2014年
中国互联网网络安全报告

国家计算机网络应急技术处理协调中心 著

CNCERT/CC

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

2014年
中国互联网网络安全报告

国家计算机网络应急技术处理协调中心 著

CNCERT/CC

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

2014年中国互联网网络安全报告 / 国家计算机网络应急技术处理协调中心著. -- 北京 : 人民邮电出版社, 2015.6
ISBN 978-7-115-39215-2

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2014 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2015)第091913号

内 容 提 要

本书是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）发布的2014年中国互联网网络安全年报。本书汇总分析了国家互联网应急中心自有网络安全监测结果和通信行业、网络安全企业相关单位报送的大量数据，具有鲜明的行业特色。报告涵盖了我国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，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、网络安全信息通报等情况进行深入细致的分析。

本书的内容依托国家互联网应急中心多年来从事网络安全监测、预警和应急处置等工作的实际情况，是对我国互联网网络安全状况的总体判断和趋势分析，可以为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，提高全社会、全民的网络安全意识。

2014年中国互联网网络安全报告

◆ 著　　国家计算机网络应急技术处理协调中心
责任编辑　牛晓敏

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京光之彩印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：12　　2015年5月第1版
字数：130千字　　2015年5月北京第1次印刷
ISBN 978-7-115-39215-2

定价：59.00元

读者服务热线：（010）81055488　**印装质量热线：**（010）81055316
反盗版热线：（010）81055315

《2014 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	严寒冰　李　佳　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
	李　挺　陈　阳　李世淙
	党向磊　徐晓燕　王适文
	刘　婧　饶　毓　赵　宸
	肖崇蕙　张　帅　贾子骁
	摆　亮

PREFACE
前言

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/CC 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、统计通信行业相关部门网络安全工作情况和数据基础上，《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。

《2014 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 2014 年开展的移动互联网恶意程序治理工作、分布式反射型拒绝服务攻击等专题进行专门介绍，并首次吸纳通信行业的网站安全监测数据。接下来，报告对 2014 年国内外网络安全监管动态、我国网络安全行业联盟和应急组织的发展、国内外网络安全重要活动等情况做了阶段性总结。最后，针对当前网络安全热点和难点问题，结合对 2014 年网络安全的威胁和形势判断，预测了 2015 年网络安全热点问题。

国家计算机网络应急技术处理协调中心

2015 年 3 月

THANKS

致 谢

《2014 年中国互联网网络安全报告》的写作素材均来自于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、网络安全厂商、安全研究机构以及相关合作单位的大力支持。在《2014 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瑞星信息技术有限公司、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、哈尔滨安天科技股份有限公司、恒安嘉新（北京）科技有限公司、北京奇虎科技有限公司、趋势科技（中国）有限公司、深信服科技有限公司、北京安管佳科技有限公司等单位征集了数据素材[1]，特此致谢。

2014 年，为维护公共互联网安全，净化公共互联网网络环境，CNCERT/CC 联合有关单位，在网络安全监测、预警、处置等方面积极开展工作。北京新网数码信息技术有限公司、厦门商中在线科技有限公司、北京新网互联科技有限公司、成都西维数码科技有限公司、厦门三五互联科技股份有限公司、阿里巴巴通信技术（北京）有限公司等单位对国家互联网应急中心事件处置要求及时响应，配合积极；北京奇虎科技有限公司、猎豹

[1] 《2014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。

移动公司、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等单位向国家互联网应急中心报送了大量有价值的信息通报，起到了很好的预警效果；百度手机助手、PP 助手、木蚂蚁、应用汇、安智网、安卓网、中国移动应用商场积极配合开展移动互联网恶意程序下架和信息报送工作。此报告的完成离不开各单位在日常工作中给予的配合和支持，在此一并感谢。

由于编者水平有限，《2014 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。

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，为非政府非营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“积极防御、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 2014 年年底，CNCERT/CC 已与世界上 63 个国家和地区的 144 个组织建立“CNCERT 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

CONTENT

目 录

1 2014 年网络安全状况综述 …… 15

1.1 我国互联网网络安全总体状况 …… 15
1.2 数据导读 …… 25

2 网络安全专题分析 …… 28

2.1 移动互联网恶意程序专项治理工作（来源：CNCERT/CC） …… 28
2.2 分布式反射型拒绝服务攻击专题分析（来源：CNCERT/CC） …… 32
2.3 智能硬件蠕虫威胁互联网安全专题（来源：奇虎 360 公司） …… 37
2.4 短信拦截黑客地下产业链案例分析（来源：安天公司） …… 45
2.5 12306 泄密事件到国内外信息泄露安全事件分析（来源：深信服公司） …… 57
2.6 工业控制网络安全分析（来源：CNCERT/CC） …… 68

3 计算机恶意程序传播和活动情况 …… 75

3.1 木马和僵尸网络监测情况 …… 75

3.2 “飞客”蠕虫监测情况 …… 84
3.3 恶意程序传播活动监测 …… 86
3.4 通报成员单位报送情况 …… 88

4 移动互联网恶意程序传播和活动情况 …… 96

4.1 移动互联网恶意程序监测情况 …… 96
4.2 移动互联网恶意程序传播活动监测 …… 98
4.3 通报成员单位报送情况 …… 100

5 网站安全监测情况 ……112

5.1 网页篡改情况 …… 112
5.2 网页挂马情况 …… 121
5.3 网页仿冒情况 …… 124
5.4 网站后门情况 …… 130

6 安全漏洞预警与处置 ……136

6.1 CNVD 漏洞收录情况 …… 136
6.2 高危漏洞典型案例 …… 139
6.3 CNVD 行业漏洞库 …… 146
6.4 CNVD 漏洞处置情况 …… 150

7 网络安全事件接收与处理 ……152

7.1 事件接收情况 …… 152
7.2 事件处理情况 …… 154
7.3 事件处理典型案例 …… 156

8 网络安全信息通报情况 ……165

8.1 互联网网络安全信息通报 …… 165
8.2 行业外互联网网络安全信息发布情况 …… 168

9 国内外网络安全监管动态 ……170

9.1 2014 年国内网络安全监管动态 …… 170
9.2 2014 年国外网络安全监管动态 …… 173

10 国内网络安全组织发展情况 ……191

10.1 网络安全信息通报成员发展情况 …… 191
10.2 CNVD 成员发展情况 …… 196
10.3 ANVA 成员发展情况 …… 198
10.4 CNCERT/CC 应急服务支撑单位 …… 200

11 国内外网络安全重要活动 ……204

11.1 国内重要网络安全会议和活动 …… 204
11.2 国际重要网络安全会议和活动 …… 211

12 2015 年网络安全热点问题 ……218

13 网络安全术语解释 ……220

1 2014年网络安全状况综述

1.1 我国互联网网络安全总体状况

2014年是我国接入国际互联网20周年，也是我国网络安全和信息化国家战略迈出重要步伐的一年。党中央高度重视网络安全工作，成立中央网络安全和信息化领导小组，党的十八届四中全会明确提出加强互联网领域立法，政府工作报告首次出现“维护网络安全”表述，相关管理办法和指导意见先后出台，各类宣传和竞赛活动接连开展，提高了各行业、各领域对网络安全的关注和重视，网络安全意识水平逐年提高，投入逐年增大，在各方共同努力下，我国互联网网络安全状况总体平稳。

近年来，我国互联网市场规模和用户体量高速增长，截至2014年12月底，网站总量保持规模化发展，为364.7万个[2]，网站使用的独立域名为481.2万余个[3]，互联网接入服务商达1068家[4]，网民规模达6.49亿[5]，手机网民规模达5.57亿[6]，互联网普及率达到47.9%[7]，“宽带中国”战略持续推进实施，互联网全面升级提速，4G商用全力推进，带动移动应用、智能终端等整个产业链条创新，促进信息消费快速增长。与此同时，信息化的迅猛发展也带来诸多网络安全威胁等伴生性问题。我国基础网络仍存在较多漏洞风险，云服务日益成为网络攻击的重点目标。域名系统面临严峻的拒绝服务攻击，针对重要网站的域名解析篡改攻击频发。网络攻击威胁日益向工业互联网领域渗透，已发现我国部分地址感染专门针对工业控制系统的恶意程序事件。分布式反射型的拒绝服务攻击日趋频繁，大量伪造攻击数据包来自境外网络。针对重要信息系

[2] 中国互联网协会《中国互联网站发展状况及其安全报告（2015）》数据。
[3] 中国互联网协会《中国互联网站发展状况及其安全报告（2015）》数据。
[4] 中国互联网协会《中国互联网站发展状况及其安全报告（2015）》数据。
[5] CNNIC《第35次中国互联网络发展状况统计报告》数据。
[6] CNNIC《第35次中国互联网络发展状况统计报告》数据。
[7] CNNIC《第35次中国互联网络发展状况统计报告》数据。

统、基础应用和通用软硬件漏洞的攻击利用活跃，漏洞风险向传统领域、智能终端领域泛化演进。网站数据和个人信息泄露现象依然严重，移动应用程序成为数据泄露的新主体。移动恶意程序不断发展演化，环境治理仍然面临挑战。

1.1.1 网络基础设施

（1）基础网络

2014年，“宽带中国”战略继续推进实施，我国基础网络建设不断升级完善，安全防护水平进一步提升，但基础网络相关设备仍存在安全风险，日益普及的云服务经常发生因系统故障、网络攻击导致的安全问题，影响业务运行和用户使用。

基础网络安全防护水平进一步提升。2014年，工业和信息化部重点围绕网络安全防护措施落实、网络数据安全、用户个人电子信息保护等内容，继续推进基础通信网络安全防护工作。基础电信企业不断加大网络安全投入，加强体系、制度和手段建设，推动工作系统化、规范化和常态化。根据抽查结果，各企业符合性测评平均得分均在90分以上，风险评估检查发现的单个网络或系统的安全漏洞数量较2013年下降72%，检查发现问题的难度逐年加大。截至2014年年底，各企业已对80%以上的漏洞完成修复，并对其余漏洞采取了应急措施，制定了整改计划。

基础网络设备仍存在较多安全漏洞风险。随着基础网络安全防护工作的深入推进，发现和处置的深层次安全风险和事件逐渐增多。2014年，CNCERT/CC协调处置涉及基础电信企业的漏洞事件1578起，是2013年的3倍。CNVD[8]收录与基础电信企业软硬件资产相关的漏洞825个，其中与路由器、交换机等网络设备相关的漏洞占比达66.2%，主要包括内置后门、远程代码执行等类型。这些漏洞将可能导致网络设备或节点被操控，出现窃取用户信息、传播恶意代码、实施网络攻击、破坏网络稳定运行等安全事件。

云服务日益成为网络攻击的重点目标。我国基础电信企业和许多大型互联网服务商纷纷加快云平台部署，大力推广云服务，大量金融、游戏、电子商务、电子政务等业务迁移至云平台。2014年先后发生了多起因电力、机房线路和网络故障导致的云服

[8] CNVD全称为国家信息安全漏洞共享平台（China National Vulnerability Database），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、软硬件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

务宕机事件，针对云平台的攻击事件也逐年增多，仅由CNCERT/CC协助处置的大规模攻击事件就有十余起，涉及UCloud公司、浙江宁波某IDC机房等国内云平台。据有关单位报告，2014年12月中旬，某大型互联网服务商的云平台的一家知名游戏公司遭受拒绝服务攻击，攻击峰值流量超过450Gbit/s。云平台运行的稳定性直接影响业务的可用性和连续性，而且针对云平台上某一目标的攻击，还可能导致其他业务受到牵连，造成大面积用户无法访问或使用。

（2）域名系统

域名是网站的入口，其解析安全直接影响网站的正常访问。域名系统承担域名解析工作，面临严重的拒绝服务攻击威胁，一些重要网站频繁发生域名解析被篡改事件。

域名系统面临的拒绝服务攻击威胁进一步加剧。据抽样监测，2014年针对我国域名系统的流量规模达1Gbit/s以上的拒绝服务攻击事件日均约187起，约为2013年的3倍，攻击目标上至国家顶级域名系统，下至CDN服务商的域名解析系统。与往年相比，攻击发生频率更高，流量规模更大。6月，我国某权威新闻网站的域名服务器遭受拒绝服务攻击，峰值流量达1.6Gbit/s，CNCERT/CC对攻击进行追溯分析，为公安部门破案提供了重要线索。同月，国内某主要CDN服务商的域名服务器遭到大规模异常流量攻击，由于其承载国内大量重要网站的CDN加速服务，导致对这些网站的访问均受到严重影响。10月，国家.cn顶级域名系统继2013年8月25日之后再次遭受大规模流量攻击，由于系统加强了安全防护措施，未受到严重影响，但在一定程度上反映出我国顶级域名系统面临的严峻外部威胁。12月，我国多个省份的递归域名解析服务器受到攻击，造成部分地区的互联网使用受到影响。

针对重要网站的域名解析篡改事件频发。2014年发生了多起国内政府网站、重要媒体或企事业单位网站的域名解析被篡改的事件。某省重要新闻网站在短时间内连续数次遭受域名解析被恶意篡改的攻击，黑客入侵该网站域名注册服务商的业务系统，直接篡改数据库中相应数据，获取该网站的域名管理权限，将其域名解析服务器篡改为专门提供免费域名解析的DNSPOD服务器地址，并将其域名指向境外地址。经CNCERT/CC对我国政府网站（以.gov.cn结尾）域名解析情况监测分析，10月期间测试的870万余个域名中，约有107万余个域名被解析到境外IP地址，其中有2.9万个域名的Web端口能

够访问，部分指向推广游戏、色情、赌博等内容的异常页面，还有部分页面被植入恶意代码，不仅影响网站管理方形象，甚至可能造成大面积网络安全危害。

（3）工业互联网

随着互联网的推进和制造业的转型升级，工业互联网成为推动制造业向智能化发展的重要支撑，将工业领域的生产、研发、管理、销售等各个环节与互联网紧密相连，网络安全风险逐渐累积和延伸，威胁扩展至传统工业基础设施。

网络攻击威胁日益向工业互联网渗透。针对工业控制系统的攻击方法和手段已逐渐成熟，并有能力影响物理生产运行环境。根据国际有关机构披露，2014年9月出现一种远程木马“Havex”，它利用OPC工业通信技术[9]，具有很强的针对性，主要功能是扫描发现工业系统联网设备，收集工控设备详细信息并秘密回传，预置后门并在必要时接收、执行控制端发送的恶意代码，全球能源行业的数千个工业控制系统曾被其入侵。据监测，我国境内已有部分IP地址感染了该恶意程序，所对应的控制端均位于境外，并存在部分IP地址持续向控制端发送信息的情况。

1.1.2 公共互联网网络安全环境

（1）木马僵尸网络

2014年，我国境内木马僵尸网络控制服务器和感染主机数量继续呈下降趋势，治理工作成效明显。

我国境内木马僵尸网络感染主机数量稳步下降。据抽样监测，2014年我国境内感染木马僵尸网络的主机为1108.8万余台，较2013年下降2.3%，境内木马僵尸控制服务器6.1万余个，较2013年大幅下降61.4%。2014年，在工业和信息化部的指导下，CNCERT/CC协调基础电信企业、域名服务机构等成功关闭了744个控制规模较大的僵尸网络，累计处置767个恶意控制服务器和恶意域名，成功切断黑客对98万余台感染主机的控制，有力净化了公共互联网网络安全环境。随着我国持续加大公共互联网环境监管和治理力度，大量僵尸网络控制服务器向境外迁移，2014年抽样监测发现境

[9] 一种开放、通用的工业数据交换协议，能够实现基于Windows平台的工业控制系统应用程序与过程控制硬件之间的交互通信。

外4.2万个控制服务器控制了我国境内1081万余个主机，境外控制服务器数量较2013年增长45.3%。

（2）拒绝服务攻击

传统拒绝服务攻击主要依托木马僵尸网络，通过控制大量主机或服务器（俗称“肉鸡”）对受害目标发起攻击，近年来，拒绝服务攻击的方式和手段不断发展变化，分布式反射型的拒绝服务攻击日趋频繁。

分布式反射型攻击逐渐成为拒绝服务攻击的重要形式。分布式反射型攻击是指黑客不直接攻击目标，而利用互联网的一些网络服务协议和开放服务器，伪造被攻击目标地址向开放服务器发起大量请求包，服务器向攻击目标反馈大量应答包，间接发起攻击。这种方式能够隐藏攻击来源，以较小代价实现攻击规模放大，且攻击目标难以防御。此类攻击在我国呈现三个明显特点。一是频繁发生且流量规模大。仅2014年10月，我国就有数十个重要政府的网站和邮件系统遭受此类攻击，部分攻击流量规模超过10Gbit/s。二是攻击方式复杂多样。攻击者综合运用DNS协议、NTP[10]、UPnP协议[11]、CHARGEN[12]等进行攻击，防御困难。三是攻击包来源以境外为主。在2014年发现的分布式反射型攻击中，绝大部分伪造的请求包来自境外，一方面是由于我国基础网络持续开展虚假源地址流量整治工作，攻击者难以从境内网络发出此类伪造包；另一方面也从一定程度上反映出境外对我国攻击频繁。

（3）安全漏洞

2014年，安全漏洞信息共享工作持续推进，重要行业和政府部门信息系统的漏洞事件备受关注，“心脏出血”、“破壳”等漏洞反映了基础应用和通用软硬件面临的高危风险，漏洞威胁向传统领域和智能设备领域演化延伸。

涉及重要行业和政府部门的高危漏洞事件增多。近年来，CNVD新增收录漏洞数量年均增长率在15%～25%之间，针对漏洞的挖掘和利用研究日趋活跃。2014年，CNVD收录并发布各类安全漏洞9163个，较2013年增长16.7%，平均每月新增收录漏洞

[10] NTP即（Network Time Protocol，即网络时间协议）。
[11] UPnP协议即（Universal Plug and Play，即通用即插即用）协议。
[12] CHARGEN即（Character General Protocol，即字符发生器协议）。

763个；其中高危漏洞2394个，占26.1%，可诱发零日攻击的漏洞3266个（即披露时厂商未提供补丁），占35.6%。漏洞研究者对重要企事业单位信息系统安全问题的关注程度日益提升，在2014年收录的漏洞中，涉及电信行业的占9.0%，涉及工控系统的占2.0%，涉及电子政务的占1.9%，CNCERT/CC全年向政府机构和重要信息系统部门通报漏洞事件9068起，较2013年增长3倍。

基础应用或通用软硬件漏洞风险凸显。2014年CNCERT/CC通报处置通用软硬件漏洞事件714起，较2013年增长1倍。由于基础应用和通用软硬件产品部署广泛，漏洞容易被批量利用，而且定位和修复困难，影响范围可能波及全网，危害程度远大于一般漏洞。4月8日，开源加密协议OpenSSL被披露存在内存泄露高危漏洞（CNVD编号：CNVD-2014-02175，对应CVE-2014-0160），又称“心脏出血（HeartBleed）”漏洞，利用该漏洞可窃取服务器敏感信息，实时获取用户的账号和密码，危害波及大量互联网站、电子商务、网上支付、即时聊天、办公系统、邮件系统等。据抽样统计，我国境内受该漏洞影响的IP地址超过3万个。9月25日，GNU BASH（Bourne Again SHell）组件被披露存在远程代码执行高危漏洞（CNVD编号：CNVD-2014-06345，对应CVE-2014-6271），又称“破壳（Bash Shell Shock）”漏洞，Redhat、Fedora、CentOS、Ubuntu、Debian、MAC OS等几乎目前所有主流UNIX/Linux操作系统平台、使用ForceCommand功能的OpenSSH SSHD、使用mod_cgi或mod_cgid的Apache服务器、DHCP客户端和其他使用BASH作为解释器的应用均受到影响，不仅是服务器系统，还包括交换机、防火墙、网络设备以及摄像头、IP电话等许多基于Linux的定制系统，影响范围比“心脏出血”漏洞更为严重。根据对部分漏洞的持续监测来看，漏洞修复的速度总体较为缓慢。“心脏出血”漏洞披露3个月后发现仍有约16%尚未修复，而知名度相对较低的Ngnix文件解析漏洞（影响Web应用）在披露1年后未修复率仍高达55%。此外，4月8日微软公司正式停止对Windows XP系统的支持服务，而从4月底至8月中旬的抽样监测统计发现，在我国使用微软操作系统的用户中，超过半数仍在使用Windows XP系统，这些用户在未来相当长的一段时间内将面临严重的“零日攻击”风险。

漏洞威胁向传统领域泛化演进。随着信息化发展，传统广播电视、公共管理、社会服务等领域与互联网紧密融合，漏洞威胁也在演化跟进。2014年CNCERT/CC处置

多起公共服务管理系统存在漏洞风险的事件，涉及公共场所LED信息管理、高速公路视频监控、区域车辆GPS调度监控等，这些漏洞一旦被利用，将直接影响日常交通管理和公众生活。

漏洞威胁向新兴智能设备领域延伸。2014年，移动互联网与传统产业结合催生智能硬件新业态，智能手环、智能手表等可穿戴设备、互联网电视等产品成为市场热点，智能汽车、智能家居、智慧城市成为新时尚，随着终端设备的功能和性能大幅提升，面临的安全威胁随之增大。例如，国外某著名电动汽车车载控制系统存在安全漏洞，导致攻击者可远程控制车辆，实现开锁、鸣笛、闪灯、开启天窗等操作。2014年已经发现一些ADSL终端、智能监控设备、智能路由器、网络摄像头、机顶盒等联网智能设备被黑客控制发起网络攻击，这些联网智能设备普遍存在弱口令、配置不当等安全问题，很容易被攻击者安装木马变成“肉鸡”长期进行控制。

（4）网络数据泄露

自2011年CSDN社区信息泄露事件后，近年来网站数据泄露事件不断发生，2014年网站拖库[13]、撞库[14]攻击现象仍然严重。

网站数据和个人信息泄露仍呈高发态势。网站管理者对数据保护的重视程度日益提升，但在网站数据和个人信息利益价值凸显的背景下，数据泄露事件仍频繁出现，有的依然是由于技术漏洞或管理问题导致的拖库事件，有的则来自撞库攻击。2014年我国多家知名电商、快递公司、招聘网站、考试报名网站等发生数据泄露事件。5月中旬，工业和信息化部处理一起某知名手机厂商论坛数据泄露事件，由于此前使用的用户管理模块存在漏洞，导致包括账号、密码和社交账号等800万条用户信息泄露，其中有140万个用户的密码从未修改过（包括开通了云平台账号的130个万用户），是此次泄露事件受威胁对象，存在黑客针对特定用户实施密码暴力破解的风险。12月25日，国内某著名交通购票网站遭受撞库攻击，导致包括用户账号、明文密码、身份证号码、手机号码和电子邮箱等在内的13万多条用户数据在互联网上流传。针对所泄露的数据分析发现，“123456”、“a123456”、“123456a”等弱口令高居榜首，用户

[13] 拖库是指黑客入侵网站，将网站的用户资料数据库全部盗走的行为。

[14] 撞库是指黑客利用从某些网站或渠道获取的用户账号和密码，在其他网站上进行登录尝试。这主要是由于目前有相当一部分互联网用户喜欢在不同网站上使用统一的用户名和密码。

的密码安全意识仍有待提高。

移动应用程序成为数据泄露的新主体。2014年，订票、社交、点评、论坛、浏览器等国内多种知名移动应用发生用户数据泄露事件。一些移动应用开发者经验不足，安全意识和水平不够，网站服务器对移动端的访问控制机制较弱，黑客利用移动应用程序与网站服务器之间的接口漏洞，对网站服务器发起攻击，能够轻易获得相应服务器的地址和接口信息，再通过挖掘接口漏洞，直接获取服务器中所有信息，造成信息泄露。2014年CNVD收录1710个涉及移动互联网终端设备或软件产品的漏洞，这些都可能成为黑客攻击获取用户信息新的入口。

（5）移动互联网恶意程序

在工业和信息化部的指导下，通信行业各方共同努力，积极开展移动互联网环境治理，国内主流应用商店的安全状况有所改善，但移动互联网恶意程序不断发展演化，给治理工作带来挑战。

移动互联网网络安全威胁治理取得明显成效。2014年4-9月，工业和信息化部联合公安部、工商总局开展打击治理移动互联网恶意程序专项行动，CNCERT/CC、基础电信企业、域名注册服务机构、安全企业、应用商店和数字认证服务企业等多家单位积极参与，取得明显成效。专项行动期间，及时有效处置了“××神器”病毒大规模传播事件，协调处置移动恶意程序控制服务器和传播源链接1.01万个；开办主体主动关停或监管部门依法关停应用商店283家；中国互联网协会反网络病毒联盟（ANVA[15]）、电子认证服务机构、应用商店、手机安全软件厂商和手机终端生产企业等多方力量联合，试点开展移动应用程序开发者第三方数字证书签名与验证，以实现移动应用程序的防篡改和可溯源；持续推进自律黑白名单共享工作，发布移动恶意程序黑名单4.9万条，传播地址黑名单1187条，发布中国农业银行、奇虎360、百付宝、搜房4张移动互联网应用自律白名单证书。

移动恶意程序逐渐从主流应用商店向小型网站蔓延。2014年，根据工业和信息化部《移动互联网恶意程序监测与处置机制》，CNCERT/CC每周协调应用商店下架移动恶意程序，累计通知139家应用商店、网盘、下载站点等下架恶意程序4.1万个，

[15] ANVA全称为中国反网络病毒联盟（Anti Network-Virus Allice of China），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、软硬件厂商和互联网企业建立的信息安全漏洞信息共享知识库，网址为www.anva.org.cn。

实际下架3.9万余个，下架率达到95.5%。经过连续两年的治理，国内30余家主流应用商店的安全意识均有提高，审核制度和检测手段逐步改善，恶意程序数量由2013年的3.73万个大幅下降至0.93万个，安全状况明显改善。移动恶意程序逐渐向个人网站、广告平台等小型网站蔓延，2014年监测发现100余个小型网站传播移动恶意程序3万余个，其中单个网站传播移动恶意程序的数量最多超过2000个，针对这类网站的监测处置将是未来移动互联网环境治理工作的重点。

移动恶意程序治理打击对抗性初显。2014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有95.1万余个。按行为属性分类[16]，恶意扣费类的恶意程序数量居首位，占55.0%；其次是资费消耗类和信息窃取类，分别占15.3%和12.9%，信息窃取类所占比例较2013年的3.2%大幅上升。据抽样监测，2014年我国感染移动恶意程序的用户数量达2292万，其中感染安卓平台恶意程序的用户数量最多，超过1575万个，发现约30万用户感染基于苹果iOS平台的恶意程序，如“Panda”、“Wirelurker”等。移动恶意程序的对抗性明显增强，制作者普遍采用“加固”技术对抗安全检测，2014年发现的移动恶意程序样本中有2.2%经过“加固”处理，检测难度加大，给治理工作带来新的挑战。

具有短信拦截功能的移动恶意程序大量爆发。目前网银、网购等普遍通过短信验证码方式对用户身份进行校验，2014年具有拦截、转发手机短信功能的移动恶意程序数量大幅增长。黑客从短信中获取用户的重要个人信息，如姓名、身份证号码、银行卡账号、支付验证码、各种登录账号和密码等，再结合其他钓鱼欺诈手段，窃取用户资金或实施诈骗活动，威胁用户财产安全。这类恶意程序开发成本低，更新速度快，一般还带有隐私窃取、远程控制、诱骗欺诈、资费消耗等其他功能。据抽样监测分析，此类恶意程序最早出现于2013年5月，2014年起开始流行爆发，目前已发现该类样本16万余个，8月爆发的“××神器”移动恶意程序通过拦截和转发短信，全国感染用户数量达到11万，波及国内31个省（自治区、直辖市），在工业和信息化部指导下，CNCERT/CC及时完成对该样本的分析，并协调进行处置，有效控制了其传播态势。

[16] 如果单个恶意程序具有多重恶意行为属性，统计时根据YD/T 2439-2012《移动互联网恶意代码描述格式》中对恶意行为属性的恶意性等级划分，按其等级最高的恶意行为属性进行统计。

（6）网页仿冒

2014年，针对金融、电信行业的网页仿冒事件大幅增长，大量钓鱼站点向云平台迁移，加大事件处置难度，影响用户经济安全和信息消费。

针对金融、电信行业的仿冒事件大幅增长。2014年抽样监测发现，针对我国境内网站的仿冒页面（URL链接）近10万个，较2013年增长2.3倍，涉及IP地址6844个，较2013年增长61.4%。在针对我国境内网站的钓鱼站点（IP地址）中有89.4%位于境外，承载仿冒页面9万余个，较2013年增长2.1倍，主要是位于中国香港地区的钓鱼页面数量将近3万个，较2013年大幅增长。从被仿冒对象来看，针对第三方支付机构、网上银行等金融机构的仿冒页面占比超过80%，主要是诱骗用户提交银行卡号、密码、身份证号码等信息，同时发现大量针对电信企业的仿冒页面，主要是虚假充值页面，占比达12%，已超过仿冒知名电视节目或大型互联网站进行虚假抽奖的页面数量。网页仿冒与移动应用结合日益紧密，许多仿冒页面仅能通过移动智能终端访问，针对手机网银、微信等移动应用的仿冒事件频发。

钓鱼站点逐渐向云平台迁移。云服务申请和使用方便、成本低廉、安全审核不严格，且云平台同时承载多种不同类型的业务，传统基于IP地址的追踪处置手段难以适用，日益成为钓鱼网站栖息的“温床”。针对2014年处置的银行类钓鱼网站分析，按所承载的钓鱼网站数量（按域名统计）排序，排名前10的IP地址有4个属于云服务提供商。

（7）网站攻击

“匿名者”等黑客组织对我国政府部门和重要企事业单位网站的攻击依然频繁，出现了向网站中植入钓鱼页面、针对性地实施拒绝服务攻击、窃取网站数据等情况。

针对政府部门和重要行业单位网站的网络攻击频度、烈度和复杂度加剧。据监测，2014年我国境内被篡改的政府网站1763个，被植入后门的政府网站1529个，分别占全部被篡改网站的4.8%和全部被植入后门网站的3.8%。据通信行业信息，出现的一个新特点是大量政府和教育类网站的子页面被篡改并植入钓鱼页面。黑客组织对我国政府部门网站的攻击依然频繁。“匿名者”等黑客组织先后篡改了我国400余个网站，在针对中国大陆和中国香港政府网站的所谓“OpHongKong”攻击行动中，黑客组织宣称对我国150余个重要政府部门的网站发动大规模攻击，并公布了大量攻击目

标的URL链接、网站服务器类型、IP地址等详细信息，据CNCERT/CC监测其攻击成功的网站有40余个，除网页篡改和植入后门外，还发现许多技术手段复杂、流量规模大的拒绝服务攻击，以及窃取网站内存储的用户信息并公布的情况，严重影响网站的正常运行。

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2014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

- 2014年木马或僵尸程序控制服务器IP地址总数为104230个，较2013年下降45.0%。其中，境内木马或僵尸程序控制服务器IP地址数量为61879个，较2013年大幅下降61.4%；境外木马或僵尸程序控制服务器IP地址数量为42351个，较2013年增加45.3%。
- 2014年木马或僵尸程序受控主机IP地址总数为13991480个，较2013年减少25.2%。其中，境内木马或僵尸程序受控主机IP地址数量为11088141个，较2013年减少2.3%；境外木马或僵尸程序受控主机IP地址数量为2903339个，较2013年大幅减少60.5%。

（2）“飞客”蠕虫监测

2014年全球互联网月均有近943万台主机IP地址感染“飞客”蠕虫，其中，我国境内感染的主机IP地址数量月均近103万台。

（3）移动互联网安全监测

- 2014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951059个，相比2013年增长35.3%。
- 按行为属性统计，恶意扣费类的恶意程序数量仍居首位，为522889个，占55.0%，资费消耗类（占15.3%）、隐私窃取类（占12.9%）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占99.9%，仍居首位；其次是Symbian平台，占0.1%。

（4）网站安全监测情况

• 2014年我国境内被篡改网站数量为36969个，较2013年的24034个大幅增长53.8%。其中，境内政府网站被篡改数量为1763个，较2013年的2430个减少27.4%，占境内全部被篡改网站数量的4.8%。

• 2014年，监测到仿冒我国境内网站的钓鱼页面99409个，涉及IP地址6844个。在这6844个IP地址中，89.4%位于境外。在仿冒我国境内网站的境外IP地址中，美国占17.7%，位居第一，中国香港（占15.2%）和韩国（占1.8%）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66.3%，其次是.pw和.cn，分别占9.0%和5.1%。

• 2014年，监测到境内40186个网站被植入后门，其中政府网站有1529个，占境内被植入后门网站的3.8%。向我国境内网站植入后门的IP地址有19168个位于境外，主要位于美国（24.8%）、韩国（6.7%）和中国香港（6.5%）。

（5）安全漏洞预警与处置

• 2014年，CNVD收集新增漏洞9163个，包括高危漏洞2394个（占26.1%），中危漏洞6032个（占65.8%），低危漏洞737个（占8.1%）。

• 与2013年相比，2014年CNVD收录的漏洞总数增长16.7%，其中高危漏洞下降8.2%，中危漏洞增长35.0%，低危漏洞下降6.8%。

• 按漏洞影响对象类型统计，排名前三的分别是应用程序漏洞（占68.5%）、Web应用漏洞（占16.1%）和网络设备漏洞（占6.0%）。

• 2014年，CNVD 共收录漏洞补丁5927个。

（6）网络安全事件接收与处理

• 2014年，CNCERT/CC共接收境内外报告的网络安全事件56180起，较2013年增长了77.5%。其中，境外报告的网络安全事件数量为885起，较2013年下降了8.9%。接收的网络安全事件中，排名前三位的分别是漏洞事件（占36.4%）、网页仿冒事件（32.1%）和网页篡改事件（16.3%）。

• 2014年，CNCERT/CC共成功处理各类网络安全事件56072起，较2013年的31180起大幅增长79.8%。其中，漏洞事件（占36.1%）、网页仿冒事件（占32.0%）、

网页篡改类事件（占16.0%）等处理较多。

（7）网络安全信息发布情况

- 2014年，CNCERT/CC共收到通信行业各单位报送的月度信息561份，事件信息和预警信息324份，全年共编制并向各单位发送《互联网网络安全信息通报》22期。
- 2014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242份。

2 网络安全专题分析

2.1 移动互联网恶意程序专项治理工作（来源：CNCERT/CC）

2.1.1 专项治理工作背景

近年来移动互联网恶意程序逐渐呈现爆炸式增长趋势，2014年CNCERT/CC监测发现移动互联网恶意程序数量951059个，是2013年监测发现移动互联网恶意程序数量702861个的1.35倍，是2012年监测发现移动互联网恶意程序数量162981个的5.84倍，是2011年监测发现移动互联网恶意程序数量6249个的152.19倍，特别是具有恶意扣费、窃听监控、资费消耗、信息窃取等恶意行为的移动互联网恶意程序，严重损害人民群众切身利益，移动互联网安全岌岌可危。

同时移动互联网恶意程序的传播蔓延情况十分严重。2014年CNCERT/CC监测发现用于传播移动互联网恶意程序的网站域名24211个，IP地址57296个，恶意程序传播次数高达81747407次。据CNCERT/CC抽样监测，2014年我国感染移动恶意程序的用户数量达2292万，较2013年的609万用户增长3.76倍，其中感染Android平台恶意程序的用户数量最多，超过了1575万。

2014年，为净化移动互联网的生态环境，保护网民合法权益，工业和信息化部联合公安部、工商总局制定并下发了《打击治理移动互联网恶意程序专项行动工作方案》（工信部联保〔2014〕153号），于2014年4-9月在全国范围组织开展了打击治理移动互联网恶意程序专项行动。在工业和信息化部的统一部署下，根据专项行动工作方案，CNCERT/CC组织基础电信企业、ANVA成员单位、手机应用商店、数字证书认证服务机构等开展专项治理工作，取得良好成效。

2.1.2 专项治理工作内容及成效

根据《关于印发打击治理移动互联网恶意程序专项行动任务分工的通知》（工保函〔2014〕316号），CNCERT/CC指定专职工作人员参与专项行动，并组织基础电信企业、域名注册管理和服务机构、网络安全企业、应用商店、数字证书认证服务机构等多家单位召开专项行动工作部署会，对各单位的工作进行梳理分工，要求各单位严格落实专项行动工作要求，着重在移动互联网恶意程序网络侧监测处置、应用商店安全管理、移动应用程序开发者源头管理、移动互联网黑白名单信息共享、恶意程序犯罪线索挖掘等方面开展具体工作，取得了良好的工作成效。

（1）移动恶意程序网络侧监测和处置方面。专项行动期间，CNCERT/CC共监测发现移动恶意程序20195个，恶意程序传播服务器相关域名3575个，恶意程序控制服务器相关域名239个，恶意程序控制服务器相关URL共589个。协调38家手机应用商店处置恶意程序传播服务器相关URL链接4779个；协调域名注册服务机构和基础电信企业处置控制规模较大的恶意程序控制服务器相关域名41个及相关URL链接 83个。专项行动期间，一款名为“××神器”的安卓手机恶意程序通过短信在国内多个地区大范围传播，大量用户受骗安装，该病毒以钓鱼方式窃取短信、购物网站账户和密码、支付验证码等信息。在工业和信息化部的指导下，CNCERT/CC会同基础电信企业对该恶意程序进行了技术分析，及时协调基础电信企业和域名注册服务机构进行处置，当日即有效控制了传播势态，并将相关线索通报给公安部门协助破案。

（2）应用商店安全管理方面。CNCERT/CC协助工业和信息化部制定应用商店网络安全责任指南，明确了应用商店在应用程序安全检测、恶意程序下架、恶意程序黑名单、用户监督举报等方面的安全要求，开展了国内应用商店信息梳理、安全检查和远程抽测等三方面工作。一是，调查国内应用商店情况，2014年上半年全国共有306家（除去关停的）应用商店，活跃安卓应用程序总数超过610万个，其中19家大型应用商店（上架应用程序数量在10万以上）的应用程序数量占活跃应用程序总数的71%，占总下载量的75%。根据CNCERT/CC提供的应用商店信息，开办主体主动关停或各省通信管理局依法关停未备案等应用商店超过200家。二是，依托CNCERT/CC的应用商店在线检测系统（https://appstore.anva.org.cn），协助上海、广东、福

建等11个省市通信管理局，接入150余家应用商店进行安全检测，累计检测应用程序4831986个，检测出恶意程序4726个。三是，受工业和信息化部委托，对境内76家手机应用商店中的移动应用程序进行了集中安全抽测工作，累计检测应用程序总数3983445个，累计检测发现存在恶意程序的应用商店15家，检测出恶意程序总数322个，其中具有信息窃取、资费消耗、恶意扣费等恶意行为的恶意程序排名前三，占所有恶意程序的80%以上，所检出的恶意程序已由各省通信管理局通知应用商店进行下架处理。

（3）移动应用程序开发者源头管理工作方面。为实现移动应用程序的防篡改和可溯源，工业和信息化部指导ANVA、电信终端测试技术协会、电子认证服务产业联盟等开展移动应用程序开发者第三方数字证书签名与验证试点工作，选取了6家电子认证服务机构、12家应用商店、5家手机安全软件厂商以及5家手机终端生产企业参与试点工作。CNCERT/CC根据工业和信息化部移动应用程序开发者第三方签名试点工作要求，组织数字证书认证服务机构、应用商店和安全企业等单位论证移动签名技术方案，制定《Android应用程序开发者第三方数字证书签名、验证和标识规范（试行）》，并于2014年10月24日组织召开“移动互联网应用程序开发者第三方数字证书签名与验证试点宣介会”。专项行动期间，百度手机助手、360手机助手、中国移动MM商城、中国联通沃商店等知名应用商店已经实现了对上架试点应用程序的签名验证和标识功能，数十款经过第三方数字证书签名的应用程序在参与试点的应用商店上架并标识。

（4）移动互联网黑白名单信息共享工作方面。CNCERT/CC通过ANVA网站[17]向外发布移动恶意程序黑名单和移动恶意程序传播源地址黑名单4078条，与中国信息通信研究院、中国互联网协会等单位共享黑名单数据，并要求应用商店接入网站及时下架黑名单中的恶意程序。在白名单信息共享方面，CNCERT/CC积极推动移动互联网应用自律白名单工作，2014年组织包括11家主流安全企业在内的白名单工作组对中国农业银行、搜房网等近百余家移动互联网公司的白名单申请进行了审查，并通过中国农业银行、百度理财、搜房网、奇虎360公司共4家企业的4款数字证书进入白名单。截至2014年，移动互联网白名单生态系统已初步建立，包括中国移动MM商城、360手机助手、腾讯应用宝、百度应用中心等20余家主流应用商店均已对白名单应用

[17] 移动恶意程序黑名单发布地址：msample.anva.org.cn，移动恶意程序传播源黑名单发布地址：appstore.anva.org.cn。

进行标识，并设立白名单专区，引导用户安装使用安全可靠的白名单应用。

（5）恶意程序犯罪线索挖掘工作方面。CNCERT/CC着重对具有恶意扣费、窃听监控等严重损害人民群众切身利益的移动恶意程序进行犯罪线索挖掘。通过对窃听用户通话、窃取用户短信等功能的手机软件和后台进行技术分析，目前移动恶意程序都运行在Android系统，且多数恶意程序在安装后会自动隐藏图标，在后台自动运行，可以执行黑客发出的远程控制指令，除监听用户通话和环境音外，还能够将通讯录、通话记录、短信、照片等个人信息上传到远程服务器和电子邮箱。CNCERT/CC根据恶意程序中涉及的手机号、邮箱及恶意服务器域名、IP地址等信息，追查移动恶意程序的开发者，形成多条犯罪线索通报公安机关。根据CNCERT/CC提供的线索，公安部部署地方公安机关查获了一起制售手机监控软件、秘密监控手机用户、受害人分布全国的特大犯罪网络，有效震慑了利用移动恶意程序从事网络犯罪活动的行为。

2.1.3 下一步工作建议

通过2014年三部委移动恶意程序专项治理行动，初步掌握了国内应用商店安全状况，明确了应用商店安全责任，集中处置了一批性质恶劣的恶意程序，达到了净化国内移动互联网环境的目的，保障了用户的合法权益。尽管专项工作取得了显著成效，但进一步推进移动恶意程序治理工作仍需解决诸多问题，移动互联网环境治理工作是一项全新的、极富挑战性的工作，建议下一步抓住移动互联网产业链的关键环节开展工作。

（1）加强对传播环节的安全管理，建议出台针对移动应用程序传播源的安全管理规章制度。移动应用程序主要通过应用商店、下载站、网盘等网站进行传播，从这些源头网站对移动应用程序进行把关，可以有效控制移动恶意程序的蔓延趋势。但是目前还未有明确的规章制度对应用程序传播源进行规范，建议下一步出台相关规章制度明确应用商店网络安全责任，建立对应用商店的监督检查制度，形成对违规应用商店曝光和惩罚机制，从根本上提高传播源头的安全性和可靠性。

（2）加强对开发者的安全管理，建议积极推进移动应用程序第三方数字证书签名认证和移动互联网应用自律白名单工作。按照政府鼓励、开发者自愿的原则，引导开发者使用第三方数字证书对应用程序进行数字签名并进行白名单认证，要求应用商店对采用第三方数字证书签名和白名单中的应用程序进行验证和标识，从开发环节保

证应用程序的安全性，逐步构建安全的移动互联网生态系统。

（3）加强移动恶意程序治理技术手段建设，建议继续加大投入建设移动恶意程序监测与处置平台，组织CNCERT/CC、基础电信企业等机构联合形成全程全网的恶意程序监测处置能力。在执行《移动互联网恶意程序监测与处置机制》的基础上，提升恶意程序检测能力，完善检测流程，建立常态化的移动应用程序监督检测和恶意程序认定工作机制。

（4）加强对用户的安全意识教育，建议通过各种形式向网民普及移动互联网安全知识。广泛协调基础电信企业、新闻媒体、移动互联网企业等组织做好智能手机、应用程序的安全使用教育和移动互联网恶意程序的危害知识教育等宣传工作，特别是涉及钱财安全和个人信息保护方面的宣传教育，切实提高网民的安全防范意识和技能。

2.2 分布式反射型拒绝服务攻击专题分析（来源：CNCERT/CC）

2.2.1 分布式反射型拒绝服务攻击原理及特点

分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是指黑客通过远程控制技术，控制大量服务器或计算机终端（俗称“肉鸡”）对攻击目标发起拒绝服务攻击，从而成倍地提高攻击威力。

分布式反射型拒绝服务（Distributed Reflection Denial of Service，DRDoS）攻击与DDoS攻击不同之处在于黑客不直接控制“肉鸡”对攻击目标发起攻击，而是利用互联网的一些网络服务以及对应开放服务的大量服务器或终端，伪造攻击目标地址向这些服务器或终端发送大量伪造的请求包，使得服务器或终端向攻击目标反馈大量应答包，间接对攻击目标发起攻击。其原理如图2-1所示，黑客（假设IP地址为1.1.1.1）想要对某目标（假设IP地址为6.6.6.6）发起攻击，其可以伪造目标IP地址为6.6.6.6向大量开放某特定服务的服务器或终端（图中IP地址为2.2.2.2、3.3.3.3等）发起服务请求。这些服务器或终端收到请求后，将进行服务应答，由于请求包中的源地址是伪造的IP地址6.6.6.6，因此应答包将发往IP地址6.6.6.6，从而间接对目标地址造成攻击流量。

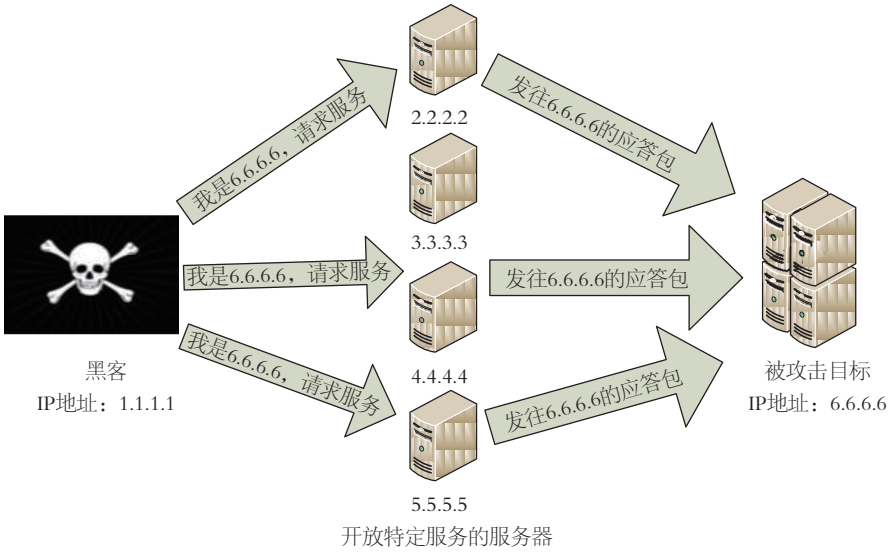


图2-1　分布式反射型拒绝服务攻击原理示意（来源：CNCERT/CC）

分布式反射型拒绝服务攻击之所以成为黑客“青睐”的攻击方式，主要是因为其具有几个显著特点。一是可以放大攻击效果。一般黑客利用发起反射攻击的服务，往往应答包远大于请求包，因此黑客可以利用较小的代价发起数十倍甚至数百倍的攻击流量，达到“四两拨千斤”的效果。二是攻击易发起。可被利用发起反射攻击的服务器或终端往往数量多、分布广，且通过扫描就能掌握互联网上开放服务的服务器或终端列表，黑客仅需要向这些服务器或终端发送特定请求即可发起攻击。三是便于隐藏攻击者。一方面，在被攻击目标端，看到的攻击源地址都是被利用反射攻击的服务器或终端IP地址，无法看到黑客自身IP地址；另一方面，在被利用的服务器或终端侧，由于被利用的服务往往都是使用无连接的UDP协议，黑客可以伪造攻击目标地址发起请求流量，因而在这些服务器或终端侧无法看到黑客真实IP地址。也就是说在整个攻击环节中，黑客的真实地址都没有暴露。

2.2.2　常见分布式反射型拒绝服务攻击类型

根据分布式反射型拒绝服务攻击的原理，被利用发起反射攻击的服务需要具备两

个要素：一是使用无连接的UDP协议，以发起伪造地址的请求包；二是应答包大于请求包，从而可以放大攻击流量。

目前互联网上具备以上要素的服务主要有DNS（Domain Name System，域名系统，默认服务端口为UDP 53端口）、NTP（Network Time Protocol，网络时间协议，默认服务端口为UDP 123端口）、UPnP（Universal Plug and Play，通用即插即用，默认服务端口为UDP 1900端口）、CHARGEN（Character Generator Protocol，字符发生器协议，默认服务端口为UDP 19端口）等。其对应的分布式反射型拒绝服务攻击类型如下。

一是DNS分布式反射攻击。DNS是域名和IP地址相互映射的一个分布式数据库，它能够使用户通过直观的域名更方便地访问网站，而不用去记住网站的IP地址。DNS分布式反射攻击的原理是攻击者伪造攻击目标地址向互联网上开放递归服务的大量DNS服务器发起域名请求。这些服务器收到请求后，将会把应答包返回给攻击目标地址，而且攻击者发起的请求往往是ANY或者TXT类型，应答包往往比请求包大数十甚至数百倍，从而利用这些服务器对攻击目标发起放大后的流量攻击。据调查，目前互联网存在约2700万台开放递归服务的DNS服务器，这些服务器均存在被黑客利用发起反射攻击的可能。

二是NTP分布式反射攻击。NTP是用来使计算机时间同步化的一种协议，可以使计算机对其服务器或时钟源（如石英钟、GPS等）做同步化，以提供高精准度的时间校正。NTP分布式反射攻击的原理是攻击者伪造攻击目标地址向互联网上开放NTP服务的大量服务器发起Monlist请求。这些服务器收到请求后，将会把应答包返回给攻击目标地址，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，因此应答包往往比请求包大出数百倍，从而利用这些服务器对攻击目标发起放大后的流量攻击。

