份证，就可以查看到公民的“开房记录”以及开房登记信息，包括身份证号、手机号码乃至家庭住址等详细个人信息，严重泄露个人隐私，引发公众恐慌。CNCERT/CC



对此高度重视，第一时间开展调查，发现该网站所使用的域名在美国注册，所使用的IP地址也位于美国。

对此，CNCERT/CC于10月22日和10月28日两次联系美国US-CERT，请其协助关闭该网站。10月29日US-CERT回复其认识到此事件的严重性，正在积极协调该网站的域名注册商GoDaddy公司进行处置。此后，CNCERT/CC与US-CERT多次就此事件的严重危害和处理进展进行沟通 and 确认。最终，2013年11月21日US-CERT反馈其已成功协调关闭“查开房信息”网。

网络安全信息通报情况

8.1 互联网网络安全信息通报

2013年,作为通信行业的通报中心,CNCERT/CC继续按照《互联网网络安全信息通报实施办法》的要求,协调组织各地通信管理局、中国互联网协会、基础电信企业、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》的规定,各信息通报工作单位每月前5个工作日向CNCERT/CC报送前一个月的月度汇总信息;同时,各单位需及时报送所监测和掌握的其他重要事件信息和预警信息。2013年,CNCERT/CC共收到各单位报送的月度信息556份,事件信息和预警信息509份。经过全面汇总、整理各类上报信息,结合CNCERT/CC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》45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],2013年通信行业报送的网络安全事件数量月度统计如图8-1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。

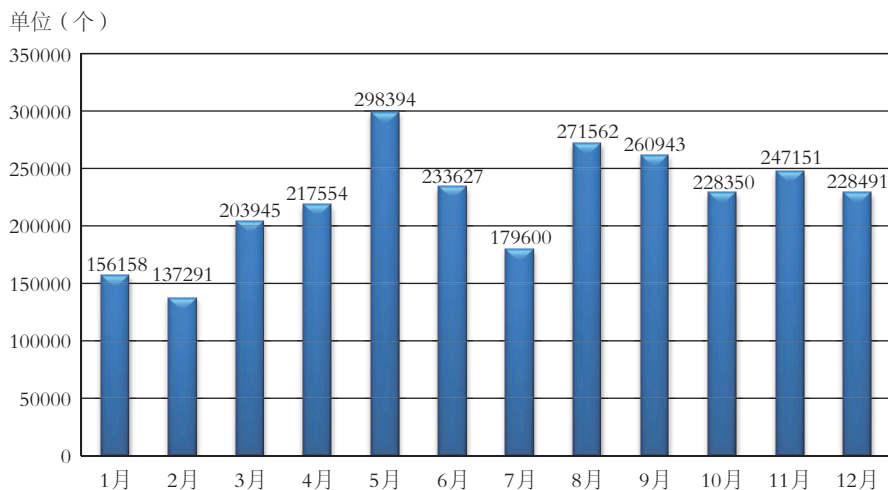


图8-1 2013年通信行业事件月度报送数量统计（来源：CNCERT/CC）

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8-2所示。可以看到，2013年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。与2012年相比，公共互联网环境事件、IP业务事件数量分别增加53.8%、26.6%，基础IP网络事件、域名系统事件、电信企业自有业务系统数量分别大幅减少99.8%、40.0%、55.2%。

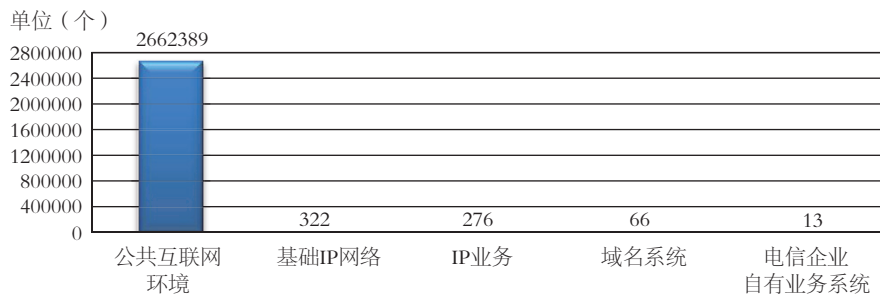


图8-2 2013通信行业报送事件按分类统计（来源：CNCERT/CC）

CNCERT/CC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8-3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24.6%；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24.4%、11.9%和10.2%。

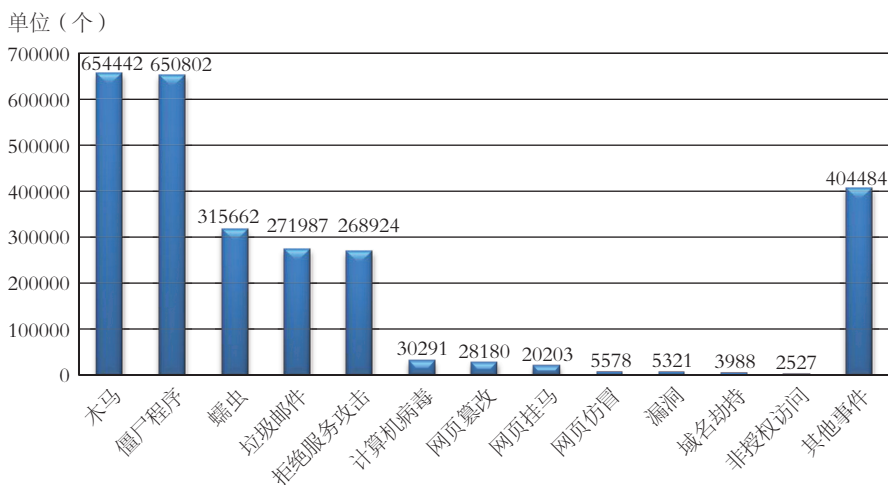


图8-3 2013年通信行业报送的公共互联网环境事件数量的分类统计
(来源: CNCERT/CC)

除每月汇总和发布月度情况通报外，CNCERT/CC还积极推动通报成员单位加强日常事件和预警信息的报送工作，如在高考等一些重要时期，各通报成员单位报送大量涉及相关网络信息系统的网页篡改、网页挂马等信息。对于日常报送的重要事件信息和预警信息，CNCERT/CC不定期地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/CC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。

2013年发布的重要通报增刊见表8-1。



表8-1 2013年CNCERT/CC发布的重要通报增刊

关于D根域名服务器变更IPv4地址的情况通报
关于“反共黑客”攻击境内网站的情况通报
关于Oracle Java存在远程代码执行零日漏洞的情况通报
关于Barbaros-DZ黑客组织攻击我国政府网站的情况通报
关于即插即用设备（UpnP）存在高危漏洞风险的情况通报
关于JBoss网站蠕虫再次大规模爆发的情况通报
关于韩国多家广播电视台及银行遭受攻击情况的通报
关于快客电邮远程代码执行漏洞的情况通报
关于域名服务软件BIND9新增拒绝服务漏洞的情况通报
关于eYou电子邮件系统存在多个漏洞的情况通报
关于Apache Struts2新增远程命令执行高位漏洞的情况通报
关于近期出现的针对TP-Link路由器的域名劫持攻击的情况通报
关于Android操作系统存在签名绕过高危漏洞的情况通报
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
关于织梦内容管理系统存在任意管理员添加高危漏洞的情况通报
关于一种利用Android签名绕过漏洞的手机扣费木马的情况通报
关于爱名网域名服务器遭受拒绝服务攻击事件的情况通报
关于奇虎360导航页被重定向的情况通报
关于Android系统WebView组件存在远程代码执行风险的情况通报
关于近期公共互联网恶意程序处置情况的通报
关于一种利用短信方式进行传播的手机木马病毒的情况通报
关于2013年9月增值电信企业漏洞风险的情况通报
关于2013年9月域名系统软件及域名机构漏洞风险的情况通报
关于2013年9月基础电信企业漏洞风险情况的通报
关于多款D-Link路由器产品存在后门漏洞的情况通报
关于近期公共互联网恶意程序处置情况的通报
关于2013年10月基础电信企业漏洞风险情况的通报
关于2013年10月域名系统软件及域名机构漏洞风险的情况通报
关于2013年10月增值电信企业漏洞风险的情况通报
关于2013年11月基础电信企业漏洞风险情况的通报
关于2013年11月域名系统软件及域名机构漏洞风险的情况通报
关于2013年11月增值电信企业漏洞风险的情况通报
关于Zimbra邮件系统存在文件包含漏洞的情况通报

8.2 行业外互联网网络安全信息发布情况

2013年，CNCERT/CC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214份，相比2012年增加48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共25期；通过邮件推送、CNCERT/CC网站发布中英文《网络安全信息与动态周报》各51期、《国家信息安全漏洞共享平台（CNVD）周报》52期、《CNCERT互联网安全威胁报告》12期、《2012年互联网网络安全态势报告》1份、《2012年中国互联网网络安全报告》1份、《移动互联网安全监测与处置专报》1期；通过期刊杂志发布网络安全数据分析文章20篇。

2013年，CNCERT/CC周报、月报、态势报告、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、新华网、中国日报、人民日报海外版、参考消息、人民邮电报等国内主流媒体纷纷前来挖掘新闻类节目或新闻稿素材，CCTV新闻频道、北京电视台、新华网、人民网、中国日报英文版、人民邮电报、参考消息、凤凰网、腾讯网、搜狐网、新浪网等20余家媒体栏目或频道播报了CNCERT/CC的监测数据和工作情况，引起各级政府部门和社会公众的高度重视。代表性的文章主要有《我国面临严重境外网络攻击威胁》、《中国面临严重境外网络攻击威胁 被篡改政府网站增长逾两成》、《我国网络安全态势严峻 钓鱼网站泛滥》、《手机病毒大爆发 年增25倍》、《网络安全事件治理需要合作》、《2012中国互联网网络安全报告发布 用户信息成黑客窃取重点》、《2013中国计算机网络安全年会：我国三千政府网站曾被黑客控制》、《Security in cyberspace still major problem》等。



国内外网络安全监管动态

9.1 2013年国内网络安全监管动态

(1) 中央决定设立国家安全委员会

2013年11月12日，中国共产党第十八届三中全会闭幕，审议通过了《中共中央关于全面深化改革若干重大问题的决定》，并指出将成立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全。目前，世界上设置国家安全委员会的国家还包括美国、巴西、智利、南非、土耳其、泰国和马来西亚等。国家安全委员会的主要职能是负责协调涉及国家安全、外交的重大战略政策，同时向国家元首提供涉及国家安全的建议，是跨部委的协调机构，其成员来自军事、外交、情报、执法等涉及国家安全的机构高层。

2014年1月24日，中共中央政治局召开会议，研究决定中央国家安全委员会设置。会议决定，中央国家安全委员会由习近平任主席，李克强、张德江任副主席，下设常务委员和委员若干名。中央国家安全委员会作为中共中央关于国家安全工作的决策和议事协调机构，向中央政治局、中央政治局常务委员会负责，统筹协调涉及国家安全的重大事项和重要工作。

(2) 人大常委会工作报告强调网络安全立法重要性

2013年3月8日，十二届全国人大一次会议在人民大会堂举行第二次全体会议。全国人大常委会委员长吴邦国受十一届全国人大常委会委托，向大会报告5年来的主要工作。报告指出：“近年来，网络技术迅猛发展、广泛运用，对促进经济社会发展发挥了重要作用，同时也带来很多严重问题。社会各方面强烈呼吁加强网络社会管理，严厉打击网络违法犯罪，全国人大代表也多次提出议案建议，要求尽快制定网络安全方面的法律。常委会认真总结网络发展和管理的实践经验，分析国外网络安全立法情况，广泛听取各方面意见，以法律形式保护公民个人及法人电子信息安全，

确立网络身份管理制度，明确网络服务提供者的义务和责任，并赋予政府主管部门必要的监管手段。”