三是UPnP分布式反射攻击。UPnP是路由器、网络摄像头、智能电视、打印机等家庭终端设备普遍应用一种网络通信协议。该协议的主要组成部分是SSDP（Simple Service Discovery Protocol，简单服务发现协议）。UPnP设备间通过SSDP进行相互感知的，利用SOAP（Simple Object Access Protocol，简单对象访问协议）来获取控制信息，并进行信息反馈。UPnP分布式反射攻击的原理是黑客伪造攻击目标地址向大量

UPnP设备发起恶意请求，进而利用大量UPnP设备的应答包对攻击目标发起反射攻击，通常可以将攻击流量放大约30倍。所有连接互联网的UPnP设备都有可能成为黑客利用的对象，其数量数以千万计。

四是CHARGEN分布式反射攻击。CHARGEN是一种发送字符的服务，开启CHARGEN服务的服务器收到客户端发出的UDP包后，将发送一个数据包到客户端，其中包含长度为0～512字节之间随机值的任意字符。CHARGEN分布式反射攻击的原理是黑客伪造攻击目标地址向大量CHARGEN服务器发出UDP请求包，进而利用大量CHARGEN服务器的应答包对攻击目标发起反射攻击，且应答包比请求包通常要大出数十倍。

2.2.3 我国分布式反射型拒绝服务攻击趋势及应对措施

据CNCERT/CC监测分析，2014年分布式反射型拒绝服务攻击在我国呈现出以下三个趋势。

一是攻击频繁发生且流量规模大。仅2014年10月期间，香港中联办等数十个网站都遭受过分布式反射型拒绝服务攻击，部分网站遭受的反射攻击流量在10Gbit/s以上。2014年12月，CSDN网站、千龙网遭受大规模的分布式反射型拒绝服务攻击，其中CSDN网站遭受的攻击流量超过30Gbit/s，千龙网遭受的攻击流量超过24Gbit/s，且反射攻击的来源涉及境内外近20万个NTP服务器地址以及UPnP设备地址。

二是攻击方式多样化。据CNCERT/CC监测分析，2014年我国发生的分布式反射型拒绝服务攻击事件中，黑客使用过的攻击方式包括DNS反射攻击、NTP反射攻击、UPnP反射攻击、CHARGEN反射攻击等多种类型，部分攻击事件中攻击者还会综合运用上述方式以达到攻击效果。2014年10月，某政府网站遭受的分布式反射型拒绝服务攻击中，黑客就同时使用了NTP和CHARGEN反射攻击。未来黑客将有可能研究并使用其他的分布式反射拒绝服务攻击方式。

三是攻击来源IP地址主要以境外为主。据CNCERT/CC监测分析，2014年发生分布式反射型拒绝服务攻击事件中，绝大部分攻击发起源（即伪造的请求包来源）来自境外。2014年10月，在中国香港中联办网站（服务器IP地址位于北京）遭受分布式反射型拒绝服务攻击事件中，CNCERT/CC分析发现大量从境外发起的，但源地址是

香港中联办网站服务器IP地址（境内地址），且目的地址也是境内IP地址的NTP请求的流量。大量来自境外发起的分布式反射型拒绝服务攻击反映出境外对我国攻击日益频繁；同时也体现出我国基础网络开展的虚假源地址流量整治工作取得一定成效。由于反射型攻击需要先伪造攻击目标发起请求包，而目前在工业和信息化部的大力推动下，我国基础电信企业均积极开展虚假源地址流量整治工作，因此攻击者从我国境内网络难以发出此类伪造请求包。

分布式反射型拒绝服务攻击具有隐藏攻击者来源、以较小代价实现放大攻击规模效果、攻击易发起等特点，因而必将成为黑客越来越“青睐”的手段，也将对我国公共互联网安全造成越来越大的威胁。因此要积极采取有效措施遏制此类攻击的泛滥，建议的主要措施包括以下几点。

一是基础电信企业要进一步加强虚假源地址流量整治工作。分布式反射型拒绝服务攻击的前提是要伪造攻击目标地址发出请求流量，而虚假源地址流量整治工作就是要让伪造的流量无法发出，从而切断分布式反射型拒绝服务攻击的源头。目前我国基础电信企业在境内城域网内基本完成了虚假源地址流量整治部署工作，下一步要进一步研究如何在国际出入口部署虚假源地址流量整治，以减少来自境外的反射型拒绝服务攻击。

二是互联网上的服务器或终端管理者要加强安全管理。首先要关闭服务器或终端无关的服务端口，停用无关服务，避免成为黑客利用的“弹药”，例如个人终端关闭UDP 1900端口以禁用UPnP服务。其次要及时修补相关漏洞，并设置必要的访问限制，例如NTP服务器及时升级NTP版本、禁用Monlist功能，并设置防火墙策略限制特定IP地址的访问次数。

三是重要网站和信息系统要加强安全防范。分布式反射型拒绝服务攻击具有攻击源端口固定的特点，例如DNS分布式反射攻击的攻击源端口为UDP 53，因此可以在防火墙设置相关策略过滤此类攻击流量，或者协调基础电信企业在上层路由进行流量清洗。重要网站和信息系统自身要配置相关的安全检测和防范设备，建立和基础电信企业的联动机制，及时发现和处置此类攻击。

2.3 智能硬件蠕虫威胁互联网安全专题（来源：奇虎360公司）

2.3.1 相关背景

2014年12月10日，全球互联网范围DNS流量异常。奇虎360公司[18]云堤团队（DamDDoS）迅速参与分析处置。本次事件攻击自2014年12月10日凌晨起开始，至今仍在持续，为近年来持续时间最长的DNS DDoS攻击。目前已监测到的最大攻击流量近1亿QPS（约合76.38Gbit/s），如图2-2所示。

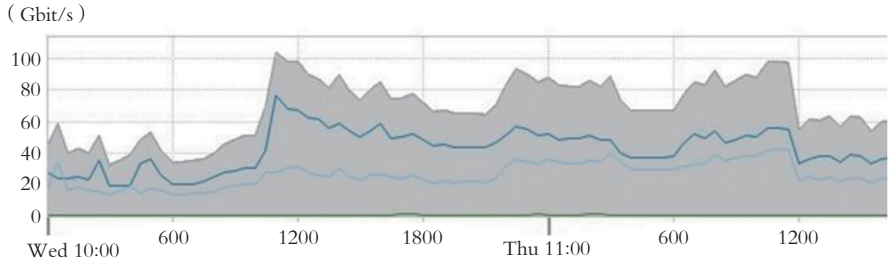


图2-2 DNS DDoS攻击情况（来源：奇虎360公司）

2.3.2 案例分析

2.3.2.1 攻击方法的分析

2014年12月10日，DNS异常故障时期，奇虎360公司网络攻防实验室工作人员对此进行了跟进。之前定位到*.arkhamnetwork.org、*.arkhamnetwork.com（针对某游戏服务提供商的权威域名服务器进行攻击，最后服务商解析内容fraud.ddos.go.away）奇虎360公司的递归DNS缓存被攻击的流量大概为30000QPS。使用的攻击方法是：通过发起对随机前缀域名查询的解析请求，造成对递归服务拒绝服务。图2-3是根据奇虎360公司大数据安全分析可视化平台发现一台Bot终端解析域名的情况，这个攻击特征非常明显，而且攻击方法非常粗暴。

[18] 奇虎360公司即北京奇虎科技有限公司，是通信行业互联网网络安全信息通报工作单位，国家信息安全漏洞共享平台成员，中国反网络病毒联盟成员，同时也是CNCERT/CC国家级应急服务支撑单位。

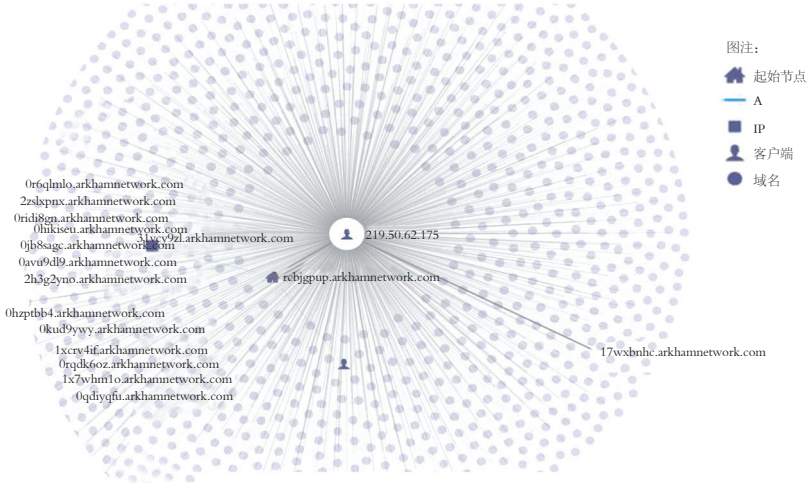


图2-3　Bot终端解析域名情况（来源：奇虎360公司）

通过图2-4可以分析出遭受拒绝服务攻击的不止*.arkhamnetwork.org、*.arkhamnetwork.com这两个根域名。其主要的两个DNS服务器是ns11.dnsmadeeasy.com和ns12.dnsmadeeasy.com，其中有多台类似IP地址167.114.25.179的Bot发起了很多针对*.arkhamnetwork.org的DNS拒绝服务攻击请求，造成两台NameServer拒绝服务。

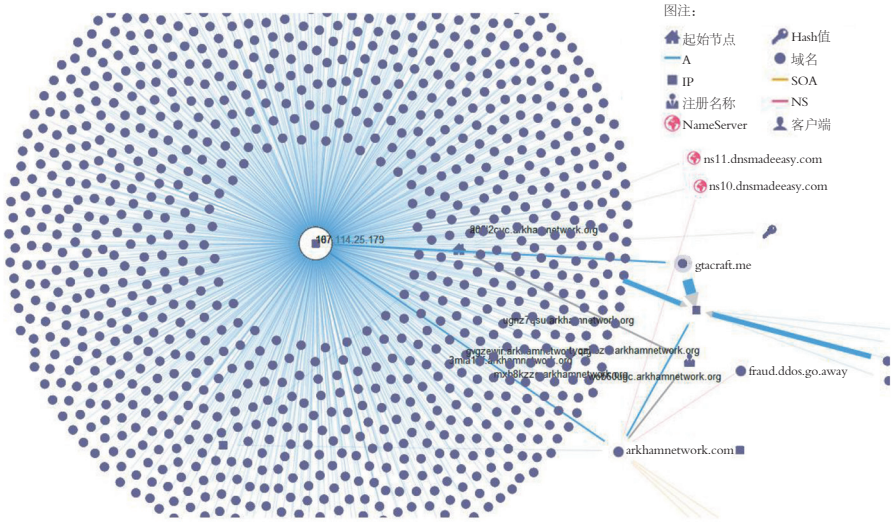


图2-4　遭受拒绝服务攻击的情况（来源：奇虎360公司）

深入分析，这些IP地址大多数都是路由器、智能摄像头等设备。初期攻击者是通过远程命令执行或者弱口令等方式获得系统权限，然后植入蠕虫程序，脚本运行后蠕虫不断地扫描任意C段的23号端口，利用弱口令抓取更多智能硬件设备，扩大点数产生更大的攻击流量如图2-5所示。

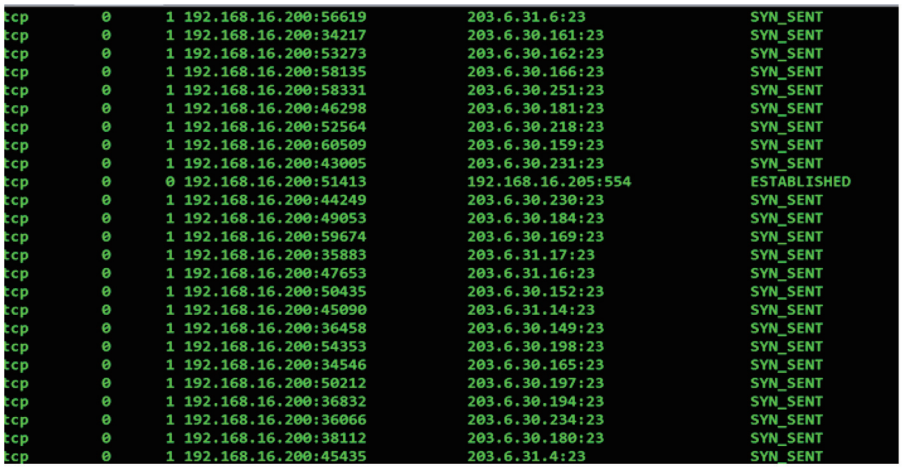


图2-5　利用弱口令抓取更多智能硬件设备，扩大点数产生更大的攻击流量
（来源：奇虎360公司）

通过网络活动定位到调用网络活动的进程文件如图2-6所示，该蠕虫程序会生成很多新的进程文件，进程文件中会包含此进程所执行的指令。

```
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17798
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17799
dr-xr-xr-x    6 root     root            0 Dec  9 17:25 178
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17800
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17801
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17802
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17803
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17804
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17805
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17806
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17807
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17808
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17809
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17810
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17811
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17812
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17813
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17814
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17815
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17816
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17817
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17818
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17819
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17820
dr-xr-xr-x    6 root     root            0 Dec 25 19:04 17839
```

图2-6　通过网络活动定位到调用网络活动的进程文件（来源：奇虎360公司）

蠕虫程序执行后会在指定目录下生成随机文件名的恶意代码，并在运行后自删除，如图2-7所示。

```
# ls -l
-r--------    1 root     root            0 Dec 25 18:53 auxv
--w-------    1 root     root            0 Dec 25 18:53 clear_refs
-r--r--r--    1 root     root            0 Dec 25 18:53 cmdline
-rw-r--r--    1 root     root            0 Dec 25 18:53 comm
-rw-r--r--    1 root     root            0 Dec 25 18:53 coredump_filter
lrwxrwxrwx    1 root     root            0 Dec 25 18:53 cwd -> /root
-r--------    1 root     root            0 Dec 25 18:53 environ
lrwxrwxrwx    1 root     root            0 Dec 25 18:53 exe -> /home/app/KrWdRug3 (deleted)
dr-x------    2 root     root            0 Dec 25 18:53 fd
dr-x------    2 root     root            0 Dec 25 18:53 fdinfo
-r--r--r--    1 root     root            0 Dec 25 18:53 limits
-r--r--r--    1 root     root            0 Dec 25 18:53 maps
-rw-------    1 root     root            0 Dec 25 18:53 mem
-r--r--r--    1 root     root            0 Dec 25 18:53 mountinfo
-r--r--r--    1 root     root            0 Dec 25 18:53 mounts
-r--------    1 root     root            0 Dec 25 18:53 mountstats
dr-xr-xr-x    5 root     root            0 Dec 25 18:53 net
-rw-r--r--    1 root     root            0 Dec 25 18:53 oom_adj
-r--r--r--    1 root     root            0 Dec 25 18:53 oom_score
-rw-r--r--    1 root     root            0 Dec 25 18:53 oom_score_adj
-r--------    1 root     root            0 Dec 25 18:53 pagemap
-r--------    1 root     root            0 Dec 25 18:53 personality
lrwxrwxrwx    1 root     root            0 Dec 25 18:53 root -> /
-r--r--r--    1 root     root            0 Dec 25 18:53 smaps
```

图2-7　蠕虫程序执行后会在指定目录下生产随机文件名的恶意代码（来源：奇虎360公司）

奇虎360公司找到了一些没有删除的恶意样本并将其下载进行分析，如图2-8所示。

```
-rwsr-sr-x    1 root     root            0 Dec 18 03:46 0QPxHF
-rwsr-sr-x    1 root     root            0 Dec 13 15:00 2cVs
-rwsr-sr-x    1 root     root            0 Dec 18 01:59 AKmnQ5bO
-rwsr-sr-x    1 root     root            0 Dec 10 09:38 G631Uot
-rwsr-sr-x    1 root     root            0 Dec 21 09:28 KeHVlN
-rwsr-sr-x    1 root     root            0 Dec  9 17:34 MZAWz
-rwsr-sr-x    1 root     root            0 Nov 26 02:05 NeEP
-rwxr-xr-x    1 root     root        87355 Dec 24 16:46 RVklNaZX2T
-rwsr-sr-x    1 root     root            0 Dec 10 17:20 YTF8qaNRt
-rwsr-sr-x    1 root     root            0 Nov 23 00:51 av68RFGe
drwxr-xr-x    2 744      hikvisio        0 Nov 17 16:39 certs
-rwsr-sr-x    1 root     root            0 Dec  9 23:26 flMFHqK
-rwsr-sr-x    1 root     root            0 Dec 11 16:31 hQGmH18z
-rwxr--r--    1 744      hikvisio  8551156 Mar  4 09:53 hicore
-rwsr-sr-x    1 root     root            0 Dec 21 09:06 iiireIvzal
drwxr-xr-x    3 744      hikvisio        0 Nov 17 16:39 iscsi
-rwsr-sr-x    1 root     root            0 Dec 18 16:39 j78N301Vq
-rwsr-sr-x    1 root     root            0 Nov 25 08:59 jRWMO
-rwxr--r--    1 744      hikvisio   424364 Feb 20 05:22 ntfs-3g
-rwsr-sr-x    1 root     root            0 Nov 24 18:33 oWfG
-rwsr-sr-x    1 root     root            0 Nov 22 09:34 pIFaq
-rwxr--r--    1 744      hikvisio   178648 Feb 20 05:22 pppd
-rwxr--r--    1 744      hikvisio    30016 Feb 20 05:22 pppoe
-rwxr--r--    1 744      hikvisio     9380 Feb 20 05:22 pppoed
```

图2-8　奇虎360公司对没有删除的恶意样本进行分析（来源：奇虎360公司）

首先判断这些恶意文件是ELF可执行文件，并不是脚本类的，如图2-9所示。

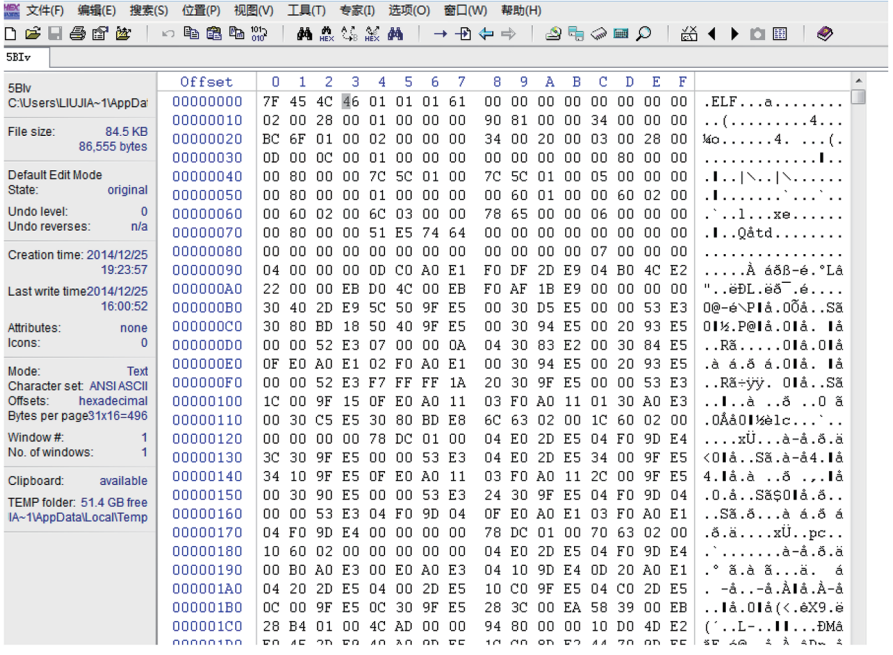


图2-9　奇虎360公司判断恶意文件为ELF可执行文件（来源：奇虎360公司）

使用反汇编分析工具对样本文件进行静态分析，能够看到该蠕虫程序的一些任务指令以及控制服务器的地址。还有一些是控制服务器IP地址显示这台智能硬件的状态。目前分析到Sleeping和Dildos两个状态，如图2-10所示。

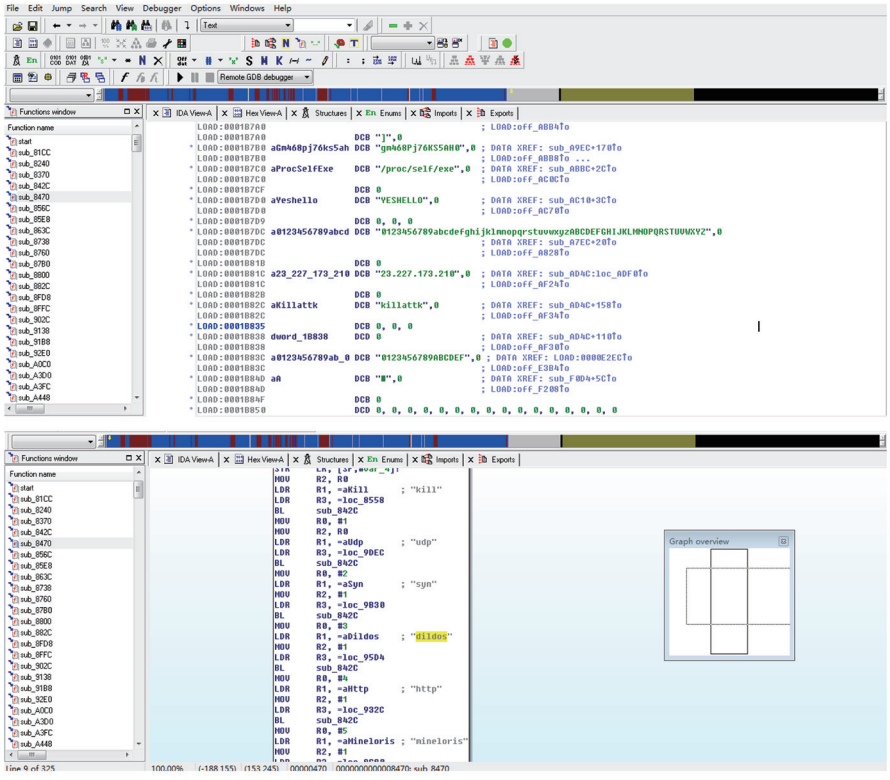


图2-10　Sleeping和Dildos两个状态（来源：奇虎360公司）

根据逆向分析后得到的关键信息，发现该智能硬件蠕虫状态存在的进一步证据，图2-11显示的是该智能硬件处于Sleeping状态。

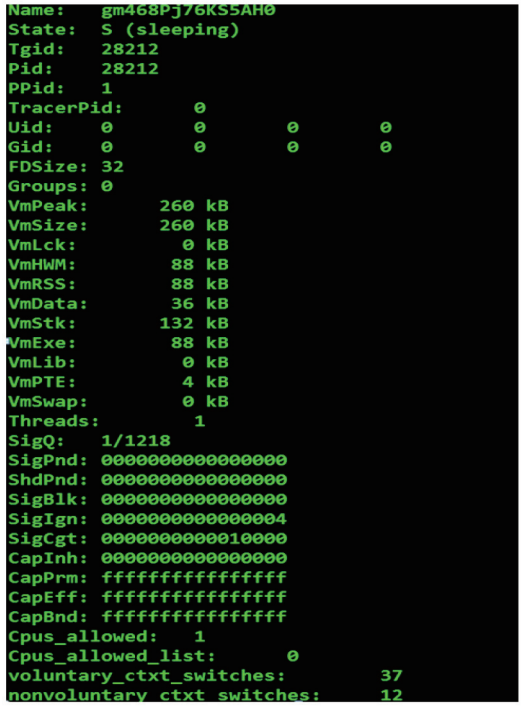


图2-11　智能硬件处于Sleeping状态（来源：奇虎360公司）

进入Sleeping状态时，这个终端只与控制服务器（23.227.173.210）连接，不执行任何扫描感染任务，也不进行DoS攻击任务，如图2-12所示。

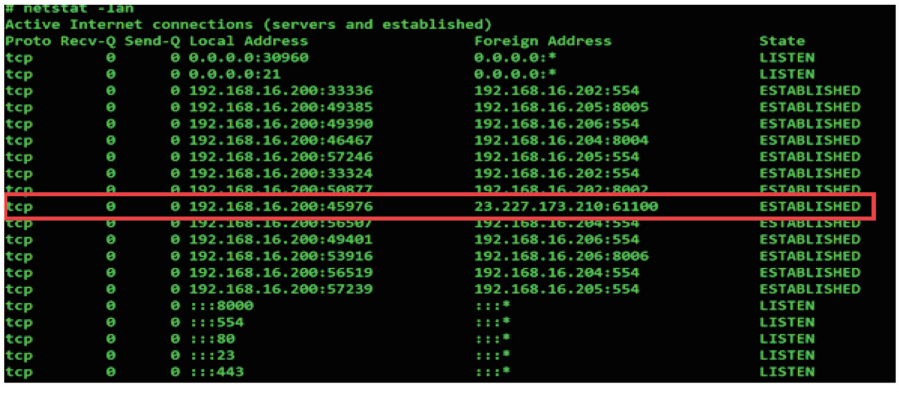


图2-12　Sleeping状态时终端只与控制服务器连接（来源：奇虎360公司）

通过对这个智能硬件的程序分析，总结出智能硬件的蠕虫感染途径。首先是由攻击者利用智能硬件漏洞获得Root权限，执行蠕虫代码；控制服务器则等待智能硬件上线，随后在默认的情况下感染蠕虫的智能硬件会自动扫描发现其他的智能硬件，并自动利用漏洞让目标感染蠕虫程序。控制程序还有一个状态就是Sleeping，这个状态就是保持与控制服务器的连接，等待下发指令，当前不做任何网络活动，最后发起攻击时就是Dildos状态，如图2-13所示。根据目前静态分析的结果有这样几个状态，不排除今后变种会有更多的状态。

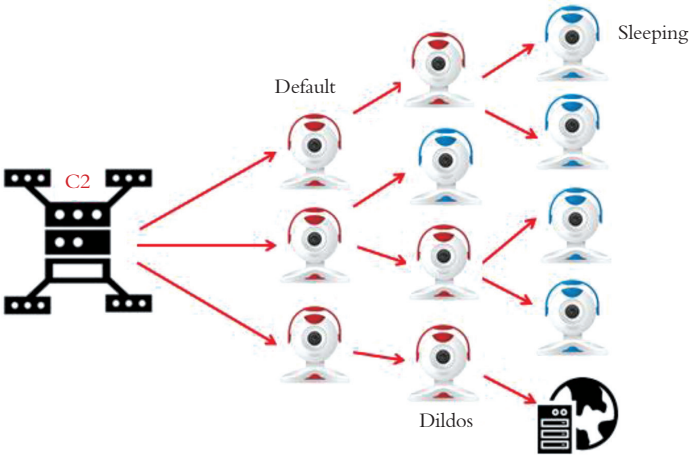


图2-13　最后发起攻击时的Dildos状态（来源：奇虎360公司）

2.3.2.2　事件危害

根据云堤的数据，2014年12月10日，已监测到的攻击最大流量近1亿QPS（约合76.38Gbit/s），结合国外的消息，推测此次发起攻击的消息，是使用了1000多个终端发起的攻击。这个数字已经很可怕了，如果有1万个这样的智能硬件受到感染发起攻击，那么流量将会在700Gbit/s左右。更何况现在的智能摄像头、路由器、智能插座层出不穷，未来出货量将成倍增长。那么当智能硬件达到一个量级时，由于其自身安全问题会给互联网造成很大的安全威胁，实际上是将网络战场延伸到智能硬件领域。

2.3.3　防范措施及建议

这类恶意程序的防范很难，由于大多数驻留在智能硬件固件系统中，固件不具备

查杀恶意程序所依赖的环境，彻底查杀起来非常难；而且很多用户在进行初次配置完成后就不会再关注这些设备，这也增加了查杀的难度。

（1）建议用户修改自己的智能摄像头、路由器等硬件的默认密码，关注官方发布的更新程序。

（2）建议厂商加强固件的安全审计，对智能硬件进行测评，保障智能硬件不存在信息安全问题，才可以供货。另外，还应关注国内外对智能硬件进行安全测试结果和漏洞，新漏洞出现时需及时打补丁。

（3）建议相关部门、基础电信企业、安全公司对Bot进行全方位监控，如果Bot发起大量的异常攻击，应从基础电信企业层面进行流量清洗。对Bot恶意版本的变化进行定期的取样和分析，研发相关查杀脚本。

2.4 短信拦截黑客地下产业链案例分析（来源：安天公司[19]）

从2013年5月至今，AVL移动安全团队持续监测到一类高活跃、高危害的短信拦截类型木马——短信拦截马。这是一种可以拦截他人短信的木马，让被攻击者收不到短信，并将短信内容截取到攻击者手机上。目前此类木马最常见的是通过钓鱼、诱骗、欺诈等方式诱导用户装上木马，然后通过拦截转发用户短信内容，以此获取各种用户重要的个人隐私信息，如用户姓名、身份证号码、银行卡账户、支付密码及各种登录账号和密码等，造成信息泄露；再利用此信息从而达到窃取用户资金的目的，严重威胁用户的财产安全。另外，此前流行的“××神器”也有短信拦截转发的功能。

2.4.1 数据统计

短信拦截马功能简单，开发成本低，但更新变化速度快，伪装目标不断更换，涉及样本量比较庞大。从最早2013年5月出现到2014年9月，共截获该类木马近2万个。

（1）活跃曲线

从2013年5月起，AVL移动安全中心每月都能监控到该类木马，从其活跃曲线可以

[19] 安天公司即哈尔滨安天科技股份有限公司，是通信行业互联网网络安全信息通报工作单位、国家信息安全漏洞共享平台成员、中国反网络病毒联盟成员，也是CNCERT/CC国家级应急服务支撑单位。

看到其呈现不断增长的趋势，如图2-14所示。

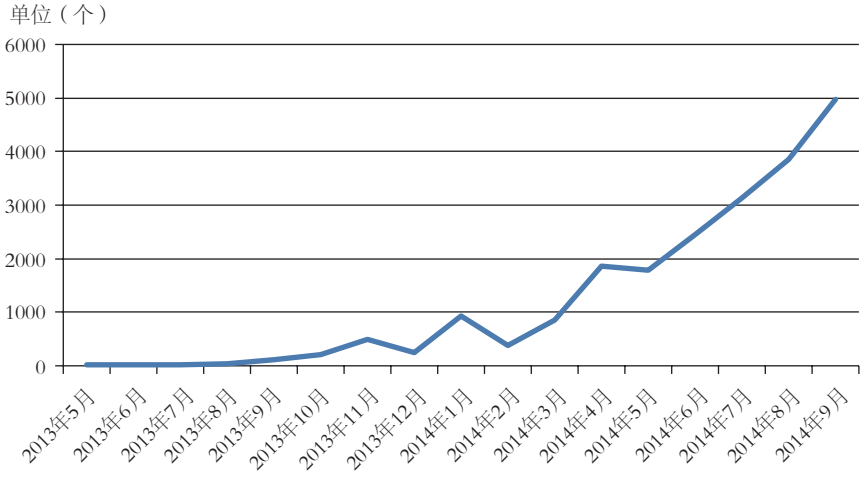


图2-14　拦截马样本捕获情况（来源：安天公司）

（2）行为分布

短信拦截马的行为主要是拦截并转发短信来窃取隐私，此外部分还带有隐私窃取、诱骗欺诈、远程控制、资费消耗、恶意扣费等。从图2-15拦截马主要行为分布可以发现，诱骗欺诈、远程控制、资费消耗都占有不小的比例。

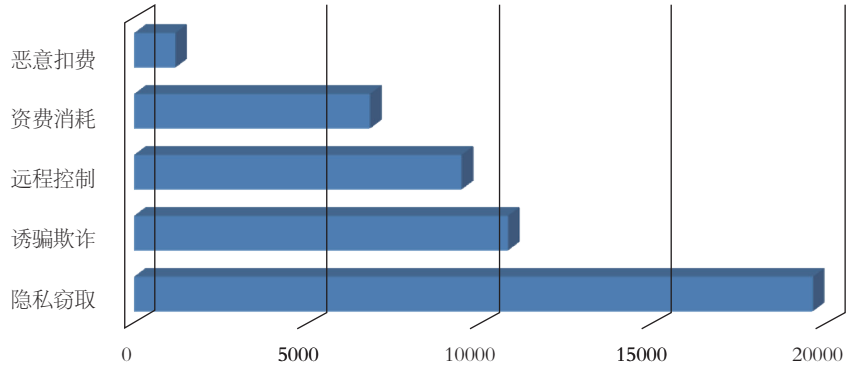


图2-15　拦截马主要行为分布（来源：安天公司）

（3）样本包名TOP20

图2-16为拦截马伪装包名TOP20，从中可以发现最多的是伪装成Android系统应用名，其次则是Example、Test等测试名称。

包名
com.android.system.emial
com.example.test
cn.android.emialvae
com.microdu.light
com.message.send
com.example.os_messagect
com.sonyericsson.androidapp.microblogci8dmdo4
cn.newjob.msgfg
com.google.app.msg
com.china.fss.lockscreen11111
cn.android.service
com.android.providers.message
com.keeper.manage
picture.image
com.sonyericsson.androidapp.microblog
cn.itcast.lockscreen2
com.system.mdemonmn
com.example.sms
com.a.b
ji.yj.ur.pd

图2-16　拦截马伪装包名TOP20（来源：安天公司）

（4）伪装应用TOP10

图2-17为拦截马样本伪装应用TOP10，中国移动最多，其次还有淘分享、移动客户端、10086、移动掌上营业厅等。

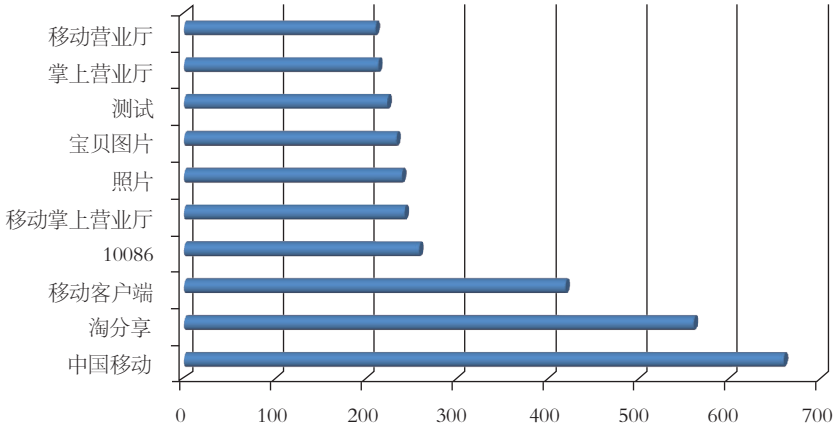


图2-17　拦截马伪装应用TOP10（来源：安天公司）

2.4.2　对抗情况

拦截马家族发展迅速，持续的演变过程中不得不与安全软件查杀对抗，除了常规恶意代码手段，拦截马家族更喜欢采用加壳这种简单有效的手段。频繁更换修改加壳方式、高频率持续更新以保证绕过安全软件。

图2-18为拦截马家族加壳样本捕获情况，从中可见拦截马最早出现的时候就已经开始使用加壳技术，不过直到2014年6月才开始持续增长，而现在正是高速爆发时期。

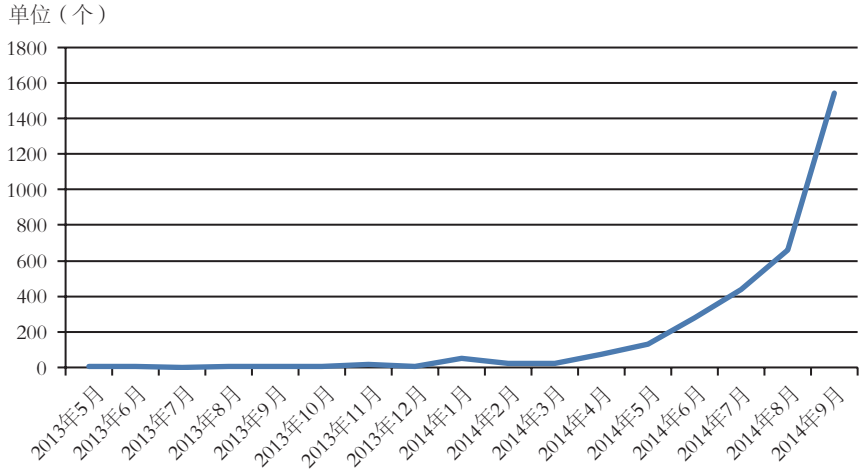


图2-18　拦截马加壳样本捕获情况（来源：安天公司）

图2-19为拦截马加壳样本与当月样本数的统计情况，拦截马的捕获数量依然在持续增长，而加壳样本比例亦在增加。

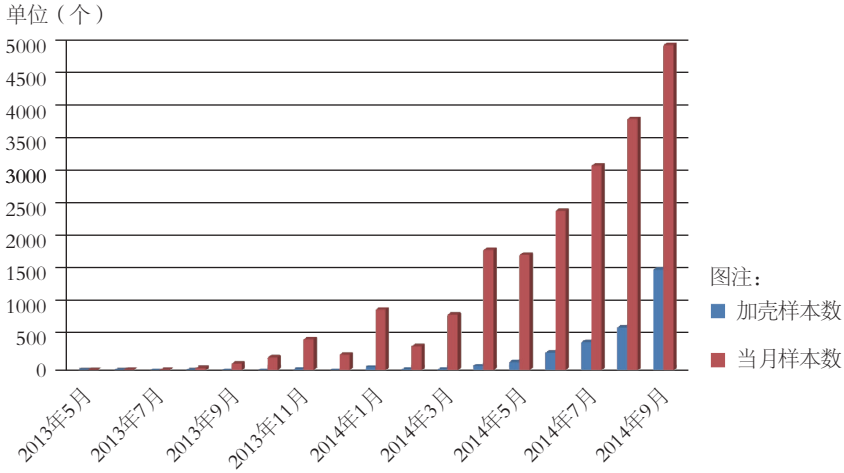


图2-19　拦截马加壳样本统计（来源：安天公司）

对拦截马加壳样本所采用的加壳方案进行统计（如图2-20所示），其中大部分都在使用apkprotect这一加固方案，其他方案则较少。

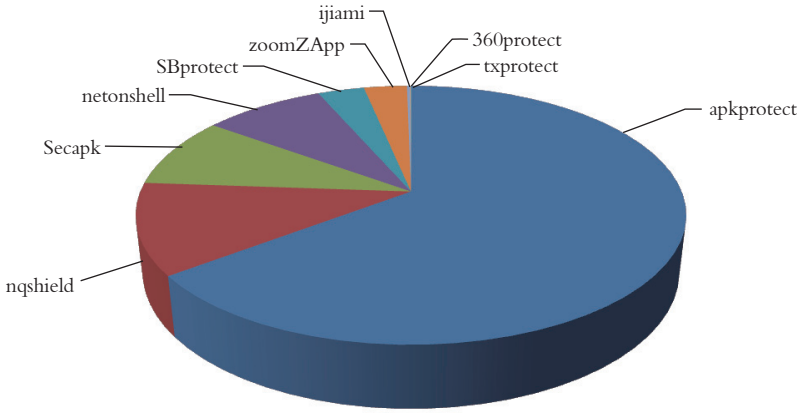


图2-20　拦截马加壳类型统计（来源：安天公司）

加固是一把双刃剑，保护开发者APP的同时也成为木马作者的一把“保护伞”，

加固公司应在加固应用前多做恶意代码审核工作。

2.4.3 黑客地下产业链揭露

拦截马的爆发有其必然原因，根据AVL团队研究人员取证以及卧底收集，最终还原了完整的黑客地下产业链。

如图2-21所示，从伪基站发送伪造钓鱼网站地址，再到用户访问钓鱼网站，欺骗用户输入个人信息，网站挂马诱导用户下载安装短信拦截木马，最后攻击者在线转账时通过拦截马转发网银验证码完成转账，这就是一个简单的拦截马工具模型。

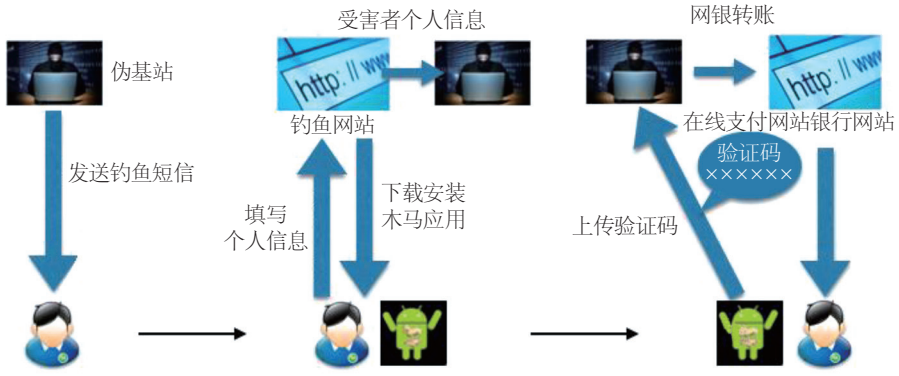


图2-21 拦截马攻击模型（来源：安天公司）

如图2-22所示，拦截马黑客地下产业链分工明确，结构简单，主要由以下4部分组成。

开发售卖：这部分主要是拦截马木马的开发以及免杀，钓鱼网站的开发出售，伪基站的出售。

木马分发：主要有钓鱼短信、网站挂马、二维码传播。

窃取售卖：拦截马植入成功即可获取拦截短信，但黑客地下产业链关注的信息主要在于各大银行、支付宝、游戏点卡、运营商话费充值卡、Q币等，这些信息都是可以直接交易。

洗钱：洗钱是获利最多的，但同时也是风险最大的。

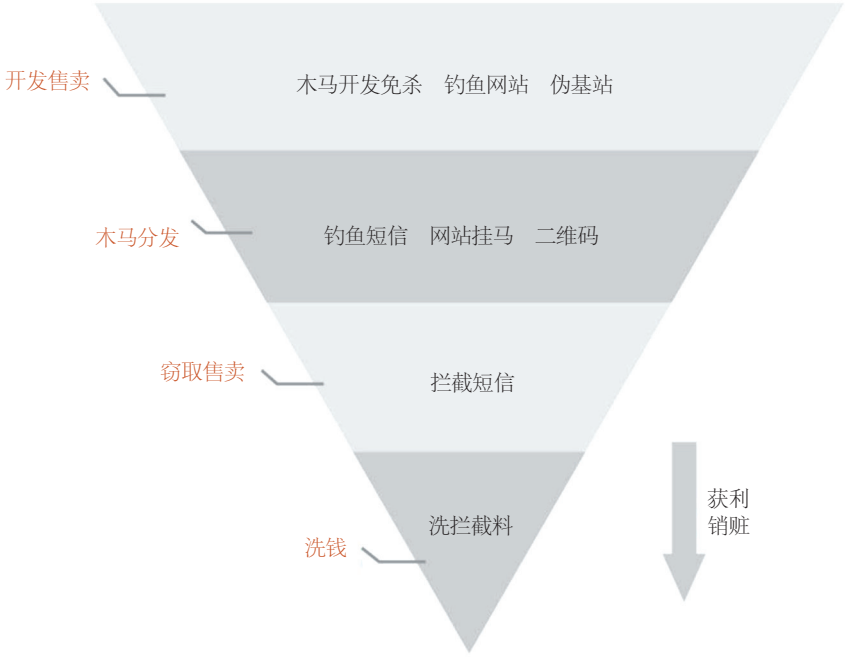


图2-22　拦截马黑客地下产业链（来源：安天公司）

2.4.4　相关产业

在百度搜索“拦截马”就有118万条结果，如图2-23所示，其中有产业链揭露，样本破解分析，更多则是交易信息。

图2-23 百度“短信拦截马”得到百万以上词条（来源：安天公司）

（1）木马开发

图2-24为猪八戒网上针对拦截马的开发需求，可见拦截马开发及免杀依然在持续

中；不过拦截马功能比较简单，开发成本较低，即便免杀也通常使用已有加固方案，所以报酬都比较低。

图2-24　猪八戒网上关于拦截马的开发需求（来源：安天公司）

（2）伪基站

伪基站是近几年开始流行的，黑客地下产业链通常用于发送伪造短信诱导用户进入钓鱼网站，图2-25即是一个伪造的中国工行短信，值得注意的是其使用了.gov.cn域名下的子页，相对加强了权威性而降低了用户警惕性。

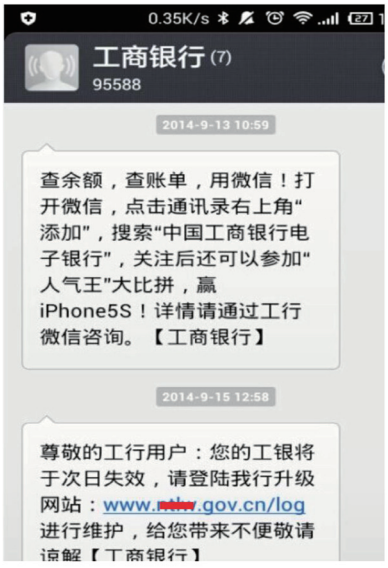


图2-25　伪基站钓鱼网站短信（来源：安天公司）

另外，伪基站还有图2-26的诈骗方式，通过伪造短信恐吓用户进行诈骗行为，不久前“小龙女”李若彤经纪人被诈骗百万元以上，手法与此类似。

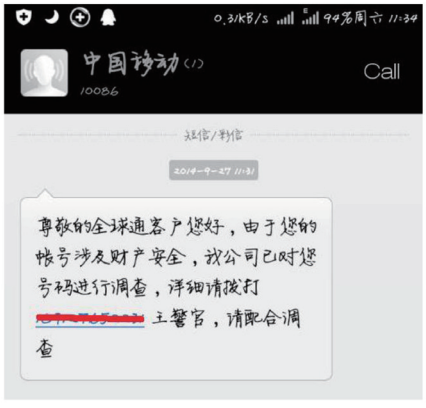


图2-26　伪基站诈骗短信（来源：安天公司）

（3）钓鱼网站

拦截马样本最爱伪装中国移动，所以发现大量的山寨中国移动钓鱼网站，如图

2-27所示。此类网站通常以积分兑换现金来诱骗用户输入相关银行账号信息，同时诱导用户下载安装短信拦截木马。

图2-27　山寨中国移动钓鱼网站（来源：安天公司）

图2-28是一个山寨中国电信钓鱼网站。其采取同样的手法获取用户个人信息并诱导用户安装短信拦截木马，该木马还会欺骗用户不要卸载，如图2-29所示。

图2-28　山寨中国电信钓鱼网站（来源：安天公司）

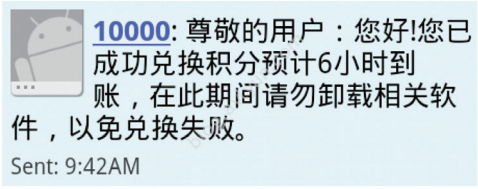


图2-29　木马欺骗用户不要卸载（来源：安天公司）

（4）洗钱

利益所驱，正是拦截马火爆的主要原因。图2-30为某黑客地下产业链人员曝光的拦截马洗钱记录，可谓日入上万不是梦。

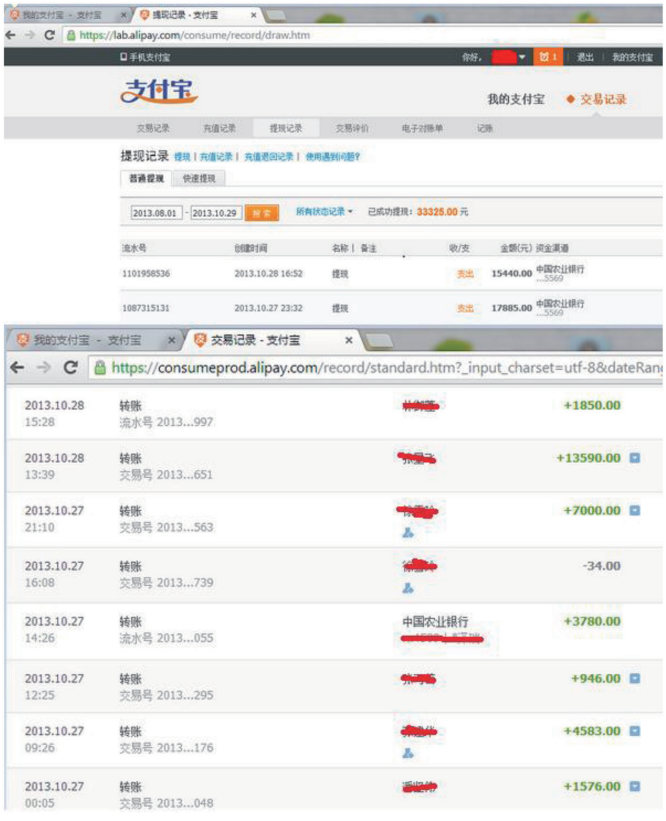


图2-30　拦截马洗钱记录（来源：安天公司）

2.4.5 总结

随着时间的推移，移动通信技术的发展，智能手机的出现，移动支付渐渐占据主流。由于手机支付安全问题日益突出，加上Android应用开发简单，以及伪基站的出现，加固方案的发展，再结合流行已久的钓鱼网站，短信拦截马作为一个功能简单、开发成本低，但获利颇高的黑色行业，不可避免地在短时间内便形成了完整的产业链。

短信拦截马家族此刻正处在高速爆发时期，无论数量还是质量都有着明显的提高，尤其大量加壳对抗样本的出现，给安全公司分析人员造成了极大的困扰。希望诸多加固公司在对应用加固的时候，多做一些恶意代码审核工作。

拦截马家族变化速度快，对抗强度高，传播渠道广，欺骗性强，极易造成用户重大经济损失以及隐私泄露。随着拦截马家族的爆发，同时会不断产生大量的伪基站诈骗短信以及钓鱼网站，希望用户能保持良好的安全上网习惯，以及对钓鱼欺诈的警觉。这样可以极大地避免威胁，用户还可以下载并使用AVL Pro对该类木马进行检测和查杀。

2.5 12306泄密事件到国内外信息泄露安全事件分析（来源：深信服公司）

在分析12306泄密事件之前，首先对2014年国内外泄密事件进行回顾。2014年是国内外多个泄密事件集中爆发的一年，涉及国内外多家网站。部分典型涉密事件见表2–1。

表 2–1 部分典型泄密事件（来源：深信服公司）

企业名称	泄露内容	泄露数量
中国高等教育学生网	学生信息	130万
美国社区医疗CHS	患者信息	450万
韩国三大信用卡公司	信用卡数据	2000万
塔吉特	用户信息及信用卡数据	1.1亿
家得宝	用户信息及邮件地址	1.1亿条
摩根大通	用户及企业信息	1.4亿条
iCloud艳照门	个人照片	100+明星
12306官网	旅客个人信息	10万

在黑客术语里面，有“拖库”、“洗库”与“撞库”之说。“拖库”是指黑客入侵有价值的网络站点，把注册用户的资料数据库全部盗走的行为。在取得大量的用户数据之后，黑客会通过一系列的技术手段和黑客地下产业链将有价值的用户数据变现，这被称作“洗库”。最后黑客将得到的数据在其他网站上进行尝试登录，叫做“撞库”。鉴于目前有相当一部分互联网用户喜欢使用统一的用户名和密码，因此大大增加了黑客“撞库”的成功几率。

2.5.1 12306泄密事件全程回顾

首先对该事件进行全程回顾。

（1）2014年12月25日10:59，乌云网http://www.wooyun.org/bugs/wooyun-2014-088532发布漏洞报告称，大量12306用户数据在网络上疯狂传播，如图2-31所示。

图2-31 乌云报告平台对12306事件的披露（来源：深信服公司）

本次泄露事件中被泄露的数据达131653条，包括用户账号、明文密码、身份证号码和邮箱等多种信息，共约14MB数据。经测试发现，该批131653条12306用户数据是真实的。

（2）12306官方及时发表公告《关于提醒广大旅客使用12306官方网站购票的公告》（www.12306.cn/mormhweb/zxdt/201412/t20141225_2448.html），如图2-32所示。


首页 > 最新动态

关于提醒广大旅客使用12306官方网站购票的公告

[2014-12-25]

针对互联网上出现“12306网站用户信息在互联网上疯传”的报道，经我网站认真核查，此泄露信息全部含有用户的明文密码。我网站数据库所有用户密码均为多次加密的非明文转换码，网上泄露的用户信息系经其他网站或渠道流出。目前，公安机关已经介入调查。

我网站郑重提醒广大旅客，为保障广大用户的信息安全，请您通过12306官方网站购票，不要使用第三方抢票软件购票，或委托第三方网站购票，以防止您的个人身份信息外泄。 同时，我网站提醒广大旅客，部分第三方网站开发的抢票神器中，有捆绑式销售保险功能，请广大旅客注意。

中国铁路客户服务中心

2014年12月25日

关 闭

图2-32　12306官方网站的公告（来源：深信服公司）

12月26日中午，中国铁路官方微博表示，铁路公安机关于2014年12月25日晚，将涉嫌窃取并泄露他人电子信息的犯罪嫌疑人抓获。

2.5.2　事件剖析

乌云网白帽子在http://www.sgklt.com/forum.php?mod=viewthread&tid=2529论坛，发现12306的信息数据在进行地下交易，如图2-33所示。

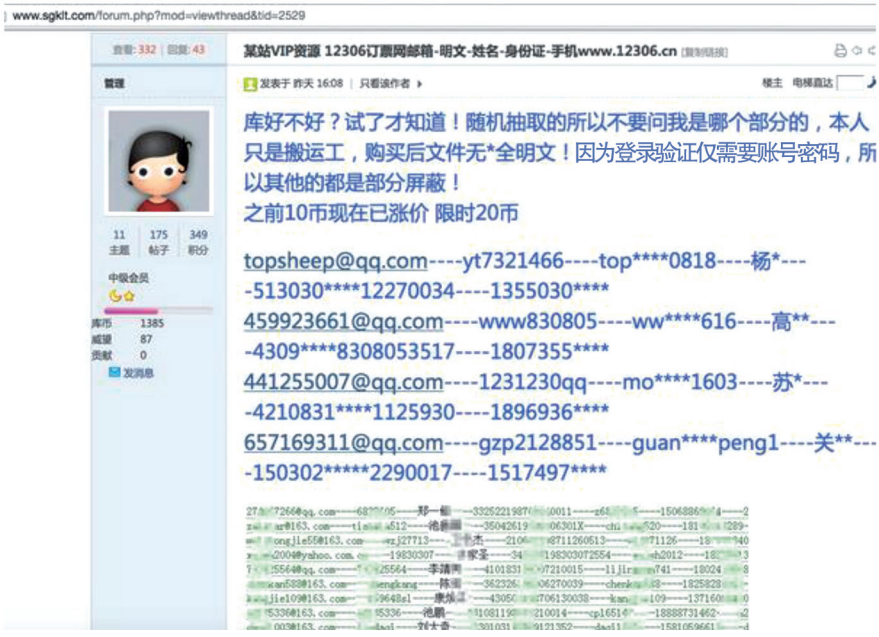


图2-33　地下社工库论坛（来源：深信服公司）

一则“12306用户数据泄露”事件通过微博、QQ、论坛等社交渠道迅速蔓延开来，部分微博大V对该事件进行转载，央视的新闻频道也对该事件进行解读与报道。

接下来，一个名为“12306%40邮箱-密码-姓名-身份证-手机%28此数据并不全%29.txt”文件，在各种云盘中传播开来，随机登录部分账号发现全部真实。

大多数人开始对14MB的数据进行挖掘，查询自己或朋友、家人的信息。

当查询不到时，更多的人选择继续寻找全的数据。此时，大家便开始重新关注“22GB、32GB”。当你打开下载文件时，再次重温了儿时经典《葫芦娃》。

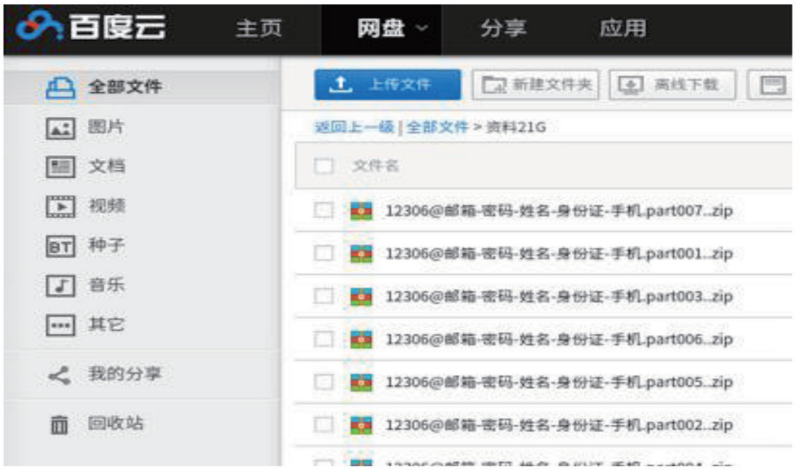


图2-34　百度云盘上共享的22GB儿时经典《葫芦娃》（来源：深信服公司）

在怀疑“撞库”的同时，也有人开始怀疑是否12306本身就存在安全漏洞。于是12306网站存在漏洞论调相继出现。深信服安全团队在排查12306网站及多个子站的时候，发现12306确实存在安全漏洞。2014年12月27日验证漏洞的截图如图2-35所示。

图2-35　12306某分站存在远程命令执行漏洞（来源：深信服公司）

可以说，攻击者使用Struts漏洞可以轻松获取服务器控制权限。这次事件都说是“撞库”，但12306多个子站真有漏洞，那么是否是这些漏洞造成的？带着这个疑问，深信服安全团队对其进行进一步分析研究。

虽说攻击者可以利用Struts 2漏洞入侵服务器，获取最高权限，但即使最高权限也不能获取服务器上本就没有的资料，也就是说受影响的服务器根本就没有旅客数据信息。

再通过数据中的密码全是明文以及数据在文件中的存储格式综合判断，得出14MB的13万用户数据信息是一次“撞库”事件。

2.5.3 触目惊心的地下数据库

可以说，本次事件的导火索是某位乌云白帽子在（http://www.sgklt.com/）地下论坛发现了12306的数据库在地下交易。那么接下来，我们来看一看这个神秘的领域。

案例一，某社工数据库只需输入姓名，便可以查询开房记录，如图2-36所示。

图2-36 地下社工库（来源：深信服公司）

案例二，某社工数据库只要提供手机或邮箱，就可以轻松查到该用户曾经注册过哪些网站。由于很多人都有使用同一邮箱或手机注册网站的习惯。那么使用邮箱或手机号便可查询相应结果，如图2-37所示。

图2-37　REG007社工网站（来源：深信服公司）

其实很多人都有相同习惯，为了方便，多个网站使用相同的账号和密码。无论是小网站还是淘宝和天猫涉及财产的网站，密码都是同一个，那么只要其中一个网站“沦陷”了，所有账号都会受到危险。

2.5.4　针对信息泄露的对策建议

（1）增加密码的复杂度，不使用弱口令，如123456、password等。为了方便记忆，可使用专门的密码软件管理自己的密码。

（2）分级管理账号和密码，记住涉及财产的、重要的账号（如淘宝、天猫）要独立设置账号、密码。

（3）定期修改密码，每隔一段时间修改账号和密码，可以有效避免数据库泄露影响到自身账号安全。

（4）工作邮箱不用于注册网络账号，避免数据泄露危及企业安全。

（5）不使用电脑自动保存密码功能，不随意在未知的第三方网站上输入账号和密码。

2.5.5 未来信息泄露安全威胁不容乐观

基于对2014年国内外信息泄露安全事件的分析，以及对2014年国内多个领域、行业的测评，深信服安全团队发现，2015年信息泄露安全威胁不容乐观，多形式的信息泄露正在向我们袭来。

（1）金融行业数据泄露威胁存在上升趋势

国外金融安全方面。金融是一个特殊行业，存放的往往是个人用户的关键数据。2014年1月21日，据报道，近半数韩国人的信用卡账户信息失窃，并被非法转卖给市场营销公司，包括姓名、居民身份证号码和信用卡详细信息。该事件波及韩国人口的40%，这绝对是一个触目惊心的数字。

国内金融安全方面。深信服安全团队对国内多家金融机构评估发现，国内金融行业安全形势不容乐观。图2-38是对国内某知名大型保险公司的一次安全测评中发现，通过SQL注入漏洞，攻击者可以直接获取数据库中任意数据。

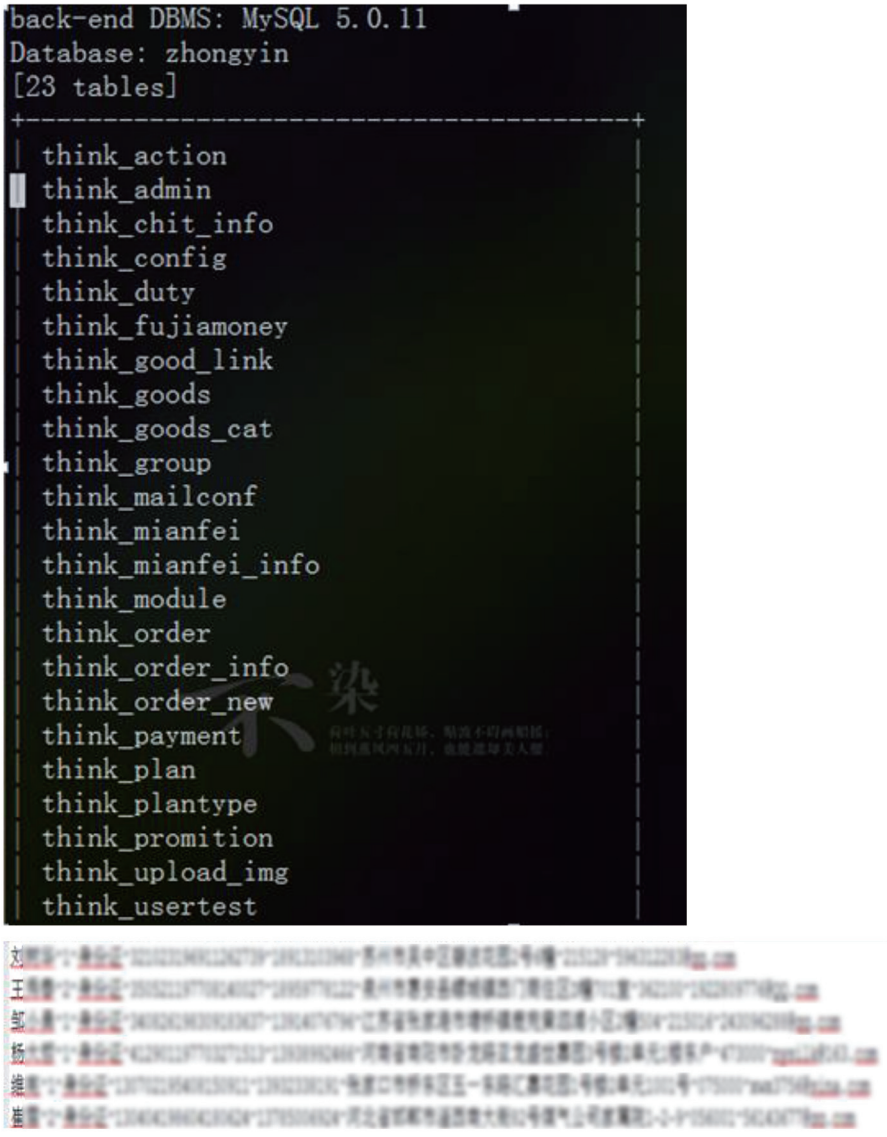
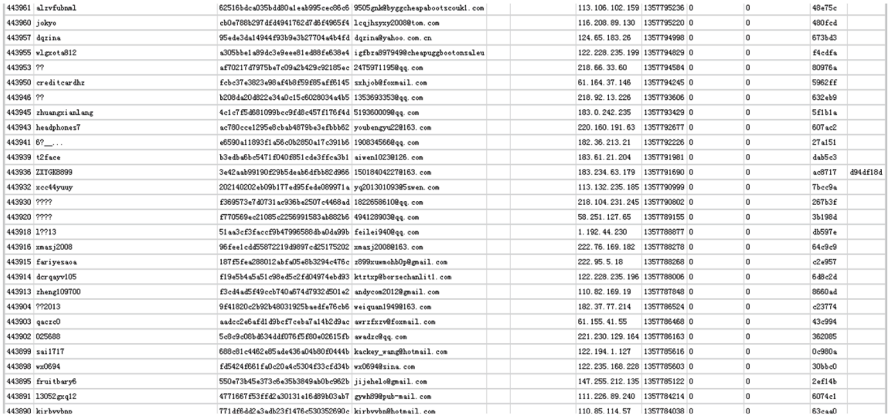


图2-38　中国某金融系统SQL注入漏洞（来源：深信服公司）

前不久央视报道一个18岁的“黑客”，竟然通过自学编程，带领一批人在网上大肆盗刷别人银行卡，涉案金额近15亿元。

一个偶然的机会，笔者通过地下产业链，获取某银行信用卡数据泄露个人信息数据。图2-39为该数据截图，笔者估算了一下，个人信息数据不少于20万。



443961	alrvfubmal	62516b4ca035b4d80a1ea995cec06c6	9505gm49byggcheapabootscouk1.com		113.106.102.159	1357795236	0	0	48e75c	
443960	jokyo	cb0e7888297dfd4941762d7464f4965f4	lcqjhsynyz2009@tom.com		116.208.89.130	1357795220	0	0	480fcd	
443957	dqrina	95ede3da14944f93b9e3b27704e4b4fd	dqrina@yahoo.com.cn		124.65.183.26	1357794998	0	0	673b43	
443955	wlgrota812	a305bb6la89dc3e9eee81ed86fe638e4	igfbrz8979498cheapruggbootsnnralen		122.228.235.199	1357794829	0	0	f4cdfa	
443953	??	af702174f975b47c99a2b429c92185ec	247597119@qq.com		218.66.33.60	1357794584	0	0	80976a	
443950	creditcardhr	fcbc37e3823e86af4b8f59f85af65145	xuhjob@foxmail.com		61.164.37.146	1357794245	0	0	5962ff	
443946	??	b2084d204822e34a0c15c6028034e4b5	1353693358@qq.com		218.92.13.226	1357793606	0	0	632eb9	
443945	zhuangxianlang	4c1e7f5d681099bcc9f48ce457f176f4d	5193600098@qq.com		183.0.242.235	1357793429	0	0	5f1b1a	
443943	headphones7	ac780cce1295e0cbab4879ba3afbbb62	youbangyu229163.com		220.160.191.63	1357792677	0	0	607ac2	
443941	67_._.	e6590a118935f1a56c0b2050a17c3916	1908345660@qq.com		182.36.213.21	1357792226	0	0	27a151	
443939	t2face	b3edb46bc5471f040f851cda3ffca3b1	aiwen10230126.com		183.61.21.204	1357791981	0	0	dab5c3	
443936	ZITGH8899	3e42aab99190f29b5dab6dfbb82d966	15018404227@163.com		183.234.63.179	1357791690	0	0	ac871f	d94df184
443932	xcc44yuuy	202140202ab09b177e495fe4e069971a	yg20130109395wxn.com		113.132.235.185	1357790999	0	0	7bcc9a	
443930	????	f3695737e7d0731ac936be2507c4468ad	1822658610@qq.com		218.104.231.245	1357790802	0	0	267b3f	
443920	????	f770569ec21085c2256991583ab882b6	4941289038@qq.com		59.251.127.65	1357789155	0	0	3b198d	
443918	1??13	51aa3cf3facef9b47995686db5d4a99b	feilei9408@qq.com		1.192.44.230	1357788877	0	0	db597e	
443916	xmanj2008	96fee1cd45587221948987c425175202	xmanj20080163.com		222.76.169.182	1357788278	0	0	64c9c9	
443915	fariyesaca	18785fea286012abfa05e8b3294c476c	z099zuwenbb0y@gmail.com		222.95.5.18	1357788268	0	0	c2e957	
443914	dcrqsyv105	f19e5545a5a51c98ed5c2fd04974ebd93	ktztzp@berschanlit1.com		122.228.235.196	1357788006	0	0	6d8c2d	
443913	zhengl09700	f3c84a45f49ccb740a574d7932d501e2	andycom20128@gmail.com		110.82.169.19	1357787848	0	0	8660ad	
443904	??2013	9f41820c2b92b4803192 5baedfe76cb6	weiquanl9498163.com		182.37.77.214	1357786524	0	0	c23774	
443903	qaccc0	aadcc2e6af4d49bcf7cab7a14b2d9ac	61.155.41.55		61.155.41.55	1357786468	0	0	43c994	
443902	025688	5c0c9c06b46344dd076f6f00e02615fb	wudcc@qq.com		221.230.129.164	1357786163	0	0	362085	
443899	zai1717	688c81c4462e05ade436a04b80d044b	kackay_wang@hotmail.com		122.194.1.127	1357785616	0	0	0c980a	
443898	wx0694	fd5424f661fa0c20a4c5304f33cfd34b	wx0694@sina.com		122.235.168.228	1357785603	0	0	30bbc0	
443895	fruitbary6	550e73b45a373c6a35b3849ab0bc962b	jijehelo@gmail.com		147.255.212.135	1357785122	0	0	2ef14b	
443891	13052gzql2	4771667f53ffd2a30131e164f9b03ab7	gzwh898pub~mail.com		111.226.89.240	1357784214	0	0	6074c1	
443890	kirbvvbnn	771df6d2a3adb23f1476e530352690c	kirbvvbn@hotmail.com		110.85.114.57	1357784038	0	0	63caa0	

图2-39　某银行信用卡数据泄露（来源：深信服公司）

（2）互联网信息泄露依然占主导作用

目前，教育行业、金融行业、医疗行业、物流行业、政府等都与互联网密切相关。

深信服安全团队对国内教育行业某系统评估发现，该信息管理系统存在网站平行权限漏洞，攻击者通过变换ID，可以获取所有学生信息。

在国外，2014年8月31日，爆发了震惊全球的“iCloud艳照门”事件。4chans和Reddit曝光了苹果iCloud系统被入侵，包括“90后”奥斯卡影后詹妮弗-劳伦斯、艾莉安娜、维多利亚等百位女星纷纷卷入。

（3）物联网时代到来，嵌入式设备信息泄露加剧

随着物联网时代的到来，家庭、企业网络摄像头安全问题随之急剧地放大。

2014年11月俄罗斯一家网站上可以观看到256个国家的7.3万个监控摄像头，包括上万个私人摄像头的流媒体视频，如图2-40所示。

图2-40　流媒体视频（来源：深信服公司）

2014年11月，深信服安全团队对受影响的7.3万个摄像头展开抽样调查，发现该款摄像头多为AXIS网络摄像头，该型号摄像头存在未授权访问可直接查看实时画面。

深信服安全团队顺势对国内家庭网络摄像头进行安全评估，发现SparkLAN网络摄像头存在任意命令执行漏洞。

输入一个摄像头控制端地址http://101.78.142.xx/cgibin/rtpd.cgi?echo&AdminPasswd_ss|tdb&get&HTTPAccount，攻击者可以轻松获取摄像头的账号和密码，使用账号、密码便可以登录该款设备。

在影响评估的过程中发现，通过HTTP头部Server字段，可以轻松在公网上找到该款设备的指纹。深信服研究发现台湾地区、香港地区受影响较为严重。

近日，海康威视“黑天鹅”事件，再次将网络摄像头的安全性推到风口浪尖。根据通报描述，省各级公关机关使用的海康威视监控设备存在严重的安全隐患，部分设备已经被境外IP地址控制。虽然该事件被外界过度解读，但不得不说的是，随着物联网时代的到来，通过嵌入式设备信息泄露问题正在加剧。

2.5.6　从12306泄密事件，我们读到了什么

12306泄密事件虽然已经过去，但却是一件值得我们深思的安全事件。随着人们

生活越来越依靠互联网、物联网、大数据和云服务，加之黑客行为的组织化和产业化，可以说，下一个重大信息泄露事件正在悄悄地向我们走来。2015年，注定是信息泄露高发的一年，应对泄密事件，你准备好了吗？

2.6 工业控制网络安全分析（来源：CNCERT/CC）

2.6.1 相关背景及概念

工业控制网络是国家关键基础设施最重要的组成部分，涉及一系列关系到国计民生的基础性行业。随着“两化”融合的推进，越来越多的基础设施领域开始采用最新的IT技术，而工业控制网络正由封闭、私有转向开放、互联，主要表现在以下几个方面：一是，很多企业为了提高“管控一体化”水平，实现生产和管理的高效率、高效益，使工业控制系统和管理系统直接进行通信，或引入生产执行系统（Manufacturing Execution System，MES）对工业控制系统和管理信息系统进行集成，进而实现管理信息网络与生产控制网络之间的数据交换。由于管理系统一般连接互联网，因此生产控制系统不再是一个封闭运行的系统，间接实现了与互联网的互联互通。二是，一些工业设备生产商为用户提供了设备远程维护服务，当设备发生故障时，厂商维修人员会远程接入到工业控制系统内网对设备进行调试，虽然远程维护主要以VPN等加密通信方式实现，但却提供了一条从互联网入侵生产内网的潜在途径。三是，一些具备GPRS、iWLAN等无线功能的新型智能仪表开始用于工业生产过程，无形中成为从互联网进入工业生产网络的入口。

“开放、互联”是“两化”融合的必然趋势，但也因此打破了工业网络与公共互联网之间的物理隔离，使得工控系统不可避免地要面对来自互联网的各种潜在的网络攻击威胁。

2.6.2 工业控制系统网络攻击特点

一是攻击威胁持续增大。CNCERT/CC依托CNVD，开展针对工业控制系统软硬件产品漏洞（简称工控漏洞）及漏洞事件的自主研究、分析验证和收录工作。

如图2-41所示，自2010年“震网”事件后， CNVD每年收录的工控漏洞数量始终处于高位，2014年共收录工控漏洞147个（包含自主挖掘零日漏洞12个），其中高危漏洞有74个，占比在50%以上。

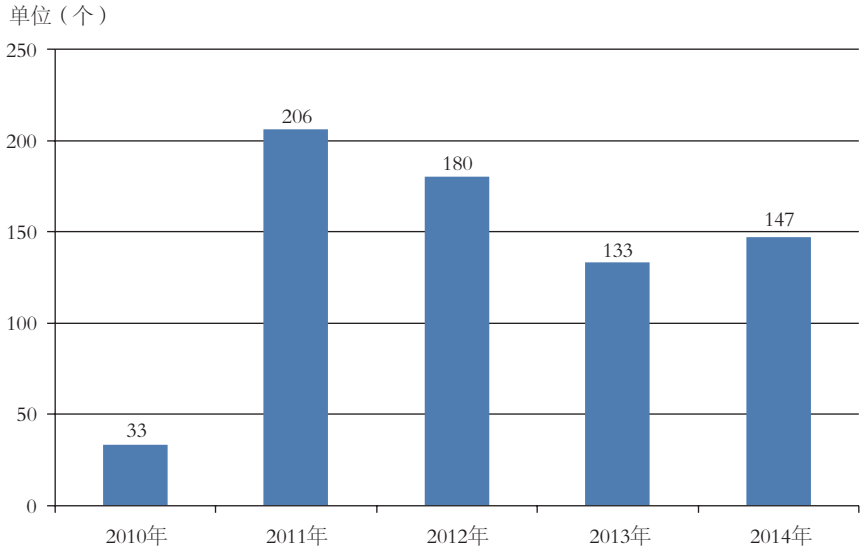


图2-41 2010-2014年CNVD工控漏洞收录情况（来源：CNCERT/CC）

2014年收录的工控漏洞涉及多个国内外工控厂商的多款产品。如图2-42所示，Siemens、Advantech等国外厂商工控漏洞较多，国内厂商则主要涉及亚控科技（WellinTech）和世纪长秋（CenturyStar）。

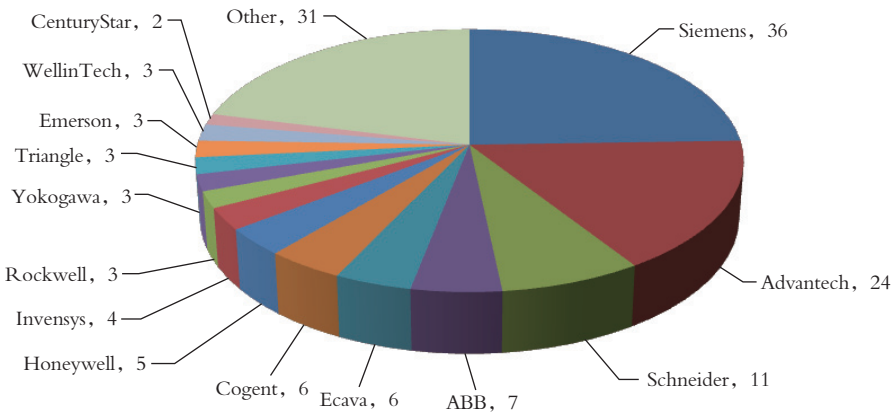


图2-42　2014年CNVD收录工控行业漏洞按厂商分布（来源：CNCERT/CC）

从图2-43的漏洞威胁类型分布看，未授权信息泄露、拒绝服务、管理员访问权限获取是较为普遍的工控漏洞威胁，主要涉及监控与数据采集（SCADA）软件以及可编程逻辑控制器（PLC）产品。

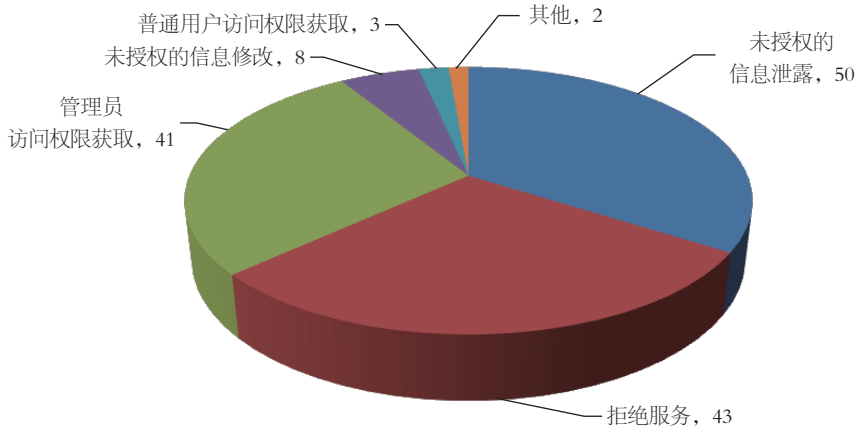


图2-43　2014年CNVD收录工控行业漏洞按类型分布（来源：CNCERT/CC）

伴随着工控系统自身脆弱性和安全隐患持续暴露，其遭受的网络攻击威胁在不断提高。目前国内在工控安全事件的监测发现、应急处置等方面，还缺乏成熟的工作机制及权威数据，但从图2-44美国的统计数据来看，2014年ICS-CERT公开报告处理的工控安全事件达245起，且约有55%的安全事件涉及APT攻击。如图2-45所示，这些事件分布在一系列重点行业，其中能源、关键制造行业的安全事件高达144起，接近所有事件总数的2/3。

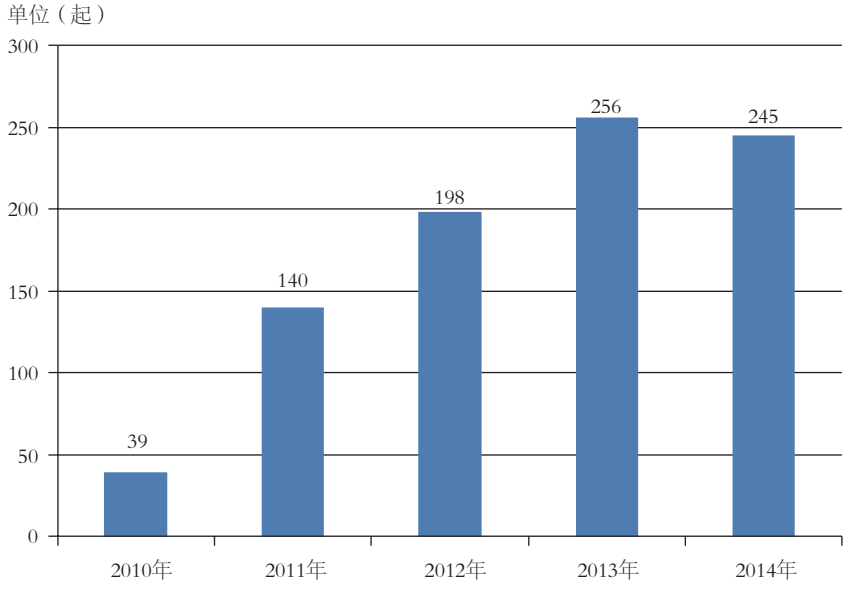


图2-44　美国ICS-CERT在2010-2014年公开报告处理的工控安全事件数量
（来源：CNCERT/CC）

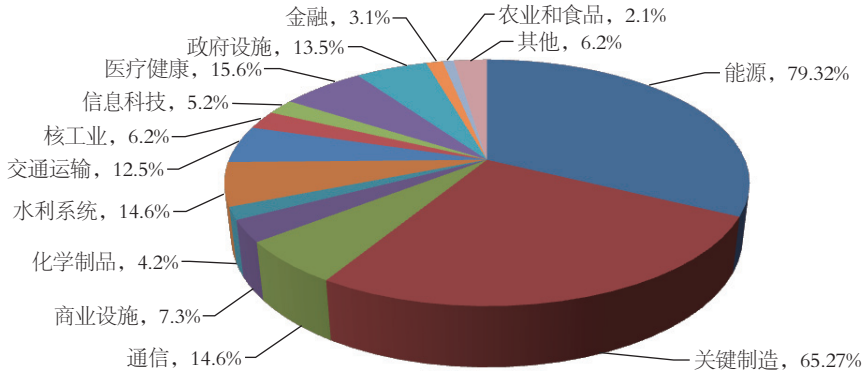


图2-45　2014年美国工控安全事件所属行业分布（来源：CNCERT/CC）

二是攻击技术不断提高。近年来，针对工业控制系统的网络攻击已经目标化、组织化和规模化。2010年，“震网”病毒导致伊朗布什尔核电站无法正常工作；2012年、2013年，高度智能化的信息烈度病毒“超级火焰”、“高斯”窃取中东和北非石油部门的相关重要文件并删除；2014年，远程木马变种“Havex”入侵全球能源行业的数个工业控制系统从事工业网络间谍活动。从技术手段的多样性和复杂性来看，这些攻击大都具有显著的APT特征，给监测发现和安全防护带来了重大挑战。

以CNCERT/CC在2014年重点分析的“Havex”为例，其至少采取了三种攻击方式传播。一是早期采用鱼叉式攻击手法，即利用电子邮件进行传播；二是2013年下半年开始采用“浇水洞”攻击，即首先入侵企业人员经常访问的网站，再把访问重定向到黑客控制的带有木马的网站，进而把恶意软件植入到这些企业人员的电脑中；三是利用具备远程控制能力的木马感染工控系统设备制造商的合法软件，使得安装这些软件的工控设备在软件更新时被感染。由于“Havex”变种木马是首个采用了OPC工业通信技术[20]的网络病毒，因此其被认为是专门针对工业控制系统量身定制而开发。

为了评估我国境内受“Havex”病毒的影响范围，在对病毒样本进行深度分析的基础上，CNCERT/CC进一步采取抽样监测，发现自2014年8月至今境内累计有47个

[20] 一种开放、通用的工业数据交换协议，能够实现基于Windows平台的工业控制系统应用程序与过程控制硬件之间的交互通信。

IP地址感染了“Havex”木马，其中位于江苏省的最多，所对应的控制端IP地址共12个，均位于境外，其中位于美国的控制服务器最多，存在部分IP地址持续向控制服务器发送信息的情况。针对这一结果，CNCERT/CC及时通报上级主管部门进行协调处置。

三是攻击破坏性显著增强。不同于传统IT系统，工业控制系统直接与物理现实世界相连接，其网络攻击一旦成功，可能造成重大经济损失、物理和人身伤害，甚至构成相当于大规模杀伤性武器的威力。

2014年12月18日，德国联邦信息安全办公室（BSI）披露了一起针对德国某钢铁厂的APT攻击事件，CNCERT/CC对此深入调研并借助美国系统网络安全协会（SANS Institute）发布的一份事件分析报告（http://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf）进行了情景分析：攻击者使用“钓鱼邮件”和其他社会工程手段获得了炼钢厂办公网络的访问控制权限后，成功“跳板”到生产网络，操控和干扰了一台高温加热炉控制系统，并最终迫使整个生产线停止运转。据悉此次攻击直接导致炼钢厂控制系统的多个关键过程组件失控，造成了大规模的物理损毁和巨大的经济损失。考虑到BSI报告的权威性和真实性，可以认定这次针对德国炼钢厂的APT攻击是继2010年震网病毒后又一起导致控制系统物理损毁的重大网络安全事件。

2.6.3 防范措施及建议

面对日益严重的工业控制系统网络攻击威胁，建议我国主要采取以下措施应对。

（1）出台政策法规。一是加强立法，当前网络安全法已纳入人大立法规划，我国正加快制定针对包括重点领域工业控制系统在内的国家关键基础设施的网络安全保护法案；二是建立网络安全审查制度，我国国家互联网信息办公室已启动相关调研工作，有望针对进入中国市场的信息技术产品与服务进行测试评估、检测分析、持续监督，以实现其安全性和可控性。

（2）制定标准及指南。2014年12月2日，我国工控信息安全领域的首个国家标准正式发布GB/T30976.1~2-2014《工业控制系统信息安全：评估、验收》。早在此之前，国际电工委员会（IEC）、美国国家标准技术研究院（ NIST）等国际标准化组织已相继出台了一系列针对工业控制系统的信息安全标准。例如，IEC 62443《工业控制过程测量和控制的安全性网络和系统安全》系列标准、NIST SP 800系列系统安全指南

等。工业控制系统信息安全标准是国家、政府、企业进行安全风险测评，实现规范化管理，建立工控信息安全多层防御策略架构的指南和方向，其建设是事关工业发展、经济安全的重大战略问题。我国需要借鉴国外的先进经验，尽快填补空白，构建符合自身发展特点的工控网络信息安全标准体系。

（3）调查网络安全态势。一是利用相关技术手段统计我国境内暴露在互联网上的工业控制系统前端管理系统和硬件设备，以及境外针对我国境内工控边界系统进行持续信息探测的网络节点，掌握我国工业互联网安全态势；二是通过自查为主、抽查为辅的方式，定期开展针对重点领域的工业控制系统的网络安全测评工作，并将测评结果汇总分析，掌握我国不同工业领域的工控行业网络安全态势。

（4）建立应急响应机制。目前世界各发达国家纷纷建立了专门针对工控网络安全事件的应急响应机制，以应对日益增长的针对现代工业基础设施的网络安全威胁。其中，美国设立了专门的工业控制系统网络安全应急响应小组（Industrial Control Systems Cyber Emergency Response Team, ICS-CERT），欧洲各国纷纷将工控网络安全漏洞与恶意代码事件处理工作指定给已有的应急协调机构。 随着我国工业基础设施网络安全保障问题的日渐紧迫，有必要建立专门的面向工业控制系统网络安全的应急响应体系和协调机制，开展针对工控安全事件的监测分析、通报预警、应急响应、测试评估等工作，并鼓励多方积极参与、信息共享、协同工作，共同应对国家范围的工控网络安全事件。

（5）推动自主研发。当前，我国在能源、制造、交通等众多工业领域的核心硬件设备、软件产品仍然大量依赖于国外进口，然而，“棱镜门”事件为我们敲响了警钟，“保障信息安全，实现核心软硬件国产化自主可控”已提升到国家战略高度。为本质上解决工控网络信息安全问题，需要国家政府持续鼓励和支持国产工控软硬件产品的自主研发和创新，从涉及国计民生的重要行业做起，逐渐缩小与国外先进水平的整体差距，最终实现工控产品及技术自主可控，从根本上完善工控网络信息安全保障体系建设。

3 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，甚至是以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、下载者木马和其他木马等，但随着木马程序编写技术的发展，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，或同时发送大量垃圾邮件等。

2014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104230个，较2013年下降45.0%，受控主机IP地址总数为13991480个，较2013年下降25.2%。其中，境内木马或僵尸程序控制服务器IP地址数量为61879个，较2013年大幅下降61.4%，境内受控主机IP地址数量为11088141个，较2013年下降2.3%。连续两年我国境内木马或僵尸程序控制服务器以及受控主机数量出现下降，体现了近两年我国木马和僵尸网络专项治理行动和日常处置工作的持续效果。

3.1.1 木马或僵尸程序控制服务器分析

2014年，境内木马或僵尸程序控制服务器IP地址数量为61879个，较2013年大幅下降61.4%；境外木马或僵尸程序控制服务器IP地址数量为42351个，较2013年有所增长，增幅为45.3%，具体如图3-1所示。经过我国木马僵尸专项打击的持续治理，境内的木马或僵尸程序控制服务器数量下降明显。

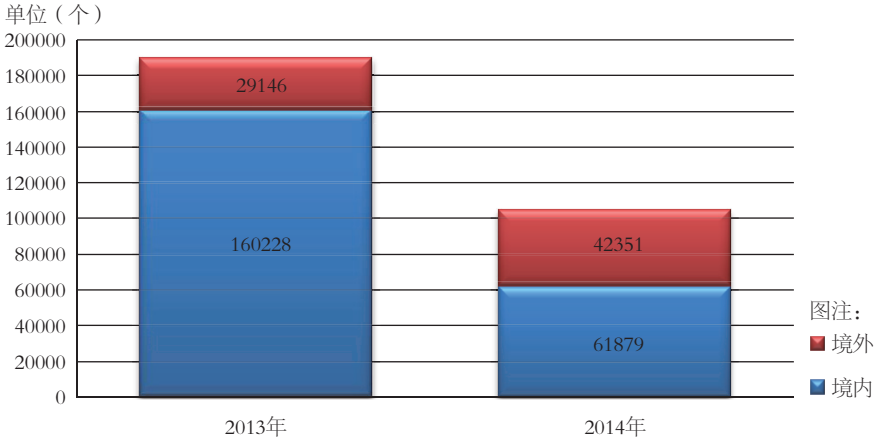
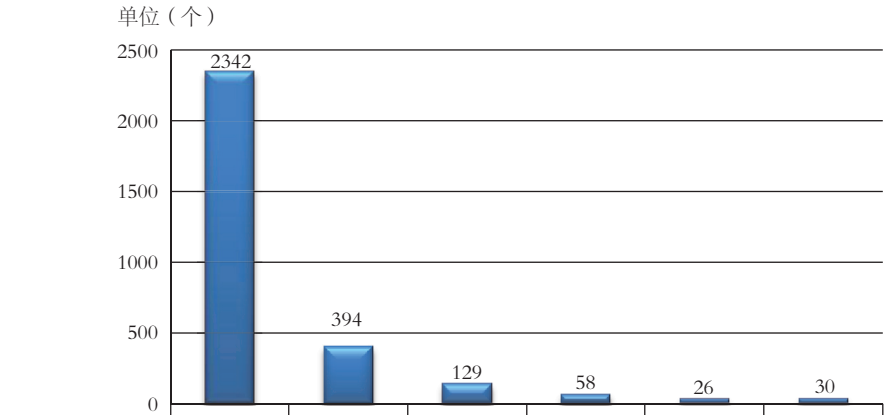


图3-1 2014年与2013年木马或僵尸程序控制服务器数据对比（来源：CNCERT/CC）

2014年，在发现的因感染木马或僵尸程序而形成的僵尸网络[21]中，规模100～1000的占78.6%以上。控制规模在1000～5000、5000～20000、2万～5万、5万～10万、10万以上的主机IP地址的僵尸网络数量与2013年相比分别减少648个、147个、18个、7个、18个。分布情况如图3-2所示。

[21] 僵尸网络刚给出现时，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，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成为僵尸网络。本处统计的是受控主机IP地址数量在100个以上的僵尸网络。



	100～1000	1000～5000	5000～20000	2万～5万	5万～10万	＞10万
僵尸网络数目	2342	394	129	58	26	30

图3-2　2014年僵尸网络规模分布（来源：CNCERT/CC）

2014年木马或僵尸程序控制服务器IP地址数量的月度统计分别如图3-3所示，全年呈波动态势，11月达到最高值17938个，10月为最低值7796个。

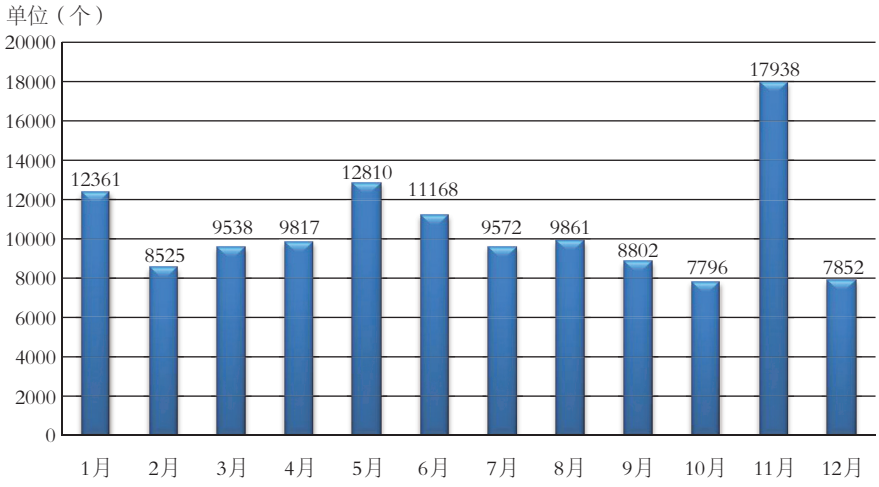


图3-3　2014年木马或僵尸程序控制服务器IP地址数量月度统计（来源：CNCERT/CC）

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、云南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，云南省、四川省、江苏省、黑龙江省居于木马或僵尸程序控制服务器IP地址相对数量的前4位。

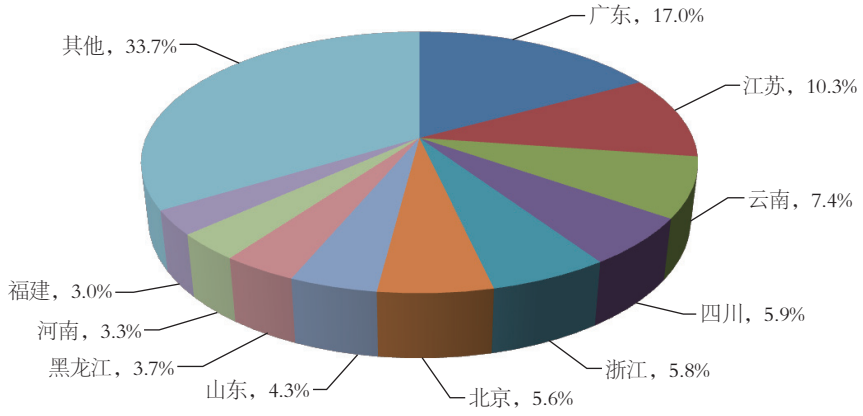


图3-4　2014年境内木马或僵尸程序控制服务器IP地址按地区分布
（来源：CNCERT/CC）

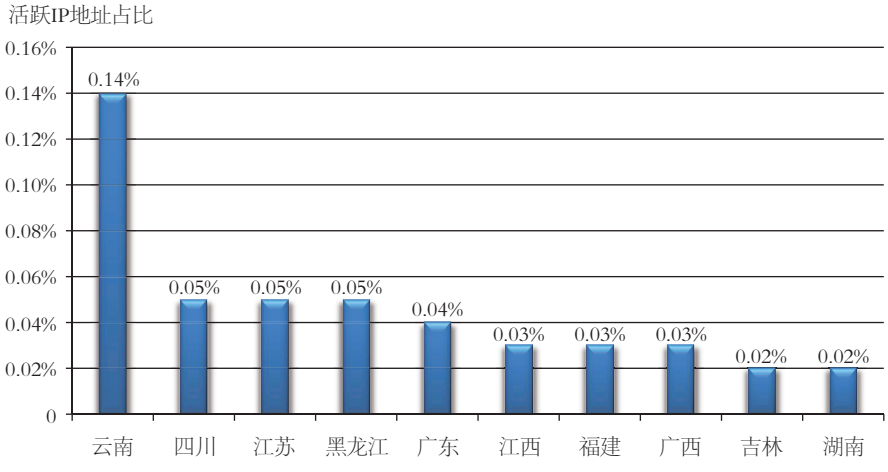


图3-5　2014年境内木马或僵尸程序控制服务器IP地址占所在地区活跃IP地址比例TOP10
（来源：CNCERT/CC）

图3-6、图3-7为2014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地址数量占据境内控制服务器IP地址数量的近2/3。

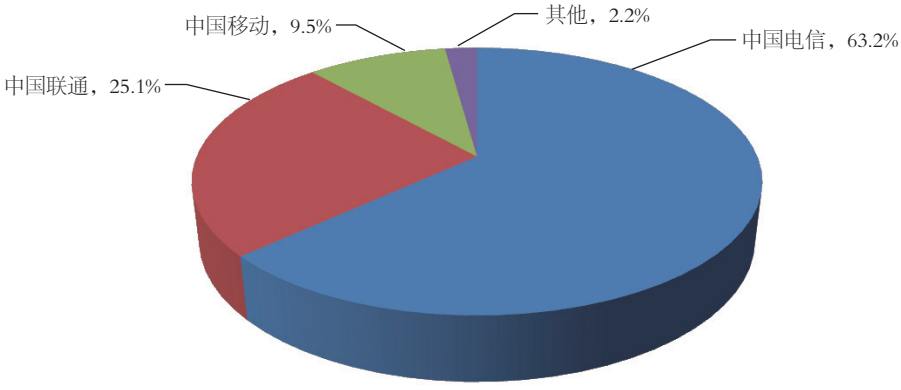


图3-6　2014年境内木马或僵尸程序控制服务器IP地址按基础电信企业分布
（来源：CNCERT/CC）

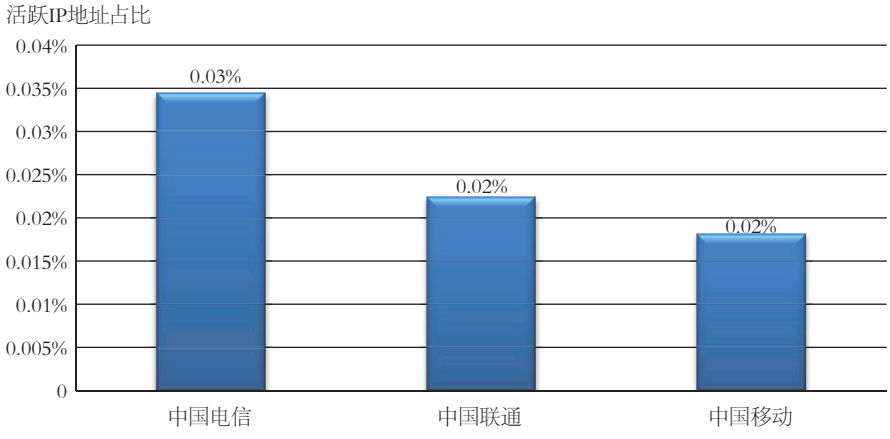


图3-7　2014年境内木马或僵尸程序控制服务器IP地址占所属基础电信企业活跃IP地址比例
（来源：CNCERT/CC）

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21.8%，中国香港和韩国分列第二、三位，占比分别为18.9%和8.2%。