（3）国务院发布《关于促进信息消费扩大内需的若干意见》

2013年8月8日，国务院发布的《关于促进信息消费扩大内需的若干意见》。意见提出，挖掘消费潜力、增强供给能力、激发市场活力、改善消费环境，建立促进信息消费持续稳定增长的长效机制，推动面向生产、生活和管理的信息消费快速健康增长。

根据意见内容，为了实现信息消费规模快速增长、基础设施显著改善、消费市场健康活跃的总体目标，我国将加快信息基础设施演进升级，增强信息产品供给能力，培育信息消费需求，提升公共服务信息化水平，加强信息消费环境建设，完善支持政策。意见明确提出深化行政审批制度改革、加大财税政策支持力度、切实改善企业融资环境、改进和完善电信服务、加强法律法规和标准体系建设、开展信息消费统计监测和试点示范六大配套措施。

（4）工业和信息化部将增设国家级互联网骨干直连点，健全电信网络信息安全制度

2013年11月21日，第九届中国通信网络运维年会在北京召开。为了加强互联网的质量监管，提升互联网通信质量，工业和信息化部电信管理局将借助部省两级管理体制，增设国家级互联网骨干直连点，提高网间流量疏导能力和互通效率，加强网间带宽扩容力度；此外，为了加强电信网络的运行安全，提升维护服务能力，将进一步健全电信网络信息安全保护管理制度。2011年至今，每年由工业和信息化部组织各省通信管理局配合开展的电信网络运行安全和安全生产巡查工作，对推动基础电信运营企业加强网络运行安全、深入推进安全隐患排查诊治等方面起到了积极的作用。2014年工业和信息化部电信管理局将在原有的工作基础上，着重开展两方面的工作：一是不断加强互联网质量监管，助力宽带中国战略；二是深入推进网络运行安全，加强网络运行维护服务能力。

（5）工业和信息化部开展防范治理黑客地下产业链专项行动

为遏制黑客地下产业链蔓延，净化网络环境，保护用户和企业切身利益与财产安



全，工业和信息化部定于2013年8-12月开展防范治理黑客地下产业链专项行动。根据《防范治理黑客地下产业链专项行动方案》规定，将加强仿冒政府、金融、传媒、电子商务类网站的监测和研判，在以行业自律方式对钓鱼网站域名进行处置的同时，加大对钓鱼网站托管主机的协调处置力度。同时落实《木马和僵尸网络监测与处置机制》（工业和信息化部保[2009]157号），加强木马和僵尸网络监测和研判，着重清理控制规模较大的木马和僵尸网络控制端主机和控制域名，加强处置效果验证，探索被控端处置方式。《防范治理黑客地下产业链专项行动方案》还将加强对网上贩卖“肉鸡”、虚拟财产、用户个人信息以及提供攻击服务的信息监测，对黑客活动受益主体进行关联分析，建立相关举报机制；依法依规关闭提供黑客技术培训和地下沟通交易渠道的网站、论坛、贴吧、即时通信群组等；指导督促提供论坛、贴吧、即时通信群组等信息服务的互联网企业落实违法信息管理责任；对在恶意吸费、广告黑链等行为中获益的SP、网站等进行依法处置，暂停业务合作或予以曝光。

（6）工业和信息化部将加快完善信息安全审查

2013年12月23日，国务院新闻办公室召开全面深化改革、加快推进新型工业化新闻发布会。目前网络安全形势日趋严峻，工业和信息化部将加快完善信息安全审查制度框架，进一步巩固提升电话用户实名登记工作，开展地下黑色产业链等网络安全环境的治理。工业和信息化部将按照国家的统一部署，针对网络安全的新情况、新问题，坚持“积极利用、科学发展、依法管理、确保安全”的16字方针，加大依法管理网络的力度，不断健全网络安全的保障体系。

（7）中美将在战略安全对话框架内设网络安全工作小组

在2013年6月8日的“习奥会”上，中美元首就网络安全问题进行交流。在回答记者关于网络安全的提问时，习近平强调，中国是黑客攻击的受害国，是网络安全的坚定维护者。中美双方在网络安全上有共同关切，双方已商定在中美战略安全对话框架内成立网络工作组，共同解决网络安全问题。习近平表示，通过一种真诚的合作，消除猜疑，反而可以使中美在信息安全领域、网络安全领域的合作成为今后加强中美关系的一个亮点，“因为这是我们共同的需求和关切，中国也是网络安全方面的受害者，我们希望切实解决这个问题。”

(8) 外交部设立网络事务办公室，负责网络事务外交活动

2013年6月14日，外交部在例行记者会上宣布，外交部近日设立了网络事务办公室，负责协调开展有关网络事务的外交活动。面对“美方多年来一直入侵中国网络却指责中国对美进行网络攻击，中方打算如何应对”的记者提问，发言人表示，中国是遭受网络攻击最严重的国家之一，中方坚决反对一切形式的黑客攻击。我们认为，网络空间需要的不是战争和霸权，而是规则和合作，中方高度重视网络安全问题。近日，外交部设立网络事务办公室，负责协调开展有关网络事务的外交活动。中方将与有关各方继续就网络安全问题开展建设性的对话与合作，主张在联合国框架内制定相关国际规则，并提出具体倡议。希望有关方面采取切实行动，增进各方互信与合作，共同维护网络空间的和平与安全。中美在战略安全对话框架下建有网络工作组，中方将在有关框架下就相关问题与美方进行深入沟通。

9.2 2013年国外网络安全监管动态

9.2.1 美洲地区网络安全监管动态

9.2.1.1 美国网络安全监管动态

(1) 美国网络安全相关法令政策

- 美国总统签署《2013财年国防授权法案》

美国总统奥巴马2013年1月3日签署的《2013财年国防授权法案》强调，网络安全和其他信息技术正扮演着越来越重要的角色，军队对信息技术越来越依赖。根据这项总额高达6330亿美元的法案，美国国防部必须采取下一代网络防御系统，并定期向美国国会报告其在网络空间方面的进展，具体内容包括网络入侵报告机制的指导方针以及军队在软件开发与软件授权方面必须采取的步骤等。“法案”的技术指导方针主要包括若干针对网络安全和网络战方面的条款，例如国防部应当“制定一项战略，以获得下一代基于主机的网络安全工具和能力”，除了能够监测恶意软件和基于特征的威胁外，还应当能够应对“不断变化的新威胁”；必须在一个开放的体系结构中应用新



技术，允许添加和集成多个网络安全工具，如内部威胁检测、连续监测和配置管理工具等。

- 美国总统签署提升关键基础设施网络安全的行政令

2013年2月12日，美国总统奥巴马签署了名为《关于提升关键基础设施网络安全的决定》的行政令，旨在保护国家基础设施免受网络攻击。奥巴马表示，“黑客们窃取人们的身份信息，入侵私人邮件，窃取企业秘密，试图破坏电力网、金融机构及空中交通管制系统”。该行政令的主要内容包括：在国家层面，美国总统正式认定“信息战”会一直持续下去，是目前显而易见的威胁。政府将与私营部门合作建立“网络安全框架”，实现网络攻击与威胁的信息共享，从而降低针对关键基础设施的网络安全风险。该基本框架包含一套标准、方法、步骤、流程以及应对网络安全风险的非指定的技术手段。“网络安全框架”的建立有助于将现有的政府项目向私营部门扩展，这样能让更多私营部门的专家在一段时间内为政府服务。与此同时，该行政令规定建立“网络安全框架”的具体时间表以及“网络安全框架”对隐私状况影响的评估报告。

(2) 美国其他网络安全相关举措

- 美国空军预备役司令部成立首个网络空间行动组

2013年3月1日，美国空军预备役司令部成立首个网络行动组：第960网络空间行动组（CYOG）。CYOG管理全美10个预备役网络机构，主要负责在作战中提供具有专业知识的作战部队，并保护空军和国防部全球信息栅格安全。该行动组是美空军预备役司令部在网络领域的关键组成部分，最终将组建两个分队，与第624作战中心、第33网络战中队联合运行。其第一分队将与第624作战中心一起建立、计划、指导、协调、评估和提供全方位的网络指挥控制行动和能力，为空军和联合部队提供支持；第二分队将会与第33网络战中队合作，通过采取同步的网络防御行动来检测、响应和阻止网络入侵，为空军和网络空间作战指挥人员提供支持。

- 美军将组建13支网络进攻部队

2013年3月12日，美国网军司令基斯·亚历山大表示，美国国防部网络司令部将在2015年秋季前新增40支网络部队，其中13支用于进攻，在遭到国外网络攻击时发动网

络战。除了位于美国马里兰州的网络战司令部总部917名人员之外，还有来自所有4个军种的超过1.1万人参与网络战司令部。从公开数据估计，美国的网络部队包括海陆空总人数为5.3万~5.8万人。五角大楼每年在网络安全方面的投入超过30亿美元。美国遭受的战略威胁正在恶化，亚历山大敦促国会通过立法，使私营企业能与政府共享计算机威胁数据，而不用担心被起诉。

- 美国国家安全局建造新计算中心以加强网络防御能力

2013年5月，美国国家安全局（NSA）宣布，将建造一个新的计算中心，并于2016年投入使用，以更好地抵御网络攻击。该新中心将加强监测和打击网络攻击的能力，以应对不法分子侵入美国的计算机网络，窃取身份、知识产权或国家机密的行为。新中心占地60万平方英尺，约有6000名工作人员将参与新计算中心的设计与施工。NSA局长、美军网络司令部最高指挥官基斯·亚历山大表示，新的高性能计算中心将在网络空间的实时对抗中发挥作用。

- 美国网络部队组建即将完成，总数4000人

2013年7月18日，美国国防部副部长阿什顿·卡特宣称，五角大楼组建网络部队的工作即将完成，总人数达4000人的网军将很快全部就位。国防部希望尽快完成网军组建工作，网军将由兼任国家安全局局长的美军网络司令部司令基斯·亚历山大指挥，与国家安全局相互支持，确保美国网络安全。眼下网军成员都是来自各兵种的电脑专家，但今后这支部队可能会按照特种部队的思路来建设。

9.2.1.2 美洲其他国家网络安全监管动态

（1）墨西哥成立网警部队加强监管网络犯罪

2013年4月，墨西哥联邦区公安部门正式成立网警部队，以加强对科技化、网络化犯罪的监管。该部队目前由30名成员组成，绝大多数成员为系统工程师和网络专家，日常任务为维护墨西哥联邦区网络安全，同时预防和阻止以网络为平台的犯罪形式，如勒索、欺诈、身份资料窃取乃至网络团伙卖淫等。对此，联邦区治安负责人赫苏斯·罗德里格斯表示，通过网警部队的努力，将会切实维护该地区乃至墨西哥网络用户的人身、财产安全和利益不受侵犯。这次行动由墨西哥和韩国合作完成，这支队伍的所有成员此前均接受了韩国网警专家的相关培训。



(2) 阿根廷巴西开展网络防御合作

2013年9月13日，阿根廷国防部长阿古斯丁·罗西与到访的巴西国防部长塞尔索·阿莫林签署声明，把网络防御列为双边国防合作的重要内容。罗西在接受媒体采访时表示，两国已商定2013年年底前在巴西利亚召开会议，强化两国在网络防御上的互补合作。他认为，鉴于目前存在的网络间谍行为，两国除了各自需要加强防御能力外，还应通过互补减少彼此网络的安全漏洞。阿莫林认为，作为合作的第一步，双方首先了解彼此在网络安全方面的部署，然后通过双边工作小组提出具体的网络安全合作项目。他强调，两国在网络安全软件开发方面有巨大的研发能力与合作潜力。

9.2.2 欧洲地区网络安全监管动态

(1) 北约卓越协同网络防卫中心正式发布《塔林手册：适用于网络战的国际法》

2013年3月15日，北约专门研究网络战的“卓越协同网络防卫中心”在其官方网站上发布了《塔林手册：适用于网络战的国际法》。“塔林手册”被认为是西方第一份公开出版的系统化的网络战国际法，被誉为网络战领域的“日内瓦公约”，是以美国为首的北约争夺“网络战争规则”制订权的重要步骤。

在国际红十字会和美国网络司令部的协助下，“塔林手册”由20名国际法律专家耗时三年完成。该手册总计215页，包括关于网络战的95条硬性规则，“明确了一个国家可以在何时、以何种方式合法地针对另一个国家发动网上攻击”，并声明“不属于官方文件，仅代表各位法律专家的个人意见”。其中一项条款规定：当一国计算机网络受他国黑客入侵，且因此造成伤亡或重大财产损失时，该国可用传统作战予以回应。该手册指出，对计算机系统发起的网络攻击可引发大规模战争，参与网络攻击的非军事人员属于合法打击目标。

(2) 北约2013年秋全面运行网络防御体系

2013年6月4日，来自北约28个成员国的国防部长在布鲁塞尔召开会议，专门就网络安全问题进行了讨论，并同意加强北约网络防御能力建设。北约秘书长拉

斯穆森在会后举行的新闻发布会上宣布，北约网络防御体系将在2013年秋季达到完全运行标准。拉斯穆森说，保护自身网络安全对北约来说只是最基础的任务，下一步北约将考虑如何作为一个军事联盟来应对网络威胁。他说，如果一个成员国遭到网络袭击而未能及时得到有效处理，将影响到北约整体。北约明确表示，网络已成为一个没有硝烟的新战场。北约“集体防御”被认为适用于网络空间，北约成员国遭遇网络袭击，其他国家应给予政治、经济甚至是军事支持。按照北约网络防务规划，自2013年起，所有北约国家都将推出网络防御国家政策，建立网络防御国家主管机构，并形成针对网络攻击的即时响应能力。

（3）北约举行史上最大规模网络防御演习

2013年11月26-28日，北约在爱沙尼亚举行了代号为“网络联盟2013”的网络防御演习，旨在预防对北约成员国及其盟友的大规模协同网络攻击。此次演习是参与国最多、规模最大的一次网络演习。自2008年以来，北约每年都会举行一次网络防御演习，而此次参与演习国家的国家则达到33个，包括28个北约成员国和5个非北约成员国，观察员则有欧盟和新西兰，包括300多名网络防御领域的专家，另有80名专家在东道国爱沙尼亚进行军事训练设备方面的工作，其他相关参与人员来自参与国的武装部队、执法及相关部门。此外，北约总部民用领域和军事领域的专家也参与其中。

（4）欧盟公布网络安全战略

2013年2月7日，欧盟委员会公布了新的综合性网络安全战略，就如何预防和应对网络中断和袭击提出全面规划，以确保数字经济安全发展。欧盟外交和安全政策高级代表阿什顿说，欧盟出台这一战略的根本目的在于构建一个“公开、自由和安全”的网络空间。根据新战略，欧盟在网络安全方面有5项优先工作：提升网络的抗打击能力、大幅减少网络犯罪、在欧盟共同防务的框架下制定网络防御政策和发展防御能力、发展网络安全方面的工业和技术、为欧盟制定国际网络空间政策。新战略提出一项立法建议，要求关键机构在遭受网络袭击时要向欧盟汇报，包括重要基础设施的提供商、关键的网络企业及公共行政部门。欧盟还要求各成员国制定相应的战略，成立专门机构以预防和处理网络安全风险和事故，并与欧盟委员会共享早期风险预警信息。



（5）俄罗斯将建国家计算机信息安全机制

2013年1月，俄罗斯总统普京责成俄联邦安全局建立监测、防范和消除计算机信息隐患的国家计算机信息安全机制。根据普京日前签署的一项总统令，这一涉及多个部门的机制主要任务是评估国家信息安全形势，控制重要信息基础设施的安全等级，确定计算机安全事故的原因。同时，联邦安全局还将建立计算机攻击信息的资料库，定期更新监测“黑客”攻击的方案。与此同时，俄外交部打算成立国际信息安全司，主要任务包括推进俄外交部和安全会议起草的《联合国保障国际信息安全公约草案》，以及上合组织成员国倡导的网络行为规范；在欧洲安全与合作组织（OSCE）框架内和双边机制中拟定增进网络空间信任的措施；在国际平台上坚持俄罗斯对网络管理的主张（首先是争取国际社会承认主权和不干涉别国内政的原则也适用于互联网领域）。

（6）俄军2013年内建网络安全部队增新兵种

2013年8月，俄罗斯国防部副部长奥斯塔边科声明，俄武装力量将增新兵种，其主要任务是向网络威胁作斗争。俄新成立的网络安全部队的主要任务是“猎捕”有害的软件，反击黑客的攻击，同时寻找外国进口设备中敌人的“暗藏物”。当重要武器和技术都达到由本国电子元件组建时，才能谈到网络安全的保障。此前，俄罗斯联邦安全局曾声明建立反网络威胁特种部队，但由于它具有特工性质，不可能在俄罗斯国防部推广。俄专家表示，两种部队有不同的任务，俄安全局将在存在恐怖行动阴谋情况下，通过正常的网络联系渠道与网络威胁作斗争；而俄国防部需要保障对战略设施无间断地控制，使任何人都不可能妄想破坏军队的战备状态。西方国家网络部队任务中，可能有全面破坏潜在敌人军队管理系统的措施，而俄网军的主要任务是自卫性的。俄国防部声明，2013年内俄武装力量中将出现网络安全部队。

（7）英国将设立全球网络安全中心

2013年4月，为了对抗全球网络威胁，英美阵营决定整合网络安全资源，由英国在其中唱主角，未来一所全球网络安全中心将落户剑桥大学。英国外交大臣威廉·黑格近日宣布，剑桥大学将设立全球网络安全中心。该中心将帮助各国制定应对网络威胁的综合计划。英国政府在未来两年将为该中心提供100万英镑的资助。这处新的全球

网络安全中心将与全球各国合作，研究如何应付网络威胁和制定网络政策，这不仅将有助于保护英国的安全还会“成为专业的灯塔”。剑桥大学未来的这所中心将把资金部分用于保证各国获得必要技巧、人员和技术，在一些关键问题上设立指南，设法确保各国获得相关知识或技能解决网络威胁问题。

（8）英国将建立网络安全预备役部队，可实施网络攻击

2013年9月29日，英国国防大臣菲利普·哈蒙德宣布，将建立一支网络安全预备役部队，以应对并在必要时实施网络攻击。过去一年中英国拦截的针对政府安全内网发起的高级别恶意攻击就超过40万次，然而，消极地应对网络攻击是不够的，应当成立专门的网络部队，并作为全方位军事力量的重要组成部分发挥作用。英国已于2013年5月成立联合作战网络小组，隶属于国防部联合作战司令部。10月将启动网络预备役计划，开始征召军队离职人员、具备必要技能的现任或曾任预备役军人，以及无从军经历但具备一定能力的人才，利用他们的专业技能为英国的网络安全提供保护。

（9）荷兰计划立法允许警察以黑客手段打击网络犯罪

2013年5月，荷兰政府宣布计划立法允许警察以黑客手段打击网络犯罪。如果这项新法案获得通过，警方调查人员将被允许以黑客手段攻击其他计算机，并在里面安装病毒，阅读邮件或销毁文件，还有权通过黑客攻击进入国外的服务器。荷兰政府强调说，调查人员取得上述权力需要经过法官的批准。该法案还将嫌疑人在接受调查期间拒绝破解加密文件的行为视为犯罪，公布盗窃来的数据将受到惩罚。

（10）法国拟立法加强网络安全

2013年12月，法国国民议会通过2014-2019年军事纲领法案。在这份以军事内容为主的法案中，多个条款涉及网络监控。法国日益重视网络安全，此次将网络监控列入军事纲领法案凸显网络安全的重要性。此份军事纲领法案首先扩大网络监控领域。监控的领域也由针对恐怖分子扩大至经济犯罪等领域。除之前的内政、国防、海关等部门外，经济、预算部门将获得这一权力。其次，法案增加了网络监控的内容。之前，只有互联网服务提供商需提供用户的元数据、个人验证信息和地理定位。按照新法案，行政机关还可以要求谷歌这样的网页寄存服务商提供元数据，网民浏览网页、



观看视频、发送邮件的历史记录都可以被查阅。自反恐法实施以来，法国每年要进行4.5万次信息收集，新法案通过后这一数字势必继续上升。

(11) 西班牙制定信息安全战略

由西班牙首相马利亚诺·拉霍伊领导的西班牙国家安全委员会于2013年12月5日检查国家信息安全战略，其目的是加强检测、阻止和应对网络攻击的能力，并确保网络系统的使用安全。西班牙是欧洲国家中最后一批为应对最主要的网络威胁采取类似的全球战略的国家之一。西班牙此次出台的信息安全战略的主要目的是加强预防、侦查、调查和应对网络威胁的能力；保护信息系统和通信管理网络的安全；强化涉密部门信息交流技术；加强对专业人士的训练，促进产业发展；推动信息安全文化的发展，并加强国际间的交流合作。

9.2.3 亚洲地区网络安全监管动态

(1) 中国香港警方将成立特别办公室检查网络安全

2013年7月，香港特区保安局局长黎栋国宣布，香港警方已经成立特别办公室检查情况。香港网络系统被入侵的情况时有发生，特别是因为香港互联网已经成为市民生活不可或缺的一部分，用途越来越广泛，被入侵的次数也会相应增加。近期，入侵香港网络的事件都已向香港警方和香港个人资料隐私专员公署报告，有关部门会通知受影响的人士立刻更改所有密码。相关部门会调查网络系统被入侵的原因，并加强漏洞检查。但由于网络入侵者的入侵方式复杂，入侵地点可能在国外，因此需要国外的执法机关配合，调查时间可能较长。

(2) 中国台湾安全范围扩及网络，以防网军黑客攻击窃取情报

2013年5月30日，中国台湾当局行政机构通过“安全法”部分条文修正草案，为免网军、黑客攻击窃取官方情报，新增维护当局安全范围扩及互联网，并将函请立法机构审议。面对全球化、信息化时代来临，台湾安全的威胁不再限于实体，甚至已扩及资通安全，为防网络黑客入侵互联网进行破坏，结合当年“第五空域（网际空域）”观念及资通安全威胁顾虑，新修正草案增列台湾安全的维护应包含互联网。因此，未

来进行网络监控、公文密码传递等资通安全管理，均有法源依据。此外，为发挥防止境外势力渗透，强化民众国防警觉，新修正案增列为鼓励民众检举危害台湾安全案件，给予检举人奖金及保护的规定。

(3) 日本政府启动APT数据库建设项目应对网络攻击

2013年2月，为了应对APT威胁的不断增加，日本政府将建立APT数据库，整合威胁情报，同时与国内信息安全管理机构和其他国家政府进行信息共享。日本政府将投资850万美元与其他国家的政府机构及公司开展合作，共同建设APT数据库。日本经济产业省（MEIT）信息安全部门在其中将起到协调作用。APT数据库主要包括来自美国和亚洲等国家的相关信息。数据库将与日本受到网络攻击的组织共同搜集威胁信息，利用与特定目标服务器相似的仿真服务器吸引APT攻击。日本政府及其他组织将根据APT数据库中的威胁信息制定更有效的网络防御策略，并与美国共享相关情报。

(4) 日美举行首次网络安全综合对话

2013年5月9-10日，日美两国政府在日本外务省举行首次网络安全综合对话，双方一致认为可导致重要基础设施系统瘫痪的网络攻击是安全上的威胁，并就官民合作防范网络攻击进行磋商，就合作制定网络空间的国际规则进行讨论。出席此次对话的有日本外务省、防卫省及内阁信息安全中心负责人和美国国务院、国防部及国土安全部官员。该综合对话会议今后预计将定期举行。日美两国目前都在为东盟各国构建网络安全能力提供支持，两国有意与东盟一同合作，为制定“开放的国际规则”营造国际舆论。