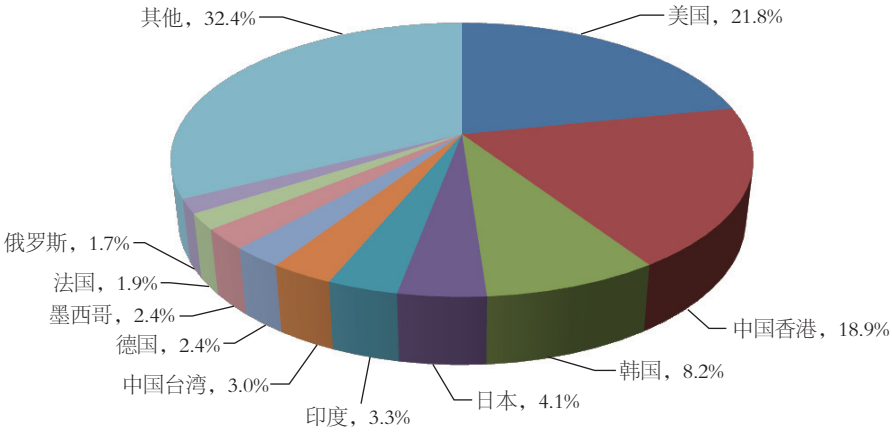


图3-8　2014年境外木马或僵尸程序控制服务器IP地址按国家和地区分布
（来源：CNCERT/CC）

3.1.2　木马或僵尸程序受控主机分析

2014年，境内共有11088141个IP地址的主机被植入木马或僵尸程序，境外共有2903339个IP地址的主机被植入木马或僵尸程序，数量较2013年均有所下降，降幅分别达到了2.3%和60.5%，具体如图3-9所示。

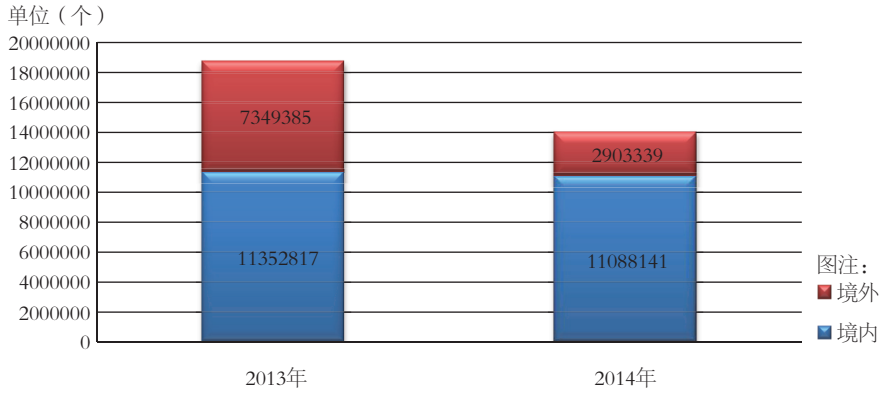


图3-9　2014年和2013年木马或僵尸程序受控主机数量对比（来源：CNCERT/CC）

2014年，CNCERT/CC持续加大木马和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，12月达到最高值3628571个，10月为最低值909068个。2014年木马或僵尸程序受控主机IP地址数量的月度统计如图3-10所示。

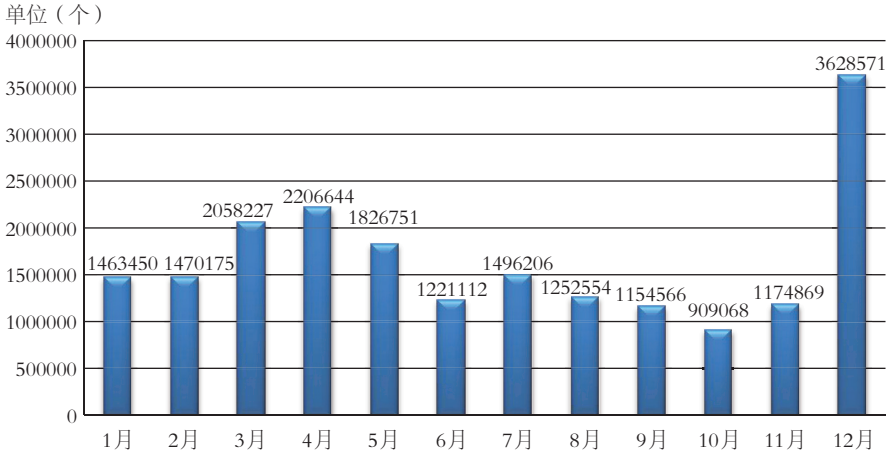


图3-10　2014年木马或僵尸程序受控主机IP地址数量月度统计（来源：CNCERT/CC）

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、湖南省、江苏省居于木马或僵尸程序受控主机IP地址绝对数量前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地址数量绝对数量位于全国前列。湖南省、青海省、陕西省居于木马或僵尸程序受控主机IP地址相对数量的前3位。

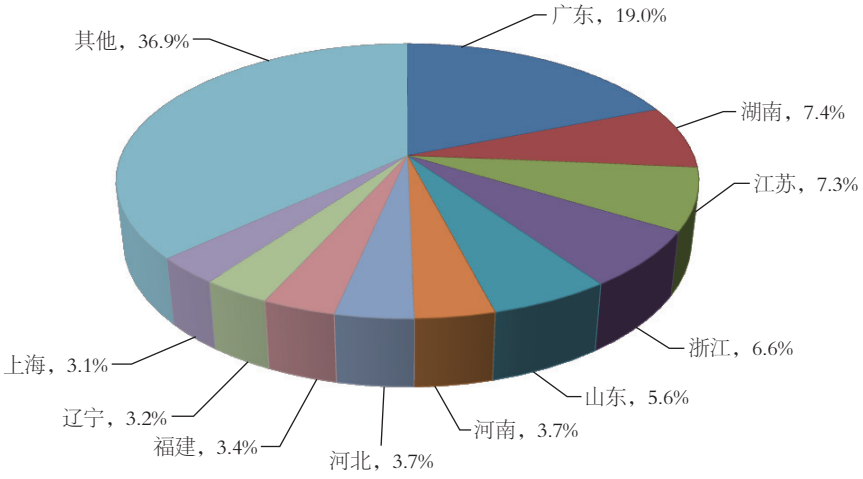


图3-11　2014年境内木马或僵尸程序受控主机IP地址数量按地区分布（来源：CNCERT/CC）

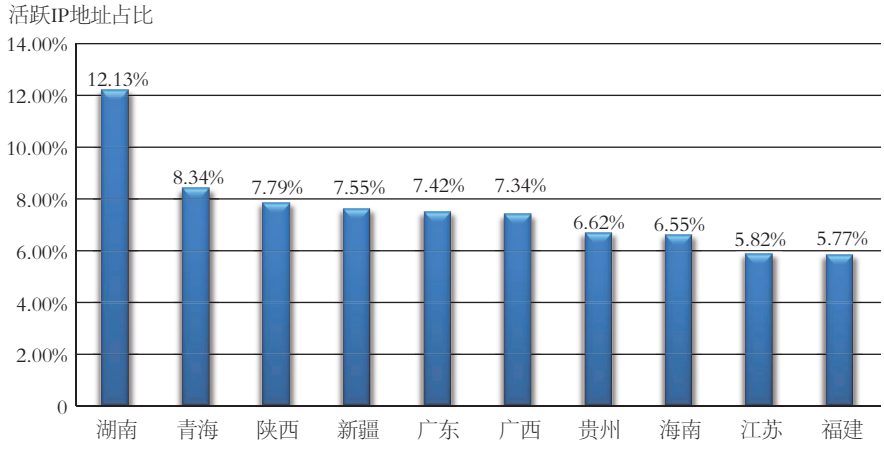


图3-12　2014年境内木马或僵尸程序受控主机IP地址数量占所在地区活跃IP地址比例TOP10（来源：CNCERT/CC）

图3-13和图3-14为2014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。从绝对数量上看，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4.0%。

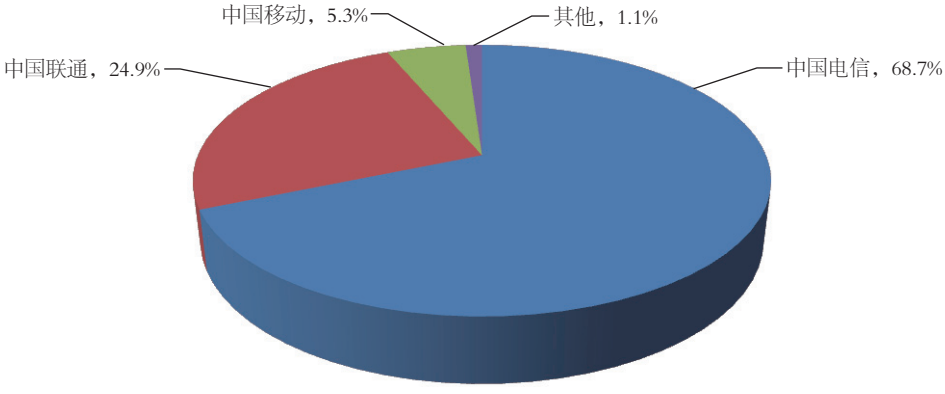


图3-13　2014年境内木马或僵尸程序受控主机IP地址数量按基础电信企业分布（来源：CNCERT/CC）

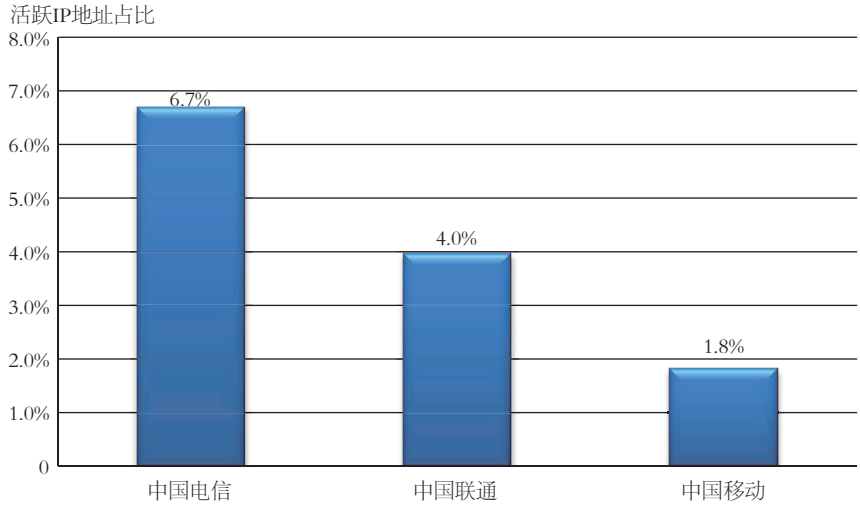


图3-14　2014年境内木马或僵尸程序受控主机IP地址数量占所属基础电信企业活跃IP地址数比例（来源：CNCERT/CC）

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位居前10位的如图3-15所示，其中，印度、泰国、埃及居前3位。

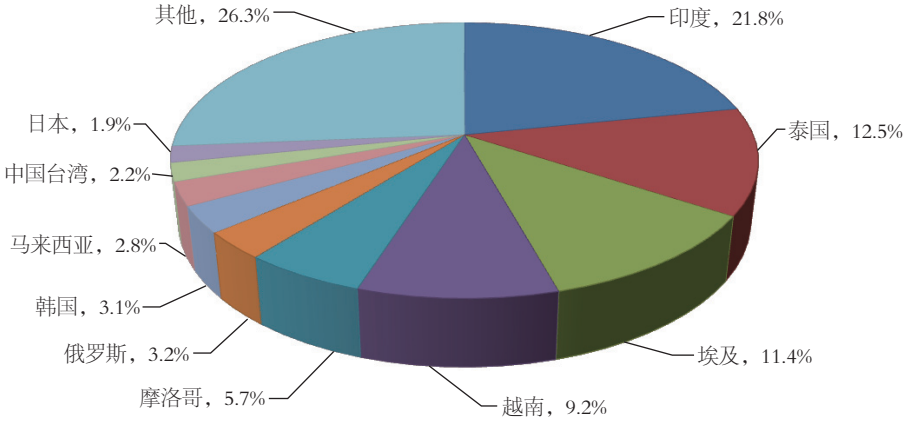


图3-15　2014年境外木马或僵尸程序受控主机IP地址数量按国家和地区分布
（来源：CNCERT/CC）

3.2　“飞客”蠕虫监测情况

“飞客”蠕虫（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，最早出现在2008年11月21日。“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，不仅能够被用于大范围的网络欺诈和信息窃取，而且能够被利用发动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，2010年12月超过6000万台主机，2011年月均3500万台主机，2012年月均2800万台主机，2013年月均1722万台主机，2014年月均943万台主机。

据CNCERT/CC监测，2014年，排名前三的国家或地区分别是中国大陆

（12.7%）、印度（7.9%）和巴西（6.9%），具体分布情况如图3-16所示。其中，中国境内感染的主机IP地址数量月均近103万个，较2013年下降了41.7%。图3-17为2014年我国境内主机IP地址感染“飞客”蠕虫的数量月度统计，月度感染主机数量总体呈波动下降趋势。

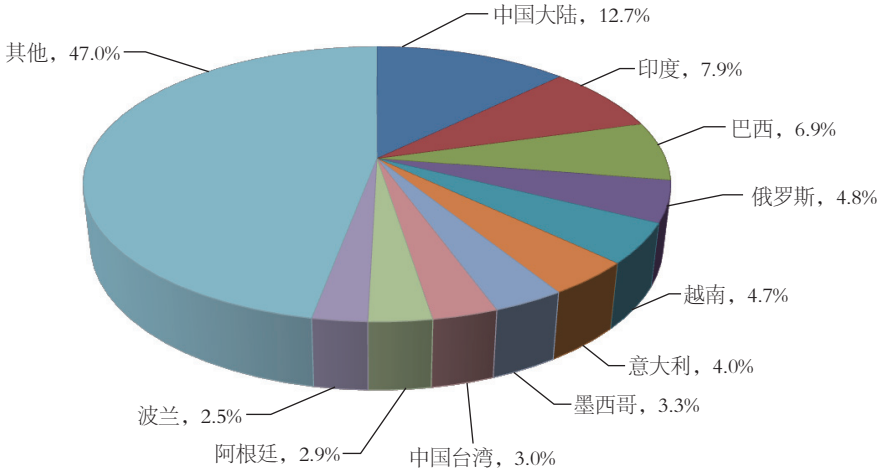


图3-16　2014年全球互联网感染“飞客”蠕虫的主机IP地址数量按国家和地区分布
（来源：CNCERT/CC）

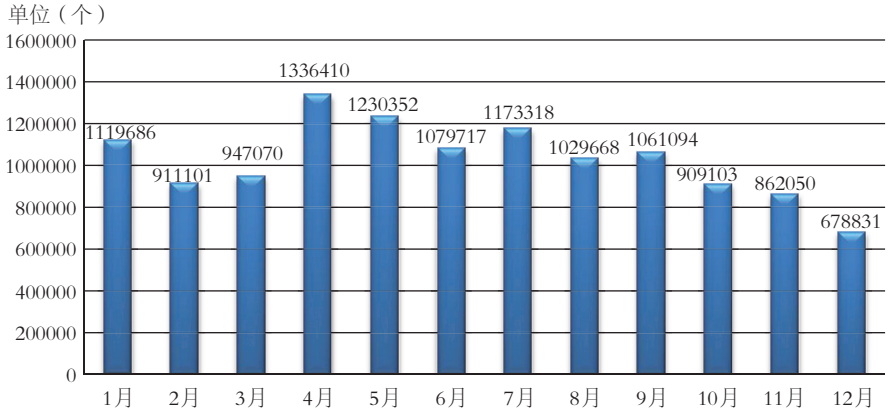


图3-17　2014年中国境内感染“飞客”蠕虫的主机IP地址数量月度统计
（来源：CNCERT/CC）

3.3 恶意程序传播活动监测

2014年，CNCERT/CC监测发现已知恶意程序[22]的传播事件158.7万次，其中涉及已知恶意程序的下载链接115096个，“放马站点”（指存放恶意程序的网络地址）使用的域名10396个，“放马站点”使用的IP地址5126个。

已知恶意程序传播事件的月度统计如图3-18所示，2014年1-4月恶意程序传播活动频次相对较低，5月的恶意程序传播事件数量较前4个月出现暴增，6月的恶意程序传播事件数量较5月有所下降但仍然维持在较高水平，7-12月的恶意程序传播活动频次回落至相对较低水平。频繁的恶意程序传播活动使用户上网面临的感染恶意程序的风险加大，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。

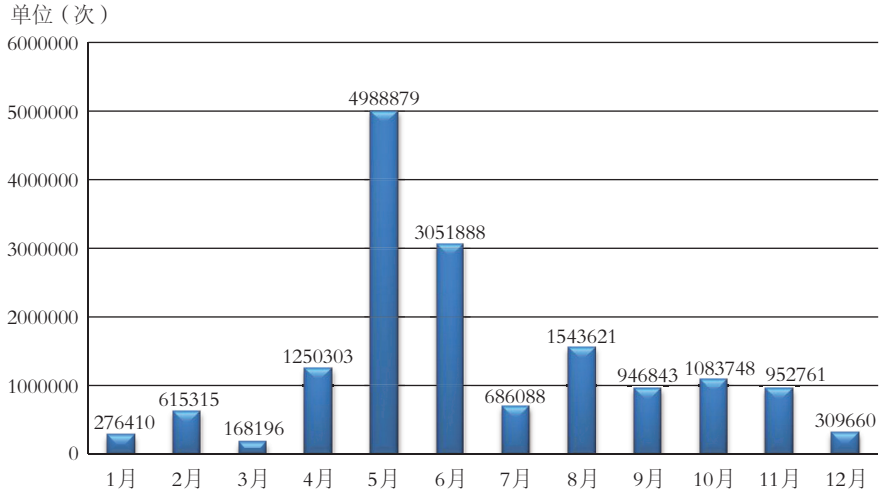


图3-18 2014年已知恶意程序传播事件次数月度统计（来源：CNCERT/CC）

“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，2014年上半年的恶意域名数量总体较为稳定，但9月有较大幅度的激增，10月虽有回落但仍然维持在较高水平，11月开始回落至相对较低水平，而全年直接访问 “放马站

[22] “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。

点”的IP地址数量总体较为稳定。对恶意域名和IP地址的清理力度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。

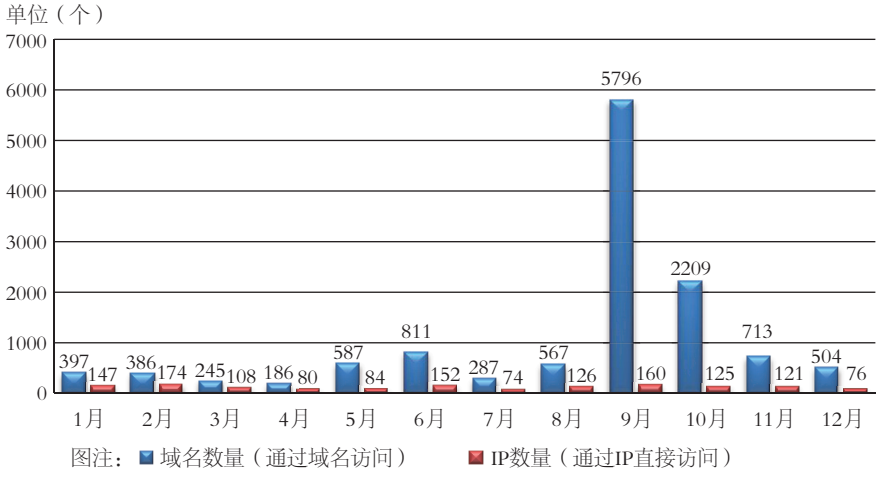


图3-19　2014年“放马站点”使用的域名和IP地址数量月度统计
（来源：CNCERT/CC）

CNCERT/CC监测发现，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端口的最多。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。2014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。

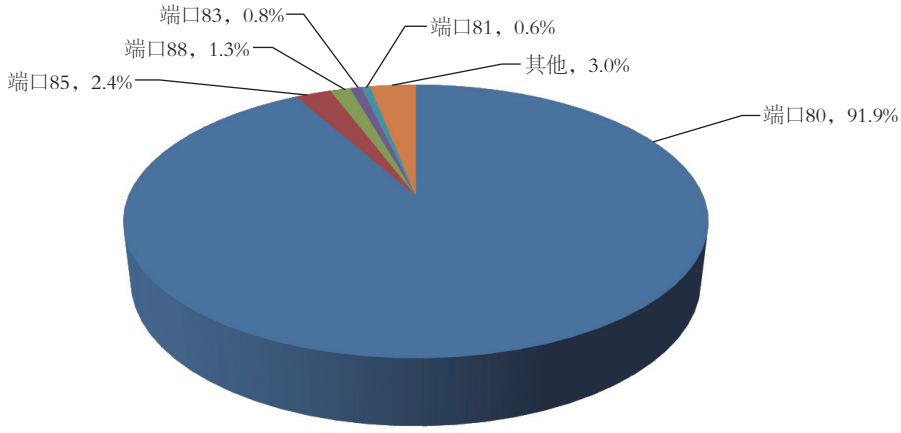


图3-20　2014年“放马站点”使用的端口分布统计（来源：CNCERT/CC）

3.4　通报成员单位报送情况

3.4.1　安天公司报送的恶意程序情况

根据安天公司监测结果，2014年全年捕获恶意程序总量为3516450个（按恶意程序名称统计），比2013年的4187306个[23]下降16.0%。2014年各月捕获数量如图3-21所示，其中9月达到全年最高值493153个，6月达到全年最低值150295个。

[23]　2014年，安天公司的数据统计结构进行了调整。

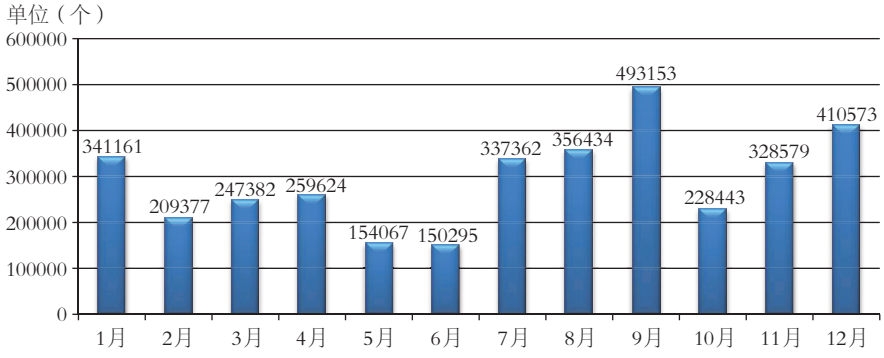


图3-21　2014年恶意程序捕获月度统计（来源：安天公司）

2014年全年捕获恶意程序样本总量为40346645个（按MD5值统计），比2013年的31728805个增长27.2%。2014年各月捕获数量如图3-22所示，其中6月达到全年最高值5774285个，4月达到全年最低值2229952个。

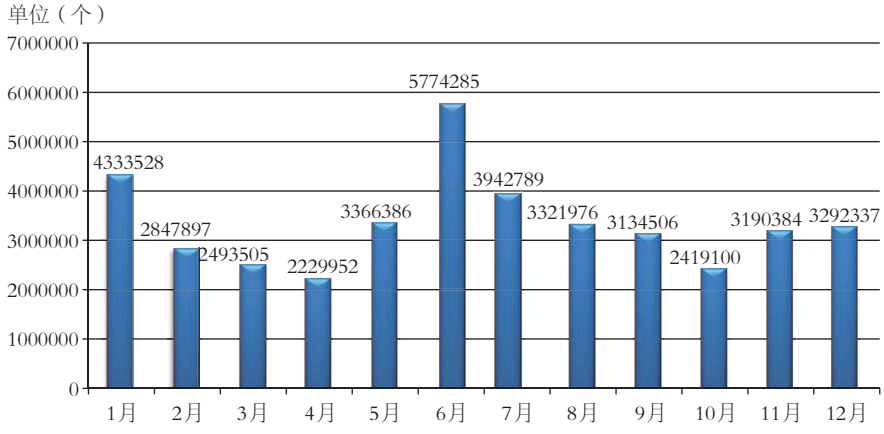


图3-22　2014年恶意程序样本捕获月度统计（来源：安天公司）

2014年全年监测到感染恶意程序的主机860162台，较2013年的360260个增长138.8%。感染恶意程序的主机数量的趋势为上升，其中感染主机数量5月为全年最高点227236个，3月达到全年最低值7582个，如图3-23所示。

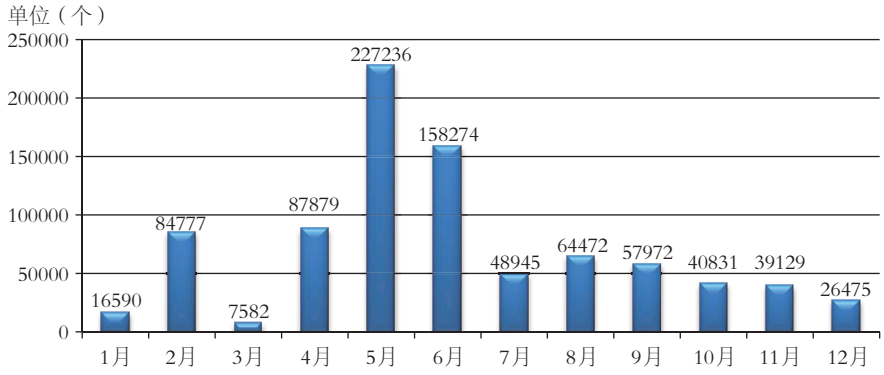


图3-23　2014年感染恶意程序主机数量月度统计(来源：安天公司)

3.4.2　瑞星公司[24]报送的恶意样本情况

根据瑞星公司监测结果，2014年全年捕获恶意程序总量为871891个（按恶意程序名称统计），比2013年的802145个增长8%。2014年各月捕获数量如图3-24所示，其中3月达到全年最高值247828个，9月达到全年最低值146157个。

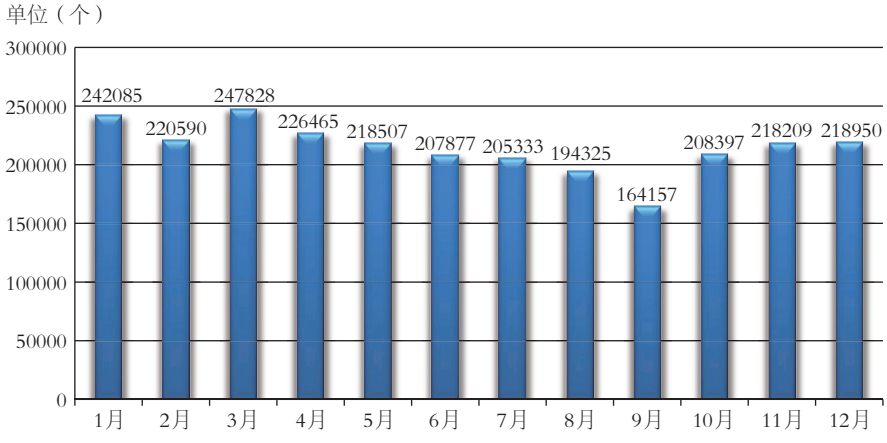


图3-24　2014年恶意程序捕获月度统计（来源：瑞星公司）

[24]　瑞星公司即北京瑞星信息技术有限公司，是通信行业互联网网络安全信息通报工作单位，也是中国反网络病毒联盟成员单位。

2014年全年捕获恶意程序样本总量为33558374个（按MD5值统计），比2013年的33277470个增长0.84%。2014年各月捕获数量如图3-25所示，其中10月达到全年最高值4012134个，5月达到全年最低值1553604个。

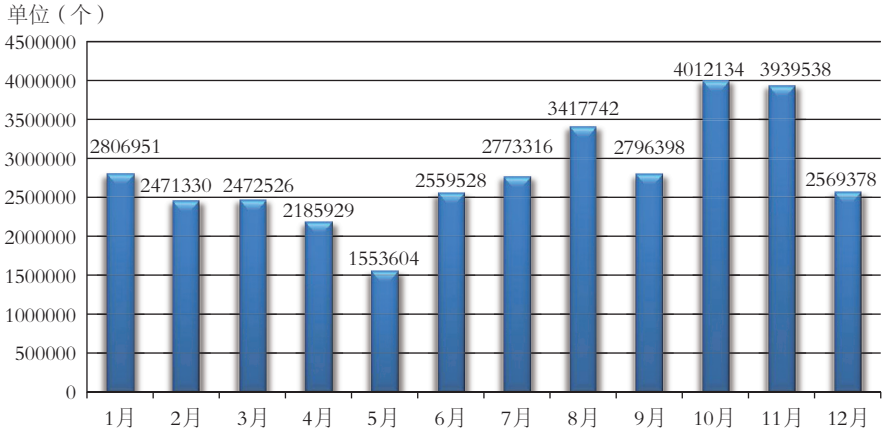


图3-25　2014年恶意程序样本捕获月度统计（来源：瑞星公司）

2014年全年监测到感染恶意程序的主机24375038台，较2013年的23443205台增长3.97%。感染恶意程序的主机数量呈上升趋势，其中感染主机数量3月为全年最高点5474363台，6月达到全年最低值2387029台，如图3-26所示。

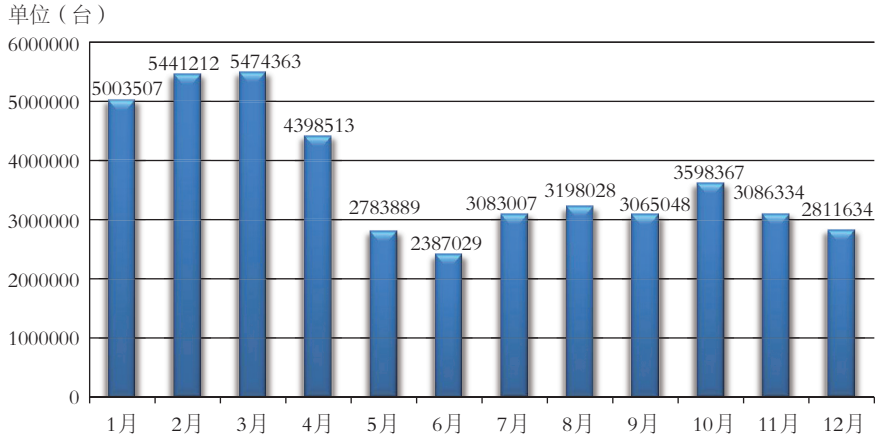


图3-26　2014年感染恶意程序主机数量月度统计（来源：瑞星公司）

2012-2014年捕获恶意程序数量（按恶意程序名称统计）走势如图3-27所示。

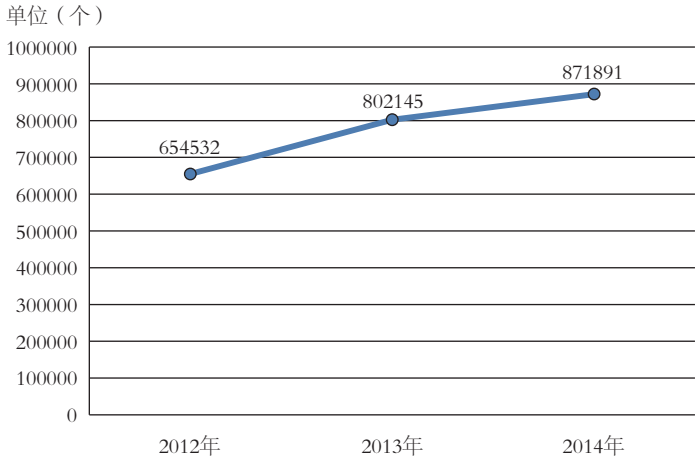


图3-27　2012-2014年捕获恶意程序数量走势图（来源：瑞星公司）

2009-2014年捕获恶意程序样本数量（按MD5值统计）走势如图3-28所示。

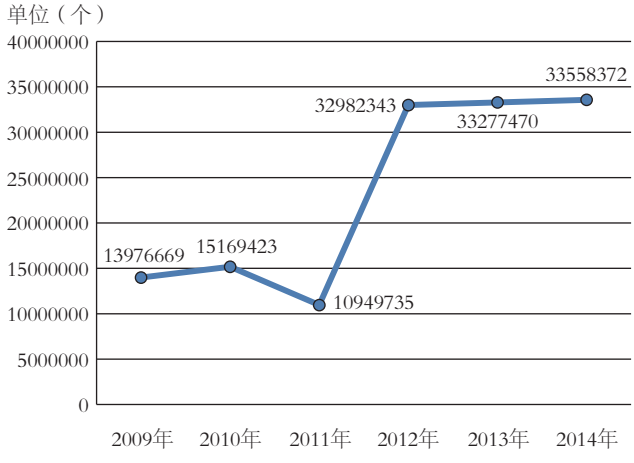


图3-28　2009-2014年捕获恶意程序样本数量走势图（来源：瑞星公司）

瑞星公司将捕获的恶意程序类型分为六大类，分别是Trojan、Worm、Virus、

Adware、Backdoor和Dropper。其中，Trojan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Trojan数量共23433008个。根据2013年和2014年监测结果对比，在捕获的各类恶意程序中，绝对数量增长最多的是Trojan，上升了27.45%，下降最多的是Worm，下降了32.04%。各类恶意程序数量增幅变化如图3-29所示。

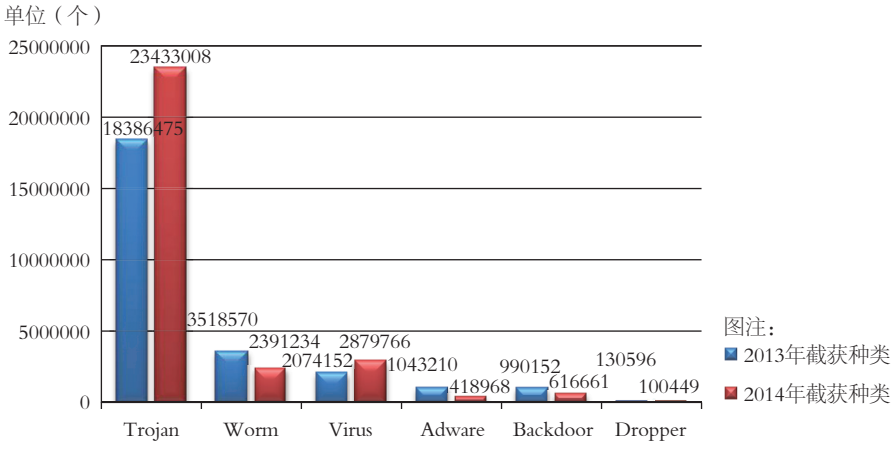


图3-29　2013年与2014年捕获恶意程序数量分类对比（来源：瑞星公司）

2014年，恶意程序样本表现出越来越强的对抗性。恶意程序样本加壳的比例由2013年的14.8%上升至2014年的19.6%，如图3-30所示。2014年恶意程序所使用的主要壳类型TOP10统计见表3-1。

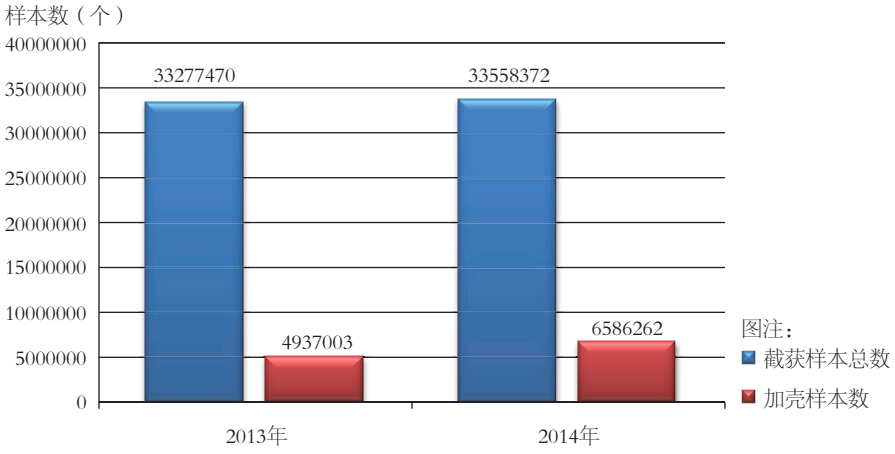


图3-30　2013年与2014年加壳样本数、总样本数统计对比（来源：瑞星公司）

表3-1　2014年恶意程序所使用的壳类型TOP10（来源：瑞星公司）

序号	壳名称	数量
1	upx_c	4531726
2	pecompact2x	825824
3	mpress	554552
4	aspack212r	182175
5	packman1x	169514
6	aspack22	87532
7	aspack2000	35045
8	pencrypt31	19468
9	nspack	19084
10	upack0.32	15061

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，2014年共截获新增恶意程序样本3.24亿个，平均每天截获新增恶意程序样本88.8万个。其中，10月新增恶意程序样本数最多，达到5941万。图3-31为2014年各月捕获的新增恶意程序样本数统计数量。

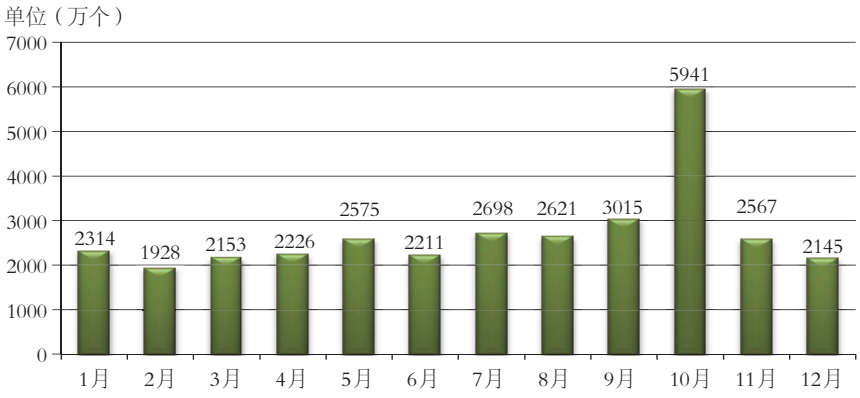


图3-31　2014年捕获新增恶意程序样本数月度统计（来源：奇虎360公司）

表3-2给出了2014年云查询拦截量排名前10的电脑恶意程序的名称、云查询拦截量和具体的恶意行为。

表3-2　2014年个人电脑恶意程序云查询拦截量 TOP10（来源：奇虎360公司）

恶意程序类别名称	云拦截查询量	恶意行为
ADWare.Win32.Clicker	2421545599	运行后以隐藏弹窗形式，在后台恶意刷流量，如果用户电脑补丁不全很可能会感染网页上的木马
Virus.Win32.FakeLPK	1011808088	LPK感染，通过系统优先加载程序自身目录DLL的特性启动自身，并不断复制自身感染用户电脑
Rootkit.Win32.Rwm	374539336	可被利用的驱动,恶意软件可利用该驱动达到隐藏自身目的，因其代码运行在特权模式下，可造成意想不到的伤害
ADWare.Win32.Acad(NotPe)	361942877	恶意修改用户浏览器默认主页，弹出恶意、虚假广告页面等
Trojan.Win32.DDOS	292049365	DDoS木马，中招后电脑即变成被黑客控制的僵尸电脑。黑客可以利用僵尸电脑来发起DDoS攻击，在攻击过程中，用户电脑会出现卡，网络慢，掉线等现象
ADWare.Win32.MultiDL	214904138	广告软件，安装该类型软件后通常会默认添加自启动，随着系统运行常驻进程，并在后台根据云端下发各种类型的广告
Virus.Win32.Fakelinkinfo	172978834	Linkinfo感染，通过系统优先加载程序自身目录DLL的特性启动自身，并不断复制自身感染用户电脑
Trojan.Win32.GameHacker	115951992	游戏木马，盗取用户游戏信息后发送到黑客事先搭建好的收信地址，黑客会通过洗掉用户号里的金币装备来获取利润
Virus.Win32.FakeFolder	114521827	假冒文件夹图标迷惑用户，运行后会启动感染模式，不断复制自身到各个文件夹下
Trojan.Win32.Inject	91454529	远程注入系统正常进程，修改EIP来执行自身事先准备的恶意代码，这种特性使得用户在任务管理器是无法结束该病毒的

4 移动互联网恶意程序传播和活动情况

2014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，2014年移动互联网恶意程序的数量呈增长趋势，与2012年和2013年的爆炸式增长速度相比，增长趋势有所放缓。

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。2014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951059个。

2014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522889个，占54.98%，资费消耗类145836个（占15.33%）、隐私窃取类122490个（占12.88%）分列第二、三位。通过2014年工业和信息化部、公安部和工商总局三部委联合开展的移动恶意程序专项治理行动，恶意扣费类恶意程序经过打击治理，其比例由2013年的71.5%下降了16.5%，但恶意扣费类和资费消耗类等与用户经济利益密切相关的恶意程序依旧占据恶意程序总体数量的70%以上。2014年，CNCERT/CC组织通信行业开展了11次移动互联网恶意程序专项治理行动。

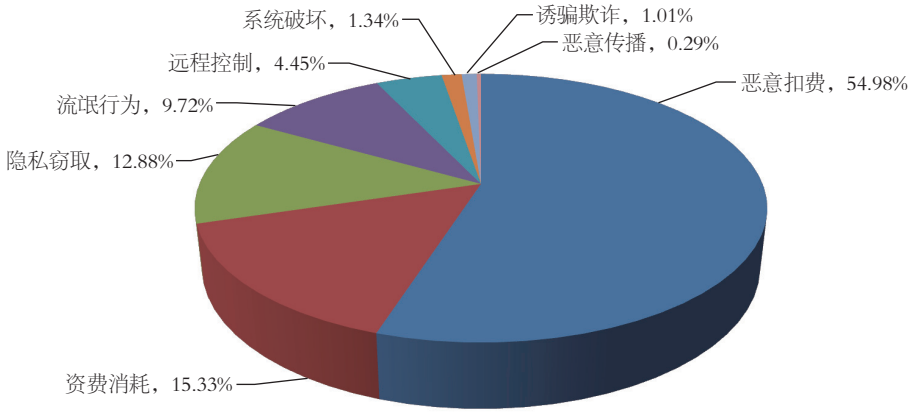


图4-1　2014年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

按操作系统分布统计，2014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949772个，占99.8%以上，位居第一。其次是Symbian平台，共有1276个，占0.13%。此外，也有少量的针对iOS平台和J2ME平台的恶意程序。值得注意的是，2014年首次出现了大规模感染苹果iOS平台的恶意程序，如“Panda”、“Wirelurker”等恶意程序，标志着黑客逐渐将目光转向iOS平台。2014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。

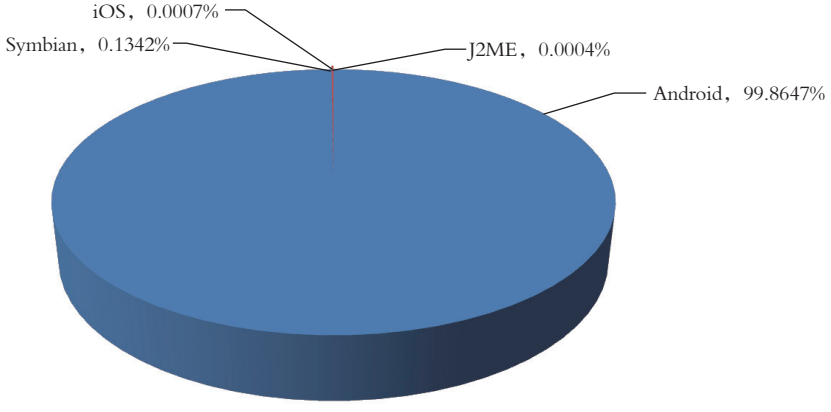


图4-2　2014年移动互联网恶意程序数量按操作系统分布（来源：CNCERT/CC）

如图4-3所示，按危害等级统计，2014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15547个，占1.7%；中危的为240926个，占25.3%；低危的为694586个，占73.0%。相对于2013年，高危、中危、低危移动互联网恶意程序分布情况略有变化，其中高危和低危移动互联网恶意程序所占比例略有提升，中危移动互联网恶意程序所占比例略有下降。

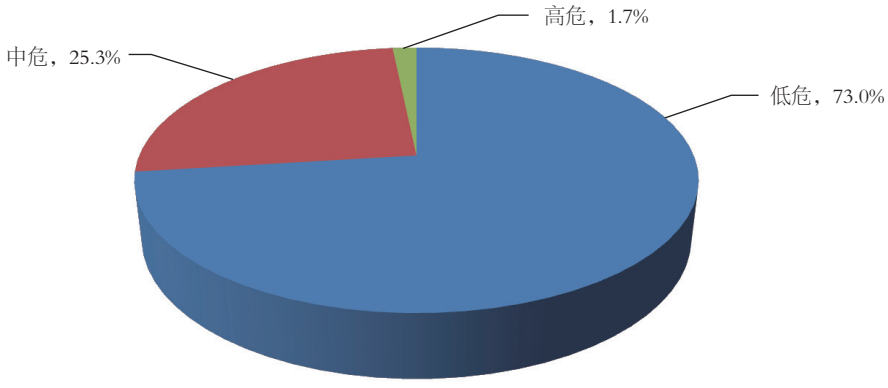


图4-3　2014年移动互联网恶意程序数量按危害等级统计（来源：CNCERT/CC）

4.2　移动互联网恶意程序传播活动监测

2014年，通过三部委联合的移动恶意程序专项打击行动，移动恶意程序传播活动有所遏制。CNCERT/CC监测发现移动互联网恶意程序传播事件81747407次，约是2013年同期12956836次的6倍，较2013年23倍的增长速度有大幅度下降。移动互联网恶意程序URL下载链接296080个，较2013年同期的1206798个大幅下降78.5%。进行移动互联网恶意程序传播的域名24211个，较2013年同期增长57.0%；进行移动互联网恶意程序传播的IP地址57296个，较2013年同期下降6.0%。由于主流应用商店的安全意识、审核制度和检测手段逐步改善，移动恶意程序生存困难，逐渐向个人网站、广告平台等小型网站蔓延。2014年CNCERT/CC监测发现100余个小型网站传播移动恶意程序3万余个，仅其中一个域名为“jinhuashenghuo.com”的网站，累计传播移动恶意程序超

过2000个，针对这类网站的监测处置将是未来移动互联网环境治理重点。

移动互联网恶意程序传播事件的月度统计如图4-4所示，由于2014年4-9月，三部委联合开展了移动互联网恶意程序专项治理行动，结果显示2014年1-8月移动恶意程序传播活动频次相对较高，4月专项行动后传播事件数量总体呈下降趋势。

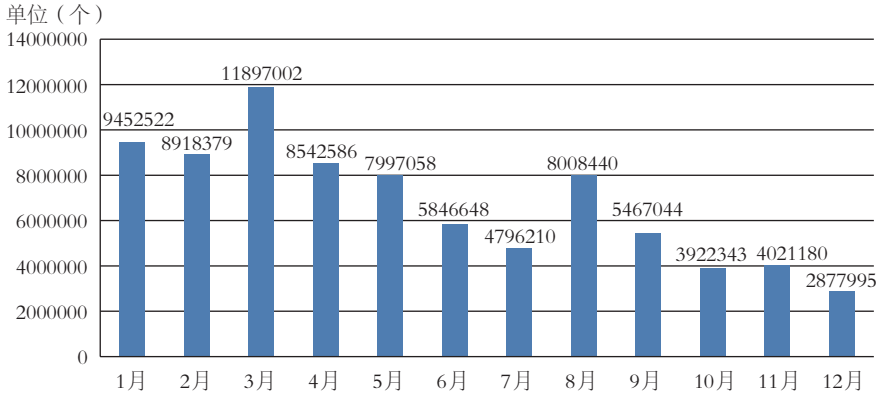


图4-4　2014年移动互联网恶意程序传播事件次数月度统计（来源：CNCERT/CC）

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。在三部委移动恶意程序专项治理行动期间，传播移动互联网恶意程序的域名和IP地址数量有所下降。

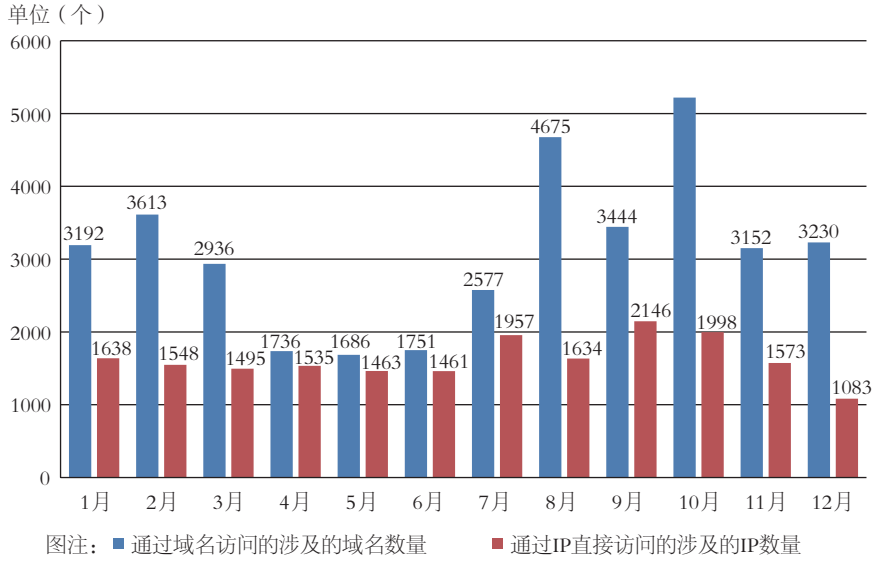


图4-5　2014年移动互联网恶意程序传播源域名和IP地址数量月度统计
（来源：CNCERT/CC）

4.3　通报成员单位报送情况

4.3.1　网秦公司[25]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2014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）13005个，其中2014年新发现1739个。截至2014年年底，累计捕获移动互联网恶意程序样本1320601个（按MD5值统计），其中2014年新捕获样本139012个。按照《移动互联网恶意程序描述格式》的八类分类标准，2014年发现的移动互联网恶意程序分类统计数据为：恶意扣费62360个；资费消耗55709个；远程控制13020个；信息窃取4016个；流氓行为2226个；系统破坏1010个；诱骗欺诈542个；恶意传播129个。

2014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

[25]　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，中国反网络病毒联盟成员单位，也是CNCERT/CC省级应急服务支撑单位。