(5) 日本政府“网络安全战略”最终草案出炉

2013年5月21日，日本政府信息安全政策会议汇总出“网络安全战略”最终草案。该草案提出多项强化措施，其中包括在自卫队设立“网络防卫队”。日本政府将就最终草案进行公开意见征集，并于6月正式决定并加紧落实，防止政府、企业和普通网民成为网络攻击的对象。最终草案具体列举了在2015年度前需要开展的工作，例如针对疑似外国政府参与的国家层级的网络攻击等，强调必须加强自卫队的应对能力和防范力度。此外还提到要提升分析仪器的性能，培养高度专业性人才等。草案还提出，



2015年度结束前要改善政府机构及重要基建领域的软件病毒感染率，在遭受网络攻击时可开展合作的国家数量应在现有的80多个国家基础上增加3成。此外，还要在2020年底前将目前规模为6000亿~7000亿日元（合人民币360亿~420亿元）的国内信息安全市场扩大一倍。

（6）日拟在自卫队设网络防卫队，与美共防范网络攻击

2013年9月，日本防卫相小野寺五典表示，要加强与美国合作，共同应对网络黑客攻击，并计划在自卫队内设置专门部队。10月举行的日美外交、防卫部门负责人会谈上，双方将会交换相关文件，加强合作，将成立一个叫作“网络防卫队”的组织，做好网络攻击的应对，并在自卫队内设置专门部队来应对网上的黑客攻击。此外，小野寺五典还表示，日美双方将会缔结针对网络黑客攻击的备忘录，共同应对网络攻击，日本政府希望日美携手应对网络黑客攻击，此后有必要将警戒监视范围扩大至太平洋，有必要提高自卫队警戒监视能力。

（7）韩国公布《国家网络安保综合对策》加强互联网安全措施

为系统应对类似“3·20”、“6·25”的网络威胁，韩国未来创造科学部2013年7月4日公布了《国家网络安保综合对策》。根据该对策，为了及时应对分布式拒绝服务（DDoS）等网络攻击，将在总统府青瓦台新设网络应对组织来发挥控制塔的作用。国情院将担任实务总管，与未来部、国防部等部门进行合作。同时还决定在2014年前构筑“网络威胁信息共享系统”，扩大与民间部门的信息共享。与此同时，按照规定发电站、铁路、港口以及水电站等国家基础设施的内部网必须与外部网分离。为了增强网络安全，将在2017年前培养5000多名应对黑客攻击的“反黑客”人员。此外，韩国金融委员会7月4日表示已制定《金融计算机安保强化综合对策》，该规定包括金融公司若发生重大计算机事故，首席执行官（CEO）将有可能受到“停职”等严惩，以及大型金融公司的内部网和外部互联网应当分离等。

（8）韩国重视网络安全，政府大力打造信息安保产业

2013年7月，韩国政府计划在2017年之前培养约5000名信息安保专业精英人才，开发包括下一代密码软件、自动感应技术等10项世界一流安保技术。韩国未来创造科学

部在2013年7月4日发表了题为《信息安全产业发展综合对策》的报告，内容包括推动信息安全产业市场规模增长2倍，扩大到10兆韩元（约合87.1亿美元）的规模。为了使信息安全产业成为新增长的动力产业，政府将积极支持这一领域的发展。韩国未来部信息化战略局长朴载文表示，国家的发展和人民生活水平的提高离不开网络安全的发展和信息安保产业，韩国将成为信息安全的国家。

（9）新加坡军队建立网络防卫中心抵御黑客袭击

2013年7月，新加坡国防部长黄永宏透露，新加坡武装部队为提升对抗网络袭击的能力，将成立网络防卫行动中心（CDOH），以更全面并系统地防御日益严峻的网络袭击威胁。新成立的网络防卫行动中心将从新加坡国防部、武装部队和国防科技机构现有的人员当中调用这方面的专门人才，执行探测、识别、控制和消除网络威胁的工作。该中心将全天候运作，除了检测和应对网络威胁，必要时也能快速修复新加坡的军事网络。此外，网络防卫行动中心还将与新加坡资讯通信科技安全局（SITSA）合作，以获取最新的资讯安全科技和了解网络威胁。

（10）新加坡制作网络安全蓝图，2014年将举行防御演习

2013年7月，为应对黑客的袭击，新加坡制定了新的全国网络安全总蓝图。根据新的全国网络安全总蓝图，新加坡2014年将举行首个跨行业抵御网络袭击的演习，演习将着重提升交通、能源、医疗、金融、资讯通信与政府这些关键领域的防御能力。目前，全国通信安全委员会正同新加坡的大学探讨开办有关网络安全的文凭课程，以扩大专业人才的市场。

（11）马来西亚个人数据保护法令生效

2013年11月15日，马来西亚公布了该国的《2010年个人数据保护法令》（PDPA）并已生效，政府将给予公司企业3个月的过渡期以适应新法案的规定。该法律规定，通信、银行及金融机构、保险、医疗保健、旅游及酒店、交通、教育、直销、服务、房地产及公用设施11个在商业交易中使用个人资料的用户，最迟必须在2014年2月15日前注册。逾期者将面临最高约合人民币101.9万元罚款或最高两年监禁。该法案还规定，任何人不可在未经当事人允许的情况下，处理包括当事人的宗教信仰、政治性或



取向、身份证号码、电话号码、薪水单、评估报告等个人资料，规定除非获得当事人同意，否则不能透露其个人资料给第三者。法案包含7个数据保护原则，这些原则将为个人数据提供保护，也为消费者、电子商务、网络及非网络设施从业人员的利益提供保障。随着该法案范围、权利和义务的界定变得清晰，相关法规、准则、行为守则和法院判决更趋标准化，马来西亚的企业组织现在必须重新审视当前的政策、流程、合同权的权利和义务以及涉及个人数据的第三方通知等问题。

(12) 印度武装部队将设立网络司令部

2013年5月，印度国防部长A·K·安东尼表示，作为加强印度网络防务安全的一部分，武装部队将设立网络司令部，并表示网络司令部的成立工作已经处于最后阶段。印度政府以前就有处理网络安全事务的机构，网络司令部的设立是考虑到网络战构成的威胁越来越大，为了保护印度的海陆空安全，需要更好的基础设施和新装备。作为武装部队现代化的一部分，如今正在建设基础设施，而且印度对其国防的信心有了大幅提高。印度军方拥有的资源远远超过过去，而且用于国防现代化的专项资金现已得到充分运用。

(13) 印度计划成立国家网络协调中心，拟监控网络账号

2013年6月，印度政府已开始计划成立由印度国家安全委员会秘书处、情报局、调查分析局、计算机应急响应小组、国家技术研究院、国防研究与发展组织、陆海空三军、电信部等机构组成的国家网络协调中心（NCCC）。该机构将隶属于印度通信与信息技术部，负责网络安全的实时评估，并对威胁行动提供可供执法机构提起诉讼或警告的报告，预计将耗资100亿卢比（约合10.6亿元人民币）。印度政府表示，“在必要时会监视脸谱网或推特账号”。NCCC成立后，会为执法机构提供直接访问所有网络账号的途径，用户的电子邮件、博客或社交网络信息将全面暴露。另据报道，NCCC还将覆盖互联网服务供应商和民间组织，以“确保实时监控网络安全”，该机构将成为印度监视网络威胁的第一道防线。

(14) 以色列启用最新网络防御控制中心

2013年2月，以色列国防军最近正式启用了网络防御控制中心。据参与网络防御的

以色列陆军高层消息透露，以色列国防军的数字化基础设施受到的网络攻击威胁和范围正急剧上升，攻击方包括敌对国家和业余黑客。该控制中心由20名士兵组成，将使陆军能够监视所有的网络攻击企图，并与以色列政府网络防御系统（Tehila）保持密切联系。该中心还将与以色列负责保护国家能源基础设施、金融市场、通信网络和交通运输行业的安全局（Shin Bet）保持联系。该中心将是网络防御的神经中枢，全天不间断运行，以应对全球迅速变化的网络攻击。

9.2.4 澳洲、非洲地区网络安全监管动态

（1）澳大利亚发布首个国家安全战略，将成立国家网络安全中心

2013年1月23日，澳大利亚总理朱莉娅·吉拉德在澳大利亚国立大学发表演讲，公布了澳大利亚首个“国家安全战略”，维护亚太地区的和平稳定将成为澳大利亚在“后9·11”时代的首要安全任务。同时，澳大利亚的战略报告一大重点是将网络安全放到一个空前的战略高度。根据这份报告，网络安全将在未来5年内作为澳大利亚国防、司法和情报机构工作的焦点之一。澳大利亚政府将于2013年内建立一个新的国家网络安全中心，以打击日益增加的网络威胁。这一具有世界级设施的新中心将把目前司法部、国防部、安全情报组织、联邦警察和犯罪委员会下设的网络安全机构全部纳入一套设施之内。该中心将使得澳大利亚具备更加广泛和灵活的应对所有网络问题的能力，并成为私营企业、联邦政府、地方政府及国际合作伙伴开展广泛合作创造机会，全面打击网络威胁，还将为制定预防战略提供咨询和支持。澳大利亚还将推出更为先进的国家宽带网项目（NBN），以防范有政治动机的黑客、犯罪分子和民族主义国家的网络恶意行为者及政府、企业和社区所面临的网络威胁。

（2）新西兰通过电子邮件及电话监听法案

2013年11月，新西兰议会通过《电信截听性能与安全法》（TICS），迫使电信公司允许情报机构获取顾客电子邮件、短信和电话信息。此法案通过后，电信公司建设新基础设施和网络时，必须与电子窃听机构“政府通讯安全局”（GCSB）协商，允许该部门在网络中安装监听装置。该法案或将赋予新西兰政府通讯安全局与英国政府通讯总部和美国国家安全局相同的权力，以及在电信网络设备升级和最新部署方面的



最终话语权。

（3）东非共同体成员国计划在网络安全方面展开合作

肯尼亚通信监管机构肯尼亚通信委员会（CCK）日前称，东非共同体（EAC）的成员国将在网络安全方面展开合作。CCK信息技术主管Michael Katundu在内罗毕举行的区域网络安全论坛上表示，区域合作有助于加强整个东非地区的网络安全。来自肯尼亚、乌干达、坦桑尼亚、布隆迪和卢旺达的超过100名利益相关者参加此次会议，讨论如何打击网络犯罪。CCK正在对肯尼亚国内的电子商务水平进行研究。该研究完成后，该国将成为第一批使用数字证书的非洲国家之一。布隆迪电信管理部门（ARCT）技术主管Jeremy Hageringwe表示，布隆迪将接受国际电信联盟（ITU）的技术援助，根据双方的协议成立计算机事件响应小组（CIRT）。乌干达通信委员会（UCC）的专家表示，乌干达正在成立一支CIRT小组，以应对日益严峻的网络威胁。

10 国内网络安全组织发展情况

10.1 网络安全信息通报成员发展情况

2013年，CNCERT/CC作为通信行业网络安全信息通报中心，积极贯彻落实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》，协调和组织各地通信管理局、中国互联网协会、基础电信企业、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安全企业开展通信行业网络安全信息通报工作。CNCERT/CC及各分中心积极拓展信息通报工作成员单位，并努力规范各通报成员单位报送的数据。

截至2013年12月，全国共有432（2012年是284家）家信息通报工作成员单位，形成较稳定的信息通报工作体系。与2012年相比，新拓展安全企业、增值电信业务企业、域名注册服务机构共163家单位成为信息通报工作成员单位；另外，受部分企业的业务变更等因素影响，无法继续进行网络安全信息报送，共有15家单位退出信息通报工作体系。自2011年1月起，CNCERT/CC建设并启用网络安全协作平台，试行开展电子化信息报送工作。2013年，CNCERT/CC进一步规范信息报送流程，加强管理，保证信息报送工作效率。全国432家信息通报工作成员单位情况见表10-1。

表10-1 通信行业互联网网络安全信息通报工作单位（排名不分先后）

各地通信管理局（31家）	全国31个省、自治区、直辖市通信管理局
基础电信运营企业（123家）	中国电信集团公司及各省分公司、中国联合网络通信集团有限公司及各省分公司、中国移动通信集团公司及各省分公司
域名注册管理和服务机构（18家）	中国互联网络信息中心、政务和公益域名注册管理中心、北京新网互联科技有限公司、北京新网数码信息技术有限公司、北京万网志成科技有限公司、厦门东南融通在线科技有限公司、厦门易名网络科技有限公司、厦门三五互联科技股份有限公司、厦门市纳网科技有限公司、厦门易名网络科技有限公司（北京）、厦门市中资源网络服务有限公司、广东金万邦科技投资有限公司、广东时代互联科技有限公司、广州名扬信息科技有限公司、广东互易科技有限公司、广东今科道同科技有限公司、深圳市万维网信息技术有限公司、杭州创业互联科技有限公司



(续表)

增值电信业务 经营企业 (119家)	263网络通信股份有限公司、深圳市腾讯计算机系统有限公司、世纪互联数据中心有限公司、东北新闻网、广东世纪龙信息科技有限公司、广东天盈信息技术有限公司、广东茂名市群英网络有限公司、广西英拓网络信息技术有限公司、广西博联信息通信技术有限责任公司、杭州阿里巴巴网络有限公司、淘宝网、杭州世导科技有限公司、华数网通信息港有限公司、辽宁鸿联九五信息产业有限公司、山东大众传媒股份有限公司、山东新潮信息技术有限公司、山东维平信息安全测试有限公司、汕头市恒信科技有限公司、深圳市互联时空科技有限公司、厦门蓝芒科技有限公司、厦门数字引擎网络技术有限公司、厦门鑫飞扬信息工程有限公司、厦门翼讯科技有限公司、厦门优通互联科技开发有限公司、泉州商博科技有限公司、泉州市中亿网络科技有限公司、网龙计算机网络技术有限公司、厦门达腾网络科技有限公司、福州哈唐网络科技有限公司、厦门市世纪网通网络服务有限公司、厦门市讯海信息科技有限公司、上海长城宽带网络服务有限公司、上海东方有线网络有限公司、上海科技网络通信有限公司、上海乾万网络科技有限公司、上海世纪互联信息系统有限公司、漳州市比比网络服务有限公司、南昌市秀网信息技术有限公司、南昌天业网络科技有限公司、南昌比翼网络科技有限公司、江西嘉维科技有限公司、江西华邦经济发展有限公司、江西中亚电信技术发展有限公司、南昌利晨科技有限公司、南昌舰网科技有限公司、南昌市恒州科技有限公司、南昌首页科技发展有限公司、南昌引航网络科技有限公司、南昌悦游科技有限公司、萍乡互通信息有限责任公司、南昌艾泰科技有限公司、青岛速科评测实验室有限公司、海南天涯社区网络科技股份有限公司、海南凯迪网络资讯有限公司、海南南海网传媒有限公司、新疆科技网络、长城宽带网络服务有限公司(河北)、广州壹网网络技术有限公司、广州恒汇网络通信有限公司、深圳市容大信息技术有限公司、成都思维世纪科技有限责任公司、郑州紫田网络科技有限公司、河南新飞金信计算机有限公司、河南亿恩科技有限公司、河南电联通信技术有限公司、湖北楚信计算机网络有限责任公司、中电科长江数据股份有限公司、武汉捷讯信息技术有限公司、武汉新软科技有限公司、武汉天楚通信有限公司、武汉华通数码有限公司、东风通信技术有限公司、武汉华通信息产业有限公司、武汉丰网信息技术有限公司、南京太极网络通信有限公司、江西飞天网络科技有限公司、江南都市网、南昌市思锐广告有限公司、大江网、江西人才网、江西中投科信科技有限公司、江西缴费通信技术有限公司、江西金利达电子商务有限公司、江西省国荣医疗信息股份有限公司、江西新华发行集团有限公司、江西省凯恩科技信息有限公司、江西朗博文通信有限公司、江西省天域星空文化传播有限公司、江西洪城信息自动化有限公司、江西大集供应链管理有限公司、江西中投科信科技有限公司、江西省鸿联九五信息产业有限公司、江西嗨喇叭科技有限公司、南昌资博信息科技有限公司、江西省中亚电信技术发展有限公司、江西华科技术开发有限公司、江西星动传媒网络科技有限公司、江西瑞科投资有限公司、南昌市福克斯科技有限公司、南昌市钦永软件开发有限公司、南昌利晨科技有限公司、南昌市万佳通信息服务有限公司、南昌康庄网络科技有限公司、赣州市拓维信息技术有限公司、赣州久易人力资源发展有限公司、江西今视公众信息技术有限公司、景德镇市瓷都晚报新闻发展有限责任公司、南昌秦歌科技有限公司、江西合纵电脑技术应用有限责任公司、江西利德音像书刊发行有限公司、南昌水牛科技发展有限公司、南昌市鹿台信息技术有限责任公司、吉安万吉物流运输有限公司、江西那时快信息技术有限公司、南昌市天业科技有限公司、江西捷信通通信技术有限公司、江西省宇创网络科技开发有限公司、南昌中天飞华通信有限公司、南昌嘉维科技有限公司
-----------------------	--

(续表)

非经营性 互联单位(4家)	中国长城互联网、中国国际电子商务中心(经贸网)、中国教育和科研计算机网、中国科技园
安全企业(132家)	北京安信华科技有限公司、北京安氏领信科技发展有限公司、北京安氏领信科技发展有限公司(新疆)、北京互通网络科技有限公司华南分公司、北京启明星辰信息安全技术有限公司、北京启明星辰信息安全技术有限公司广州分公司、北京启明星辰信息安全技术有限公司黑龙江分公司、北京启明星辰信息安全技术有限公司上海分公司、北京启明星辰信息安全技术有限公司江西分公司、北京启明星辰信息安全技术有限公司新疆分公司、北京瑞星信息技术有限公司、北京瑞星信息技术有限公司(江苏)、北京瑞星信息技术有限公司(上海)、北京瑞星信息技术有限公司(成都)、北京瑞星信息技术有限公司(陕西)、北京神州绿盟科技有限公司、北京神州绿盟科技有限公司江西分公司、北京神州绿盟科技有限公司广州分公司、北京神州绿盟科技有限公司河南办事处、北京神州绿盟科技有限公司上海分公司、北京神州绿盟科技有限公司湖北分公司、北京神州绿盟信息安全科技公司新疆分公司、北京神州绿盟科技有限公司陕西分公司、北京神州绿盟科技有限公司江苏分公司、北京天融信科技有限公司、北京天融信科技有限公司成都分公司、北京天融信科技有限公司广州分公司、北京天融信科技有限公司上海分公司、北京天融信科技有限公司江西分公司、北京天融信科技有限公司郑州分公司、北京天融信科技有限公司沈阳分公司、北京天融信科技有限公司内蒙古分公司、北京天融信网络安全技术有限公司济南分公司、北京天融信网络安全技术有限公司重庆分公司、北京天融信网络安全技术有限公司贵州分公司、北京天融信网络安全技术有限公司甘肃分公司、北京天融信网络安全技术有限公司青海分公司、北京天融信科技网络安全技术有限公司新疆分公司、北京天融信网络安全技术有限公司江苏分公司、北京网秦天下科技有限公司、北京知道创宇信息技术有限公司、北京知道创宇信息技术有限公司(沈阳)、北京知道创宇信息技术有限公司江西分公司、北京知道创宇信息技术有限公司(上海)、北京知道创宇信息技术有限公司(江苏)、东软系统集成工程有限公司、东软系统集成工程有限公司沈阳分公司、东软系统集成工程有限公司(重庆)、广东科达信息技术有限公司、广东蓝盾信息安全技术股份有限公司、广东天讯瑞达通信技术有限公司、广州三零盛安信息安全有限公司、哈尔滨安天信息技术有限公司、哈尔滨安天信息技术有限公司(黑龙江)、哈尔滨安天信息技术有限公司(河北)、哈尔滨安天信息技术有限公司(内蒙古)、哈尔滨安天信息技术有限公司(辽宁)、哈尔滨安天信息技术有限公司(上海)、哈尔滨安天信息技术有限公司(江西)、哈尔滨安天信息技术有限公司(湖北)、哈尔滨安天信息技术有限公司(湖南)、哈尔滨安天科技股份有限公司(重庆)、哈尔滨安天科技股份有限公司(甘肃)、哈尔滨安天科技股份有限公司(贵州)、哈尔滨安天科技股份有限公司(新疆)、哈尔滨安天科技股份有限公司(陕西)、哈尔滨安天科技股份有限公司(江苏)、郑州信大捷安信息技术股份有限公司、河南郑州景安计算机网络技术有限公司、华为技术有限公司、金山网络科技有限公司、浪潮集团有限公司、北京网御星云信息技术有限公司、北京网御星云信息技术有限公司(江西)、奇虎360软件(北京)有限公司、奇虎360软件(北京)有限公司(陕西)、奇虎360软件(北京)有限公司(辽宁)、奇虎360软件(北京)有限公司(上海)、奇虎360软件(北京)有限公司(江苏)、恒安嘉新(北京)科技有限公司、恒安嘉新(北京)科技有限公司(重庆)、恒安嘉新(北京)科技有限公司(山东)、



(续表)

安全企业（132家）	恒安嘉新（北京）科技有限公司（陕西）、恒安嘉新（北京）科技有限公司（新疆）、恒安嘉新（北京）科技有限公司（河北）、恒安嘉新（北京）科技有限公司（内蒙古）、恒安嘉新（北京）、科技有限公司（辽宁）、恒安嘉新（北京）科技有限公司（江苏）、恒安嘉新（北京）科技有限公司（湖北）、青海源创科技有限责任公司、上海三零卫士信息安全有限公司、上海谐润网络信息技术有限公司、上海中科网威信息技术有限公司、上海银基信息安全技术有限公司、上海电信科技发展有限公司、上海金电网安科技有限公司、上海安言信息技术有限公司、深圳安络科技有限公司、深圳任子行网络技术股份有限公司、深圳任子行网络技术股份有限公司（新疆）、深圳任子行网络技术股份有限公司（湖北）、网御神州科技有限公司、福建富士通信息软件有限公司、福建伊时代信息科技股份有限公司、莆田市莆阳网络有限公司、厦门市艾亚网络科技有限公司、厦门百优科技有限公司、厦门乙天科技有限公司、福州创网软件科技有限公司、亚信联创科技(中国)有限公司（新疆）、南京南谷云信息技术有限公司、江苏君立华域信息技术有限公司、南京翰海源信息技术有限公司、江苏天创科技有限公司、南京铭迅信息技术有限公司、贵州亨达信通网络信息安全技术有限公司、中国电信集团系统集成有限责任公司山东分公司、中国电信集团系统集成有限责任公司（新疆）、长沙雨人网络安全技术有限公司、重庆爱思网安信息技术有限公司、重庆远衡科技发展有限公司、深圳市深信服电子科技有限公司（重庆）、深圳市深信服电子科技有限公司（西宁）、深圳市深信服电子科技有限公司（新疆）、江西神州信息安全评估中心有限公司、成都宇扬科技信息技术有限责任公司、杭州迪普科技有限公司（新疆）、杭州迪普科技有限公司（湖北）、杭州安恒信息技术有限公司（湖北）、江苏国瑞信安科技有限公司、趋势科技中国有限公司
其他（5家）	国家计算机网络应急技术处理协调中心、中国互联网协会、新疆大学、上海交通大学信息中心、中国电科院南京分院

10.2 CNVD成员发展情况

CNVD是由CNCERT/CC联合国内重要信息系统单位、基础电信企业、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共享知识库，旨在团结行业和社会的力量，共同开展漏洞信息的收集、汇总、整理和发布工作，建立漏洞统一收集验证、预警发布和应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，有效应对信息安全漏洞带来的网络信息安全威胁。