示，其中5月达到全年最高值343个，11月达到全年最低值44个。

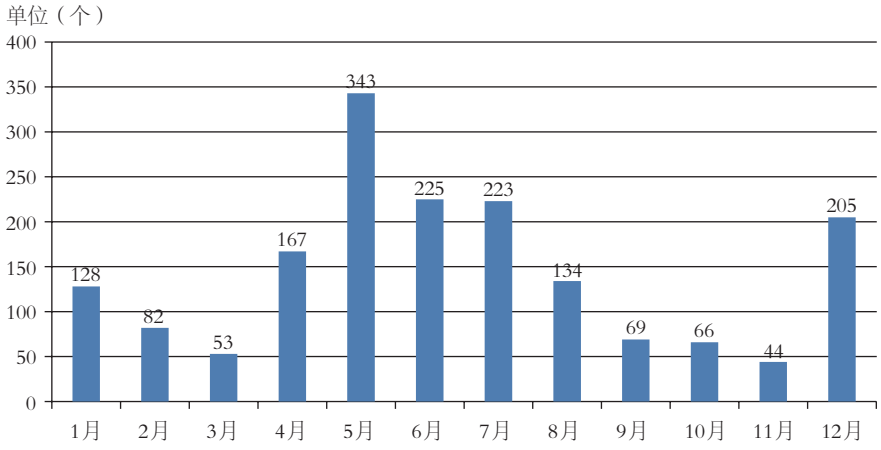


图4-6　2014年移动互联网恶意程序捕获月度统计（来源：网秦公司）

2014年各月捕获移动互联网恶意程序样本数量（按MD5值统计）如图4-7所示，其中1月达到全年最高值25430个，2月达到全年最低值5643个。

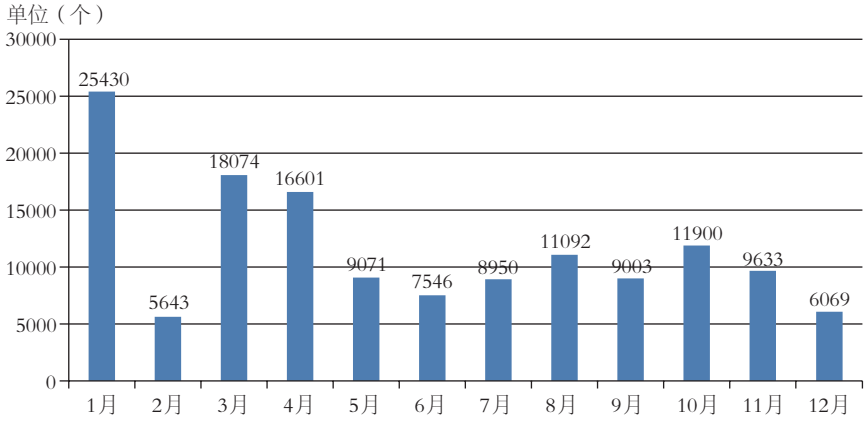


图4-7　2014年移动互联网恶意程序样本捕获月度统计（来源：网秦公司）

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，截至2014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）283181个，其中2014年新发现131337个。截至2014年年底，累计捕获移动互联网恶意程序样本1586098个（按MD5值统计），其中2014年新捕获样本812327个。按照《移动互联网恶意程序描述格式》的八类分类标准，2014年发现的移动互联网恶意程序分类统计数据为：恶意扣费471280个；信息窃取116642个；远程控制29390个；恶意传播2574个；资费消耗137366个；系统破坏11714个；诱骗欺诈9187个；流氓行为34174个。

2014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4-8所示，其中3月达到全年最高值51920个，11月达到全年最低值10421个。

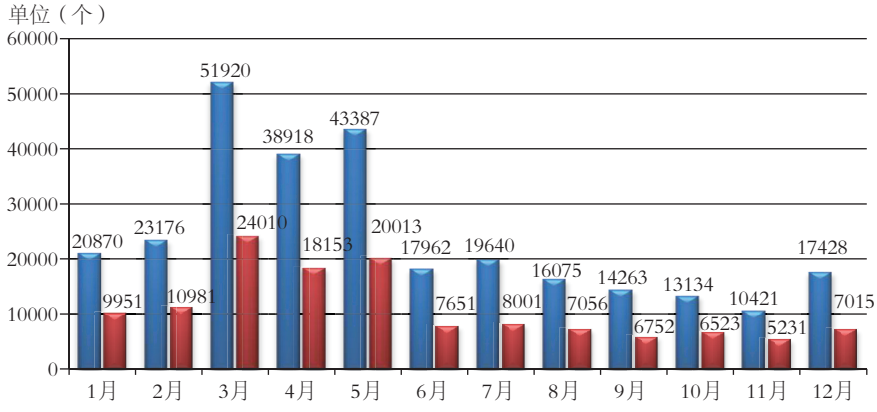


图4-8　2014年捕获移动互联网恶意程序数量月度统计（来源：安天公司）

2014年各月捕获移动互联网恶意程序样本数量（按MD5值统计）如图4-9所示，其中3月达到全年最高值138266个，11月达到全年最低值24188个。

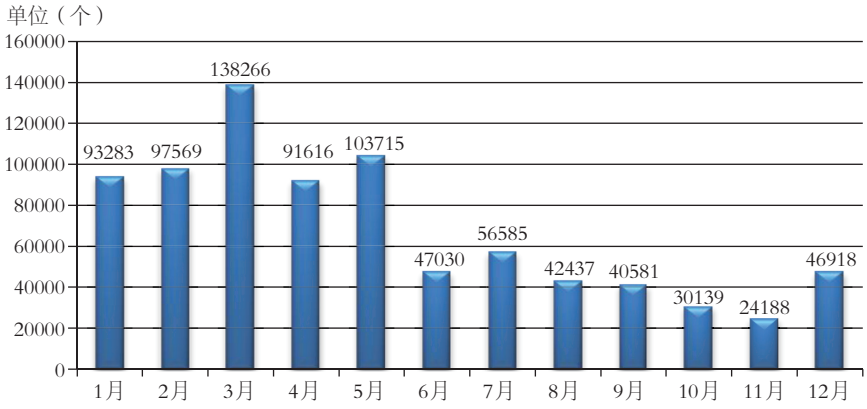


图4-9　2014年捕获移动互联网恶意程序样本数量月度统计（来源：安天公司）

截至2014年，累计发现移动互联网恶意程序下载链接716202条。其中，2014年共发现移动互联网恶意程序下载链接283305条，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　手机应用商店按恶意程序下载链接数排行TOP10（来源：安天公司）

手机应用商店域名	恶意程序下载链接数（条）
down.hualianintledu.cn	28608
gdown.baidu.com	24750
s.iyd.cn	20842
ii.mm60.com	17566
shouji.360tpcdn.com	16626
cdn.cdn.zhxone.com	11487
cdn.market.hiapk.com	11356
apk.dm95.com	9298
www.apk.anzhi.com	9292
wap.apk.anzhi.com	9273

4.3.3 恒安嘉新公司[26]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2014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）3804个，其中2014年新发现751个。截至2014年年底，累计捕获移动互联网恶意程序样本2796278个（按MD5值统计），其中2014年新捕获样本2636996个。按照《移动互联网恶意程序描述格式》的八类分类标准，2014年发现的移动互联网恶意程序分类统计数据为：恶意扣费458655个；信息窃取649658个；远程控制86435个；恶意传播764300个；资费消耗382285个；系统破坏76508个；诱骗欺诈180876个；流氓行为38279个。

2014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4-10所示，其中4月达到全年最低值32个，10月达到全年最高值97个。

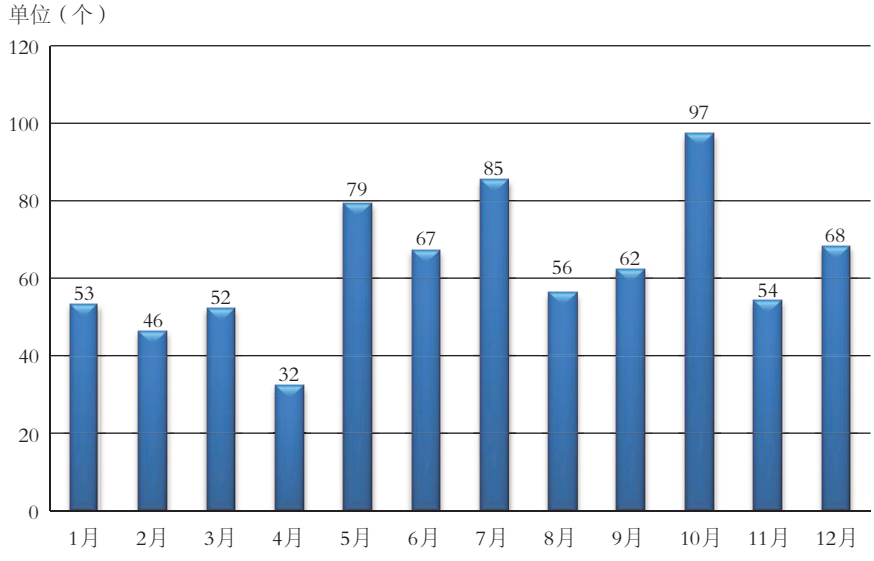


图4-10 2014年移动互联网恶意程序捕获月度统计（来源：恒安嘉新公司）

2014年各月捕获移动互联网恶意程序样本数量（按MD5值统计）如图4-11所示，其中3月达到全年最低值138422个，8月达到全年最高值277682个。

[26] 恒安嘉新公司即恒安嘉新（北京）科技有限公司是国家信息安全漏洞共享平台成员、中国反网络病毒联盟成员，也CNCERT/CC国家级应急服务支撑单位。

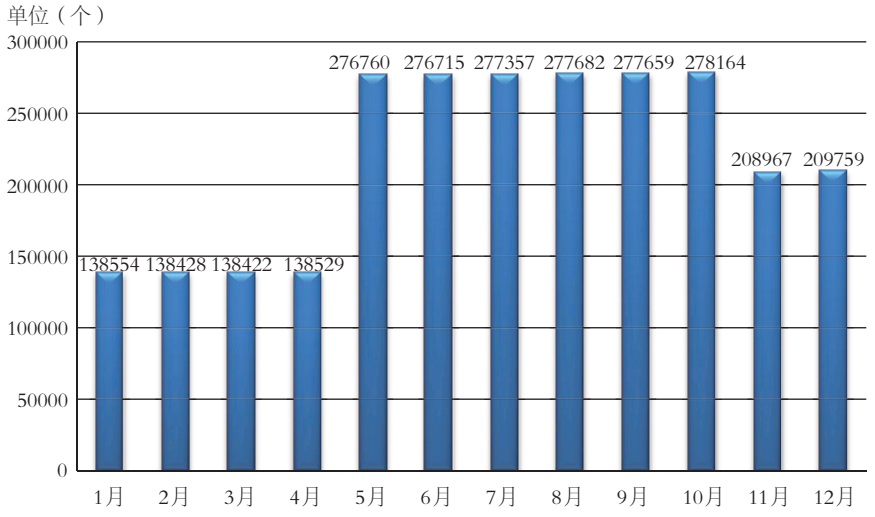


图4-11　2014年移动互联网恶意程序样本捕获月度统计（来源：恒安嘉新公司）

2008-2014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4-12所示。

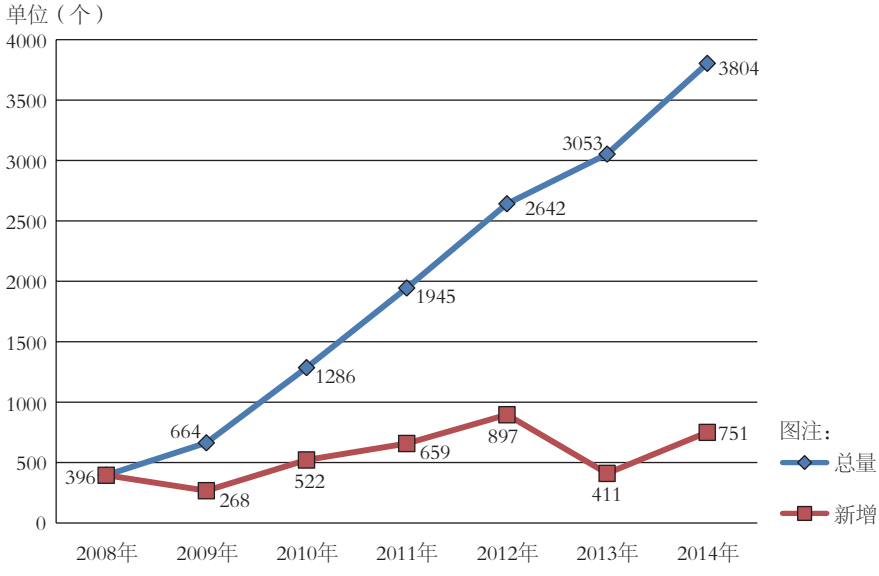


图4-12　2008-2014年移动互联网恶意程序数量走势（来源：恒安嘉新公司）

2008-2014年发现移动互联网恶意程序样本数量（按MD5值统计）走势如图4-13所示。

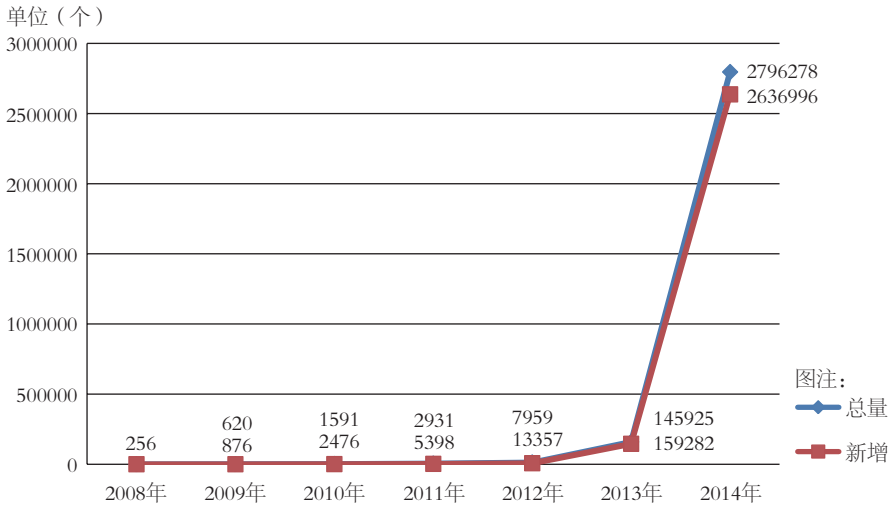


图4-13　2008-2014年移动互联网恶意程序样本数量走势（来源：恒安嘉新公司）

截至2014年，累计发现移动互联网恶意程序下载链接57676条。其中，2014年共发现移动互联网恶意程序下载链接20033条，涉及326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4-2。

表4-2　手机应用商店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（条）
www.3g29.com	4208
izhuti.com	921
www.3g6k.com	395
hzhuti.com	246
www.aisjzt.com	242
nduoa.com	229
liqucn.com	201
angeeks.com	200
hiapk.com	187
gfan.com	178

4.3.4 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，2014年新增捕获Android平台恶意程序样本326.0万个，较2012年、2013年分别增长了25.3倍与3.86倍，平均每天截获新增恶意程序样本近8932个，如图4-14所示。按照《移动互联网恶意程序描述格式》的八类分类标准，2014年发现的Android平台新增移动互联网恶意程序分类统计数据主要是资费消耗，占比高达74.3%；其次为隐私窃取（10.8%）和恶意扣费（10.6%）。远程控制和恶意传播这两类恶意程序数量非常少，仅占新增恶意程序总量的0.1%。

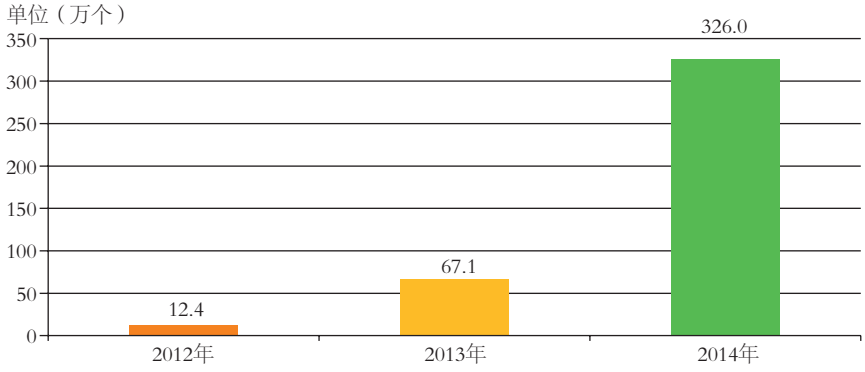


图4-14 2012-2014年Android平台新增恶意程序样本数（来源：奇虎360公司）

2014年各月捕获Android平台移动互联网恶意程序样本数量如图4-15所示，其中3月达到全年最低值6.67万个，12月达到全年最高值86.6万个，新增恶意程序在5、6、7月有小幅度增长，8、9月略有下降，然而，从10月起，新增恶意样本数快速增长，在12月达到高峰，为86.6万个，远高于全年其他月份截获的恶意程序样本数。

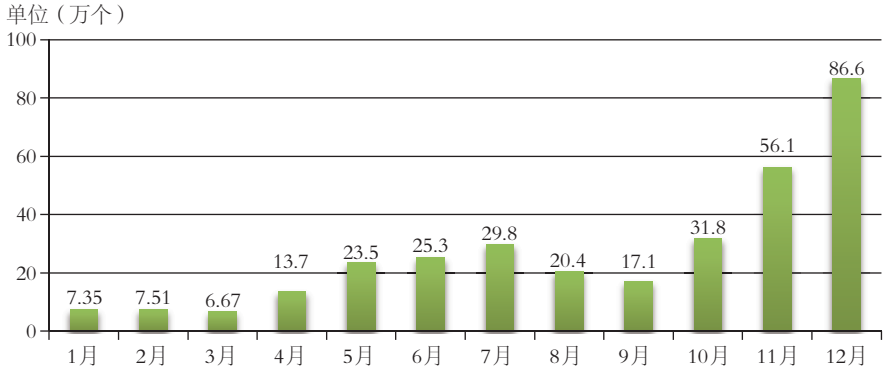


图4-15　2014年Android平台新增恶意程序样本数（来源：奇虎360公司）

4.3.5　趋势科技公司[27]移动互联网恶意程序捕获情况

根据趋势科技公司监测结果，截至2014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）701916个，其中2014年新发现248189个。截至2014年年底，累计捕获移动互联网恶意程序样本（按MD5值统计）4386638个，其中2014年新捕获样本2244731个。

2014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4月达到全年最低值70011个，12月达到全年最高值287630个。

[27]　趋势科技公司即趋势科技（中国）有限公司，是通信行业互联网网络安全信息通报工作单位，也是中国反网络病毒联盟成员单位。

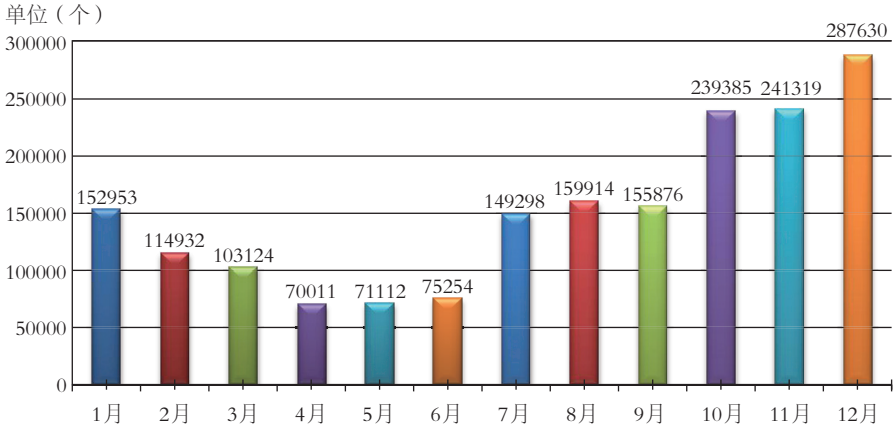


图4-16　2014年移动互联网恶意程序数量捕获月度统计（来源：趋势科技公司）

2014年各月捕获移动互联网恶意程序样本（按MD5值统计）如图4-17所示，其中5月达到全年最低值193855个，12月达到全年最高值898372个。

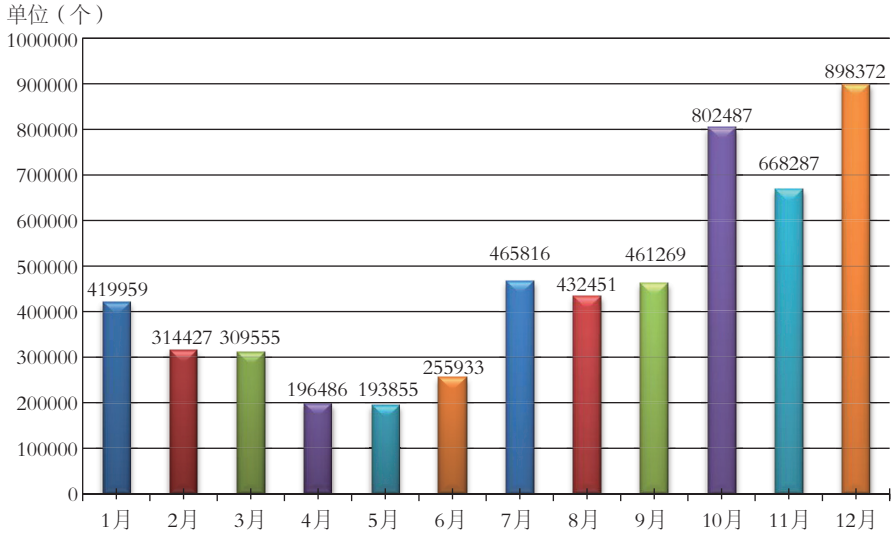


图4-17　2014年移动互联网恶意程序样本捕获月度统计（来源：趋势科技公司）

4.3.6 安管佳公司[28]移动互联网恶意程序捕获情况

根据安管佳公司监测结果，截至2014年年底，累计发现移动互联网恶意程序339707个（按恶意程序名称统计），其中2014年新增225594个。截至2014年年底，累计捕获移动互联网恶意程序样本2909131个（按MD5值统计），其中2014年新捕获样本1979349个。按照《移动互联网恶意程序描述格式》的八类分类标准，2014年发现的移动互联网恶意程序分类统计数据（按恶意程序名称统计）为：恶意扣费23959个；信息窃取33413个；远程控制570个；恶意传播11521个；资费消耗120027个；系统破坏7909个；诱骗欺诈21400个；流氓行为6795个。2014年发现的移动互联网恶意程序分类统计数据（按MD5值统计）为：恶意扣费327850个；信息窃取170509个；远程控制5457个；恶意传播141987个；资费消耗1036368个；系统破坏41197个；诱骗欺诈221970个；流氓行为34011个。

2014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4-18所示，其中9月达到全年最高值61415个，2月达到全年最低值9146个。

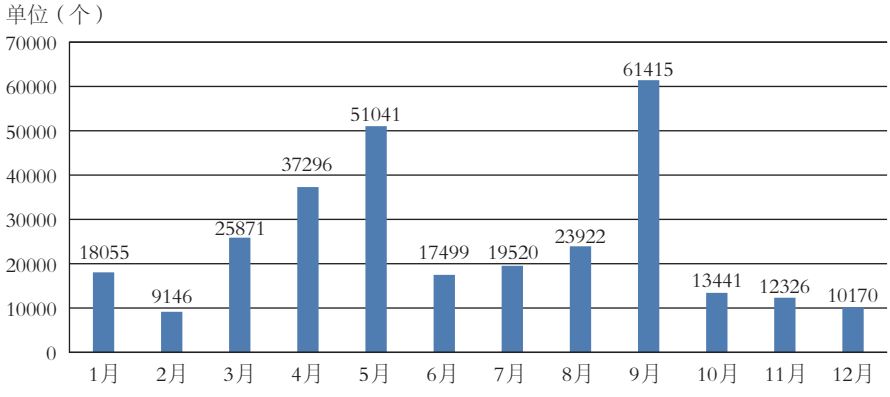


图4-18 2014年移动互联网恶意程序样本捕获月度统计（来源：安管佳公司）

2014年各月捕获移动互联网恶意程序样本数量（按MD5值统计）如图4-19所示，其中12月达到全年最高值613353个，2月达到全年最低值44963个。

[28] 安管佳公司即北京安管佳科技有限公司，是中国反网络病毒联盟成员单位。

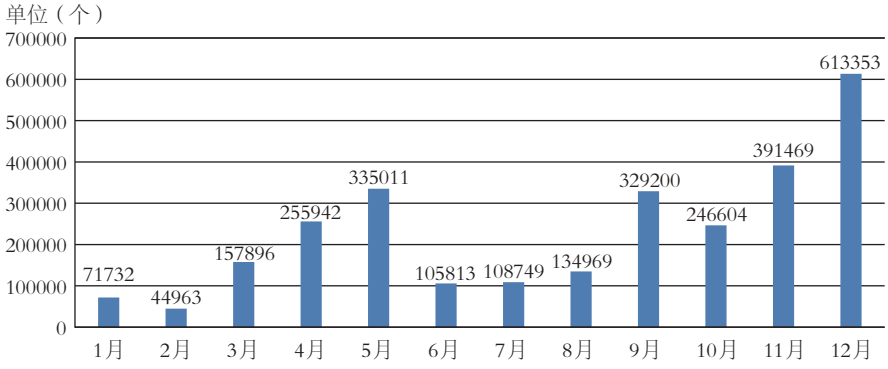


图4-19　2014年捕获移动互联网恶意程序样本数量月度统计（来源：安管佳公司）

5 网站安全监测情况

5.1 网页篡改情况

按照攻击手段，网页篡改可以分成显式篡改和隐式篡改两种。通过显式网页篡改，黑客可炫耀自己的技术技巧，或达到声明自己主张的目的；隐式篡改一般是在被攻击网站的网页中植入被链接到色情、诈骗等非法信息的暗链中，以助黑客谋取非法经济利益。黑客为了篡改网页，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，以争取在第一时间内恢复被篡改的网站，减少攻击事件带来的影响。

5.1.1 我国境内网站被篡改总体情况

2014年，我国境内被篡改的网站数量为36969个，较2013年的24034个大幅增长53.8%。我国境内被篡改网站的月度统计情况如图5-1所示。2014年2月开始，CNCERT/CC加强了对我国境内网站被植入暗链情况的监测,同时扩大了境内网站监测数量，使得2014年全年较2013年被篡改网站的总数有大幅度增长。

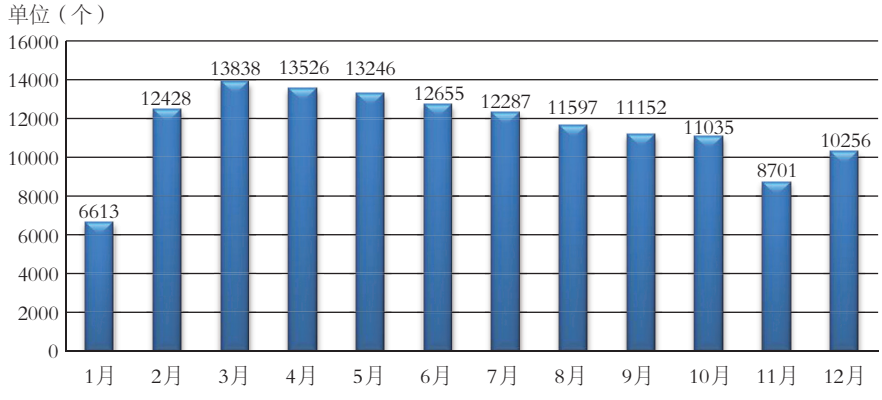


图5-1 2014年我国境内被篡改网站数量月度统计（来源：CNCERT/CC）

从篡改攻击的手段来看，我国被篡改的网站中以植入暗链方式被攻击的占83.3%，对比2013年以植入暗链方式攻击的网站占57%的差异来看，2014年以植入暗链方式攻击的手段大幅度提升。

从域名类型来看，2014年我国境内被篡改的网站中，代表商业机构的网站（.com）最多，占71.8%，其次是网络组织类（.net）网站和政府类（.gov）网站，分别占6.7%和4.8%，非营利组织类（.org）网站和教育机构类（.edu）网站分别占2.0%和0.2%。对比2013年，我国商业机构类网站被篡改情况有小幅度上升，从2013年的67.2%上升至2014年的71.8%。2014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。

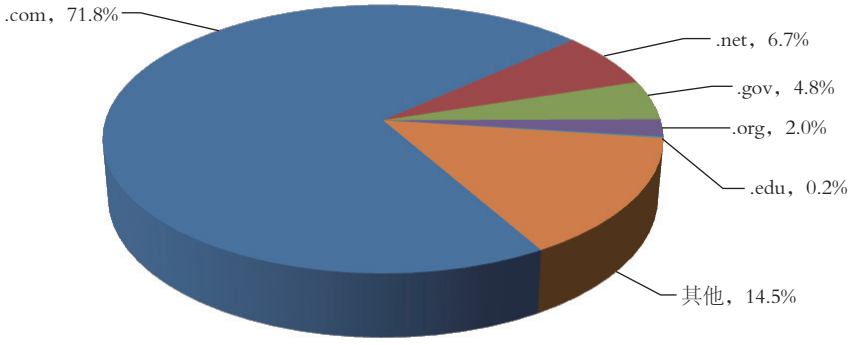


图5-2　2014年我国境内被篡改网站按域名类型分布（来源：CNCERT/CC）

如图5-3所示，2014年我国境内被篡改网站数量按地域进行统计，前10位的地区分别是：北京市、江苏省、上海市、广东省、浙江省、福建省、河南省、四川省、安徽省、天津市。2014年的情况与2013年类似，仅仅为天津市代替了山东省。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。

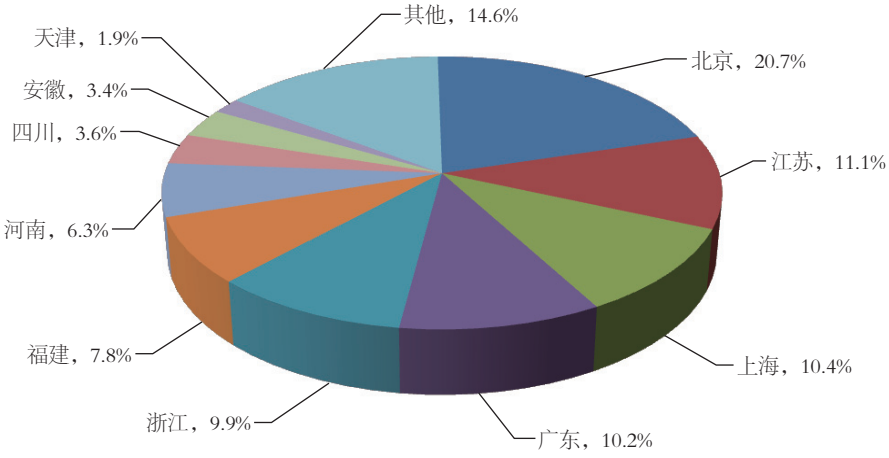


图5-3　2014年我国境内被篡改网站按地区分布（来源：CNCERT/CC）

5.1.2　我国境内政府网站被篡改情况

近年来，各级政府逐渐重视信息化建设，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重视和维护，已成为中国网络安全中最薄弱的一环。同时，由于政府网站不可替代的权威性，对它的攻击严重影响中国的网络信息安全。

2014年，我国境内政府网站被篡改数量为1763个，较2013年的2430个减少27.4%。2014年，政府网站被篡改数量的下降，一方面是由于政府网站的安全意识提高，另一方面得益于加大了对政府网站的重点监测和及时处置。2014年我国境内被篡改的政府网站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。

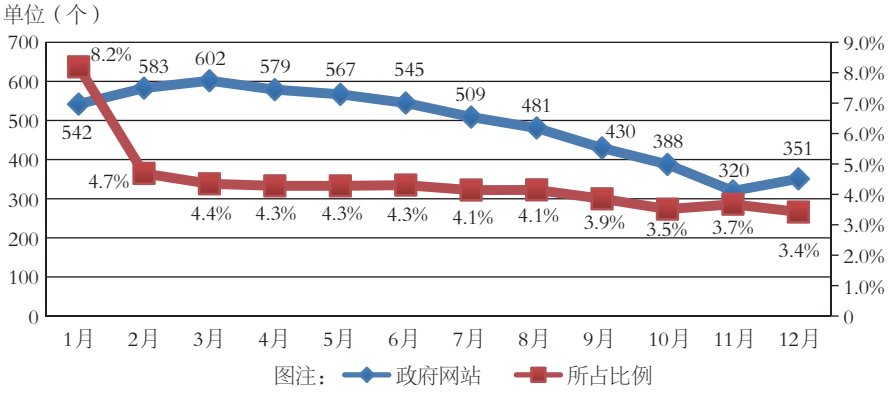


图5-4　2014年我国境内被篡改的政府网站数量和所占比例月度统计
（来源：CNCERT/CC）

2014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。2014年，我国省市级政府网站维护保障水平提升，未发现2013年间多个省市级网站被同时篡改的现象。

表5-1　2014年CNCERT/CC监测发现被篡改的部分省市级政府网站
（来源：CNCERT/CC）

网站所属部门	被篡改后的 URL	监测时间
哈尔滨市工商行政管理局	http://www.hrbgs.gov.cn/id.htm	2014/7/15
江苏人力资源和社会保障服务大厅	http://map.jshrss.gov.cn/kurd.txt	2014/8/11
安徽交通高级检索	http://chaxun.ahjt.gov.cn/index.htm	2014/2/18
北京市丰台区人民政府网站	http://lgqjd.gov.cn/index.htm	2014/2/6
中华人民共和国司法部	http://www.moj.gov.cn/node_7341_2.htm	2014/3/6
重庆市食品药品监督管理局北碚区分局	http://www.bbfda.gov.cn	2014/4/19
国家中医药管理局	http://satcm.gov.cn	2014/10/27
安徽林业信息网	http://ahhsly.gov.cn	2014/2/20
湖北旅游网湖北省旅游局官方网站	http://www.hubeitour.gov.cn/naizui.html	2014/9/25
河北物价局	http://www.hebwj.gov.cn//WinSec.htm	2014/6/2
内蒙古出入境检验检疫局	http://www.nmciq.gov.cn/1.html	2014/4/16
辽宁人保局	http://www.lntl.hrss.gov.cn/110.htm	2014/3/31
中国民主同盟上海市委员会	http://www.minmengsh.gov.cn/110.htm	2014/3/28

5.1.3 通报成员单位报送情况

5.1.3.1 安天公司报送的网页篡改情况

2014年，安天公司监测发现我国境内被篡改网站数量为5606个，较2013年的3876个增加44.6%，我国境内被篡改网站数量月度统计如图5-5所示。

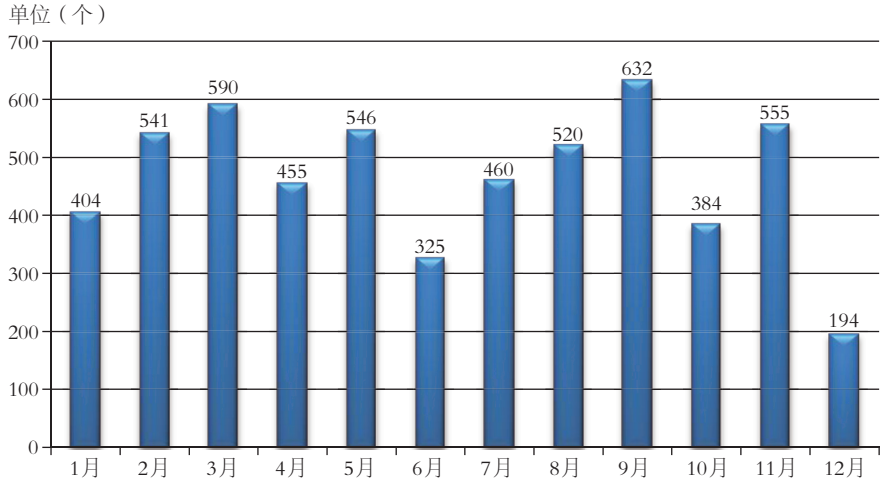


图5-5 2014年我国境内被篡改网站数量月度统计（来源：安天公司）

从域名类型来看，2014年我国境内被篡改网站中，政府类（.gov）网站占67.3%，教育类（.edu）网站占30.8%，其他占1.9%。2014年我国境内被篡改网站按域名类型分布情况如图5-6所示。

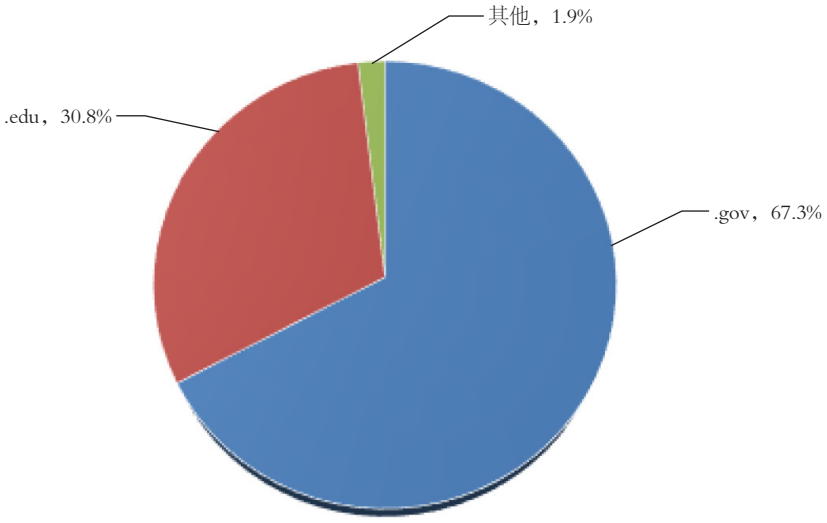


图5-6　2014年我国境内被篡改网站按域名类型分布（来源：安天公司）

如图5-7所示，2014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：安徽省、广东省、湖北省、江苏省、四川省、北京市、浙江省、湖南省、河南省、河北省。

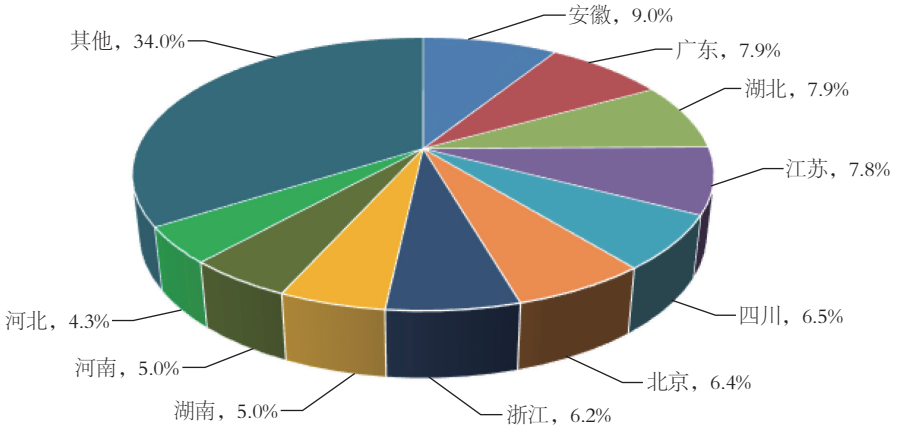


图5-7　2014年我国境内被篡改网站按地区分布（来源：安天公司）

5.1.3.2 奇虎360公司报送的网页篡改情况

2014年全年（截至11月30日），奇虎360公司共扫描各类网站164.2万个，较2013年的91.2万个增加了80.0%。其中被篡改网站17.7万个（已去重），约占扫描网站总数的10.8%，比2013年增多了2.1个百分点，具体如图5-8所示。

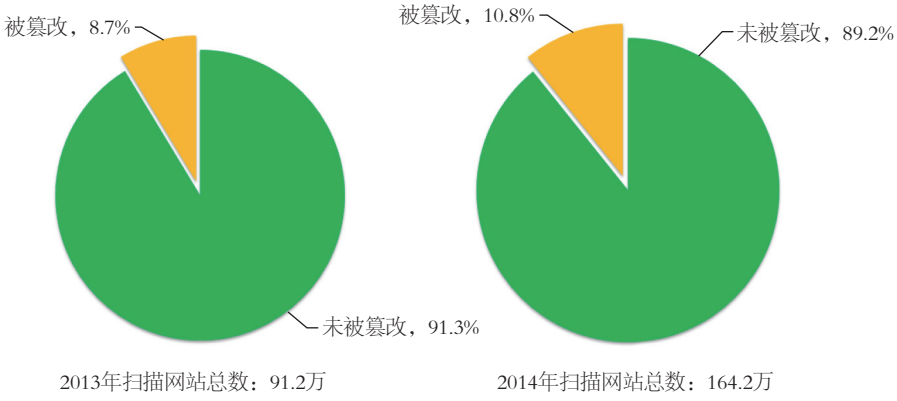


图5-8 2014年我国境内被篡改网站数量（来源：奇虎360公司）

从每月数据统计（当月去重）来看，2014年1-11月平均每个月扫描检出被篡改网站3.28万个，比2013年的1.34万个增长了144.8%。其中，7月监测发现数量最多，达到11.7万个，其次是8月（7.8万个）、9月（4.0万个），图5-9为各月监测发现的网页篡改数量。

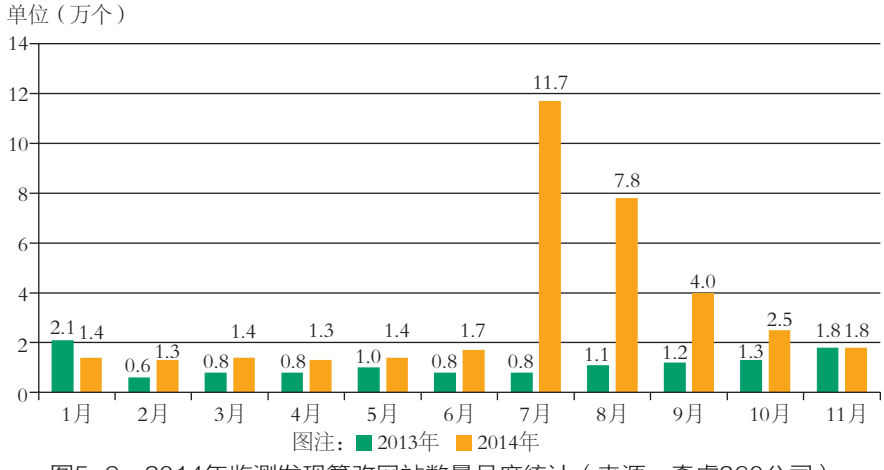


图5-9 2014年监测发现篡改网站数量月度统计（来源：奇虎360公司）

5.1.3.3 知道创宇公司[29]报送的网页篡改情况

2014年，知道创宇公司监测发现我国境内被篡改网站数量为224733个，较2013年的24034个增长幅度较大，主要原因是统计数据过程中加入了大量暗链、域名劫持等类型的篡改数据。我国境内被篡改网站月度统计情况如图5-10所示。

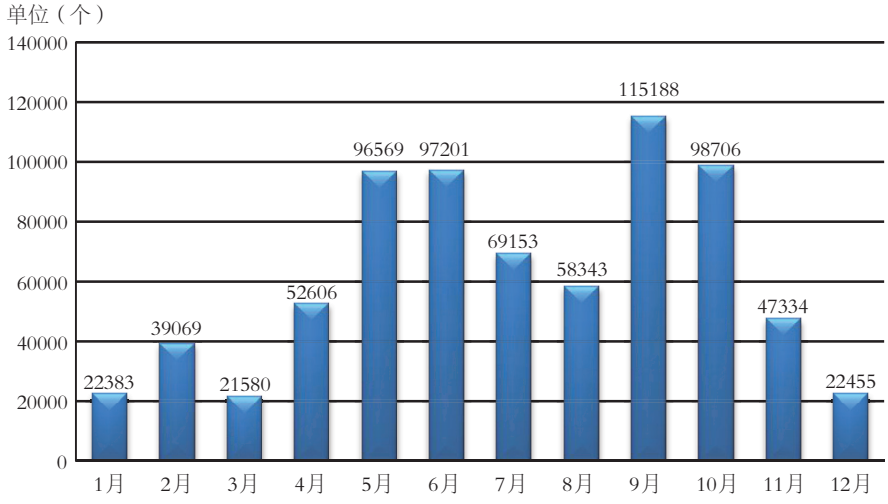


图5-10 2014年我国境内被篡改网站次数月度统计（来源：知道创宇公司）

从域名类型来看，2014年我国境内被篡改网站中，代表商业机构的网站（.com）占75%，网络组织类（.net）网站占6%，政府类（.gov）网站占4%，非营利组织类（.org）网站占2%，教育机构类（.edu）网站占1%。2014年我国境内被篡改网站按域名类型分布情况如图5-11所示。

[29] 知道创宇公司即北京知道创宇信息技术有限公司，是通信行业互联网网络安全信息通报工作单位、国家信息安全漏洞共享平台成员、中国反网络病毒联盟成员，也是CNCERT/CC省级应急服务支撑单位。

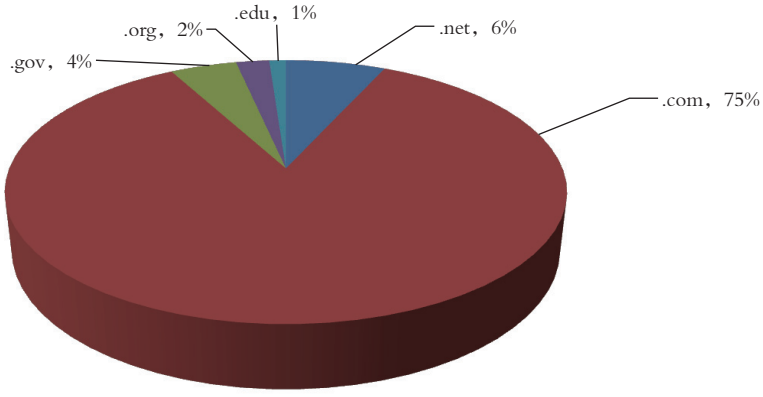


图5-11　2014年我国境内被篡改网站按域名类型分布（来源：知道创宇公司）

如图5-12所示，2014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、广东省、江苏省、上海市、福建省、浙江省、河南省、安徽省、四川省、陕西省。

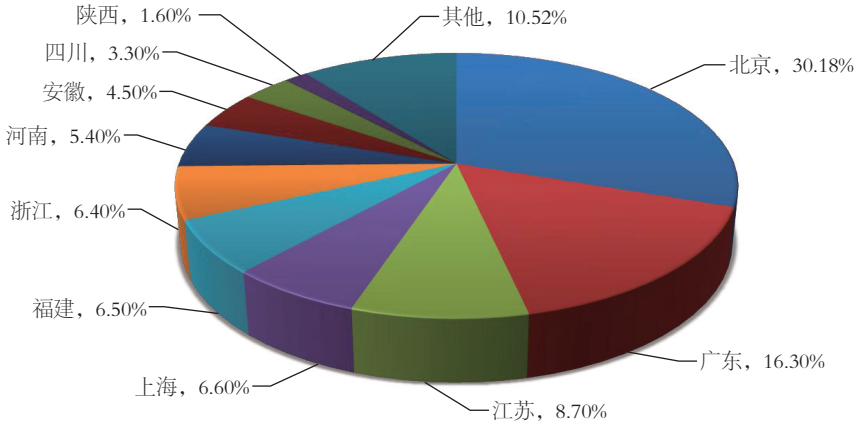


图5-12　2014年我国境内被篡改网站按地区分布（来源：知道创宇公司）

2014年，北京知道创宇信息技术公司监测发现我国境内政府网站被篡改数量为8702个，涉及74209个子域名，共9.5万个URL。较2013年境内政府网站被篡改的2430

个大幅度增长258%，占监测的政府网站列表总数的8.1%，即平均每1000个政府网站中就有81个网站遭到了篡改。2014年我国境内被篡改的政府网站数量和其占被篡改网站总数比例按月度统计如图5-13所示。

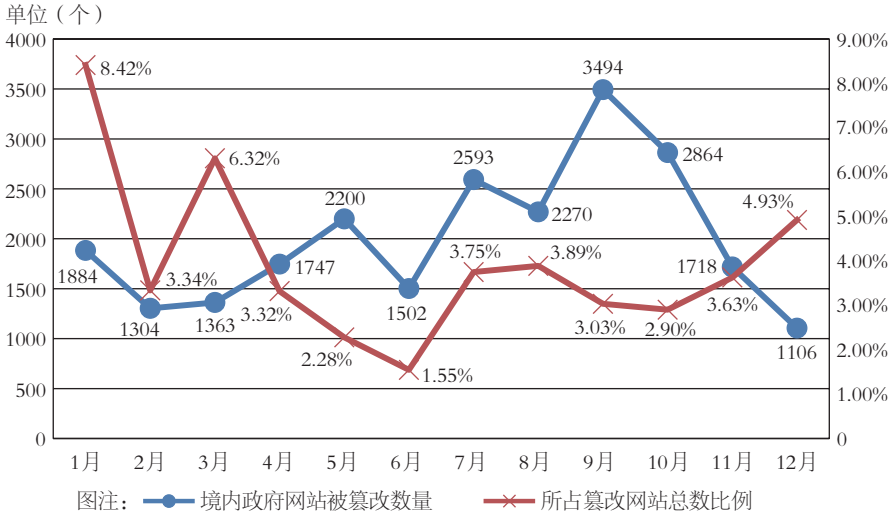


图5-13　2014年我国境内政府网站被篡改数量和所占比例月度统计
（来源：知道创宇公司）

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，这是黑客传播恶意程序的常用手段。通信行业相关单位在网页挂马和恶意程序传播监测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

根据瑞星信息技术有限公司对中国大陆地区30万个网站的检测结果，2014年共监测到24万个网站（去重后或各月累计）被挂马，图5-14是瑞星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，挂马网站数量在2014年呈现波动趋