2013年CNVD全年新增信息安全漏洞7854个，较2012年的6824个增加15.1%，其中高危漏洞2607个，漏洞收录总数和高危漏洞收录数量在国内漏洞库组织中位居前列。全年发布周报50期、月报12期，进行1200余次漏洞分析和验证工作。

2013年，CNVD通过加强与国内外软硬件厂商、安全厂商以及民间漏洞研究者的合作，积极开展漏洞的收录、分析验证和发布工作，协调处置2100余起涉及国内政府机构、重要信息系统部门、电信行业和教育机构的漏洞事件，有力地支撑国家网络信息安全监管工作。CNVD在工作中与超过300家国内应用软件生产厂商以及企事业单位建立处置联系，并与超过500位白帽子建立协作关系，漏洞和补丁信息的报送、验证、发布等工作机制持续运转，提高了漏洞预警能力和修复速度。2013年，针对电信、工业控制、移动互联网等特定行业领域，CNVD依据资产关联和技术分析，建立并开放了电信、工业控制系统、移动互联网三个行业漏洞库。为进一步提升漏洞信息共享，CNVD向成员单位开放漏洞信息同步、资产关联等数据接口应用。

截至2013年12月月底，CNVD平台体系的成员单位情况见表10-2。

表10-2 CNVD成员单位（排名不分先后）

CNVD工作委员会（8家）	国家互联网应急中心 国家信息技术安全研究中心 北京神州绿盟科技有限公司 北京启明星辰信息安全技术有限公司 沈阳东软系统集成工程有限公司 奇虎360软件（北京）有限公司 恒安嘉新（北京）科技有限公司 北京安氏领信科技发展有限公司
CNVD技术合作单位（10家）	北京信息安全测评中心 北京天融信科技有限公司 北京网御星云信息技术有限公司 北京安天电子设备有限公司 北京焜安信息技术有限公司 北京知道创宇信息技术有限公司 华为技术有限公司 深圳市腾讯计算机系统有限公司 北京暴风网际科技有限公司 看雪安全网站 杭州安恒信息技术有限公司



(续表)

CNVD用户支持组（8家）	中国工程物理研究院计算机应用研究所 百度在线网络技术（北京）有限公司 新浪网技术（中国）有限公司 北京搜狐互联网信息服务有限公司 网之易信息技术（北京）有限公司 上海盛大网络发展有限公司 北京雷霆万钧网络科技有限责任公司 上海巨人网络科技有限公司
---------------	--

10.3 ANVA成员发展情况

2009年7月，中国互联网协会网络与信息安全工作委员会发起成立中国反网络病毒联盟ANVA，由CNCERT/CC负责具体运营管理。联盟旨在广泛联合基础电信企业、互联网内容和服务提供商、网络安全企业等行业机构，积极动员社会力量，通过行业自律机制共同开展互联网网络病毒信息收集、样本分析、技术交流、防范治理、宣传教育等工作，以净化公共互联网网络环境，提升互联网网络安全水平。

2013年移动应用程序在数量上继续呈现爆炸性增长，特别是Android平台应用长尾效应逐步凸显，长尾中的移动应用良莠不齐，大部分移动应用处于灰色地带；对正版应用进行二次打包的仿冒应用，用户难以辨别正版应用和仿冒应用，导致正版应用淹没在大量的仿冒应用中，使得用户难以安装正版的移动应用，“劣币驱逐良币”效应明显。基于传统“黑名单”的防护方式，已经不能满足用户进行移动安全信息消费的需要。

另外，2013年移动互联网恶意程序增速3.3倍，继续呈现爆发式增长趋势，使移动安全面临严峻的挑战。特别是以“手机预装马”为代表的恶意程序，具有很强的隐蔽性，使得手机安全软件无法及时辨别。目前大多数手机安全软件都是基于“黑名单”机制来查杀移动恶意程序，但是“黑名单”机制是基于已知恶意程序建立的，无法对新出现的恶意程序进行及时识别，因此当CNCERT/CC发现“手机预装马”后，测试主流手机安全软件均无法识别“手机预装马”，这也是造成“手机预装马”感染200

多万用户的一个主要原因。

由于传统“黑名单”方式在保护优质移动应用、打击恶意应用这两方面都存在越来越多的局限性，仅仅依靠“黑名单”方式已经难以适应当前移动互联网环境治理的需要。为营造健康的移动互联网生态系统，有效解决目前“黑名单”机制的局限性，中国反网络病毒联盟ANVA于2013年8月推行“移动互联网应用自律白名单”，帮助应用商店标示白应用，帮助开发者推广白应用，帮助用户选择白应用，通过建立可信的“白名单”保护正版的优质应用，同时防止“未知”移动恶意程序的入侵。

由于移动互联网企业发布应用程序所使用的数字证书具备相对固定和不易伪造的特点，ANVA采用数字证书作为“白名单”的实体。如果一家移动互联网企业成功申请将本企业数字证书加入“白名单”，则该企业出品的带有该证书的所有移动互联网应用均被ANVA认定为安全可信的“白应用”。

2013年，为应对日益严峻的移动互联网网络安全威胁，ANVA扩充移动互联网领域的工作体系，积极吸纳安全管家、赛门铁克等移动互联网安全企业加入联盟，组织23家国内主流的应用商店成立ANVA应用商店自律组，并大力开展“移动互联网应用自律白名单”工作，成立了由11家安全企业组成的白名单工作组。2013年共新增6家企业，截至2013年12月，ANVA联盟成员单位数量已达37家，成员单位情况见表10-3。

表10-3 ANVA成员单位（排名不分先后）

国家互联网应急中心
中国电信集团公司
中国移动通信集团公司
中国联合网络通信集团有限公司
中国互联网络信息中心
中国软件测评中心
北京百度网讯科技有限公司
深圳市腾讯计算机系统有限公司
北京启明星辰信息安全技术有限公司
北京神州绿盟科技有限公司
奇虎360软件(北京)有限公司
阿里巴巴（中国）有限公司
金山网络科技有限公司
北京江民新科技术有限公司
北京搜狐互联网信息服务有限公司



(续表)

新浪网技术（中国）有限公司
网之易信息技术（北京）有限公司
北京万网志成科技有限公司
北京世纪互联宽带数据中心有限公司
北京天融信科技有限公司
北京瑞星信息技术有限公司
哈尔滨安天科技股份有限公司
北京网秦天下科技有限公司
华为技术有限公司
西门子（中国）有限公司
优视科技有限公司
北京西塔网络科技股份有限公司
北京知道创宇信息技术有限公司
北京洋浦伟业科技发展有限公司
趋势科技（中国）有限公司
恒安嘉新（北京）科技有限公司
北京联想软件有限公司
北京安管佳科技有限公司
赛门铁克软件（北京）有限公司
深圳市深信服电子科技有限公司
招商银行
卓望公司

10.4 CNCERT/CC应急服务支撑单位

互联网作为重要信息基础设施，社会功能日益增强，但由于本身的开放性和复杂性，互联网面临巨大的安全风险，因此面向公共互联网的应急处置工作逐步成为公共应急服务事业的重要组成部分，建立高效的公共互联网应急体系和强大的人才队伍，对及时有效地应对互联网突发事件有着重要意义。

为拓宽掌握互联网宏观网络安全状况和网络安全事件信息的渠道，增强对重大突发网络安全事件的应对能力，强化公共互联网网络安全应急技术体系建设，促进互联网网络安全应急服务的规范化和本地化，经工业和信息化部批准，2004年CNCERT/CC首次面向社会公开选拔一批国家级、省级公共互联网应急服务试点单位，随后在

2007年、2009年、2011年，CNCERT/CC分别举办第二届、第三届和第四届评选评审会。经过多年发展，应急服务支撑单位已成为我国公共互联网网络安全应急体系的重要组成部分，为维护我国互联网网络安全做出积极贡献，在国家重大活动期间为保障网络安全发挥重要的技术支撑作用。

2013年5月，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/CC启动第五届CNCERT/CC网络安全应急服务支撑单位评选工作。评选公告发布后，受到通信行业和网络安全服务行业相关单位的大力支持和积极响应，申请单位数量较往年有较大幅度增长，涌现出一些新生的应急响应服务力量。经过两轮细致评估和审查，最终评选出8个国家级和37个省级网络安全应急服务支撑单位。评选工作有效促进各单位间的了解和沟通，增强各单位的竞争和服务意识，推动我国网络安全服务行业和公共互联网网络安全应急技术体系的发展。

第五届CNCERT/CC网络安全应急服务支撑单位见表10-4，所列单位享有该称号的有效时限为2013年7月3日至2015年7月3日。

表10-4 CNCERT/CC应急服务支撑单位（排名不分先后）

单位名称	级别	证书编号
北京启明星辰信息安全技术有限公司	国家级	CNCERT-2013-150703GJ001
哈尔滨安天科技股份有限公司	国家级	CNCERT-2013-150703GJ002
北京神州绿盟科技有限公司	国家级	CNCERT-2013-150703GJ003
恒安嘉新（北京）科技有限公司	国家级	CNCERT-2013-150703GJ004
沈阳东软系统集成工程有限公司	国家级	CNCERT-2013-150703GJ005
北京奇虎科技有限公司	国家级	CNCERT-2013-150703GJ006
北京天融信网络安全技术有限公司	国家级	CNCERT-2013-150703GJ007
中国电信集团系统集成有限责任公司	国家级	CNCERT-2013-150703GJ008
北京互联互通网络科技有限公司	省级	CNCERT-2013-150703SJ001
北京网秦天下科技有限公司	省级	CNCERT-2013-150703SJ002
北京知道创宇信息技术有限公司	省级	CNCERT-2013-150703SJ003
成都思维世纪科技有限责任公司	省级	CNCERT-2013-150703SJ004
四川无声信息技术有限公司 ^[17]	省级	CNCERT-2013-150703SJ005
成都宇扬科技信息技术有限责任公司	省级	CNCERT-2013-150703SJ006
福建富士通信息软件有限公司	省级	CNCERT-2013-150703SJ007

[17] 原成都天融信网络安全技术有限公司，2013年9月16日更名为四川无声信息技术有限公司。



(续表)

单位名称	级别	证书编号
福建网龙计算机网络信息技术有限公司	省级	CNCERT-2013-150703SJ008
福建伊时代信息科技股份有限公司	省级	CNCERT-2013-150703SJ009
广东天盈信息技术有限公司	省级	CNCERT-2013-150703SJ010
贵州亨达信通科技有限公司	省级	CNCERT-2013-150703SJ011
杭州安恒信息技术有限公司	省级	CNCERT-2013-150703SJ012
杭州杨立网络科技有限公司	省级	CNCERT-2013-150703SJ013
杭州思福迪信息技术有限公司	省级	CNCERT-2013-150703SJ014
江苏国瑞信安科技有限公司	省级	CNCERT-2013-150703SJ015
江苏天创科技有限公司	省级	CNCERT-2013-150703SJ016
蓝盾信息安全技术股份有限公司	省级	CNCERT-2013-150703SJ017
南京翰海源信息技术有限公司	省级	CNCERT-2013-150703SJ018
南京南谷云信息技术有限公司	省级	CNCERT-2013-150703SJ019
南京钛迅信息技术有限公司	省级	CNCERT-2013-150703SJ020
青岛速科评测实验室有限公司	省级	CNCERT-2013-150703SJ021
任子行网络技术股份有限公司	省级	CNCERT-2013-150703SJ022
山东维平信息安全测评技术有限公司	省级	CNCERT-2013-150703SJ023
山东新潮信息技术有限公司	省级	CNCERT-2013-150703SJ024
上海金电网安科技有限公司	省级	CNCERT-2013-150703SJ025
上海谐润网络信息技术有限公司	省级	CNCERT-2013-150703SJ026
上海银基信息安全技术有限公司	省级	CNCERT-2013-150703SJ027
上海中科网威信息技术有限公司	省级	CNCERT-2013-150703SJ028
深圳市深信服电子科技有限公司	省级	CNCERT-2013-150703SJ029
太原理工天成电子信息技术有限公司	省级	CNCERT-2013-150703SJ030
天讯瑞达通信技术有限公司	省级	CNCERT-2013-150703SJ031
长沙雨人网络安全技术有限公司	省级	CNCERT-2013-150703SJ032
郑州市景安计算机网络技术有限公司	省级	CNCERT-2013-150703SJ033
郑州信大捷安信息技术股份有限公司	省级	CNCERT-2013-150703SJ034
中国移动通信集团辽宁有限公司	省级	CNCERT-2013-150703SJ035
重庆爱思网安信息技术有限公司	省级	CNCERT-2013-150703SJ036
重庆远衡科技发展有限公司	省级	CNCERT-2013-150703SJ037