势，5月达到峰值，1月为全年最低值。

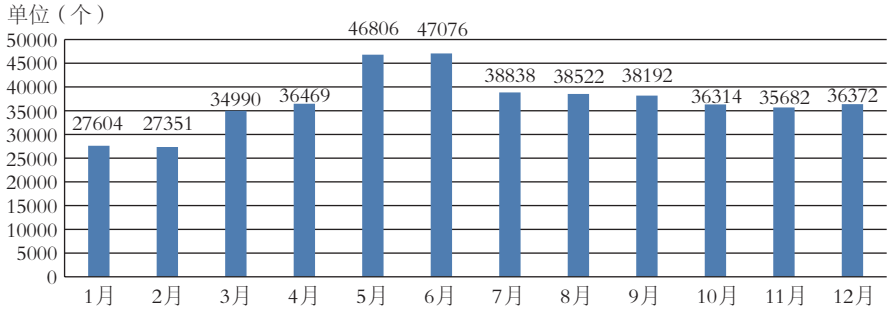


图5-14　2014年截获挂马网站数量月度统计（来源：瑞星公司）

图5-15为奇虎公司监测的2014年各月的新增挂马网站数量分布，可以看出，挂马网站数量2014年始终在低位保持稳定。

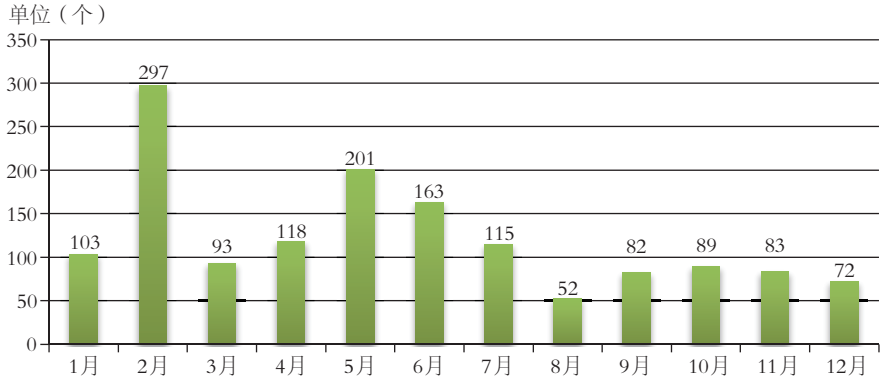


图5-15　2014年新增挂马网站数量月度统计（来源：奇虎360公司）

图5-16为瑞星监测发现的2014年中国大陆地区挂马网站按省份分布情况，列前5位的省份是广东省（12.97%）、山东省（7.03%）、江苏省（6.34%）、浙江省（5.85%）和河北省（5.54%）。挂马网站多集中在人口稠密、经济发达的省份。

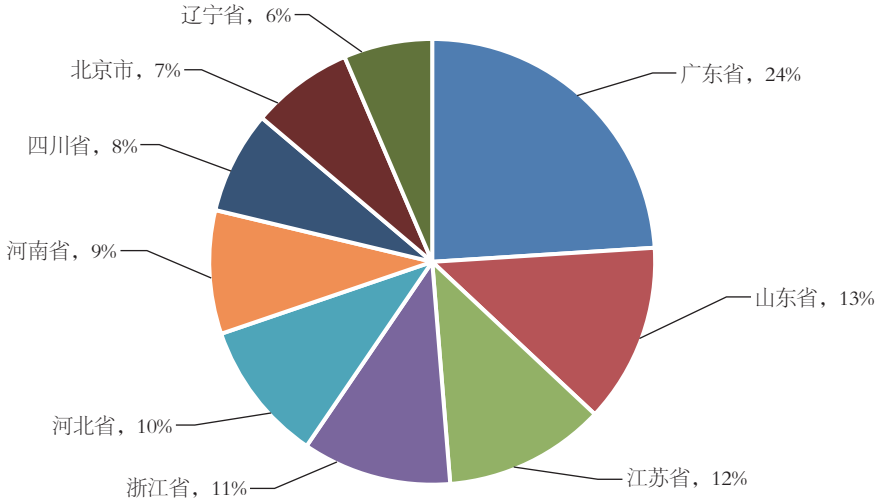


图5-16　2014年中国大陆地区挂马网站按省份分布（来源：瑞星公司）

图5-17所示为瑞星监测发现的2014年中国大陆地区挂马网站按域名分布情况。其中，排名前3位的是.com域名（51.51%）、.cn域名（19.56%）和.org域名（14.19%）。此外，被挂马的政府网站（.gov.cn域名网站）数量为23618个，占全部挂马网站总数的9.69%。

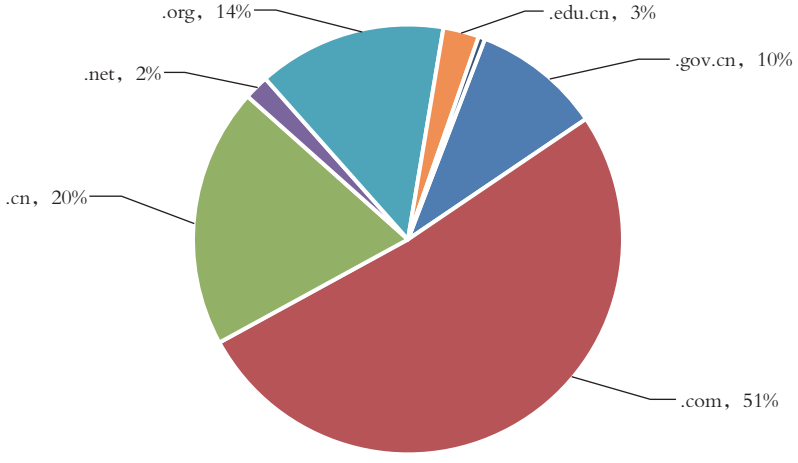


图5-17　2014年中国大陆地区挂马网站按域名分布情况（来源：瑞星公司）

5.2.2 恶意域名监测情况

一些网站或域名作为放马服务器的形式出现，这些网站或域名往往被黑客或挂马集团掌控，或用作恶意跳转链接，或作为恶意代码下载服务器。表5-2中，这些域名均为动态域名，许多可以在国内外多家域名注册商注册，且注册成本相对较为低廉。实施网页挂马的黑客或挂马集团往往会批量注册，在一段时间内不断变换使用，以隐藏自己的活动痕迹，规避监管，增加治理的难度。

表5-2 挂马网站（恶意域名）按子域名数排行TOP10（来源：瑞星公司）

挂马网站域名	相关挂马子域名数	部分挂马子域名举例
3322.org	463	rootkit004.3322.rog
myftp.biz	230	webms14.myftp.biz
noip.me	215	paypai01.noip.me
sytes.net	190	counthkfu.sytes.net
9966.org	170	srgase5463.9966.org
servehttp.com	130	wejuysegrf435.servehttp.com
myvnc.com	95	jack0079.myvnc.com
ddns.net	80	filehtyr.ddns.net
zapto.org	60	laserhgbtr56.zapto.org
3utilites.com	50	hostfree56788.3utilites.com

5.3 网页仿冒情况

5.3.1 我国境内网页仿冒情况

网页仿冒俗称网络钓鱼（Phishing），是社会工程学欺骗原理与网络技术相结合的典型应用。2014年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面99409个，涉及到境内外6844个IP地址，平均每个IP地址承载14.5个钓鱼页面。在这6844个IP地址中，有89.4%位于境外，其中美国（17.7%）、中国香港（15.2%）和韩国（1.8%）居前3位，分别承载了10265个、29237个和10790个针对我国境内网站的钓鱼页面，如图5-18和图5-19所示。

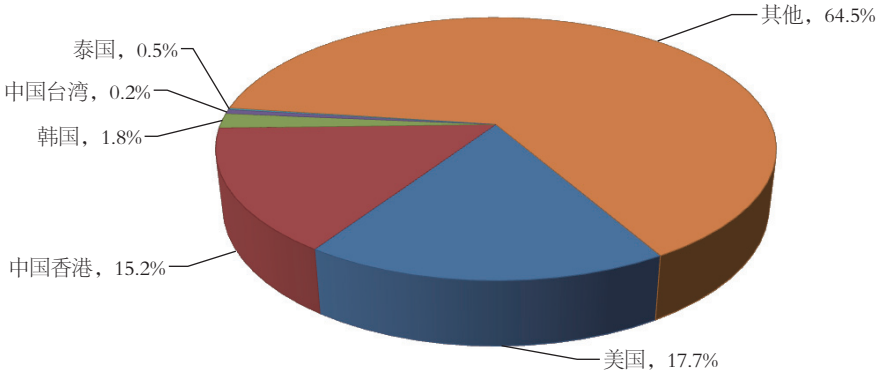


图5-18　2014年仿冒我国境内网站的境外IP地址按国家和地区分布
（来源：CNCERT/CC）

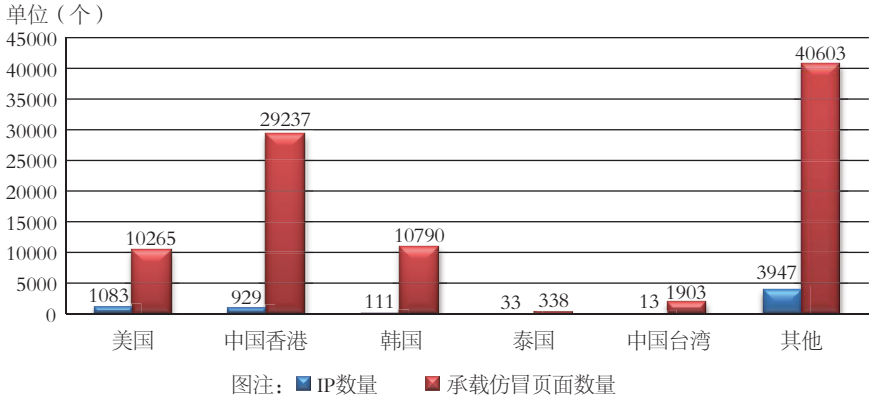


图5-19　2014年仿冒我国境内网站的境外IP地址及其承载的仿冒页面数量
按国家或地区分布TOP5（来源：CNCERT/CC）

从钓鱼站点使用域名的顶级域分布来看，以.com最多，占66.3%，其次是.pw和.cn，分别占9.0%和5.1%。2014年CNCERT/CC抽样监测发现的钓鱼站点所用域名按顶级域分布如图5-20所示。

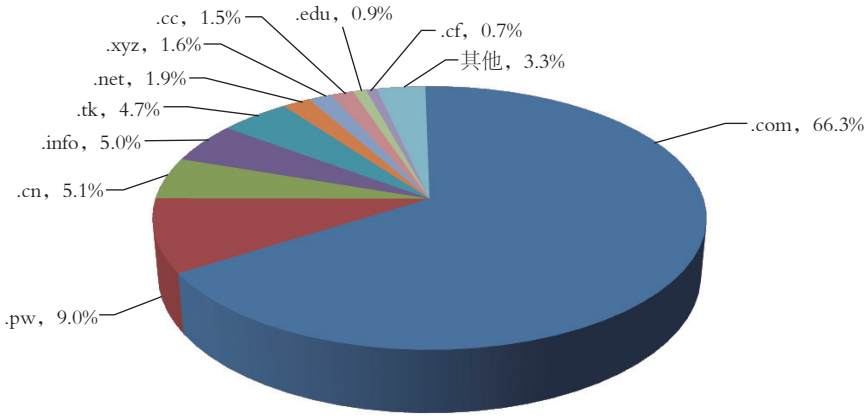


图5-20　2014年抽样监测发现的钓鱼站点所用域名按顶级域分布
（来源：CNCERT/CC）

5.3.2　通报成员单位报送情况

2014年，奇虎360公司共截获新增钓鱼网站262.1万个，较2012年、2013年分别增长了200.1%与19.1%。平均每天截获新增钓鱼网站约7080个，图5-21为2010-2014年每年新增钓鱼网站数量对比。

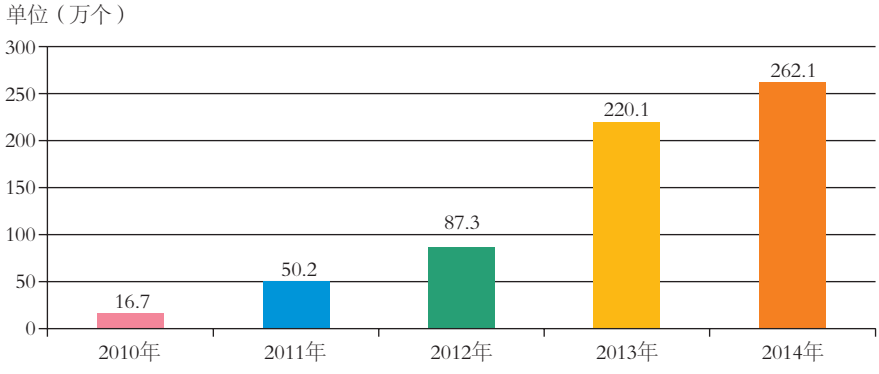


图5-21　2010-2014年每年新增钓鱼网站数量（来源：奇虎360公司）

图5-22为2014年各月新增钓鱼网站数量的变化趋势，其中，3月新增钓鱼网站数量达到峰值，高达39.2万个。

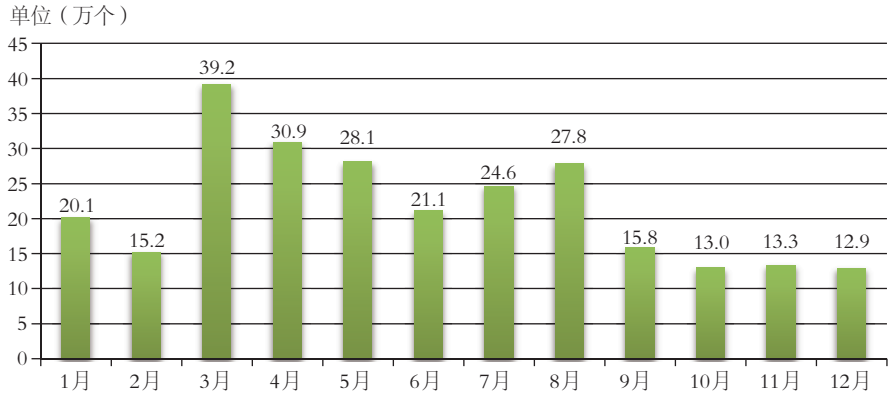


图5-22　2014年每月新增钓鱼网站数量（来源：奇虎360公司）

如图5-23所示，从新增钓鱼网站服务器的地域分布上看，大约有57.3%的钓鱼网站服务器分布在境内地区，42.7%在境外地区。这也是最近几年来，首次出现国内钓鱼网站服务器多于国外钓鱼网站服务器的情况。

从境内新增钓鱼网站服务器地域分布上看，28.9%分布在广东省，居于首位；其次分别为浙江省（19.6%）、北京市（18.2%）、江苏省（16.9%）、福建省（3.07%）。从境外新增钓鱼网站服务器地域分布上看，43.7%分布在美国，接近境外所有钓鱼网站服务器总量的一半；其次是加拿大（33.9%）、亚洲其他地区（15.3%）。

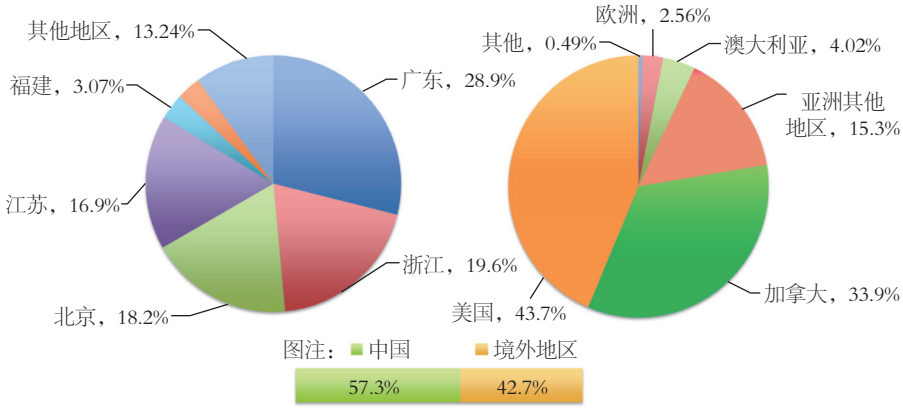


图5-23　新增钓鱼网站服务器地域分布（来源：奇虎360公司）

由于多数境外地区对于网站的注册登记审核机制比较宽松，而且钓鱼网站的受害者及相关法律诉讼大多不在当地，客观上为不法分子逃避法律监管提供了便利，所以近些年来，绝大多数的钓鱼网站服务器都分布在境外地区。但随着安全厂商对于境外钓鱼网站的识别能力和打击力度不断提升，极大地压缩了境外钓鱼网站的生存空间，迫使相当数量的攻击者开始转向租用国内服务器。此外，也有越来越多的攻击者开始通过篡改正规网站，植入钓鱼网页的方式发动钓鱼攻击，这种攻击方式更隐蔽，更不容易被发现。同时，随着云主机服务的流行，由于部分云主机服务提供商安全审核能力的不足，很多攻击者还会将钓鱼网站直接架设在第三方提供的具有合法备案资质的云服务平台上。这些因素都是导致2014年国内钓鱼网站服务器多于国外钓鱼网站服务器的重要原因。图5-24给出了2012-2014年钓鱼网站地域分布的变化趋势。

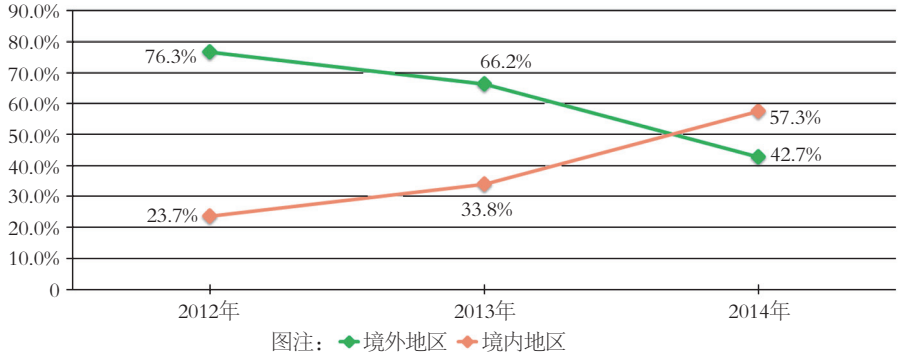


图5-24　2012-2014年钓鱼网站地域分布趋势（来源：奇虎360公司）

2014年，北京知道创宇信息技术有限公司共监测到仿冒我国境内网站的假冒仿冒页面5605.7万个。从假冒仿冒站点使用域名的顶级域类型比例来看，以.com最多，占17.28%，其次是.cn和.org，分别占0.82%和0.43%。2014年北京知道创宇信息技术有限公司监测发现的假冒仿冒站点所用域名按顶级域分布如图5-25所示，域名分布中其他类型占比较高，究其原因主要是该类型中所包含的细项较多，如.cc、.info、.tw、.us、.jp、.so等，所以占比较高。

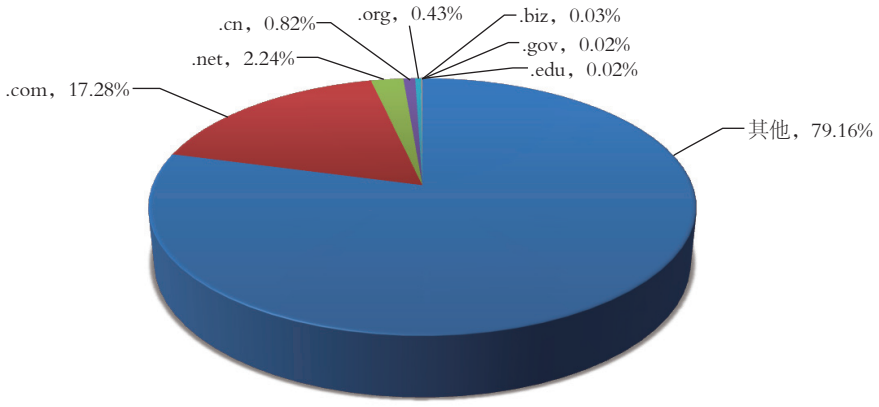


图5-25　2014年监测发现的钓鱼站点所用域名按顶级域分布（来源：知道创宇公司）

2014年，瑞星信息技术有限公司共监测到仿冒我国境内网站的钓鱼页面2931258个，涉及境内外1631258个IP地址，平均每个IP地址承载1.79个钓鱼页面。从钓鱼站点使用域名的顶级域分布来看，以.com最多，占61.29%，其次是.tk和.net，分别占14.32%和4.78%。2014年瑞星信息技术有限公司监测发现的钓鱼站点所用域名按顶级域分布如图5-26所示。

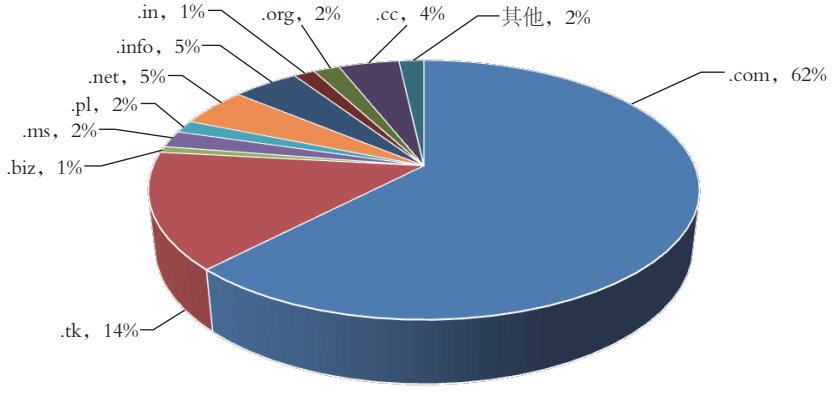


图5-26　2014年监测发现的钓鱼站点所用域名按顶级域分布（来源：瑞星公司）

2014年，趋势科技公司共监测到仿冒我国境内网站的钓鱼页面3761个。从钓鱼站点使用域名的顶级域分布来看，以.com最多，占36.5%，其次是.tk和.cc，分别占20.6%和9.5%。2014年趋势科技公司监测发现的钓鱼站点所用域名按顶级域分布如图5-27所示。

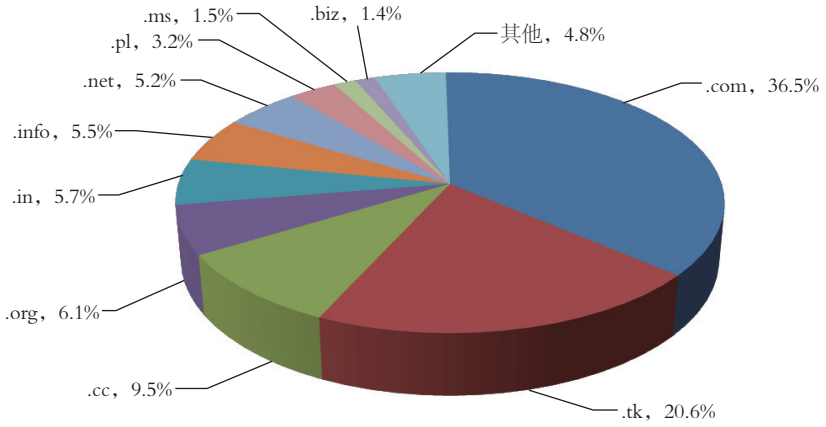


图5-27　2014年监测发现的钓鱼站点所用域名按顶级域分布（来源：趋势科技公司）

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。

5.4.1　我国境内网站后门情况

2014年CNCERT/CC共监测到境内40186个网站被植入后门，其中政府网站有1529个。我国境内被植入后门网站月度统计情况如图5-28所示。

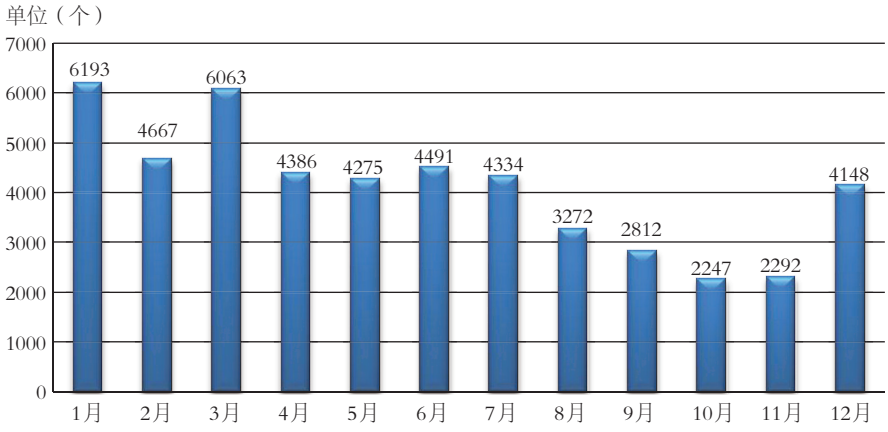


图5-28　2014年我国境内被植入后门网站数量月度统计（来源：CNCERT/CC）

从域名类型来看，2014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57.7%，其次是网络组织类（.net）和政府类（.gov）网站，分别占6.4%和3.8%。2014年我国境内被植入后门的网站数量按域名类型分布如图5-29所示。

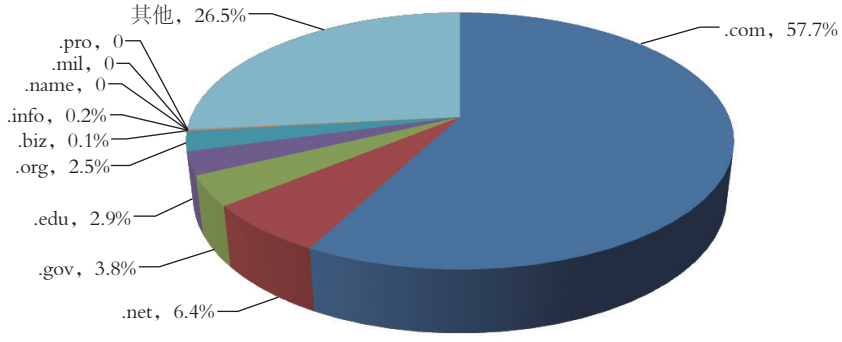


图5-29　2014年我国境内被植入后门网站数量按域名类型分布（来源：CNCERT/CC）

如图5-30所示，2014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、江苏省、浙江省、广东省、上海市、四川省、河南省、福建省、江西省、山东省。

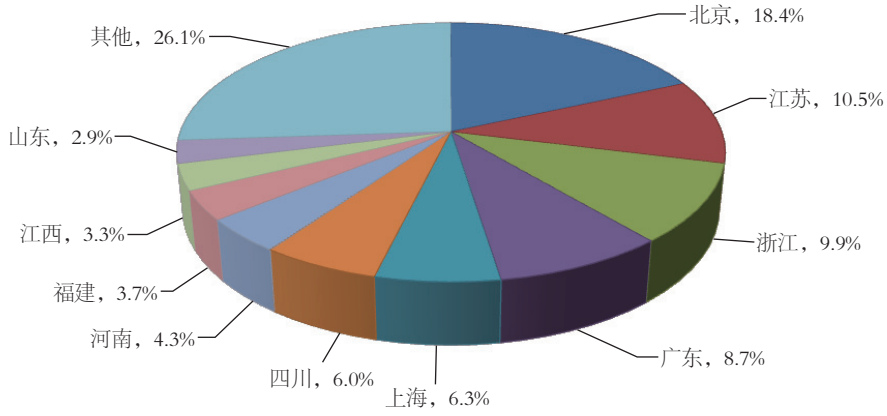


图5-30　2014年我国境内被植入后门网站数量按地区分布（来源：CNCERT/CC）

向我国境内网站实施植入后门攻击的IP地址中，有19168个位于境外，主要位于美国（24.8%）、韩国（6.7%）和中国香港（6.5%）等国家和地区，如图5-31所示。

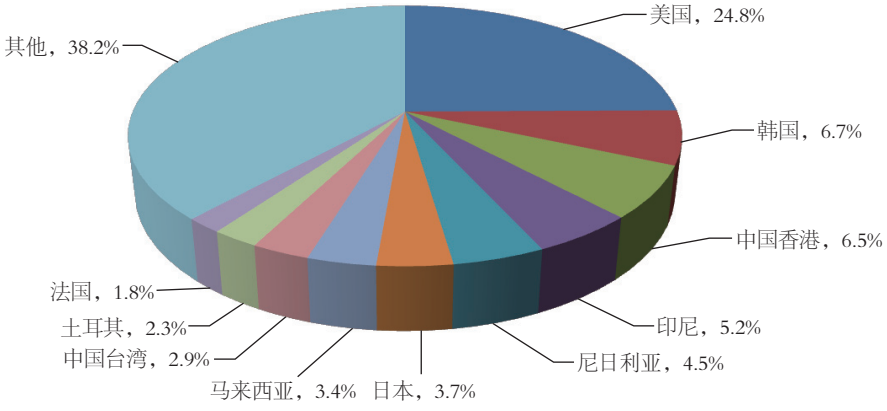


图5-31　2014年向我国境内网站植入后门的境外IP地址按国家和地区分布
（来源：CNCERT/CC）

其中，位于美国的4761个IP地址共向我国境内5580个网站植入了后门程序，侵入网站数量居首位，其次是位于中国香港和位于韩国的IP地址，分别向我国境内5023个

和3719个网站植入了后门程序，如图5-32所示。

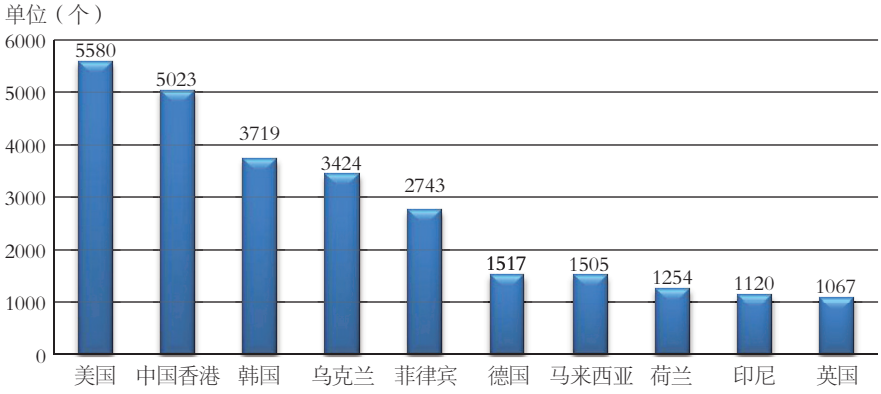


图5-32　2014年境外通过植入后门控制我国境内网站数量TOP10
（来源：CNCERT/CC）

5.4.2　通报成员单位报送情况

2014年全年（截至11月30日），奇虎360公司网站安全检测共对8409台网站服务器进行了网站后门检测，覆盖网站199.6万个，扫描发现约3465台服务器存在后门，占所有扫描网站服务器的41.2%，比2013年增加了7.4个百分点。总体而言，2014年，服务器被检出后门的绝对数量和比例都较2013年有大幅提升，如图5-33所示。

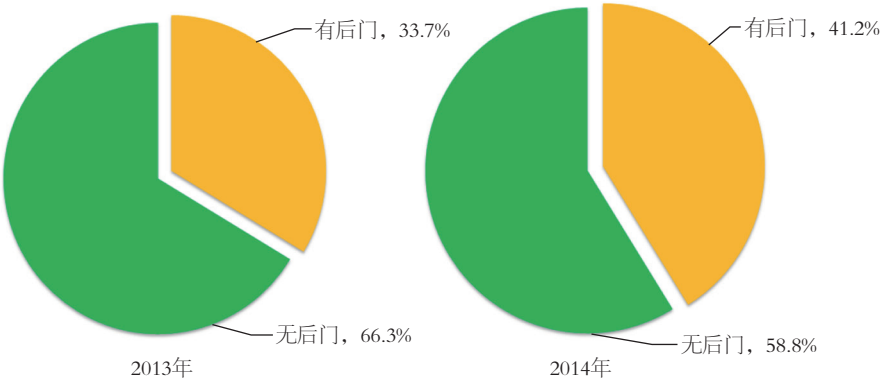


图5-33　2013年和2014年服务器被植入后门状况对比（来源：奇虎360公司）

2014年，瑞星公司共监测到境内12563个网站被植入网站后门，其中政府网站有1051个。我国境内被植入后门网站月度统计情况如图5-34所示。

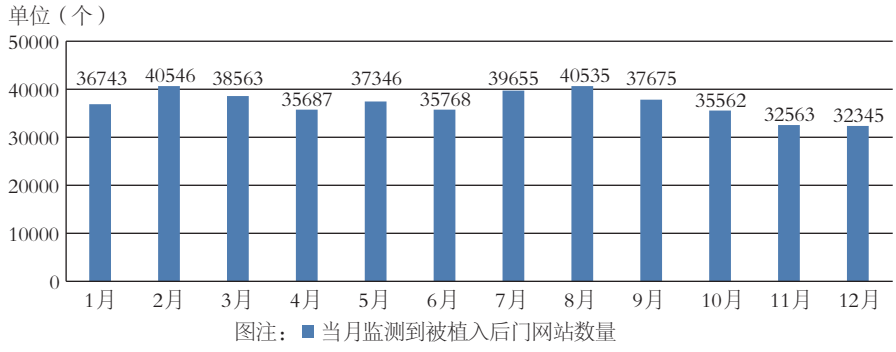


图5-34　2014年我国境内被植入后门网站数量月度统计（来源：瑞星公司）

从域名类型来看，瑞星信息技术有限公司监测发现2014年我国境内被植入后门的网站中，.com类域名最多，占61.32%，.edu类和.gov类网站，分别占12.91%和6.60%。2014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5-35所示。

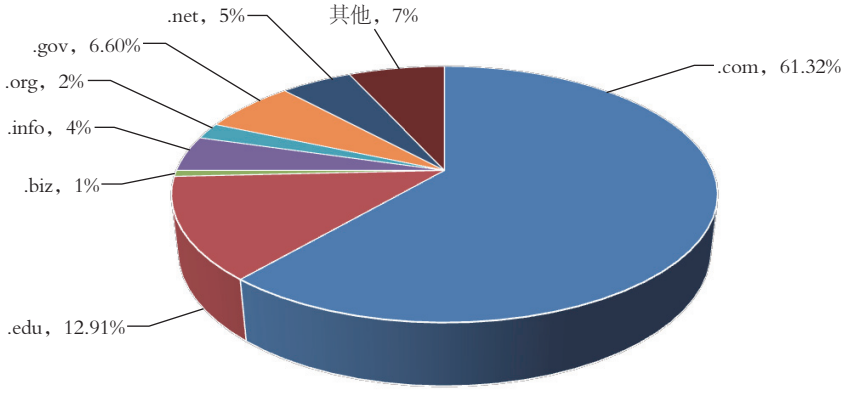


图5-35　2014年我国境内被植入后门网站数量按域名类型分布（来源：瑞星公司）

如图5-36所示，2014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：浙江省、广东省、北京市、江苏省、山东省、上海市、河南省、湖北省、河北省、天津市。

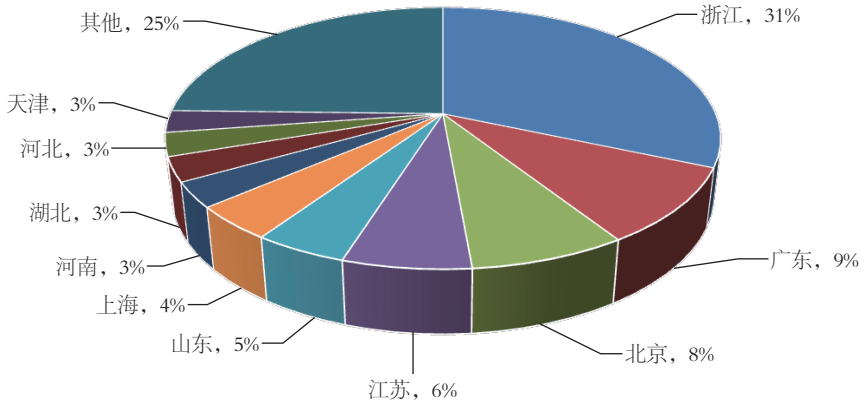


图5-36　2014年我国境内被植入后门网站数量按地区分布（来源：瑞星公司）

6 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安全防范工作的重中之重。

6.1 CNVD漏洞收录情况

2014年，CNVD收录新增漏洞9163个，包括高危漏洞2394个（占26.1%）、中危漏洞6032个（占65.8%）、低危漏洞737个（占8.1%）。各级别比例分布与月度数量统计如图6-1和图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8357个，可用于实施本地攻击的漏洞有806个。

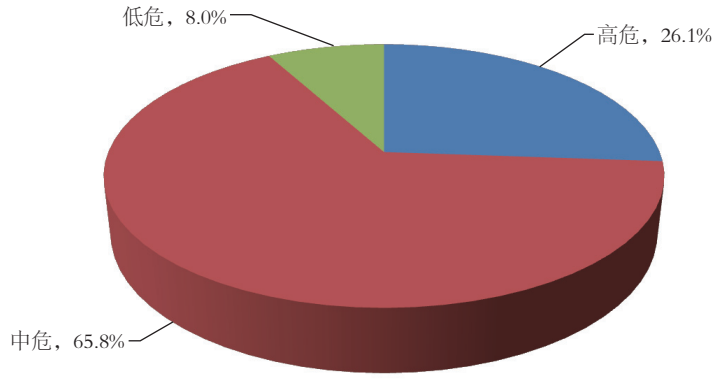


图6-1 2014年CNVD收录漏洞按威胁级别分布（来源：CNVD）

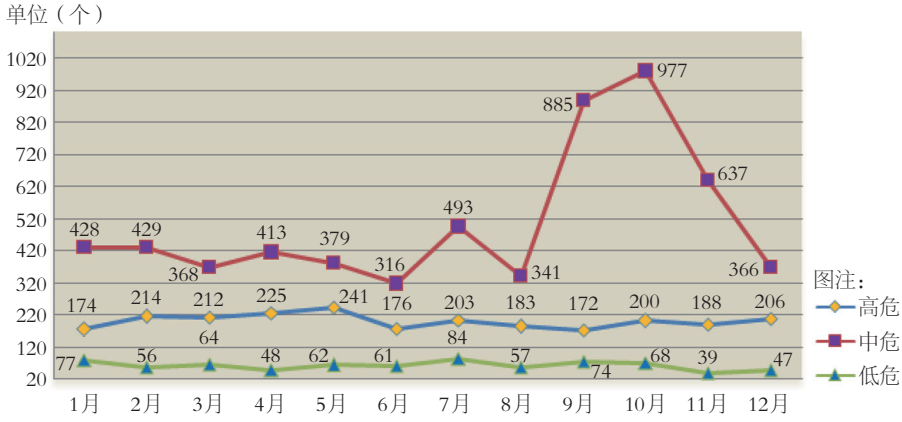


图6-2　2014年CNVD收录漏洞数量月度统计（来源：CNVD）

2014年，CNVD共收集整理了2394个高危漏洞，涵盖Microsoft、Adobe、IBM、Cisco、Google、WordPress、Oracle、Mozilla、Apple、IBM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Microsoft产品的高危漏洞最多，占全部高危漏洞的11.9%。

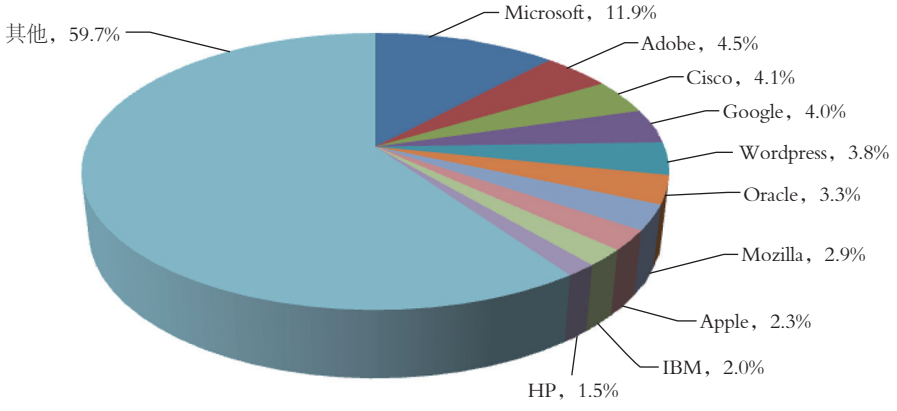


图6-3　2014年CNVD收录高危漏洞按厂商分布（来源：CNVD）

根据影响对象的类型，漏洞可分为：操作系统漏洞，应用程序漏洞，Web应用漏洞，数据库漏洞，网络设备漏洞（如路由器、交换机等），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 2014年度收集整理的漏洞信息中，操作系统漏洞占5.9%，应用程序漏洞占68.5%，Web应用漏洞占16.1%，数据库漏洞占1.8%，网络设备漏洞占6.0%，安全产品漏洞占1.7%。

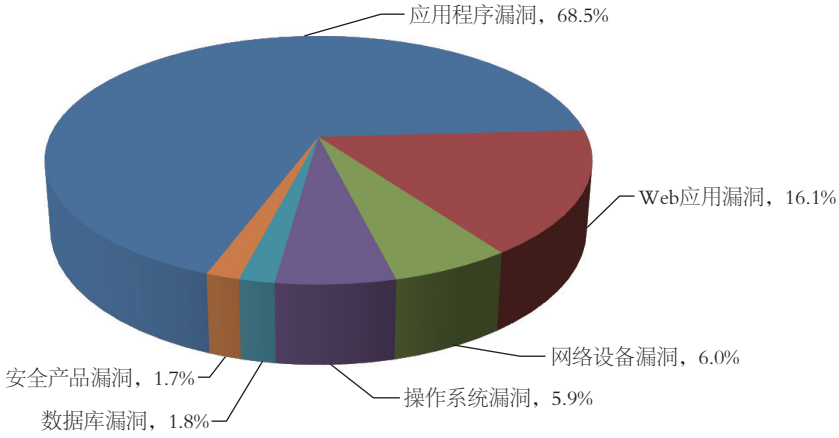


图6-4　2014年CNVD收录漏洞按影响对象类型分类统计（来源：CNVD）

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了较为全面的分析研判。2014年，CNVD 共进行了1337次验证，其中比较重要的包括TLS 1.2存在中间人攻击漏洞，BIND9存在远程拒绝服务漏洞，SSL V3 Protocol存在高危漏洞，Microsoft IE浏览器存在远程代码执行漏洞，Android存在APP FakeID签名漏洞，GNU BASH存在远程代码执行漏洞，Apache Struts 2存在补丁绕过漏洞，OpenSSL存在高危漏洞，Linksys路由器产品受 “the moon”蠕虫攻击及存在高危零日漏洞，美国凹凸科技公司（O2security）SSL-VPN设备存在多个高危漏洞，南京大汉网络CMS后台存在通用Fckeditor文件上传漏洞，深圳太极软件有限公司政府政务服务系统存在SQL注入和远程命令执行漏洞，MetInfo企业网站管理系统存在SQL注入漏洞，微泛协作办公平台存在远程代码执行漏洞，时光协同政务类网站存在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，就可能被利用来发动大规模网络攻击。2014 年 CNVD共收录了3266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。

2014年，CNVD 共收录漏洞补丁5927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。

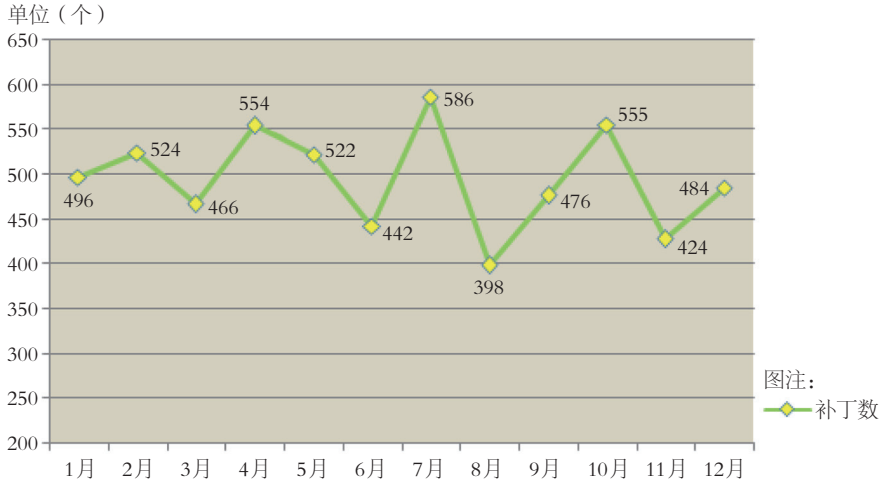


图6-5　2014年CNVD收录漏洞补丁数量按月统计（来源：CNVD）

6.2　高危漏洞典型案例

（1）TLS 1.2存在中间人攻击漏洞

2014年12月，CNVD收录了安全传输层协议TLS 1.2存在的一个中间人攻击漏洞（CNVD 编号：CNVD-2014-08824，对应CVE-2014-8730）。TLS（Transport Layer Security，安全传输层）协议用于在两个通信应用程序之间提供保密性和数据完整性。这种安全协议建立在SSL协议规范之上。

近期，TLS 1.2被披露存在一个中间人攻击漏洞，该漏洞与此前披露的SSL V3 “POODLE”（中文名：贵宾犬）漏洞攻击原理相同，漏洞产生的原因是TLS 1.2

未能正确校验PADDING，导致终止TLS 1.x CBC密码链接时，接收不正确的TLS PADDING，允许攻击者用中间人的攻击方法绕过传输层加密机制，窃取用户的敏感信息，例如Cookies信息、账号信息等。根据厂商自查结果，F5、A10等知名厂商网络设备受到漏洞影响。CNVD对该漏洞的技术评级为“中危”，但漏洞攻击威胁有可能存在于网络设备相邻网络区域（内部网络）内，对企业级用户造成广泛影响。

（2）BIND9存在远程拒绝服务漏洞

2014年12月，CNVD收录了域名解析系统软件BIND9存在的一个远程拒绝服务漏洞（CNVD 编号：CNVD-2014-08772，对应CVE-2014-8500）。BIND（Berkeley Internet Name Daemon）是由互联网软件系统联盟（ISC）负责维护的一款互联网上广泛应用的DNS域名解析系统软件。

漏洞原理利用显示，攻击者可通过恶意构造的DNS区域配置文件或者伪造服务器的方式，变更管理BIND9影响区域委派的相关配置，进而使其他BIND服务器跟随区域委派的配置进行无限制次数查询，导致消耗大量的内存或系统资源。如果攻击者可控制接受权威服务器遍历的委派配置，那么也会对权威服务器造成影响。

分析结果表明，所有的递归解析器都会受到漏洞影响，在部分攻击条件下权威服务器也会受到影响。CNVD对该漏洞的综合评级为“高危”。

（3）SSL V3 Protocol存在高危漏洞

2014年10月，CNVD收录了SSL V3协议存在的一个可导致信息泄露的高危漏洞（CNVD 编号：CNVD-2014-06718,对应CVE-2014-3566）。SSL V3是一项传输层安全协议，主要用于网站、邮件服务器等相关应用服务的网络安全传输。

近日，SSL V3协议被披露存在安全漏洞，攻击者可以利用此漏洞发起中间人欺骗攻击，当通信两端的用户主机均使用SSL V3进行安全传输时，可发起攻击窃取敏感信息。SSL V3协议最早启用于1996年，目前已被TLS 1.0、TLS 1.1、TLS 1.2等高级协议代替，同时由于兼容性原因，大多数的TLS协议实现兼容SSL V3。用户浏览器在与服务器端的TLS握手阶段进行版本协商时，首先提供其所支持协议的最新版本，若该握手失败，则尝试以较旧的协议版本协商，即降级协商。

研判结果显示，漏洞存在于SSL V3的CBC块加密漏洞，攻击者可成功破解SSL连

接的加密信息。进一步分析表明，攻击者很有可能会通过控制客户端和服务器之间的数据通信，使受影响版本浏览器与服务器端使用较新协议的协商建立失败，从而导致直接应用SSL V3的降级通信协商，达成攻击条件。此外，受漏洞影响的除了SSL V3本身外，还包括采用TLS 1.0和TLS 1.2等协议组件的客户端产品。CNVD对该漏洞的综合评级为“高危”。

（4）Microsoft Windows OLE组件存在远程代码执行高危漏洞

2014年10月15日，CNVD收录了最新披露的Windows OLE远程代码执行漏洞（CNVD 编号：CNVD-2014-06717,对应CVE-2014-4114）。OLE（对象链接与嵌入）是一种允许应用程序共享数据和功能的技术，用来增强Windows应用程序之间相互协作性。Microsoft Office文档也可以使用OLE对象。

Windows OLE组件功能中存在一个远程代码执行漏洞，漏洞产生的原因是某些特制的OLE对象可加载并执行远程INF文件。INF文件是Windows的安装信息文件，里面包含需要下载并安装的软件信息，攻击者可通过INF文件中设定的远程恶意可执行程序进行下载，通过操作注册表信息成功执行恶意文件。

进一步研究发现，通过构造一个特定的INF，让其修改Runonce注册表，重新启动即会加载同目录下的目标文件，造成远程任意代码执行。由于漏洞的基本攻击原理是触发右键菜单的默认关联项，因此，攻击者可以不局限于通过INF发起攻击，比如利用控制面板程序CPL或者其他可以右键操作执行的都可以发起攻击，更高级的攻击则可以实现无需重启实时高权限执行代码的功能。CNVD对该漏洞的综合评级为“高危”。

目前，互联网上披露的攻击分析一般是通过各种使用OLE组件的文档发起攻击。例如：通过PowerPoint文件，特别是.pps和.ppsx等可以自动播放的文件。用户打开攻击者精心构造的包含特定OLE 对象的文件，即可获得与当前登录用户相同的操作系统权限。根据国内外安全研究机构的分析和监测情况，该漏洞已经应用在互联网上一些APT攻击。攻击者可通过精心构造包含文件并诱使用户执行文件触发远程代码执行漏洞，进而控制用户操作系统主机。

（5）GNU BASH存在远程代码执行漏洞

2014年9月，CNVD收录了GNU BASH远程代码执行漏洞（CNVD 编号：

CNVD-2014-06345，对应CVE-2014-6271）。GNU BASH是一个命令语言解释器，能够从标准输入设备或文件读取、执行命令，结合了部分ksh和csh特点，同时也执行IEEEPOSIX Shell（IEEE Working Group 1003.2）规范，广泛运行于大多数类UNIX系统的操作系统之上，包括Linux与Mac OS X v10.4都将它作为默认Shell。