11 国内外网络安全重要活动

11.1 国内重要网络安全会议和活动

(1) CNCERT/CC发布《2012年我国互联网网络安全态势综述》

2013年3月19日，CNCERT/CC在京举办了“2012年我国互联网网络安全态势综述”（简称“态势综述”）发布会，对2012年我国互联网网络安全总体态势和主要特点进行发布和说明。来自重要信息系统运行部门、基础电信企业、域名注册管理和服务机构、行业协会、互联网企业和网络安全厂商等73家单位的97位专家和代表出席发布会。CNCERT/CC运行部有关同志对态势综述做了详细阐述和讲解，并回答了媒体提问。

态势综述从CNCERT/CC视角出发，结合CNCERT/CC监测数据和通信行业报送信息，经归纳分析后，总结概括2012年我国互联网网络安全威胁的新特点、新趋势，介绍CNCERT/CC在维护网络安全方面开展的相关工作，展望2013年值得关注的网络安全威胁和热点问题，提出若干对策建议。态势综述主要依据CNCERT/CC及通信行业相关单位在日常工作中积累的数据和资料编撰而成，具有较鲜明的行业特色和技术特点。

(2) 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，由CNCERT/CC主办的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5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。

中国计算机网络安全年会历经10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400余人参加了本次会议。

(3) 45家单位荣获第五届CNCERT/CC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/CC于2013年5月启动第五届CNCERT/CC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/CC在内蒙古自治区呼和浩特市举行了第五届CNCERT/CC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/CC、国家网络安全技术研究所的相关专家组成评选委员会，从企业实力、应急技术能力、应急服务规范、支撑CNCERT/CC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/CC自2004年开始启动“CNCERT/CC网络安全应急服务支撑单位”的选拔工作。经过9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积极贡献，在国家重大活动期间为保障网络安全发挥重要的技术支撑作用。

（4）2013（第十二届）中国互联网大会在京召开

由工业和信息化部、国家互联网信息办公室等单位指导，中国互联网协会主办的2013（第十二届）中国互联网大会8月13日在北京国际会议中心隆重开幕。本届大会主题为“共建良好生态环境，服务美好网络生活”。工业和信息化部副部长尚冰出席大会开幕式并在主旨报告中指出，随着移动互联网、大数据、云计算、物联网的加速发展，我国互联网行业呈现出一些新的特点：移动互联网高速普及，网络应用更加多元化，网络带动信息消费强劲增长，下一代互联网建设取得积极进展。作为行业主管部门，工业和信息化部将着眼我国经济结构调整和转型升级的大局，一如既往地推动我国互联网企业加快发展和行业整体水平的提高做好服务。同时也要不断加强行业管理和网络信息安全工作，为企业营造良好的外部环境。就互联网行业当前和未来的发展，尚冰提出：一要进一步完善信息基础设施，加快推动互联网技术业务的创新和应用；二要加强市场监管和行业自律，共建和谐健康的互联网行业生态，进一步健全和完善政府部门、企业、行业组织等相关各方各司其职、各负其责，共同参与的互联网治理体系，努力为互联网发展创造公平公正、有序有效的市场环境；三要全力保障网络与信息安全，服务美好网络生活，要从战略和全局的高度重视网络与信息安全，共同构建安全可信的网络环境，为行业持续、健康发展和广大网民享受美好的网络生活提供坚实的保障。

（5）ANVA召开中国互联网协会反网络病毒联盟大会

2013年9月27日，ANVA在中国国际科技会展中心隆重召开联盟大会，来自网络安全企业、移动互联网应用厂商的30余家相关单位出席此次大会。大会介绍了构建移动互联网良性生态环境的关键要素“白名单”。建立“白名单”旨在对移动互联网企业进行可信认证，并对APP开发者、安全软件和应用商店三个关键环节进行约束，推动打造良性的移动互联网产业链条。大会公布申请ANVA移动互联网“白名单”的准入机制和审核办法。同时会上还成立ANVA应用商店自律组和移动互联网应用自律白名单工作组，并举行签约仪式。



11.2 国际重要网络安全会议和活动

(1) APCERT举办2013年网络安全应急演练

2013年1月29日，国家计算机网络应急技术处理协调中心（CNCERT/CC）参加了由亚太计算机网络应急组织联盟（APCERT）发起举办的2013年亚太地区网络安全应急演练，并作为核心组成员圆满完成各项演练任务。本次演练旨在检验亚太地区的计算机安全事件应急响应组织（CSIRT）协作应对和处理大规模拒绝服务攻击事件的能力。共有来自22个国家和地区的26个应急响应组织参加了此次演练，其中包括CNCERT、HKCERT、JPCERT、KrCERT等22个APCERT成员，以及埃及、巴基斯坦、阿曼、突尼斯4个伊斯兰计算机应急响应合作组织(OIC-CERT)成员。这是自2011年签订合作备忘录以来，伊斯兰计算机应急响应合作组织(OIC-CERT)第二次参加APCERT网络安全应急演练。此次应急演练是CNCERT/CC自2004年以来连续第10年参加APCERT网络安全应急演练。

(2) FIRST论坛主题锁定网络安全与国际协作

2013年6月16-21日在泰国曼谷举行的第25届“事件响应与安全组织论坛（FIRST）”主题锁定为网络安全与国际协作。来自全球各国的网络安全领域专家和网络公司代表就网络参与者所面临的风险以及打击网络犯罪最新技术等议题进行探讨。泰国总理英拉6月17日在论坛发表讲话。前来参加会议的中国国家网络信息安全技术研究所所长杜跃进认为，为应对与日俱增的网络安全隐患，各国专家如果在技术领域加强合作则能达到事半功倍的效果；在政府层面，各国需要加强彼此信任，共同分享案例及经验；在运行层面，很多网络犯罪都是跨境事件，需要不同组织之间合作，这次论坛还对国际组织间如何开展合作进行探讨。除加强国际协作外，杜跃进认为世界各国还面临法律体系不适应的问题，加快完善法律体系对保障网络信息安全十分重要，此外，每个网络参与者都应增强防范意识。例如，不用公共计算机登录网上银行，社交网站账号要设置密码，注意在网络上保护个人隐私等，尽量减少网络安全隐患。

(3) 中美网络工作组在美举行首次会议

2013年7月8日，中美网络工作组会议在华盛顿举行，这是中美网络工作组设立后

的首次会议。中方外交部、国防部、公安部、工业和信息化部、商务部、国务院新闻办公室和美国国务院、国防部、国土安全部、司法部、财政部、商务部、联邦调查局及总统国家安全事务委员会等部门官员参加了本次会议。会上，中美双方分别提出各自对网络安全问题的担忧，并就网络工作组机制建设、两国网络关系、网络空间国际规则等问题进行坦诚、深入交流，建设性地提出一些合作倡议。双方同意2013年内再举行一次网络工作组会间会。

(4) CNCERT/CC组织召开第一届中日韩互联网应急年会

2013年7月30-31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，召开第一届中日韩互联网应急年会。会上，回顾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/CC、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他重大网络安全事件，并遏制危机蔓延。三方7×24h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，其他地区（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，继续为降低地区网络安全风险做出贡献。

(5) 第五届中英互联网圆桌会议在伦敦举行

第五届中英互联网圆桌会议2013年9月9日在英国伦敦举行，中国国家互联网信息办公室主任鲁炜，英国文化、媒体和体育部部长艾德·韦泽出席会议并代表中英双方作主旨演讲。中英两国政府部门、行业组织、知名互联网企业和学术机构的100多名代表，围绕“数字技术促进发展”、“互联网的社会责任”、“物联网——推动商业发展和市民生活”、“无障碍应用技术”等议题进行对话交流。鲁炜在题为“网络空间的自由与秩序”的主旨演讲中，对互联网自由与秩序的关系作了深入阐述。就中英双



方加强交流合作提出五点建议。第一，构建常态化交流机制；第二，构建协同创新机制；第三，构建研究磋商机制；第四，构建网络安全合作机制；第五，构建网络信息共享机制。艾德·韦泽在主旨演讲中，介绍英国在互联网领域加强基础设施建设、保护青少年合法权益、打击网络犯罪、推广应用物联网等方面的情况，提出希望通过互联网进一步加深中英双方的沟通合作，加深彼此间对互联网的共识理解，鼓励两国公司加大投资力度，共同推动社会进步。中英互联网圆桌会议由中国国家互联网信息办公室与英国文化、媒体和体育部联合主办，自2008年以来已连续举办5届，对促进两国政府和业界在互联网领域的交流合作发挥了积极作用。

（6）东盟地区论坛2013年网络安全研讨会在京召开

2013年9月11日，东盟地区论坛（ARF）2013年网络安全研讨会在北京召开，20个东盟地区论坛成员、联合国毒品和犯罪问题办公室、亚太安全理事会代表出席本次论坛，共同推动东盟地区论坛在网络问题的对话与合作方面继续发挥积极影响。本次研讨会由中国和马来西亚联合举办，主题是“AFR加强网络安全措施研讨会——法律和文化视角”，具体包括5项议题：网络安全国家和地区实践的最新发展、网络安全能力建设、网络安全的文化范畴、打击网络犯罪地区合作和国家在网络空间中的作用。中国外交部部长助理郑泽光在开幕致词中表示，互联网发展至今日，更需要法律规则的引领，法治应成为加强网络治理，促进网络安全的基本方式。中国愿和有关各方，尤其是本地区各国加强网络安全领域的对话交流，增进互信，促进合作，共同构建和平、安全、开放、合作的网络空间。马来西亚国家安全理事会秘书长默罕默德·达祖丁表示，网络发展不仅为全球化带来新的机遇，同时也有挑战。当今网络的飞速发展给国家和社会安全带来威胁，这将是我們急需正视的问题。他表示，相信通过交流互信和合作，与会各方将就共同应对网络安全出谋划策，达成共识。本次研讨会为期两天，这也是中方首次举办东盟地区论坛框架下的网络安全研讨会。

（7）CNCERT/CC参加东盟地区年度应急演练

2013年10月9日，CNCERT/CC参加了第八届东盟地区网络安全应急演练。参加本次演练的CERT组织来自东盟成员国及其对话伙伴国等13个国家，包括澳大利亚CERT Australia和AUSCERT、文莱BruCERT、柬埔寨CamCERT、中国CNCERT/CC、印度

CERT-In、印度尼西亚ID-SIRTII、日本JPCERT、马来西亚MyCERT和MCMC、缅甸mmCERT、挪威NorCERT、新加坡SingCERT和SAFCERT、泰国ThaiCERT和越南VNCERT共16个组织。

本次演练模拟一个公司遭受网络攻击后，CERT组织协助开展恶意代码分析，提取恶意代码特征，阻止恶意代码进一步感染和扩散，有效应对网络攻击。各CERT组织按照自身事件处理流程，对接收到的投诉事件进行调查分析和应急处置，完成恶意代码和攻击源分析以及事件的应急处理，并提交详细的恶意代码分析报告。演练有效检验和提升各国CERT组织的网络安全事件处置能力和协同配合能力。

（8）第五届中国-东盟网络安全研讨会在成都召开

2013年10月15-17日，由工业和信息化部国际合作司主办，CNCERT/CC承办的第五届中国-东盟网络安全研讨会在中国成都召开。来自文莱、柬埔寨、印度尼西亚、老挝、马来西亚、菲律宾、泰国、越南8个国家的电信政府部门和网络安全应急组织代表出席本次会议。各方在会议上充分交流各自在互联网网络安全领域的发展状况、技术情况和管理经验，并就如何进一步扩展和深化合作，增强信任关系和互助，制订详细的实施计划。会议期间，CNCERT/CC还面向东盟参会代表开展网络安全调查和取证技术培训，东盟代表希望中方能进一步为东盟各国开展有针对性的网络安全技术培训。本次中国-东盟网络安全研讨和培训为双方交流学习、增进信任、开展务实合作，以及提高网络安全相关技术水平提供良好的平台。

（9）中美网络反黑客攻击报告在全球网络空间合作峰会上发布

2013年11月5日，在美国斯坦福大学举行的“第四届世界网络安全峰会”上，中国互联网协会网络与信息安全工作委员会秘书长周勇林与美国东西方研究所高级技术总监卡尔·劳舍尔（Karl Rauscher）共同发布了《真诚沟通务实合作，共同抵制黑客攻击活动》的报告，该报告是中国互联网协会与美国东西方研究所开展的“中美网络安全对话”项目的重要成果文件，中美双方超过100名专家参与了该项目的研究，对当前网络空间安全趋势、中美网络安全合作中的问题进行冷静的思考和坦诚的沟通，进而就如何加强中美网络安全互信、如何开展务实合作共同提升网络空间安全提出具体的、务实的建议。



（10）金砖国家安全事务高级代表第四次会议在南非召开

中国国务委员杨洁篪2013年12月6日在南非开普敦出席金砖国家安全事务高级代表第四次会议时指出，网络和信息安全事关国家安全和社会稳定，是国际社会面临的新的综合性挑战，金砖国家应该共同倡导信息安全理念。杨洁篪指出，一是相互信任，维护网络空间和平稳定，坚持以协商方式解决网络争端；二是坚持安全互利，尊重各国主权安全利益，不以任何方式破坏别国政治、经济、社会和文化环境；三是促进平等共治，确保网络公平开放，各国有权平等参与网络空间国际秩序与规则建设，在联合国框架下建立公平、民主、透明的互联网国际治理机制；四是加强国际协作，实现“数字共赢”，各国应该加强信息共享和技术交流，向发展中国家加大“数字援助”力度。杨洁篪建议，金砖国家加强网络安全合作，建立对话交流平台，探讨更加紧密的机制化安排，共同引导国际规则制定进程，支持中俄等已提出的“信息安全国际行为准则”倡议。

（11）中韩互联网圆桌会议在韩举行聚焦网络安全

2013年12月10日，中韩互联网圆桌会议在韩国首尔举行。会议以“发展与安全”为主题，中韩两国政府部门、行业组织、知名互联网企业和学术机构近百位代表参加会议。在维护互联网安全的具体举措方面，中方代表重点强调以下4个方面：一是共同维护网络主权安全，将互联网纳入到联合国多边治理框架下，构建和平共处、互利共赢的网络主权安全新秩序；二是共同维护信息安全，加强网络信息安全合作，打击网络不法行为，让信息安全有序流动；三是共同维护隐私安全，加大个人信息保护力度；四是共同维护技术安全，希望加强与韩方合作，推动核心技术、关键设备、移动终端等方面攻关，为互联网保驾护航。韩国未来创造科学部长官崔文基表示，互联网已经成为世界经济发展的强力引擎，对建立智能社会和传播优秀文化产生巨大的积极影响。同时，互联网也带来挑战，如个人信息泄露、网络犯罪等，迫切需要中韩加强合作，共同应对难题。

1.2 2014年网络安全热点问题

2014年，我国互联网面临的安全形势将更为复杂，值得关注的热点问题如下。

（1）设备智能化促使网络安全威胁向物联网延伸。随着工业控制系统、医疗器械、办公及家用设备的逐步智能化，物联网产业蓬勃发展，然而，新兴技术发展的不完善和对网络安全问题的忽视，往往导致智能设备设计存在漏洞缺陷。黑客利用这些漏洞可以轻易实施网络攻击。2013年，美国“黑帽子”大会展示10多项针对电网、智能家居、汽车等控制系统智能设备的攻击或监控技术，同时出现大规模“冰箱僵尸网络”等针对智能家电的恶意攻击事件，表明针对物联网中智能设备的攻击技术已取得突破。此外，由于安卓系统已成为智能设备的主流平台，针对安卓系统的攻击威胁会迅速从移动互联网辐射至物联网。2014年，物联网的脆弱性将伴随其应用和发展而更加凸显。

（2）社交网络成为黑客攻击和网络犯罪的新途径。实施网络攻击的重要手段之一，便是利用社会工程学（社工库），而逐渐深入人们生活的社交网络，成为黑客实施社会工程攻击的“温床”。由于大多数社交网络基于人与人之间的信任关系构成，包含的信息内容和用户生活密切相关，带有很强的真实性。黑客通过社交网络广泛收集、挖掘用户个人信息，形成社工库，并基于用户网络习惯实施高效的定向攻击，散播恶意程序、钓鱼欺诈信息等，命中率极高。受经济利益驱使，2014年基于社交网络的恶意程序攻击将增多，甚至可能出现利用社交网络发布命令、实施控制的新型僵尸网络，社交网络免费开放的第三方应用接口将成为黑客进行违法犯罪活动的突破口。

（3）云平台的应用普及加大信息泄露风险和事件处置难度。随着云平台的应用普及和大数据技术的发展，涵盖互联网行业、金融服务业、医疗保健业、制造业的大量行业数据快速增长，越来越多的用户数据从个人电脑转向云平台。一方面，集成大量同类数据的云端如同“地下宝藏”，吸引攻击者的目光，其一旦发生信息泄露，将对整个行业造成影响。另一方面，由于云平台使用方便、成本低廉，黑客将大量利用云平台进行钓鱼网站部署、恶意程序传播控制和网络攻击跳板，而云平台的使用给传



统基于IP地址的追踪溯源带来困难，事件处置难度进而增大。

(4) 实施APT攻击的手段将更加多维化。随着网络空间对抗的日益加剧，APT攻击以其精准高效的特点，将成为黑客组织乃至国家间网络对抗的主要方式。APT攻击将综合运用多种技术手段协作互补，形成一体化监视和攻击体系，除传统的恶意程序、软硬件漏洞等技术外，还包括多种新型的手段和技术。2013年12月30日，斯诺登披露美国国家安全局研制出数十种间谍工具，包括通过直接将后门嵌入主板、硬盘驱动器、SIM卡等硬件设备，实现物理入侵；将后门植入固件以保障攻击连续性，避免受到更换系统平台、升级系统和程序、安装查杀软件的影响；通过无线射频技术破解传统局域网的物理隔离问题，实现远距离隔空攻击等。这些手段将提高APT攻击渗透的广度和深度，增强间谍行动的隐蔽性和可持续性，对APT攻击检测能力提出更高要求。

(5) 移动支付安全和移动终端漏洞成为移动互联网发展的新挑战。2014年，随着4G网络的大面积商用、移动互联网带宽的提速和Wi-Fi热点普及，智能手机和移动应用在日常生活中日益普及，人们将更习惯使用移动支付方式，这将进一步推动各类金融、证券、电商等移动应用的普及。受经济利益驱使，黑客将更多地把移动互联网作为主阵地，这将导致针对移动互联网应用的仿冒APP和恶意插件增多，并可能引发更多移动互联网经济犯罪事件。此外，针对智能终端设备硬件、操作系统、应用程序等的安全漏洞挖掘将增多，移动互联网零日漏洞数量将迅速增长，这将导致针对移动互联网和智能终端的攻击增多。大量智能终端设备通过家用无线路由器、公用Wi-Fi等接入互联网，但路由器后门、通过公用Wi-Fi进行网络劫持和网络钓鱼等事件的曝光，暴露出诸多安全隐患，这将加深移动互联网面临的攻击威胁。

(6) 分布式反射拒绝服务攻击规模呈持续增大趋势。2014年，依靠僵尸网络和带宽构造大规模攻击流量的传统方式已无法达到预想的攻击效果，黑客将更多地运用DNS、NTP (Network Time Protocol, 网络时钟协议) 和CHARGEN (Character Generator Protocol, 字符发生器协议) 等进行分布式反射放大拒绝服务攻击，能轻易把攻击流量放大几十倍到几百倍，耗尽有限的服务器、路由器和带宽资源，隐藏攻击僵尸主机IP地址的攻击方式给追踪溯源带来难度。此外，攻击者还将不断寻找更多类似的新技术手段，以最小代价实现攻击流量的放大，增加攻击威力，实现“借刀杀

人”的目的，使拒绝服务攻击与防护的对抗进一步激烈。

（7）微软停止对Windows XP系统的服务支持可能导致零日漏洞攻击增多。2014年4月8日，微软将正式停止对Windows XP系统的技术支持与更新，不再提供对该操作系统的安全补丁、升级、杀毒软件更新以及其他相关服务，这意味着此后针对该系统的病毒与漏洞攻击，微软将不再负责。由于Windows XP系统市场占有份额高，据统计在我国安装和使用该系统的计算机将近2亿台，一旦停止系统支持与更新，这些计算机将面临严重安全风险，黑客可能会加强对该系统的零日漏洞挖掘，用于对高价值目标计算机攻击或控制，造成信息泄露、系统瘫痪、经济损失等严重后果。

（8）传统短信验证和新兴二维码扫描方式背后均面临安全风险。当前进行网购和网络支付时经常会用到短信验证码。2014年通过手机木马劫持支付验证码短信，窃取用户账户信息的活动将呈高发态势。黑客利用手机木马拦截验证码短信，并进一步套取用户网络支付账号和密码，使得用户的个人财产面临巨大损失。此外，随着二维码的日益普遍使用，由于隐蔽性高，制作成本低，二维码背后未经安全认证的网站链接和应用程序逐步成为黑客的青睐对象。缺乏安全意识的手机用户在扫描来历不明或无法确认安全性的二维码后，进入黑客预先埋伏的网站链接或下载应用程序，导致手机被植入病毒或恶意插件，造成个人信息泄露和经济损失。



13 网络安全术语解释

- 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。对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程序。由于它像间谍一样潜入用户的计算机，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^[18]、网银木马^[19]、窃密木马^[20]、远程控制木马^[21]、流量劫持木马^[22]、下载者木马^[23]和其他木马7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程序。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僵尸程序和其他僵尸程序4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程序。按照传播途径，蠕虫可进一步分为邮件蠕虫、即时消息蠕虫、U盘蠕虫、漏洞利

[18] 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。

[19] 网银木马是用于窃取用户网银、证券等账号的木马。

[20] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。

[21] 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。

[22] 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。

[23] 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。

用蠕虫和其他蠕虫5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程序。

⑤其他

上述分类未包含的其他恶意程序。

随着黑客地下产业链的发展，互联网上出现的一些恶意程序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，我们按照恶意程序的主要用途并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（如银行账号和账户密码）。

- 网页挂马

网页挂马是通过在网页中嵌入恶意程序或链接，致使用户计算机在访问该页面时触发执行恶意脚本，从而在不知情的情况下跳转至“放马站点”（指存放恶意程序的网络地址，可以为域名，也可以直接使用IP地址），下载并执行恶意程序。



- 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：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；收件人无法拒收的电子邮件；隐藏发件人身份、地址、标题等信息的电子邮件；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，黑客通过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。

- 移动互联网恶意程序

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。按照行为属性分类，移动互联网恶意程序包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为8种类型。

感谢您阅读CNCERT/CC《2013年中国互联网网络安全报告》，如果您发现本报告存在任何问题，请您及时与我们联系，电子邮件为cncert@cert.org.cn。

对此我们深表感谢。

国家互联网应急中心