CNVD组织完成的多个测试实例表明，GNU BASH 4.3及其之前版本均存在远程命令执行漏洞，该漏洞起因于BASH的ENV指令，通过对BASH源代码进一步分析得出，ENV本身并不是任意指令执行，真正导致命令任意执行的原因是BASH没有对传入的参数进行正确的边界检查，导致数据和代码的混杂，产生了和PHPEVAL Code Injection类似的漏洞。从BASH变量解析文件中查看ENV中进行的临时环境变量设置，得出漏洞是由于initialize_shell_variables函数对外部发送的数据进行错误信任判断而执行代码所致，允许攻击者构造包含代码的值创建环境变量，执行任意代码。目前为止，发现通过HTTP请求CGI脚本是主要的攻击途径。CNVD对该漏洞的综合评级为“高危”。

研判结果，漏洞会影响目前主流的操作系统平台，包括但不限于Redhat、CentOS、Ubuntu、Debian、Fedora、Amazon Linux 、OS X 10.10等平台，由于抽样验证当前出厂预装的Andriod操作系统暂不支持ENV命令，因此，可推测针对Andriod操作系统受影响的可能性较小。该漏洞还可能会影响到使用ForceCommand功能的OpenSSH sshd，使用mod_cgi或mod_cgid的Apache服务器，DHCP客户端，其他使用BASH作为解释器的应用等。

（6）Android存在APP FakeID签名漏洞

根据BlueBox在2014年7月30日披露的公告称，Android 操作系统存在APP FakeID签名漏洞（CNVD 编号：CNVD-2014-04764 ，对应Google Bug 13678484）。攻击者可以利用漏洞开发恶意APP并绕过Android操作系统权限认证限制，发起后续攻击。

漏洞产生原因在于Android校验应用身份时采取的方式存在“单个证书充分条件”风险。PackageManger在安装APP软件（APK格式）时并不校验证书链上所有证书的合法性，只要存在被指定的签名（SIGN）能够校验APK中所有文件的合法性即可。Android操作系统使用getPackageInfo获取安装包证书时，如果获取到多个证书，只要有一个证书确保APK可信即可。

FakeID签名漏洞可导致恶意程序取得信赖应用的签名，绕过Android操作系统的安全验证机制，在高权限下甚至可以取得Android终端设备的控制权限。潜在的攻击场景包括：该漏洞可导致使用Webview组件的应用被恶意监控或隐私数据失窃；可能对Google Wallet类的支付应用产生威胁，如可获得NFC（近距离无线通信）设备的控制权限。CNVD对该漏洞的综合评级为“高危”。

（7）Apache Struts 2存在补丁绕过漏洞

2014年3月，CNVD收录了Apache Struts 2存在的拒绝服务和ClassLoader安全绕过漏洞（CNVD编号：CNVD-2014-01552，对应CVE-2014-0050和CVE-2014-0094），官方同步提供了Apache Struts 2.3.16.1作为升级版本。2014年4月23日晚，安全人员研究发现其提供的升级版本并未完全修复漏洞，相关安全机制可被绕过，对互联网上应用Apache Struts 2的大量服务器构成拒绝服务和远程控制威胁。

根据分析，Apache Struts 2.0.0-2.3.16版本的默认上传机制是基于Commons FileUpload 1.3版本，其附加的ParametersInterceptor允许访问“class”参数（该参数直接映射到getClass()方法），并允许控制ClassLoader。在具体的Web容器部署环境下（如Tomcat），攻击者利用Web容器下的Java Class对象及其属性参数（如日志存储参数），可向服务器发起远程代码执行攻击，进而植入网站后门，控制网站服务器主机。

目前，已经验证的测试案例表明，Tomcat服务器易被发起拒绝服务或远程渗透攻击，同时CNVD认为ClassLoader安全绕过漏洞可进一步涉及部署其他Web容器的网站服务器。CNVD对该漏洞的综合评级为“高危”。

研判结果，由于黑客的攻击代码可根据部署环境以及调用参数的不同而变化出多种形式，不排除目前防护措施未来存在被绕过的可能。建议相关用户对于Web服务器，一方面要积极采用应用层过滤的防护措施，另一方面也要及时关注Apache Struts 2官方发布的最新漏洞补丁信息。CNVD将持续监测后续攻击情况，包括利用代码变种以及网站后门植入攻击等。

（8）OpenSSL存在高危漏洞

2014年4月8日，国家信息安全漏洞共享平台CNVD收录了OpenSSL存在的一个内存泄露高危漏洞（CNVD编号：CNVD-2014-02175，对应CVE-2014-0160）。OpenSSL

是由一款开放源码的SSL实现，用来实现网络通信的高强度加密。该漏洞与OpenSSL TLS/DTLS传输层安全协议HeartBeat（心跳部分）扩展组件（RFC6520）相关，因此漏洞又被称为“HeartBleed Bug”（中文名称：“心血”漏洞）。CNVD测试结果表明，该漏洞无需任何特权信息或身份验证，就可以获得X.509证书的私钥、用户名与密码、Cookies等信息，进一步可直接从服务提供商和用户通信中窃取聊天工具消息、电子邮件以及重要的商业文档和通信等私密数据。CNVD对该漏洞的综合评级为“高危”。

2014年4月9日，CNVD对OpenSSL存在的一个内存信息泄露高危漏洞结果进行分析，该漏洞存在于ssl/dl_both.c文件的心跳部分。由于OpenSSL应用极为广泛，包括政府、高校网站以及金融证券、电子商务、网上支付、即时聊天、办公系统、邮件系统等诸多服务提供商均受到漏洞影响，直接危及互联网用户财产和个人信息安全。当攻击者向服务器发送一个特殊构造的数据包，可导致内存存储多达64kB字节的数据输出。

CNVD组织完成的多个测试实例表明，根据对应OpenSSL服务器承载业务类型，攻击者一般可获得用户X.509证书私钥、实时连接的用户账号和密码、会话Cookies等敏感信息，进一步可直接取得相关用户权限，窃取私密数据或执行非授权操作。研判结果，受该漏洞影响的产品包括OpenSSL 1.0.1-1.0.1f版本，其余版本暂不受影响。综合各方测试结果，国内外一些大型互联网企业的相关VPN、邮件服务、即时聊天、网络支付、电子商务、权限认证等服务器受到漏洞影响，此外一些政府和高校网站服务器也受到影响。

此外，抽样检测数据显示，国内网站有2.3万个（占其抽样的1.5%）和1.1万个（占其抽样的1.0%）服务器主机受到影响。目前互联网上已经出现了针对该漏洞的攻击利用代码，预计在近期针对该漏洞的攻击将呈现激增趋势，对网站服务提供商以及用户造成的危害将会进一步扩大。

（9）Linksys路由器产品受 “the moon”蠕虫攻击及高危漏洞

2014年3月，CNVD联合上海交通大学网络信息中心对Linksys多款路由器产品受到漏洞和“the moon”蠕虫攻击威胁的情况进行了分析和监测，获知互联网上有近2.5万个IP地址对应的路由器设备受到攻击威胁，其中中国境内用户有近600个设备IP地址，对企业和用户上网安全构成较大的威胁。

Linksys是知名路由器品牌，2013年以前归属思科公司（Cisco），现该品牌归属贝尔金公司（Belkin）。2014年2月16日，Linksys多款路由器产品被披露存在一个安全绕过高危漏洞（CNVD编号：CNVD-2014-01260），由于产品未能对tmUnblock.cgi、hndUnblock.cgi等CGI页面以及后台服务的访问权限进行限制，攻击者可利用漏洞执行特定指令，取得路由器设备的控制权，继而可发起DNS劫持、网络钓鱼等攻击，对用户个人信息安全构成威胁。

2014年2月中旬，国外研究者发现一种名为“the moon”蠕虫正在发起对Linksys路由器的攻击。该蠕虫利用的是Linksys相关CGI页面的漏洞，对暴露在互联网上的Linksys路由器80或8080端口开展扫描，利用漏洞从黑客控制的服务器下载恶意程序至路由器设备，完成对路由器的远程控制。进一步分析，该蠕虫还会使用SSL协议进行远程控制，并对其他的恶意攻击采取排他措施。

CNVD对漏洞的综合评级为“高危”。根据国外研究者的分析结果，受漏洞和“the moon”蠕虫影响的Linksys路由器产品不仅包括LinksysE系列的E4200、E3200、E3000、E2500、E2100L、E2000、E1550、E1500、E1200、E1000、E900和E300，还包括其他系列的WAG320N、WAP300N、WAP610N、WES610N、WET610N、WRT610N、WRT600N、WRT400N、WRT320N、WRT160N和WRT150N。上述版本产品在企业及个人用户中应用较为广泛。

根据CNVD和上海交通大学网络信息中心的联合监测结果，截至2014年3月13日，共检测发现互联网上有近2.5个IP地址对应上述Linksys路由器设备，位于美国、加拿大和中国的IP地址数量排名前三。建议广大用户参考上述步骤进行加固，并随时关注厂商主页以获取最新版本或补丁信息。同时，CNVD建议国内路由器厂商排查本公司产品，如产品与上述Linksys产品代码同源，需及时做好用户的安全响应工作。CNVD将持续跟踪漏洞处置情况。

（10）美国凹凸科技公司SSL-VPN设备存在多个高危漏洞

2013年6月和2014年1月，CNVD分析了凹凸科技公司以PHP为开发语言的部分SSL-VPN设备存在的文件包含、远程代码执行、调试后门默认口令、信息泄露等漏洞（CNVD 编号：CNVD-2013-06510、CNVD-2014-00666）。凹凸科技公司是美

国知名网络设备生产商。VPN设备主要用于建立从互联网直接访问内部网络的连接。近期，CNCERT/CC主办的CNVD对美国凹凸科技公司生产的SSL-VPN设备进行分析，确认其存在多个高危漏洞。利用漏洞可远程控制VPN设备，进而窃取内部网络的敏感信息。CNVD测试发现漏洞还影响到多家国内网络设备厂商的代码同源产品，有数十家国内政府、高校和重要部门用户受到漏洞威胁。CNVD对上述漏洞的综合评级为“高危”。

此外，测试发现多家国内设备厂商生产的SSL-VPN设备采用了与凹凸科技公司SSL-VPN设备代码同源的软件系统，同样会受到漏洞的影响。目前，CNVD尚未能通过技术测试明确受漏洞影响的设备具体型号和版本。

6.3 CNVD行业漏洞库

2013年7月，CNVD对现有漏洞进行了进一步的深化建设，建立起基于重点行业的子漏洞库，目前涉及的行业包含：电信、移动互联网、工业控制系统和电子政务。面向重点行业客户包括：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进行匹配。2014年行业漏洞库资产总数为：电信733类，移动互联网1631类，工控系统142类，电子政务173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12个。

CNVD共收录电信行业漏洞4078个，移动互联网行业漏洞2516个，工控行业漏洞714个，电子政务漏洞971个。其中，近3年各行业漏洞统计数如图6-6所示，2014年由于Android系统的证书验证绕过漏洞，导致Android平台近千个APP存在衍生漏洞，导致移动互联网行业漏洞的大幅增长。

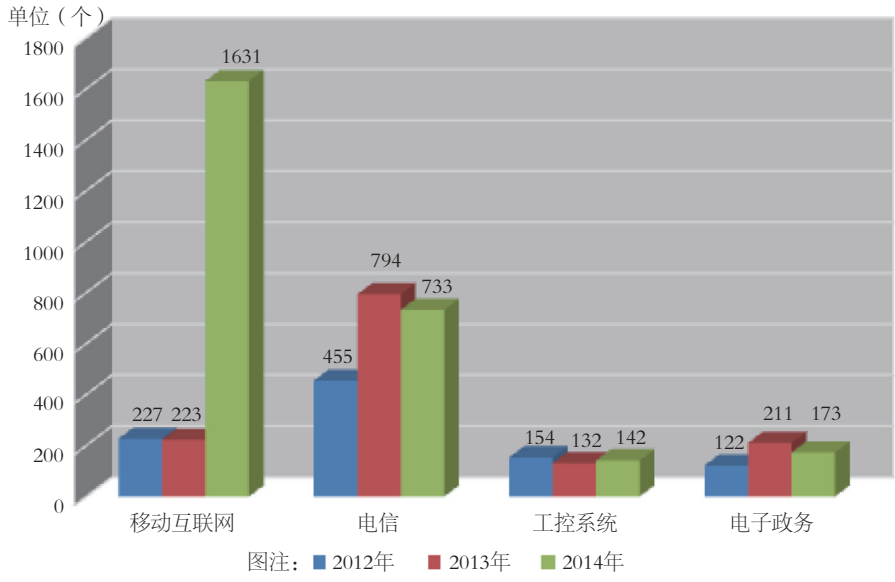


图6-6　2012-2014年CNVD收录行业漏洞对比（来源：CNVD）

移动互联网行业漏洞最为相关的厂商包括：Apple、Adobe、Google、BlackBerry、Samsung。厂商分布如图6-7所示。

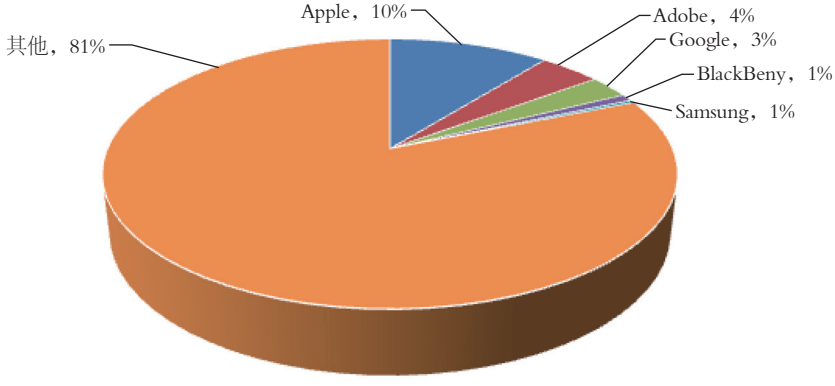


图6-7　2012-2014年CNVD移动互联网行业漏洞厂商分布（来源：CNVD）

工控行业漏洞最为相关的厂商包括：Siemens、Advantech、Schneider Electric、Rockwell Automation、Invensys。厂商分布如图6-8所示。

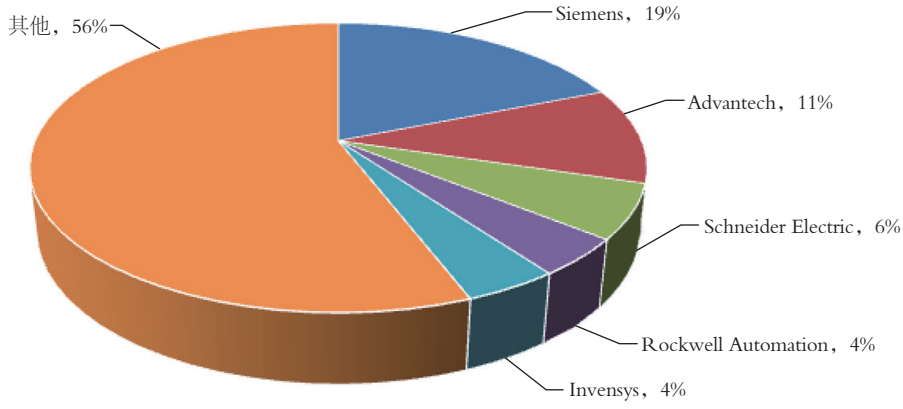


图6-8　2012-2014年CNVD工控行业漏洞厂商分布（来源：CNVD）

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。

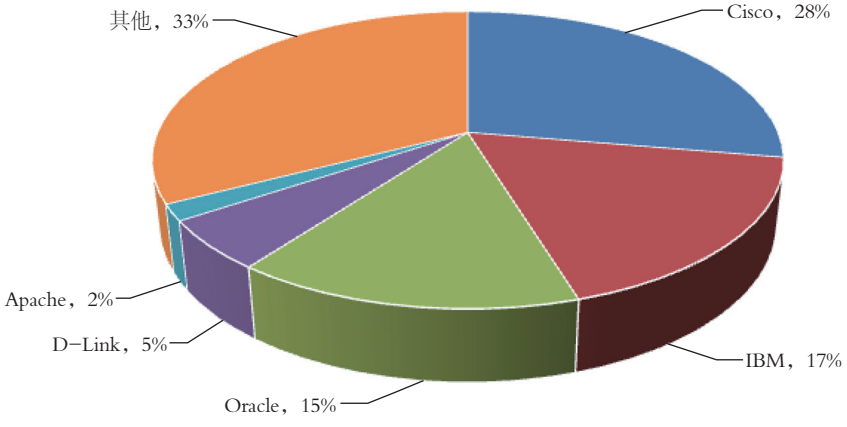


图6-9　2012-2014年CNVD电信行业漏洞厂商分布（来源：CNVD）

电子政务行业漏洞最为相关的厂商包括：Phpmyadmin、Phpcms、DedeCMS、Aspcms、 eYou。厂商分布如图6-10所示。

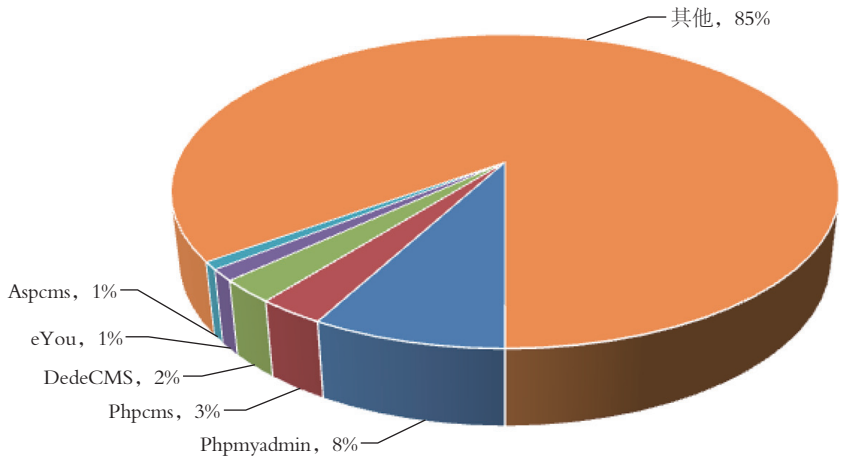


图6-10　2012-2014年CNVD电子政务行业漏洞厂商分布（来源：CNVD）

2014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 APP FakeID签名漏洞（CNVD编号：CNVD-2014-04764）和Google Android API WebView组件远程代码执行漏洞（CNVD编号：CNVD-2014-06698）。

（1）Android是基于Linux开放性内核的操作系统。攻击者利用漏洞开发恶意APP并绕过Android操作系统权限认证限制，发起恶意攻击。

（2）Google Android API WebView组件存在远程代码执行漏洞，由于Google Android在Android/Webkit/AccessibilityInjector.java的实现上存在安全漏洞，一旦Android设备开启了“accessibility”或“accessibilityTraversal”服务，攻击者可利用此漏洞在应用上下文中执行任意代码。

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远程命令执行漏洞（CNVD编号：CNVD-2014-01475），多个TP-Link路由器输入验证漏洞（CNVD编号：CNVD-2014-05708）。

（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 DIR-100 Ethernet Broadband Router存在命令执行漏洞，远程攻击者可利用漏洞提交请求，无需验证即可执行特权命令。

（2）多个TP-Link路由器存在请求伪造，跨站脚本和HTML注入漏洞。由于未能充分过滤用户提供的输入，攻击者可以利用此漏洞来执行某些未经授权操作，在受影响站点上下文不知情用户浏览器中执行任意脚本或HTML代码或者窃取基于Cookie的认证证书。

影响电子政务行业的重大漏洞包括：WebCarrier WCM远程调用接口对外开放漏洞（CNVD编号：CNVD-2014-08747），AnyMacro Mail安宁邮件系统SQL注入漏洞（CNVD编号：CNVD-2014-02528），Apache Struts ClassLoader操作安全绕过漏洞（CNVD编号：CNVD-2014-01552）。

（1）时光网站内容管理系统（WebCarrier WCM）是一套针对大中型企业、政府与组织而开发的基于设施类门户管理产品。WebCarrier WCM内容管理系统存在远程调用接口对外开放漏洞，允许攻击者通过此接口查询、修改数据，上传文件等，进而获得系统管理员账号、密码信息，或者执行SQL语句，导致网站挂马、网站数据库存储内容泄露或者被篡改以及网站服务器被控制等。

（2）AnyMacro是一家企业级邮箱系统，客户主要为教育、政府机构。AnyMacro Mail安宁邮件系统存在SQL注入漏洞。由于“share.php”未进行授权检查，可以进行任意访问，同时其中的F_email参数未能进行有效过滤，导致SQL注入，允许攻击者获取所有邮箱的账号以及密码和执行恶意行为的PHP代码。

（3）Struts 2是第二代基于Model-View-Controller (MVC)模型的Java企业级Web应用框架。Apache Struts存在一个安全绕过漏洞，由于ParametersInterceptor允许访问直接映射到getClass()方法的“class”参数，导致攻击者利用漏洞，通过请求参数未授权操作ClassLoader。

6.4 CNVD漏洞处置情况

2014年，CNVD协助CNCERT/CC处置漏洞1337次，涉及国内外软件厂商433家，联系次数最多的厂商见表6-1。

表6-1　2014年协调软件厂商处置漏洞情况（来源：CNVD）

厂商	漏洞数（个）
民航系统单位	51
万户网络技术有限公司	15
江南科友科技股份有限公司	12
山东浪潮齐鲁软件股份产业有限公司	11
南京大汉网络有限公司	7

其中，江南科友科技股份有限公司、山东浪潮齐鲁软件股份产业有限公司、万户网络技术有限公司、正方软件股份有限公司、北京春笛网络信息技术服务有限公司、江南科友科技股份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。有部分厂商未给予配合，如北京天生创想信息技术有限公司、北京富基融通科技有限公司等。

此外，CNVD合作伙伴上海交通大学、赛尔网络有限公司也配合CNVD进行漏洞检测和协调处置。其中上海交通大学验证漏洞358次，主要包括：多所高校CMS系统存在多处SQL注入漏洞，哈尔滨新中新电子股份有限公司金龙卡金融化一卡通校园卡查询系统任意文件上传漏洞，正方软件高校迎新系统远程命令执行漏洞，中央广播电视大学现代远程教育资源中心学习系统SQL注入漏洞，浙江浙大万朋软件有限公司ZDSOFT教育信息发布系统文件包含漏洞。赛尔网络有限公司协助处置漏洞2678次，主要事件包括：中国人民大学心理学系网存在SQL注入漏洞，中航大学培训管理系统存在命令执行漏洞，首都师范大学国际文化学院留学网站存在SQL注入漏洞，北京大学数学科学学院网站后台存在弱口令漏洞，多所大学网站存在SQL注入漏洞等。

7 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

2014年，CNCERT/CC共接收境内外报告的网络安全事件56180起，较2013年增长了77.5%。其中，境内报告的网络安全事件55302起，较2013年增长了80.2%，境外报告的网络安全事件数量为878起，较2013年下降了9.6%。2014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。

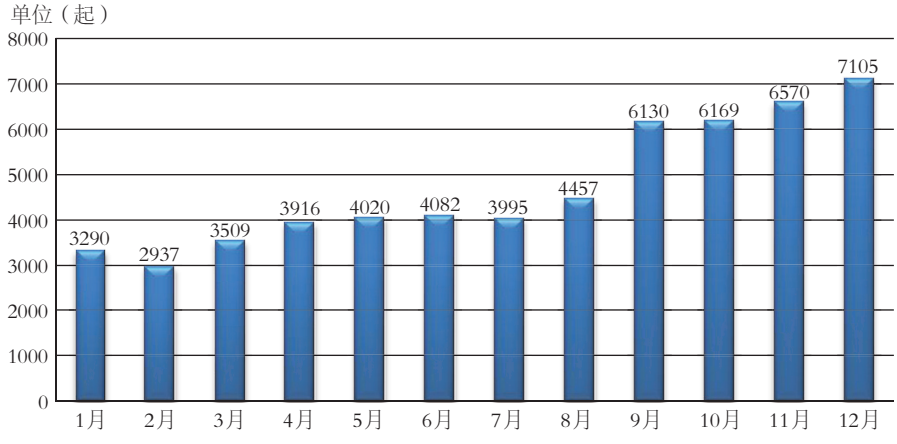


图7-1 2014年CNCERT/CC网络安全事件接收数量月度统计（来源：CNCERT/CC）

2014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。事件类型主要包括漏洞、网页仿冒、网页篡改、恶意程序、网站后门、网页挂马、拒绝服务攻击等，具体分布如图7-2所示。

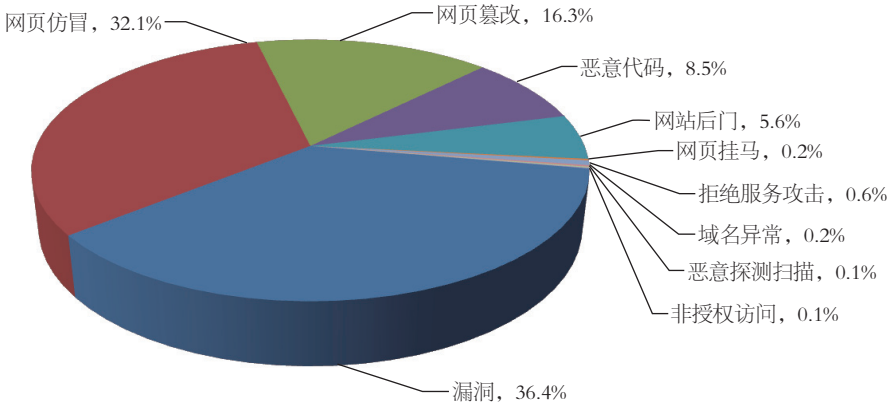


图7-2　2014年CNCERT/CC接收到网络安全事件按类型分布（来源：CNCERT/CC）

2014年，CNCERT/CC接收的网络安全事件数量排前3位的依次是漏洞、网页仿冒和网页篡改，与2013年相同。具体情况如下。

漏洞事件数量为20311起，较2013年的10936起增加了85.7%，占所有接收事件的比例为36.4%，位居首位。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2013年继续保持增长态势。

网页仿冒事件为17873起，占所有接收事件的比例为32.1%，位居第二。原因是随着电子商务和在线支付的普及与发展，人们使用互联网进行在线经济活动越来越频繁，网页仿冒事件虽排名第二，但其数量较2013年的10578起增加了69.0%，继续保持增长态势。

网页篡改事件数量为9074起，较2013年的4552起增加了99.3%，超过恶意程序事件数量，位居第三，占所有接收事件的比例为16.3%。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，从而牟取非法经济利益；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自主监测发现的事件中危害大、影响范围广的事件，CNCERT/CC积极进行协调处理，以消除其威胁。2014年，CNCERT/CC共成功处理各类网络安全事件56072起，较2013年的31180起增长79.8%。2014年CNCERT/CC网络安全事件处置数量的月度统计如图7-3所示。针对互联网尤其是移动互联网恶意程序日益猖獗的发展趋势，CNCERT/CC全年共开展了12次木马和僵尸网络，11次移动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，基础电信企业和域名注册服务机构的积极配合有效提高了事件处置的效率。

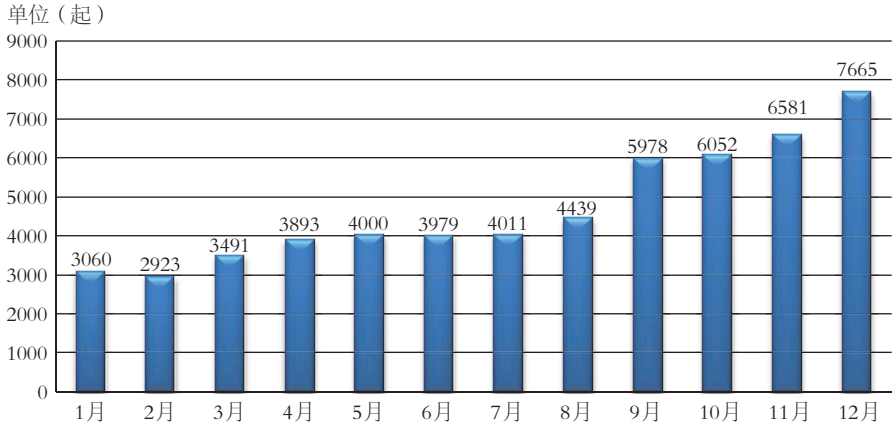


图7-3 2014年CNCERT/CC网络安全事件处置数量月度统计（来源：CNCERT/CC）

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20247起，占36.1%，主要来源于CNVD收录并处理的漏洞事件。

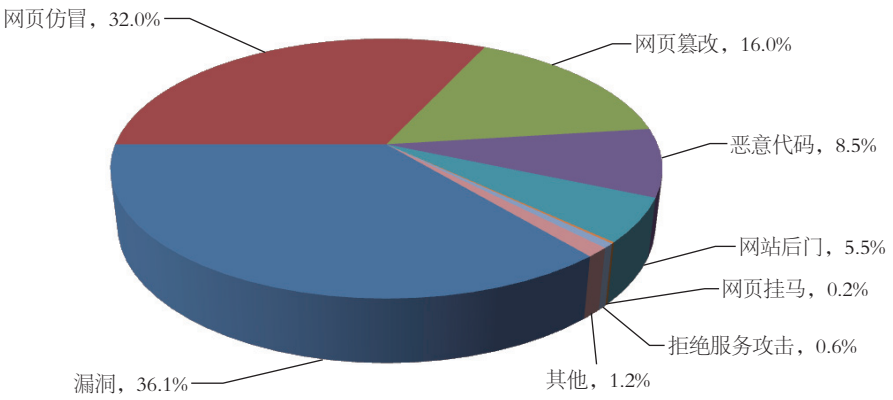


图7-4　2014年CNCERT/CC处理的网络安全事件按类型分布（来源：CNCERT/CC）

网页仿冒事件处置数量排名第二，全年共处置17926起，占32.0%，较2013年的10211起大幅增长了75.6%。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12312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、中国邮政储蓄银行、淘宝等境内著名金融机构和大型电子商务网站，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，进而窃取钱财。同时，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，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，有效避免了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。2014年，CNCERT/CC处理网页篡改类事件8989起，占16.0%，较2013年的4551起增长了97.5%。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形象、威胁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2014年CNCERT/CC事件处理工作的重点。

2014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及各地分中心积极组织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12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744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所用IP地址及域名767个，成功切断黑客对近98.3万台感染主机的控制。在移动互联网方面，下架8644个恶意APP程序，处置103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210条恶意程序控制URL链接。

常态治理工作方面，2014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4749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4.3万个。

2014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取得良好效果，我国境内感染木马僵尸网络主机数量已连续两年下降，公共互联网安全环境持续好转。

7.3 事件处理典型案例

（1）处置攻击冬奥会网站事件

2014年1月27日，CNCERT接到投诉称中国一台IP地址为211.139.119.218的主机攻击索契冬奥会官方网站，此时正值冬奥会开幕前夕，国际影响十分恶劣。CNCERT接到投诉后启动紧急处置流程，协调江苏分中心将此主机进行断网，并到现场进行取证，分析事件原因。经过取证分析，发现黑客于2014年1月10日凌晨通过

多个跳板主机扫描IP地址为211.139.119.218的SSH登录密码并成功破解。1月27日左右黑客登录该主机，从立陶宛IP地址为31.170.160.74的主机上下载anca.tgz文件后对外实施攻击。CNCERT第一时间将处置情况和分析结果反馈给投诉方，该事件进一步证明了我国是网络攻击的严重受害国，许多我国境内主机被境外控制，并作为跳板机对外发起网络攻击。

（2）协调处置手机刷机病毒“手机预装马”

2014年2月CNCERT/CC接到网民投诉，称其在电商“1号店”购买的联想A820T手机中存在预装的手机病毒。CNCERT/CC在收到投诉后，立即进行取证调查和分析。通过取证分析，CNCERT/CC发现该手机中存在一例伪装成安卓系统服务“SystemScan”的应用程序，该应用程序在用户不知情的情况下通过后台窃取用户手机号码、IMEI号、IMSI号、用户联网IP地址、用户手机当前位置信息、用户手机上所有已安装的应用程序信息以及当前系统运行任务信息等，并将窃取到的用户信息进行压缩后上传到远端服务器。同时，CNCERT/CC还发现在“1号店”所购联想A820T手机所预装的应用程序与正版联想A820T手机中预装的应用程序并不一致。依据通信行业标准，CNCERT/CC判定该应用程序属于“信息窃取”类恶意程序，并将该恶意代码家族的中文名称命名为“手机预装马”。

正版联想A820T手机中并未预装名为“SystemScan”的手机预装马，因此手机预装马系手机出厂后通过二次刷机方式植入手机。通过对该手机预装马进行持续监测，截至2014年1月CNCERT/CC发现全国范围内感染该手机预装马的用户数达216.7万个。CNCERT/CC协调相关单位对“手机预装马”所使用的控制域名进行停止解析处理，对控制服务器进行停止接入处理。

本次“手机预装马”的广泛传播表明，以刷机、手机ROM制作等为代表的移动互联网源头环节已被严重“污染”，直接破坏移动互联网的生态健康，严重危及移动互联网生态下游用户的切身利益。大多数手机安全软件都是基于“黑名单”机制查杀移动恶意程序，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，因此经CNCERT/CC测试发现当时多数手机安全软件无法识别“手机预装马”，这也是造成“手机预装马”泛滥的一个重要原因。

（3）协助分析并破获我国某重要新闻网站遭受攻击事件

2014年6月8日，我国某重要新闻网站遭受大规模拒绝服务攻击，峰值攻击流量达到1.6Gbit/s，导致该网站无法正常访问。我中心及时对事件进行分析，确定了攻击类型、主要攻击源地址，并进一步追溯到黑客使用的控制端地址、域名，以及黑客使用的QQ号码等信息，根据我中心提供线索，公安部门在山东抓获了犯罪嫌疑人。

（4）联合通信行业及时有效处置“××神器”事件

2014年8月2日凌晨开始，一则短信在国内爆炸式传播，这条短信上包含机主姓名和一个网址链接。一旦机主点击短信中的链接，下载安装对应的安卓程序文件，就会感染一个名为“××神器”的手机病毒。病毒会读取用户通讯录，向全部联系人发送这条传播病毒的短信。短信中还有机主的姓名，具有很强的欺骗性，大量用户点击并安装恶意APP，造成病毒迅速传播蔓延。

经过分析，该病毒主要有以下四大危害。第一，以钓鱼的方式收集用户个人信息。该病毒在安装后有一个登录注册页面，如果用户填写了自己的身份证号和姓名，这些个人信息就将被病毒窃取。第二，回传用户信息。该病毒会将用户手机中存储的短信等信息打包后回传到黑客的控制端。第三，拦截并回传敏感短信。病毒会识别哪些短信可能是淘宝等金融购物类网站发送的验证码、支付密码等敏感短信，并将此类短信拦截后回传。第四，接收控制指令。病毒可以接收黑客发送的控制指令，根据指令控制用户手机的各项功能。

面对该病毒的迅速蔓延之势，CNCERT/CC做出了应急响应与及时处置。2014年8月2日9:00，CNCERT/CC接到多家单位举报该病毒，随即启动应急响应机制，于10:00时完成对该病毒的初步分析。根据分析结果，11:00通知三大运营商对短信和URL链接进行封堵，11:30通知恶意链接的域名解析商协助删除该恶意链接，防止已经接到短信的用户继续点击下载病毒。14:00左右，CNCERT/CC进一步分析该病毒后得到两个控制端手机号码，该手机号码为湖南联通号码，CNCERT/CC立即将控制端手机号码下发湖南分中心处理，经查发现该手机用户当时漫游在深圳；于是又联系广东分中心处理并将相关线索提交公安部门，协助公安部门破案。经过一系列处置，8月2日下午短信传播量明显下降。

（5）协调处置“OpHongKong”对我国政府网站攻击事件

2014年10月初黑客组织为支持中国香港“占领中环”运动，发起针对中国内地和中国香港网站的“OpHongKong”攻击行动。10月6日，黑客组织开始对政府网站进行攻击，并于10月9日、12日发布了两批被攻击网站列表。CNCERT/CC立即协调各地分中心对被攻击网站进行协调处置，共协调处置被攻击网站13个，协助被攻击网站进行整改，及时恢复被攻击网站的正常业务。同时CNCERT/CC根据黑客攻击特征，从中提取出监测特征，并梳理了存在相似后门的110家政府网站。CNCERT/CC联合全国15个分中心对其中52家重点网站进行处置，避免后续隐患。黑客组织10月14日又发布消息，声称18日拟对我境内的政府网站展开大规模攻击，CNCERT/CC得到了黑客组织拟攻击的155个网站列表，并联合17个分中心向其中重点的76个网站发出了预警，并时刻监测黑客攻击情况。10月18日CNCERT/CC未监测发现大规模攻击事件。在该事件处置过程中， CNCERT/CC还与中国香港HKCERT多次共享了发现的被篡改网站信息，黑客的活动情况以及双方CERT的处置办法，紧密的双边合作有效地保障了我国政府网站的安全，避免因大规模网络攻击而引发社会事件。

（6）协调处置菲律宾“匿名者”组织篡改境内网站事件

2014年5月20日，我国境内大量网站被菲律宾匿名者组织篡改，其中包括153个政府网站和41个商业网站。5月21日上午，CNCERT/CC验证发现大量篡改页面仍然存活，立即组织各地分中心进行处置。截至5月22日中午，全国27个分中心共处置125个被篡改网站，CNCERT/CC验证后被篡改页面已经全部不存活，有效地保护了政府网站的形象。

（7）协调处置多起NTP反射和放大跨境攻击事件

2014年，CNCERT/CC监测到我国公共互联网上发生多起NTP反射放大攻击事件，攻击流量逐步增大，且有进一步扩大蔓延的趋势。同时CNCERT/CC收到多家境外国家级CERT、安全组织关于此类安全事件的投诉。中国电信报告，网内此类攻击事件流量高达300GB。

NTP是网络时间协议的简称，攻击主机可伪造受害主机的IP地址，向网上的NTP服务器发送请求，NTP服务器向受害主机返回大量的数据包从而造成其网络拥塞，达到攻击目的，其反射放大效果可达200倍。这是一种典型的分布式反射拒绝服务

（DRDoS）攻击方式。

经CNCERT/CC监测数据初步分析，互联网上开放UDP 123端口的服务器约有80万台。其中，频繁被请求的服务器约为1800台，粗略计算，若1800台NTP服务器每台均收到1MB的请求流量，总共会反射发出360GB的攻击流量。在监测发现的被请求次数最多的前50个NTP服务器，其IP地址主要位于美国（56%）和中国（26%）。

据中国电信报告，国内互联网存在大量来自境外的利用NTP等服务进行DRDoS攻击的行为，在此情况下，中国电信检查了所有核心路由器的NTP配置，并发现有部分接入侧路由器已受到过NTP DRDoS攻击，并在国际出入口和互联互通层面对NTP流量进行整体调控，效果明显。

目前，基础电信运营企业对此尚无法做到完全有效控制。建议各单位进一步加强安全威胁防范：尽快将受影响的NTP服务器程序升级到4.2.7版本及以上；加强异常流量监测，对NTP流量过大的自有系统服务器进行NTP访问控制，或限制NTP服务器的流出流量；各基础电信企业在国际出入口和互联互通层面对NTP流量进行监测和调控，降低来自国外大规模NTP DRDoS攻击的可能性，在全网范围内切实认真组织实施源地址验证，建设完善流监测技术手段，增强对DRDoS攻击的监测发现和分析能力。

CNCERT/CC对此类NTP DRDoS攻击行为进行了有针对性的监测和通报，会同相关单位防范和处置利用NTP等服务进行DRDoS攻击的黑客行为，共处置NTP放大攻击事件37起，涉及IP地址1975个。

（8）协调处置某省重点新闻网站被劫持事件

2014年9月3日晚，CNCERT/CC接到某省重点新闻网站投诉，称其在新网数码注册的域名被劫持到境外地址，访问网站会显示博彩等违法信息。此网站为该省政府官方新闻网站，该事件极大地影响了政府部门形象。CNCERT/CC立即联系新网数码处置该事件，新网数码立即恢复了该网站的正常解析，并添加域名注册商锁定（用户权限无法修改域名解析）。但该域名9月5日再次被劫持到境外地址，CNCERT/CC根据新网数码提供的日志分析推断，该域名为黑客利用新网数码域名解析服务相关漏洞进行篡改。因此CNCERT/CC要求新网数码检查相关服务器漏洞，并向CNNIC申请为该域名提供域名注册局锁定服务。在CNCERT/CC协调下，9月5日晚该域名完成CNNIC注册局锁

定，锁定后该域名解析已无法通过注册商系统进行更改。后续新网数码发现黑客利用其业务服务器为跳板攻击了其域名解析系统，恶意修改了该网站域名解析记录，新网数码立即对相关漏洞进行了修补和整改。该事件反映出我国域名注册解析服务提供商系统存在的安全隐患仍然较为严重，CNCERT/CC联合CNNIC与新网数码的快速响应和协调处置保障了重要新闻网站域名的安全，避免了因为网络安全事件而引发社会事件。

（9）协调处置境内受OpenSSL漏洞影响的重要用户网站或邮件服务器

2014年4月8日，开源加密协议OpenSSL被曝光存在内存泄露高危漏洞，该协议被网站和邮件服务器广泛使用，利用该漏洞可以获取密钥、用户账号和密码等敏感信息。CNCERT/CC监测发现，我国境内受此漏洞影响的IP地址超过3万个，大量重要单位的网站和邮件服务器都受到影响，其中政府网站或邮件服务器77个，电信企业网站或邮件服务器8个，金融电力企业网站或邮件服务器16个，高校科研机构网站或邮件服务器199个，媒体网站或邮件服务器3个。为第一时间消除安全隐患，CNCERT/CC对受该漏洞影响的网站或邮件服务器的用户单位全部进行了通报，并指导其进行修复，该漏洞在国内未造成重大安全隐患。

（10）协调处置海康威视公司网络摄像头相关网络安全事件

2014年2月和11月，CNCERT/CC接到日本JPCERT投诉，称杭州海康威视数字技术股份有限公司（以下简称“海康威视公司”）所生产的网络摄像头存在漏洞，很有可能受到恶意程序的感染，成为了僵尸网络的一部分。海康威视公司是中国安防产品和行业解决方案提供商，其网络摄像头等产品的营销和服务覆盖全球。CNCERT/CC验证后，请浙江分中心联系海康威视公司协调处置。海康威视公司积极响应，及时升级库存产品的固件，在官网上发布中英文防范公告，提供升级程序下载，并要求经销商加大处理力度。

2014年9月和11月，CNCERT/CC接到海康威视公司投诉，称其网络摄像头设备被植入恶意程序，可能发起拒绝服务攻击。经CNCERT/CC分析和验证，该恶意程序与美国、瑞典和荷兰的IP地址存在通信连接。CNCERT/CC立即联系了美国、瑞典和荷兰的国家级CERT协调处置位于上述国家的恶意程序下载链接。

（11）协调处置多起境外组织投诉境内厂商产品漏洞事件

2014年1月14日，CNCERT/CC接到美国计算机紧急事件响应小组协调中心

（CERT/CC）投诉中兴 F460/F660 电缆调制解调器存在web_shell_cmd.gch非授权后门。其称该后门已经广为人知，互联网上已出现后门威胁分析以及临时删除后门的处置措施。CNCERT/CC收到后立即对事件进行分析，确认CERT/CC所述漏洞为互联网已披露情况且在CNVD中收录。CNVD向中兴通讯通报了互联网用户以及安全组织关切的情况。中兴提供了反馈报告，称该风险在新版设备中已经修复，并早已通过售后渠道发布安全公告，后续中公司将着手联合基础电信企业对存在风险的设备进行远程升级。CNCERT/CC将上述情况向CERT/CC进行反馈。

2014年3月18日，CNCERT/CC接到美国国土安全部工业控制系统网络应急响应小组(ICS-CERT)投诉，称 “世纪星SCADA V7.12存在漏洞”（漏洞编号：ICS-VU-863300）。 CNCERT/CC按照CNVD的处置流程，请US-CERT提供了ICS-VU-863300编号的漏洞文档，通过技术分析确认漏洞情况属实。在处置过程中，CNCERT/CC联系世纪星SCADA软件的生产厂商“北京世纪长秋科技有限公司”，通报漏洞情况，并向ICS-CERT反馈生产厂商对外邮件联系方式，以便其后续跟进处置情况。

（12）协调处置免费邮箱收集韩国个人信息事件

自2014年2月起，CNCERT/CC接到韩国KrCERT关于移动互联网恶意程序通过境内免费邮箱窃取韩国公民个人信息的投诉事件20余起。CNCERT/CC对KrCERT提供的一批移动互联网恶意程序样本进行分析验证，发现投诉样本为仿冒韩国银行手机客户端的恶意程序，其伪造韩国多家手机银行界面，诱骗用户输入银行账户等敏感信息。在用户不知情的情况下，拦截用户电话、短信、彩信，窃取用户终端本地存储的银行“NPKI”数字证书及用户短信、彩信、通讯录、通话记录、录音等文件，通过后台联网上传至国内免费邮箱。CNCERT/CC通过取证验证了56个确实被用于收集用户敏感信息的免费邮箱，并协调该免费邮箱提供商注销以上56个邮箱，切断黑客通过邮箱获取用户信息的途径。

（13）协调处置仿冒Visa和巴林国家银行的恶意APP

2014年3月27日，接到国际反网络钓鱼组织（Phishlab）投诉，其在搜狐某页面发现Visa未授权手机应用，侵犯Visa品牌，并发动恶意攻击。CNCERT/CC对事情的真实性进行验证后，协调搜狐应用中心对该应用进行下架处理。

2014年4月30日，澳大利亚安全公司FraudWatch向CNCERT/CC投诉未授权的虚假手机APP下载网址。FraudWatch称该APP未获得巴林国家银行（National Bank of Bahrain）的授权，并非官方APP，企图通过冒充官方巴林国家银行来窃取用户的登录信息。CNCERT/CC收到投诉后对事情的真实性进行验证，随后联系应用商店voga360.com对该应用进行下架处理。

（14）协调处置哈萨克斯坦共和国总统官网遭受攻击事件

2014年10月，CNCERT/CC接到哈萨克斯坦KZCERT投诉，称中国大陆的1个IP地址攻击了哈萨克斯坦共和国总统官网（www.akorda.kz）。CNCERT/CC验证后，协调北京联通处置。北京联通定位涉及的IP地址为百度土城IDC，并通知百度通告IP地址使用人处置，最终成功协调并停止攻击行为。

（15）协调处置韩国三星公司遭受拒绝服务攻击事件

2014年10月29日，韩国KrCERT投诉了我国部分主机针对三星公司数据系统（SDS）的拒绝服务攻击事件。CNCERT/CC分析了KrCERT提供的攻击日志核实了本次攻击事件，于10月30日立即协调中国电信和中国联通两家基础电信运营企业对网内的15台攻击主机进行处置，及时消除安全隐患。

（16）协调处置罗马尼亚机构遭受DNS放大攻击事件

2014年11月，罗马尼亚CERT-RO投诉DNS放大攻击，涉及中国大陆的IP地址有7个。攻击者利用开放的DNS服务器或存在漏洞的SOHO路由（家用或小型办公室用路由器）发动攻击。CNCERT/CC验证后，协调分中心通知用户进行清理，并采取相应措施，提高存在漏洞的主机的安全性。

（17）协调处置西班牙一网站遭受拒绝服务攻击事件

2014年11月，CNCERT/CC接到西班牙INTECO-CERT投诉，西班牙一网站遭受源自中国的拒绝服务攻击。CNCERT/CC分析发现，该事件可能是黑客伪造被攻击网站IP地址向大量机器的1900端口（对应upnp服务）发送upnp数据包以反射攻击被攻击网站。此次事件共涉及6万多个中国IP地址， CNCERT/CC将攻击次数位于前20的IP地址发给运营商进行协调处置。

（18）协调处置宙斯僵尸网络控制服务器

2014年11月，CNCERT/CC接到香港HKCERT投诉，称www.d13ad.com 和www.wlhydh.co被用于宙斯僵尸网络控制服务器。HKCERT请求CNCERT/CC协调联系该域名注册商，通知网站托管公司清理服务器，以免服务器被黑客利用运行宙斯僵尸网络。CNCERT/CC验证后，协调域名注册服务机构进行相关处置。

（19）协调美国US-CERT处置中国基础电信企业递归域名服务器遭受攻击事件

2014年12月10日，我国基础电信企业的多省递归服务器遭受攻击。经CNCERT分析，位于美国的IP地址为23.227.173.210的主机是该攻击的控制端。12月18日CNCERT向US-CERT投诉该IP地址，请求其进行处置；12月30日US-CERT反馈已将该事件交由相关运营商进行处理。通过邮件、电话等多种联系，CNCERT持续对该事件的处置进展进行跟踪。

（20）协调处置谷歌公司广告产品遭受恶意攻击事件

2014年，CNCERT/CC多次接到美国谷歌公司投诉，称谷歌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，确认了因部分用户的DNS解析请求遭到了劫持和篡改，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，有效地保障用户的权益。

（21）CNCERT/CC组织开展12次恶意程序专项打击行动

2014年，CNCERT/CC共组织基础电信企业、互联网接入企业、域名注册服务机构和手机应用商店等先后开展12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744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所用IP地址及域名767个，成功切断黑客对近98.3万台感染主机的控制。在移动互联网方面，共下架8644个恶意APP程序，处置103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210条恶意程序控制URL链接。

8 网络安全信息通报情况

8.1 互联网网络安全信息通报

2014年，CNCERT/CC继续按照《互联网网络安全信息通报实施办法》要求，作为通信行业内的通报中心，协调组织各地通信管理局、中国互联网协会、基础电信企业、域名注册管理和服务机构、非经营性互联单位、增值电信业务经营企业以及网络安全企业开展通信行业网络安全信息通报工作。

按照《互联网网络安全信息通报实施办法》规定，各信息通报工作单位每月前5个工作日向CNCERT/CC报送前一个月的月度汇总信息；对于监测和掌握的其他重要事件信息和预警信息则需及时报送。2014年，我中心共收到各单位报送的月度信息561份，事件信息和预警信息324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》33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，提供了及时有效的预警和指导。

根据各互联网网络安全信息通报工作单位报送的月度汇总信息[30]，2014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。

[30] 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。

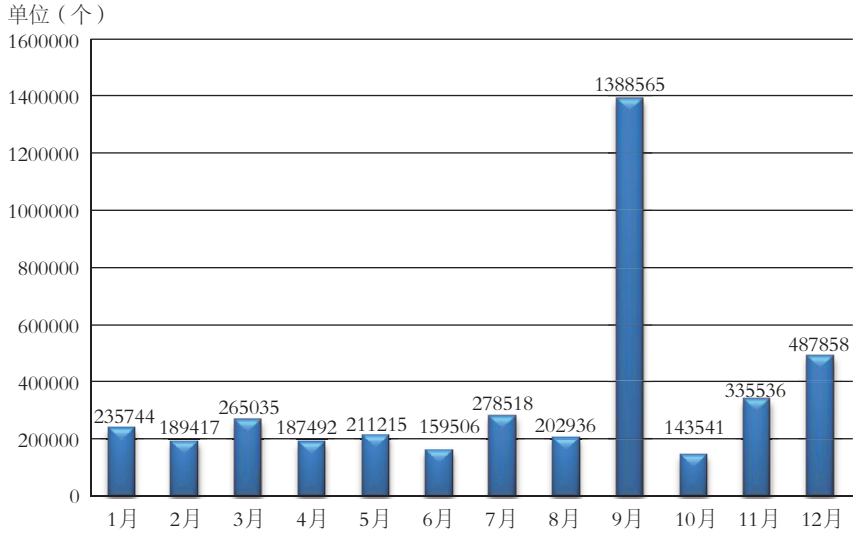


图8-1　2014年通信行业事件月度报送数量统计（来源：CNCERT/CC）

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5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，2014年报送的事件类型主要为公共互联网环境以及IP业务中的网络安全事件。与2013年相比，各类别报送的数据均呈现增长，基础IP网络、IP业务、运营企业自有业务系统、域名系统、公共互联网环境分别增长33.2%、1345.3%、269.2%、497.0%、53.3%。

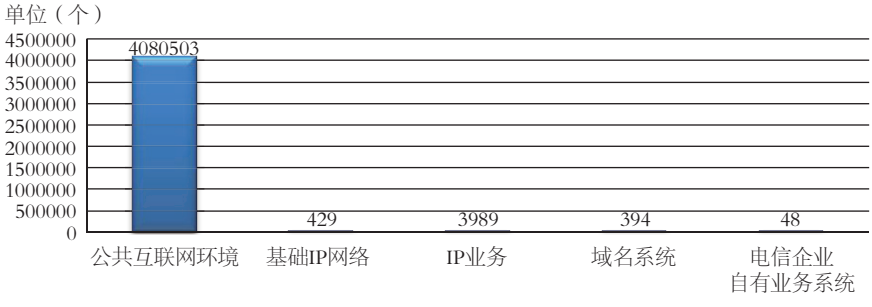


图8-2　2014通信行业报送事件数量的分类统计（来源：CNCERT/CC）

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，计算机病毒事件数量最多，占公共互联网环境事件总数的比例为31.3%；其他数量较多的事件类型还有：木马事件、僵尸程序事件和蠕虫事件，分别占21.1%、11.4%和8.4%。

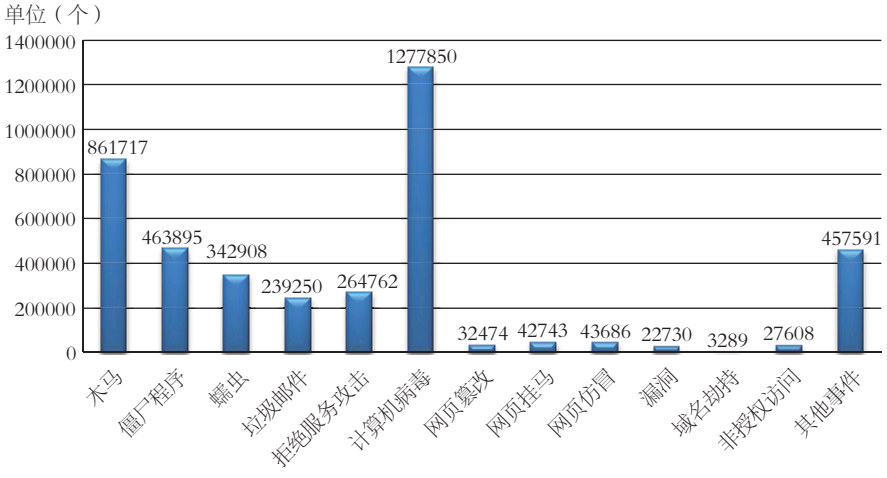


图8-3　2014年通信行业报送的公共互联网环境事件数量的分类统计
（来源：CNCERT/CC）

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。如高考等一些重要时期，各通报成员单位报送了大量涉及相关网络信息系统的网页篡改、网页挂马等信息；在Windows XP停止服务后，相关通报成员单位及时报送了针对XP的攻击事件、漏洞等信息，对确保基础信息网络和重要信息系统业务的运行安全发挥了积极作用。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。

2014年发布的重要通报增刊见表8-1。

表8-1　2014年CNCERT/CC发布的重要通报增刊

互联网网络安全信息通报（总第197期），关于2013年12月基础电信企业漏洞风险情况的通报
互联网网络安全信息通报（总第198期），关于2013年12月域名系统软件及域名机构漏洞风险的情况通报
互联网网络安全信息通报（总第199期），关于2013年12月增值电信企业漏洞风险的情况通报
互联网网络安全信息通报（总第201期），关于利用刷机方式植入“手机预装马”进行用户信息窃取的情况通报
互联网网络安全信息通报（总第202期），关于美国凹凸科技（O2Security）SSL-VPN设备存在高危漏洞的情况通报
互联网网络安全信息通报（总第203期），关于多款路由器设备存在预置后门漏洞的情况通报
互联网网络安全信息通报（总第205期），关于警惕近期多发NTP反射放大攻击的预警通报
互联网网络安全信息通报（总第207期），关于OpenSSL存在高危漏洞可被利用发起大规模攻击的情况通报
互联网网络安全信息通报（总第214期），关于Bash存在环境变量远程命令执行漏洞利用发起大规模攻击的情况通报
互联网网络安全信息通报（总第215期），关于近期黑客组织拟对我发起网络攻击的预警通报

8.2　行业外互联网网络安全信息发布情况

2014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242份，相比2013年增加了28份。其中通过印刷品向有关部门发布月度网络安全专报和简报各12期；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52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、《网络安全月报》12期、《2013年互联网网络安全态势报告》1份、《2013年中国互联网网络安全报告》1份；通过期刊杂志发布网络安全数据分析文章36篇。

2014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、中国日报等国内主流媒体纷纷前来挖掘新闻类节目或新闻素材，CCTV新闻频道、新华网、人民网、中国日报英文版、参考消息、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《2013互联网网络安全态势综述发布》、《地方政府网站成为黑客攻击“重灾区”》、《多家路由器被爆存在安全后门》、《扣话费窃隐私，岂能太恣意》、《网络威胁“瞄”上信息消费领域，恶意程序大幅增长》、《中国互联网面临大量境外地址攻击威胁》、《Android targeted most by malware》、《Hacking into computers drops as nation beefs up protection》等。

9 国内外网络安全监管动态

9.1 2014年国内网络安全监管动态

（1）中央网络安全和信息化领导小组成立

2014年2月27日，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长。新设立的中央网络安全和信息化领导小组将着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

习近平总书记指出：“没有网络安全，就没有国家安全；没有信息化，就没有现代化。”会上透露的信息显示，领导小组将围绕“建设网络强国”，重点发力以下任务：要有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。会议还强调，建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力增强、信息经济全面发展、网络安全保障有力的目标不断前进。

（2）人大常委会立法计划公布，网络安全法将制定

2014年4月14日，十二届全国人大常委会第二十一次委员长会议通过了全国人大常委会2014年立法工作计划，并于4月17日向社会公布了这份计划。2014年全国人大常委会立法工作的总体要求是把立法决策与改革决策结合起来，加强重点领域和关键环节改革的立法，发挥立法的引领、推动和保障作用，积极推进科学立法、民主立法，

扩大公民有序参与立法途径，着力提高立法质量，切实增强法律的可执行性和可操作性，更加注重法律的有效实施。为进一步加强网络安全工作，在2014年的立法工作计划中，将制定网络安全法。

（3）国信办表示将出台网络安全审查制度，强化国家安全审查

2014年5月22日，国家互联网信息办公室表示，我国即将推出网络安全审查制度。该项制度规定，关系国家安全和公共利益的系统使用的重要信息技术产品和服务，应通过网络安全审查。据了解，我国即将推出的网络安全审查制度，规定对进入我国市场的重要信息技术产品及其提供者进行网络安全审查。审查重点在于该产品的安全性和可控性，旨在防止产品提供者利用提供产品的方便，非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息。对不符合安全要求的产品和服务，将不得在我国境内使用。

（4）中共中央决定加强互联网领域立法

2014年10月23日，中国共产党第十八届中央委员会第四次全体会议通过的《中共中央关于全面推进依法治国若干重大问题的决定》提出，加强互联网领域立法，完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规，依法规范网络行为。

（5）工业和信息化部开展打击移动互联网恶意程序专项行动

2014年7月28日，为净化公共互联网网络环境，进一步遏制利用移动互联网恶意程序从事违法犯罪活动的蔓延势头，创造安全的移动互联网信息消费环境，保护用户权益，维护网络安全，工业和信息化部联合公安部、工商总局自2014年4-9月在全国范围开展打击移动互联网恶意程序专项行动。

本次专项行动坚持依法治理、标本兼治的工作思路，充分发挥通信、公安、工商等部门的职能作用和行业自律、社会监督的作用，在移动互联网应用程序制作、传播、使用环节加强安全管理，推动建立移动互联网恶意程序治理的长效机制。开展的工作主要有：一是，三部门联合印发了《打击治理移动互联网恶意程序专项行动工作方案》，督促应用商店落实安全责任，开展应用程序安全检测，实施应用程序开发者签名试点，依法打击相关网络违法犯罪行为；二是，对专项行动进行了任务分解，组

织各地通信管理局、基础电信企业和相关支撑单位召开会议，专题部署了有关工作任务，明确工作要求；三是，研究制定了《移动互联网应用商店网络安全责任指南》，明确了应用商店应当承担的安全责任，为应用商店安全检查工作奠定基础；四是，组织开展针对安卓应用程序的开发者签名试点工作，强化应用程序开发源头管理，实现应用程序的防篡改和可溯源。同时，督促指导相关单位，切实落实应用商店安全检查、应用程序安全检测、开发者签名试点、深挖地下产业链线索等各项工作任务，加大用户宣传，加强跨部门协作配合，确保专项行动取得实效。

（6）工业和信息化部发布加强网络安全工作指导意见

2014年8月28日，工业和信息化部发布《关于加强电信和互联网行业网络安全工作的指导意见》，从网络基础设施安全防护，突发网络安全事件应急响应，安全可控关键软硬件应用，网络数据和用户个人信息保护，移动应用商店和应用程序安全管理等方面加强网络安全监管。

其中，《关于加强电信和互联网行业网络安全工作的指导意见》特别指出，将通过建立健全钓鱼网站监测与处置机制，加强木马病毒样本库、移动恶意程序样本库、漏洞库、恶意网址库等建设，促进网络安全威胁信息共享，加强对黑客地下产业利益链条源头治理等方面切实监管网络安全，强化用户个人信息保护。并推动建立国家网络安全审查制度，从行业层面加强规范和治理。

此外，针对近年来安全事件频发的移动互联领域，工业和信息化部将特别加强移动应用商店和应用程序安全管理，督促应用商店建立程序开发者真实身份信息验证、应用程序安全检测、恶意程序下架、恶意程序黑名单、用户监督举报等制度，建立健全移动应用程序第三方安全检测机制。

（7）工业和信息化部新增7个国家级互联网骨干直联点建设全面竣工

为推进宽带中国战略，解决我国互联网顶层结构不均衡，骨干网间互联互通薄弱的问题，优化互联网产业布局，2014年年初工业和信息化部在大量调研、评估、论证的基础上，在成都、西安、武汉、沈阳、南京、重庆、郑州7个城市启动了国家级互联网骨干直联点建设工程。

截至2014年10月1日，7个新增骨干直联点全部建成，经过2个多月的试运行，目

前已全面投入使用。工程直接投资达29.2亿元，建成网间互联能力6676GB，已经开通810GB，超额完成全年扩容500GB的目标，全国互联总带宽大幅增长近50%，达到2450GB。本次工程安装大型互联路由器56套，配套改造机房56个，升级本地网络节点13个，铺设网间互联光缆3000余千米，开通至北上广等骨干核心节点直达电路60余条，全面完成了预定计划。至此，我国互联网骨干直联点从3个增加到10个，互联网架构布局得到明显优化，网间通信质量显著提升，流量疏通效率和安全性能大幅改善，达到了预定目标。7个国家级骨干直联点的建成，对地方经济的带动和促进、互联网的发展和优化、用户的服务和体验，都有着积极而深远的影响，使网络质量有了明显改善，网络安全性能得到提升，给群众带来了实惠。

9.2 2014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

- 美国白宫正式推出“网络安全框架”

2014年2月12日，美国白宫正式推出一项可自愿加入的“网络安全框架”项目，旨在加强电力、运输和电信等所谓“关键基础设施”部门的网络安全。“网络安全框架”根据美国总统奥巴马2013年2月签署的行政命令制定，私营部门可在自愿基础上使用该框架加强自身的网络安全能力。

美国白宫在一份声明中指出，“网络安全框架”吸纳了全球现有的安全标准以及做法，以帮助有关机构了解、交流以及处理网络安全风险。此外，该框架也就隐私与公民自由问题提出了指导方针，因此，通过该框架，美国私营企业和政府部门可以联手加强“关键基础设施”的安全与适应性。奥巴马在另外一份声明中称，“网络威胁是美国面临的最大国家安全危险之一。”他说，美国的经济繁荣，国家安全以及个人自由都依赖于开放、互通、安全、可靠的互联网，但美国的“关键基础设施”持续面临来自网络空

间的威胁，“美国经济也被知识产权的偷窃行为所伤害”，“尽管我相信今天推出的框架是一个转折点，但很明显还需要做更多工作加强我们的网络安全”。奥巴马敦促国会就网络安全问题进行立法，以便给予政府部门更多权力处理私营部门的网络安全问题，但美国私营部门一直反对这一要求，美国国会的相关立法也因此陷入僵局。

• 美国国家安全局公布监听改革计划

2014年3月底，美国白宫正式公布国家安全局监听改革计划。美国总统奥巴马表示，美国国家安全局（NSA）将停止对公民电话通信数据进行大规模监听和储存，如涉及国家安全问题，政府可在美国的外国情报监视法庭批准许可下查看监听数据。

美国政府一名官员表示，美国总统奥巴马计划向美国国会提出议案，停止NSA对电话通信数据进行大规模监听和储存。数百万条在美国境内发生的通话信息都处于NSA的监听范围之内。如果美国国会批准奥巴马终止监听项目的提议，NSA将不再收集和存储此类信息，假如遇到疑似恐怖主义的通话记录，美国政府有权在得到美国外国情报监视法院的允许后查看相关信息。美国政府于“9·11”事件后开始进行监听项目。2013年6月，前美国中央情报局（CIA）技术分析员爱德华·斯诺登曝光了美国监听项目，引起世界关注。

• 美国联邦通信委员会通过“网络中立”新法规

2014年5月16日，美国联邦通信委员会（FCC）通过了“网络中立”新提议。这项提议禁止互联网供应商阻止或减缓用户访问网页，但允许内容公司向宽带供应商付费，以获得更快的网速。FCC发布该提议4个月以来，消费者权益保护者以及众科技公司站成一边，同美国共和党以及互联网供应商展开了激烈的拉锯战。消费者权益保护者希望FCC重新将互联网供应商归纳到公共事业部（如电信公司），以便对其加强监管，而宽带公司、议会以及FCC的共和党成员都强烈反对这项提议。FCC最终以3:2的票数通过法案，开始收集公众的意见和建议。

（2）美国其他网络安全相关举措

• 美国国会将对一项新网络安全法案进行投票表决

2014年7月8日，美国参议院情报委员会通过了2014《网络安全情报分享法案（CISA）》。这一由民主党议员Diane Feinstein主持并参与编写的新网络安全法案即将在国

会进行投票表决。该项法案的初始影响将会对“网络威胁指标”提出一个全新的分享信息要求。当一家公司向政府提供一份关于威胁指标的报道，CISA将可以要求将这些信息分享给包括NSA在内的多个联邦机构。另外，CISA还将要求公司对其网络进行监控，进而获得更多关于目标威胁的信息。这意味着CISA为NSA提供访问私人网络的权限。民主科技中心（CDT）称，CISA潜藏着为网络安全项目提供窃听后门的威胁，缺少隐私保护的重要规定。电子前沿基金会则把这一法案称为“致命的缺陷”，并呼吁建立独立于NSA的数据保存公司。CISA的起草团队却认为这项法案是打击网络犯罪必须要走的一步。

• 美国建立数字服务部门，网络信息安全再获关注

2014年8月11日，美国白宫宣布，美国政府已成立了一个全新的数字服务部门团队（US Digital Service，USDS），负责美国医保等诸多政府网站的数据服务。该团队由前谷歌网站管理人员麦克·迪克森挂帅。2014年团队的预算额度高达2000万美元。

美国白宫曾在2014年2月12日正式推出一项可自愿加入的“网络安全框架”项目，旨在加强电力、运输和电信等所谓“关键基础设施”部门的网络安全。白宫当时在声明中表示，通过该框架，美国私营企业和政府部门可以联手加强“关键基础设施”的安全与适应性。本次白宫为政府官方网站成立USDS，是在网络安全框架之下第一次为政府本身而非企业用户成立服务团队，另外USDS的信息安全深层任务值得挖掘。美国政府首席信息官史蒂文·范·洛克尔是其中的关键人物。范·洛克尔曾在2014年5月举行的美国国土安全参议院会议上极力呼吁，美国政府应在网络安全领域投入远比现在更多的资金和精力，来完成政府方面的升级换代。就在网络安全这一议程，范·洛克尔提出了设立USDS部门的申请。值得注意的是，范·洛克尔当时申请的部门名称为“信息科技监管与改革部门”，而本次美国政府选择了“数字服务部门”这一更为中立的名称，并把团队意义的宣传重点调整为“维持网站稳定性”。范·洛克尔11日接受采访时表示，美国终于有了自己的数字服务部门，希望能为所有的政府网站建立稳定可靠的运营环境，并向外推广。

• 美军成立工作组防堵“棱镜门”漏洞

2014年3月6日，美军参谋长联席会议主席邓普西在出席国会听证会时说，美军已设立专门工作组，评估前美国防务承包商雇员斯诺登泄密行为给军方造成的损失，预计军方须斥资数十亿美元防范安全隐患。

邓普西与国防部长哈格尔当天就2015财年国防预算出席众议院军事委员会听证会。邓普西在作证时说，目前还无法完全估算斯诺登所曝光的内容给美国军方总共造成多大损失，但不少内容涉及美军作战能力、军事行动、技能战术和工作流程等方面信息，因此军方已成立专门工作小组评估损失，并研究这些泄密文件会被他人如何利用，如何防堵安全漏洞。邓普西说，面对严峻挑战，预计这一工作组需要至少两年时间来完成上述评估工作，军方恐怕要花费数十亿美元来防堵潜在安全漏洞。

• 美空军将建网络安全设施，可容纳一支网络作战大队

2014年9月11日消息，美国空军正在建立一个新的网络/ISR设施。该设施占地2700平方英尺，座落在马里兰州沃菲尔德的空军国民警卫队基地。“该设施的建设目的是容纳一支网络作战大队和ISR中队，”信息征询书中写道。“其网络使命由一系列能力和专业知识构成，它们能够满足永远在线、实时感知和全球范围的综合运行响应，使运营者能够紧跟网络攻击者的步伐，并能够为其提供7×24小时的情报和全源信息。”该设施预计将花费1000万～2500万美元。

• 美国打造“网络安全军团”以加强网络安全

2014年4月15日，美国国防部部长查克·黑格尔（Chuck Hagel）称美国五角大楼将推动“网络安全军团”（CyberCorps）项目进一步实施，计划于2016年前增加其网络安全部员工。

联邦调查局督导特工查尔斯·吉尔根（Charles Gilgen）在一次防范网络犯罪会议上表示，联邦调查局在2015年计划召入1000名特工和1000名分析师。联邦调查局和五角大楼计划在明后两年增加6000名网络安全技术人员，并通过提供大学奖学金来鼓励计算机人才加入此计划。

该“网络安全军团”启动于2000年。政府为学生提供学费、书本和职业发展奖学金，其中也包括每年2万～3万美元（约合12万～18万元人民币）固定津贴。受到资助的学生毕业后在政府任职，任期为受资助期长。该项目总监维克多（Victor Piotrowski）表示，在过去三个财年内，预算增长到每年450亿美元，已有1554名学生加入该计划，另有463名在校学生。

• 美陆军将成立新网络防护旅

2014年9月，针对日趋复杂的网络安全局势，美国陆军正在加强网络防护旅建

设，可能成立一个新的网络支队。陆军网络司令部一级军士长罗德尼·哈里斯表示，网络防护旅正由佐治亚州哥登堡的美国陆军网络企业技术司令部筹备。这是美国陆军拥有的此类型的第一个旅，核心是其网络保障团队。

哈里斯表示，在过去的两年中，陆军网络司令部始终服务于哥登堡的团队和具有初始作战能力的整个部队，然而，陆军需要的网络团队数量是目前的两倍。在未来两年内，陆军在网络事业领域的士兵数量需要增加一倍。他称，在8月召开的一次会议上，重点研究了对网络战士的管理，称为17职业管理领域（CMF17）。与会者讨论了新的军事职业分工，如建议17C为网络战专家和17A为网络战军官。17系列将信号情报和军事情报的技能混为一体。他表示，“这些士兵独一无二，技能高超，少之又少。因此，陆军参谋长要求我们专注于人才管理、招聘和保留网络战士。”

他补充说，网络防护旅和网络团队将提供更灵活、反应更灵敏的网络空间力量。网络团队规模大小相当于排级编制，不过还要取决于他们的任务。执行战斗任务或进攻的团队规模较大，网络防御和网络防护团队是中等规模，保障团队规模则相对较小。

- 美国白宫拆分大型法案，改变网络安全立法推动策略

2014年10月11日，美国白宫网络安全协调主管丹尼尔（Michael Daniel）在新闻发布会上表示，为了能在国会积极推动网络安全立法，奥巴马政府决定改变策略，将一个大型法案拆分为几个小型法案，希望能以此获得国会通过。丹尼尔认为小型法案比大型法案更容易获得通过。他表示，政府将借助一切法律手段，把注意力集中在“能通过什么我们就提什么”。但是他也承认，法案很难在2014年获得通过，很有可能要在2015年1月改选后的国会上通过。他说，“我们仍将努力（通过立法），但是很明显，想在国会通过任何决定目前都是一个挑战”。奥巴马政府希望通过立法可以帮助国土安全部和其他私人公司进行合作以防止黑客进行网络攻击，避免摩根大通和其他9家财政机构遭到网络攻击的事情再次发生；与此同时，希望能提高该机构合法权力以对抗网络恐怖分子，使得国土安全部可以招募更多网络安全专家来修复目前容易被黑客利用的安全漏洞。

9.2.1.2 美洲其他国家网络安全监管动态

（1）加拿大推数字化国家计划 98%国民高速上网

2014年4月8日，加拿大工业部长詹姆斯·穆尔宣布，推出旨在帮助加拿大人尽享

数字化时代机遇的“数字加拿大150计划”。这项数字未来计划包括用以构建信息更为联通的39项新举措，其5个关键原则是：确保互联互通、增强安全保护、增加经济机会、数字政府和强化内容。

通过该计划，加政府将确保超过98%的国民获得高速上网服务，从而刺激电子商务、高清视频和远程教育的发展。政府将拨出3.05亿加元扩展和增强高速互联网服务，使28万户农村和偏远地区家庭的上网速度达到5MByte/s。“数字加拿大150计划”将提供总计3600万加元的资金，用以修理、翻新和捐赠电脑，并提供给公共图书馆、非营利组织和原住民社区，使学生有机会接触、参与数字世界所必需的设备。在此计划下，加拿大全境无线漫游资费将设置上限，违反规定的无线运营商将受到处罚。

该计划着力提升加拿大国民对网上交易安全性、隐私保护乃至远离网络欺凌和其他网络威胁的信心。计划还将确保通信网络和设备的安全，保护家庭、企业和政府的隐私。从2014年7月1日起实施《反垃圾邮件法》，保护公众免受恶意网络攻击。政府将通过加拿大商业发展银行，给数字企业提供3亿加元的风险投资，此外还将投资2亿加元支持中小企业采用数字技术，计划着力将加拿大打造成数字技术和开放数据的领导者，确保加拿大人更便捷地使用政府的在线服务。新举措亦将促进在线内容建设，让公众全面了解和关心国家大事。

（2）巴西国会众院表决通过《互联网民法》草案

2014年3月25日，巴西国会众院表决通过《互联网民法》草案，该草案还将经巴西国会参院表决通过后，最后由巴西总统批准实施。在表决中，包括反对党在内的多数议员投了赞成票。《互联网民法》草案已经在巴西国会经数次讨论。巴西政府希望在世界杯前通过这一法案，为维护巴西网络安全提供法律保障。此法中有一项规定，政府可以通过行政命令，强制要求巴西（电信）企业在巴西领土内建立用于保存所有网络用户的信息中心。

9.2.2 欧洲地区网络安全监管动态

（1）俄政府批准信息技术产业发展路线图

2014年1月8日，俄政府批准了由大众传媒和通讯部起草的信息技术产业发展路线

图，主要内容是到2018年将信息技术产业的从业人员数量翻一番，降低财政对资源性行业的依存度。该计划的落实将使信息技术产业的平均增长率超过GDP的平均增长率，同时将俄信息技术产业的产值从84.4亿美元提升至140.6亿美元，降低俄经济对原材料出口的依存度，通过普及推广信息技术来提高劳动生产率。

（2）俄国防部3年内将组建反计算机攻击专业机构

2014年1月30日，俄罗斯总参谋部第八局负责人尤里·库兹涅佐夫透露，俄国防部将于未来3年内组建一个专业机构，专事保护重要军事设施免受计算机网络攻击。库兹涅佐夫表示，组建该机构的目的是保护俄武装力量最重要的军事设施。该项工作由国家软件部门组织进行，已在分阶段实施之中，按计划将在2017年前完成，但他未披露更多细节，俄国防部此前曾宣布组建新兵种以应对计算机网络威胁的计划。俄防长绍伊古亦表示，俄军方正在吸收非军事高校毕业的青年编程员入伍，俄军队近5年内将需要构建大量必需的计算机程序。

（3）俄罗斯议会通过新法案打击国外网站

2014年7月6日，俄罗斯议会通过了一项互联网监管新法案，要求国外互联网公司将俄罗斯居民的个人数据存储在俄罗斯境内。此举明显是向Facebook和Twitter等国外网站施压，迫使他们将用户信息移交给俄罗斯当局。

“大多数俄罗斯人不希望自己的数据被存储在美国，在那里它们可能遭到黑客攻击并被犯罪份子获取”，提交该法案的俄罗斯议会议员Vadim Dengin说，“我们的整个生活都存储在那里。”他还补充说，互联网公司应该在俄罗斯建立数据中心。

该法案将使未在俄罗斯设立办事处的互联网公司面临更大的压力。一直以来，Facebook和Twitter拒绝将用户数据移交给政府。就在该法案于6月被提交给议会的几天之前，Twitter的公共政策部门主管科林·克劳威尔（Colin Crowell）访问了俄罗斯，并与俄罗斯媒体监管机构Roskomnadzor进行了会谈。这次访问的细节未被公开，但外界认为用户隐私权肯定是重要议题。俄罗斯当局一直要求Twitter在俄设立办事处，但该公司到目前为止始终表示拒绝。“没有人愿意迁到俄罗斯，但我很悲观。我认为（俄罗斯当局）会迫使他们搬迁服务器”，对俄罗斯安全机构进行过大量报道的著名记者安德烈·索尔达托夫（Andrei Soldatov）说。

“在很大程度上，这是针对的Gmail、Facebook和Twitter的”，他说。虽然该法案已被通过，但到2016年9月才正式生效。尽管如此，该法案给俄罗斯当局提供关闭不合作网站的理由。这可能会对一些俄罗斯公司，例如依赖国外网上预订服务的旅游网站和航空公司产生不利影响。

（4）俄罗斯战略导弹部队已建立网络安全部队

2014年10月16日，俄罗斯国防部战略导弹部队发言人伊戈尔·叶戈罗夫上校称，俄罗斯战略导弹部队（SMF）建立了负责检测和阻止网络攻击的“火山”部队。叶戈罗夫称，“俄罗斯战略导弹部队（SMF）在武器和部队控制上采用数字技术，并扩大了电子文件管理的应用。因此，俄罗斯战略导弹部队的工作人员正在采取预防措施提升网络安全，正在进行建立负责控制网络攻击的可持续作战部队。”叶戈罗夫还表示，必要时，网络专家将负责寻找和减少信息系统的漏洞。“火山”部队是为了装备移动式陆基导弹系统以及导弹发射井的部队而建立。2017年，俄罗斯国防部将成立专业部门负责击退瞄准其关键目标的网络攻击。

（5）英国正式启动国家计算机紧急应对小组

2014年3月31日，英国政府内政部宣布正式启动国家计算机紧急应对小组，以协调应对针对计算机网络系统的攻击。该小组的主要职能是应对“国家级别”的互联网安全突发事件，并为政府、企业和学术机构提供相关互联网安全建议和风险提示，同时作为英国在该领域的主要机构同其他国家展开国际合作。

英国内阁办公室大臣弗朗西斯·麦浩德在启动仪式上称，2013年英国93%的大型企业都受到不同程度的网络攻击，网络攻击造成的经济损失最高可能达到85万英镑。国家计算机紧急应对小组的设立有助于政府、企业及学术机构间的协调和安全信息共享，最大程度保障互联网信息安全。该小组的负责人克里斯·吉布森指出，小组的成立是英国互联网安全保障工作的里程碑，将使英国的互联网系统具有更强的风险应对和防范能力，尤其是针对银行、发电厂、能源公司等国家重要基础设施发动的网络攻击，都是该小组重点关注的对象。

设立国际计算机紧急应对小组是英国2011年启动的《国家网络安全战略》计划的一部分，《国家网络安全战略》共获得政府8.6亿英镑的支持，其目标是使英国能够更

加灵活地应对网络攻击，帮助政府与私营行业建立伙伴关系，发展网络安全知识、技能和能力。

（6）英国斥巨资保基础设施网络安全

2014年11月，英国的专家小组目前正考虑如何修复英国发电站、铁路网络和工厂运行的重要系统的安全漏洞。4个研究团队共享250万英镑（约2463万元人民币）政府基金，用于应对因日益增加的黑客攻击而引发关注的工业控制系统的安全问题。

（7）英拟斥重金应对网络威胁对抗“看不见的敌人”

2014年7月15日，英国首相卡梅伦宣布将向军方投资11亿英镑，以应对国家安全面临的新威胁。他表示，武装部队必须适应对抗“看不见的敌人”。卡梅伦说，在“情报和监视”设备，如无人机方面的开支是“国家需要”。英国面临着不断变化的全球恐怖主义威胁以及能够从海外袭击这个国家的看不见的网络犯罪威胁。该方案包括额外拨款8亿英镑，用于情报、监视、目标捕获和侦察“一揽子”计划。唐宁街表示，这将提高特种部队应对全球恐怖主义和劫持人质的威胁能力。另外的3亿英镑将用于现有的项目，包括“台风”战斗机的下一代雷达等。卡梅伦说，如果政府通过削弱英国的军事能力而从世界上“后退”，这个国家不会变得更安全。卡梅伦警告说，英国的军队必须得到增强，以打击恐怖袭击的威胁。

（8）英国情报机构推出“网络间谍”硕士专业

英国情报机构政府通讯总部（GCHQ）授权6所英国大学提供训练未来网络安全专家的硕士文凭。英国政府通讯总部与著名的英国军情五处（MI5）和六处（MI6）合称为英国情报机构的“三叉戟”。这一特殊学位是英国2011年公布的“网络安全战略”的一部分。该战略认为，高等教育是提升英国防范黑客和网络欺诈的关键内容。英国内阁办公室大臣弗朗西斯·麦浩德（Francis Maude）说，网络安全是英国经济长期发展计划的“关键部分”，这一课程能帮助英国成为网络交易最安全的国家之一。他还表示，政府通讯总部与其他政府部门、私营企业和院校共同推出这一项目，能帮助英国应对威胁。

据介绍，目前提供由GCHQ批准的网络安全课程的有：爱丁堡龙比亚大学、兰卡斯

特大学、牛津大学以及伦敦大学皇家霍洛威学院。此外，克兰菲尔德大学的网络防御和信息安全保障课程、萨里大学的信息安全课程也获得GCHQ颁发的临时认证。

（9）德国考虑建立“网络法院”对隐私权纠纷进行裁决

2014年5月28日，德国正考虑建立“网络法院”，以对搜索引擎与保护个人隐私的用户之间的冲突做出裁决。德国内政部表示，德国政府正在考虑解决隐私纠纷的方法，其选项包括“网络法院”及某种第三方仲裁程序等。拟议中的网络法院将采取专门司法机构的形式，该机构将拥有解决科技公司与个人用户间纠纷的权力。德国内政部表示，它关切的是自动删除程序使得政客和名人能够将他们认为“令人不快的”内容彻底掩盖，哪怕这些内容的报道符合公众利益。

（10）德国出台《数字议程2014–2017》打造数字强国

2014年8月20日，德国政府出台“数字议程”，目的是在变革中推动“网络普及”、“网络安全”及“数字经济发展”这三个重要进程，使德国成为具有国际竞争力的“数字强国”。为实现数字强国的目标，德国经济部、内政部等联合推出《数字议程2014–2017》。该议程分7个行动领域，不仅考虑到数字化对信息及通信技术领域的影响，还包括数字化对经济、社会等方面的影响。

如何挖掘数字化创新潜力、促进经济发展和就业至关重要。德国政府计划推动工业数字化，支持云计算和大数据等技术研发，资助新兴企业等，目标是到2017年成为欧洲数字经济增长龙头。为实现数字强国的目标，数字化基础设施建设必不可少。德国政府决定在2018年前在全国普及高速宽带。同时，为确保数字安全，德国政府拟加强数据保护，提高政府机构对网络攻击的防御能力。

（11）法拨款10亿欧元加强网络安全，扩编网络防御部队

2014年1月21日，法国国防部长勒德里昂表示，法国已拨款10亿欧元用于加强网络安全能力建设。据悉，这项10亿欧元的投资将用于建设CALID网络防御部队，该部队负责监控法军的信息安全。其工作人员数量将从2011年的20人增加到2019年的120人，位于布鲁兹的法国国防采购局信息中心的员工数量将在未来几年内从250人增加到450人。

法国国防部长勒德里昂在法国里尔举办的第六届网络安全国际论坛上表示，网络安全防御问题已经成为“国家性首要问题”，因为其“涉及国家主权”，“我们现在面临的网络危机是来自外部的控制能力、远程打击能力和摧毁国家重要基础设施的能力。因此我们面临着巨大的网络危机，包括对我国国家战略利益以及鉴别、决策和执行能力的威胁。”

勒德里昂同时称，该笔款项还将用于在法国雷恩建设一个网络防御人员培训中心，将网络防御尖端研究人员的数量增加三倍，拓展2012年组建的民间网络防御预备役组织等，“我们的目的是，动员越来越多有能力并值得信赖的人支持国家网络危机管理工作。”

9.2.3 亚洲地区网络安全监管动态

（1）日本拟设网络救援队，将应对东京奥运会网络安全

2014年1月16日，日本政府将成立“网络救援队”，负责帮助受到网络攻击的企业收集信息，分析原因以及协助修复，同时该部门也将服务于2020年东京奥运会。该救援队将设在日本独立行政法人情报处理推进机构（IPA）之下，编制为20人。着眼于6年后的东京奥运会，该救援队将建立提前防范网络攻击、并能尽快恢复正常的体制。网络攻击一旦发生，输电线和管道等电力和天然气基础设施受到影响。除了IPA平时负责信息收集的电力、天然气、化学、石油和重工业这5个行业之外，救援队还将收集通信、金融、航空、铁路、医疗等广泛行业的信息。此外，该救援队还将进入遭受网络攻击的工厂和发电站展开调查。根据企业的要求，它还将负责发生故障的系统的恢复工作。此前，IPA只能进入企业的总部，收集到的信息受到一定局限。

（2）日本政府新设“网络安全日”宣传打击黑客对策

2014年1月23日，日本政府在官邸召开官房长官菅义伟任主席的信息安全政策会议。为针对企业和个人开展有关打击黑客攻击措施的宣传警示工作，决定将2月的第一个工作日定为“网络安全日”，2014年为2月3日。菅义伟在会议伊始就黑客攻击表示，这是“在国家安全和危机管理上越来越重要的问题，有必要进一步加强支撑信息安全措施的人才培养和体制完善工作”。

（3）日本防卫省成立网络防御队，维护政府网络安全

2014年3月26日，日本防卫省为应对网络攻击，开始着手设立网络防御队的专门部队。防卫省大臣小野寺发表训话：“切实保卫好防卫省和自卫队的情报系统，是保卫日本和平稳定不可或缺的手段。”网络防御队是一支由防卫大臣直接管辖的90人规模的部队，防卫省及自卫队的电脑网络系统所遭受的监视或攻击是其防卫重点。为应对这样的攻击，网络防御队将24小时待命，并表示未来将与美国共同进行防卫网络攻击的模拟训练。

（4）日本政府计划提升组织级别，强化网络安全措施

2014年5月19日，日本政府信息安全政策会议在首相官邸召开会议，公布“网络安全推进体制的功能强化相关方针”草案。日本首相安倍晋三在会议伊始发言称，“从国家安全保障和危机管理的角度来看，确保安全是极为重要的课题，希望网络安全措施万无一失”。现行政策会议将法制化，于2015年前后升级为“网络安全政策会议”（暂定名）。除IT战略总部外，新的政策会议还将与国家安全保障会议（NSC）紧密合作，参与重要政策基本方针的起草以及在重大事件发生时查明原因。届时还将增设事务次官级别的“内阁网络安全官”（暂定名）一职管理事务局，负责与其他行政机关、民间及海外的协调工作。

（5）日自卫队将开启网络战训练，确保具备反击能力

2014年9月8日，为强化对“第五战场”的网络空间进行防御，防卫省确定方针，将于2016年度起引入网络攻击模拟训练。防卫省官员表示，希望进行针对强化网络防御能力的实效性演习，确保所有政府机构在遭遇来自他国的网络攻击时具备反击能力。

模拟攻击训练具体说来就是分别扮演实施攻击的“敌国”和展开防御的“自卫队”。“敌国”一方将真实地向自卫队的指挥系统输入病毒，由“自卫队”一方实施防御。训练中将设有称为“统裁”的裁判员一职，找出问题所在。之前进行的网络对策训练只停留在假想攻击发生，确认防御手段及信息传递顺序的程度。

防卫省已经在2015年度的政府预算概算要求中计入了“对妨碍网络空间利用能力进行相关调查”的经费，总计1000万日元（约合9.5万美元）。为真实再现网络攻击训练的环境，还将就如何实施病毒侵入、非法链接、DoS攻击等展开调查。委托民间机

构进行的调查讨论也在进行中。

（6）日本政府拟聘用“黑客”培养信息安全人才

2014年9月9日，日本政府将开始研讨直接聘用精通网络及电脑技术的“黑客”。基本方针为，在2015年度以日本内阁官房信息安全中心（NISC）下设的有聘任期限的职员或研究员岗位为主，吸纳“黑客”人才。

日本内阁官房信息安全中心负责综合应对网络攻击，此举旨在通过扩充专业人才，进一步强化对急速增加的网络攻击的应对能力。日本内阁官房信息安全中心有70人，其中一半的职员同时兼任其他省厅的职位。日本政府认为如果内阁官房信息安全中心可以直接聘用应届大学毕业生或企业的退休人员担任技术人员，将可以采取比目前更为严密、务实的防御对策。日本政府为了备战2020年的东京奥运会，正在加紧扩充和培养信息安全人才。

（7）日本国会通过《网络安全基本法》应对网络攻击

2014年11月6日，日本国会众议院表决通过《网络安全基本法》，旨在加强日本政府与民间在网络安全领域的协调和运用，更好地应对网络攻击。根据这项立法，日本政府将新设以内阁官房长官为首的“网络安全战略本部”，协调各政府部门的网络安全对策。“网络安全战略本部”还将与日本国家安全保障会议、IT综合战略本部等其他相关机构加强合作。《网络安全基本法》还规定电力、金融等重要社会基础设施运营商、网络相关企业、地方自治体等有义务配合网络安全相关举措或提供相关情报。这一法案由自民党、公明党、民主党等跨党派国会议员联合提出。日本国会参议院已于10月29日先行表决通过。

（8）日政府将设网络安全战略总部，严防网络攻击

2014年12月16日，为防备日益严重的网络攻击，日政府计划加强相关体制，并于16日通过内阁会议，决定将现在的情报安全政策会议于2015年1月9日升级为网络安全战略总部。此外，日本政府还决定加强现有的“内阁官房情报安全中心”（NISC）的职权，赋予其法律权限。2015年1月9日还将专门设置“内阁网络安全中心”。就应对网络攻击问题，日本国内一直指责各省市政府与民间企业等合作不足。日本政府认

为随着2020东京奥运会临近，日本可能发生大规模网络攻击事件，因此应强化应对措施，确保万无一失。

（9）韩国《2014信息通信、放送技术振兴实施规划》出炉

2014年3月，韩国未来创造科学部发布了《2014信息通信、放送技术振兴实施规划》，拟投入11.764亿美元促进ICT领域10大技术的发展。该规划内容包括：ICT领域的战略技术开发、标准化、人才培养和基础环境建设等方面。具体投入情况是战略技术开发将投入7.499亿美元，推进先导型标准化将投入0.278亿美元，创意融合及人才培养将投入1.004亿美元，ICT研究基础环境建设2.983亿美元等。该规划提到的10大技术为全息照片、数字内容2.0、智能型软件、物联网平台、大数据云服务、第五代移动通信、智能网络、感性终端技术、智能型ICT融合模块和应对网络攻击技术等。

（10）韩国政府拟帮助企业提高网络防御能力

2014年2月，韩国未来创造科学部从2月17日起与3家移动运营商、门户网站和网络安全企业等40多家企业和机构联合实施应对网络攻击的演习。韩国未来部将假设黑客攻击和分布式拒绝服务攻击（DDoS）、利用恶性代码泄露信息、破坏系统等三个阶段的网络攻击情况，测试企业网络攻击应对能力。

未来部还计划向网络攻击应对技术较差的企业转让技术，从2月15-21日通过韩国网络振兴院（KISA）征集有意传授4种信息保护技术的企业。被转让的技术包括：探测网页里隐藏的恶性代码的MC Finder，检查Web服务器目录中的文件并寻找黑客攻击手段的WHISTL，通知特定网页风险信息的WebCheck，探测被安装在智能手机中的恶性应用软件的Phone Keeper。

韩政府还计划进一步提高多数企业的网络安全技术水平，大力发展信息保护产业，并检验企业的个人信息保护能力。截至2月底，未来部将针对拥有大量个人信息的15家企业的信息保护管理系统（ISMS）进行检查。而从13日起，未来部将对已获得ISMS认证的130多家企业中检查结果不佳的企业进行检查，并取消存在问题的企业的ISMS认证。

（11）韩国政府拟建立网络安全队伍，防黑防毒防诈骗

2014年2月26日，韩国未来创造科学部将建立由300名专家组成的网络安全专家队

伍，以防范有关部门和单位发生个人信息泄露、遭到黑客攻击、感染病毒等。

韩国政府计划召集经验丰富的专家，将他们培养成维护网络安全的顶尖人才。这一专家队伍将隶属于韩国互联网振兴院，由从事保护信息工作5年以上者、国内外防黑客大赛获奖者、具有信息通信网络安全相关专门知识等人才组成。专家队伍负责的工作分为网络金融诈骗、软件、互联网、移动服务、数据恢复工作、高级持续性威胁（APT）等领域。

若发生黑客攻击、感染病毒等重大网络安全事件，专家队伍的部分成员将同有关部门的公务员、韩国互联网振兴院的工作人员联合成立“官民联合调查团”。虽然专家队伍的成员是普通人身份，但有关事件发生时，他们将授权出入事故现场并调查事因。韩国未来创造科学部认为，队伍的成立将有助于防范金融领域个人信息泄露、短信诈骗等网络安全事件。

（12）新加坡政府将设监控中心加强对抗黑客能力

2014年8月27日，新加坡政府将在2014年内设立一个监察与运作控制中心，加强监管政府机构的网站与网络系统，提高这些机构对抗恶意攻击的能力。新加坡通讯及新闻部长雅国博士26日在资讯通信保安研讨会致辞时，宣布成立新的“监察与运作控制中心”。控制中心将同新加坡网络监察中心联合应对网络攻击行动。

将在2015年完成提升工作的新加坡网络监察中心，负责全天候监察新加坡政府部门与法定机构的网络系统，一旦发现有恶意软件或黑客入侵，就会向监察与运作控制中心通报。控制中心拥有一套对抗网络攻击的全方位方案，其接获通知后，会结合从其他渠道取得的情报，采取一系列综合性的抵御措施。

新加坡网络监察中心成立于2007年，新加坡资讯通信发展管理局在2014年6月委任e-Cop网络保安公司，提升监察中心的探测能力，拟于2015年1月完成。监察中心将能监察到新加坡政府网站是否被人篡改内容或连接到其他网站，也能监察与分析网络系统内的可疑文件。

（13）新加坡建立网络安全研究中心

2014年12月3日，新加坡政府宣布将建立一个网络安全研究中心以保护系统正常运转，将新加坡打造成智能国家。新加坡的“智能国家平台”将分阶段开发，第一阶段

集中在互联互通和传感器方面，新加坡资讯通信发展管理局（IDA）计划2015年年底前在全国安装多达1000部传感器。传感器对政府各项目来说不可或缺，还可帮助一些地区加强监管，监控新加坡河发生洪灾的风险。该传感器系统预计会给各部门节省大量支出，因为基础设施成本将由各机构平分。大数据和分析预计会在完善日常的系统与设施中起到重要作用。企业和政府机构可以这些平台为基础，创建检测收集和解释数据的新方法，为公众提供更好的服务。

（14）印度拟允许安全部门访问用户手机数据

2014年3月19日，根据印度电信安全政策指导草案，印度政府计划部署系统并推出监管政策，允许执法部门跟踪手机用户并实时接入针对性通信、文本信息、信息数据，甚至增值服务。

印度电信部（DoT）是在内政部对执法部门在未获授权的情况下拦截通信表达强烈保留态度后，提出了全面规范草案。在一份涉及国家安全的草案版本中，印度电信部称该政策将会部署有效的系统、流程以及监管政策，以确保在必要情况下，拥有以特定的精确度追踪电信用户或设备的身份、固定地址和当前位置的能力。由于开放的电信环境易实现对网络的攻击，进而破坏网络信息，所以印度计划深入解决电信安全问题。除了执法部门要面对复杂加密技术的挑战，一项全面的电信政策还涉及与电信安全相关的其他影响。这项政策还将对电信网络中和储存在系统及设备中的信息与数据流（包括已经解密的信息）提供分析。随着减少延迟和防泄露最新技术与系统的应用，安全部门及时分析信息的能力将会进一步增强。

同时，印度还将组建和部署负责电信设备测试的安全认证中心，负责拦截和监视的中央监控系统，以及负责检测分析网络攻击、互联网流量劫持和电信欺诈的应急响应小组（CERT）。根据这份草案，基础电信企业必须将其网络受到攻击、侵入以及欺诈的信息与电信行业的应急响应小组、国家计算机应急响应小组以及国家网络协调中心（NCCC）等政府部门分享。通过分享，相关部门可以实现对境内ISP全部网络流量的监控，并在发现安全威胁时，及时向政府发布“行动警报”。

（15）印度拟成立国家网络协调中心

2014年8月18日，印度莫迪政府拟出资95亿卢比（约合9.5亿人民币）设立国家网

络协调中心。这一举措是在印度近年来频频遭受网络攻击，尤其是最近披露的印度人民党曾遭受美国国家安全局窃听的背景下做出的。

新成立的国家网络协调中心将与现有的印度情报局（IB）和印度计算机应急响应小组（CERT-IN）加强协调，通力合作，确保印度关键部门的网络安全。印度政府已经向内阁安全委员会（CCS）提交了一份长达250页的报告。报告建议设立国家网络协调中心，预计很快获得批准。根据该报告，国家网络协调中心将由一名副部长级的官员领导，旨在加强该中心与其他部门的协调能力，便于调动各方资源，加强网络安全。

9.2.4 澳洲、非洲地区网络安全监管动态

（1）澳参院通过反恐法案，情报机构可全面监控互联网

2014年9月27日，澳大利亚参议院通过一套更严厉的反恐法案，允许澳洲情报机构全方位监控互联网，而泄露国家机密者将面对长达10年的监禁。

根据新法案，澳洲安全情报机构将被赋予更大的权力，在监控某个目标时，可在仅获得一次授权的情况下，登录电脑网络中不限数量的电脑。由于法案没有列明“电脑网络”的定义，这导致人权组织、律师、学者和媒体批评该法案基本上允许情报机构监控整个互联网。新法案允许情报机构进入受监控的电脑，复制、删除或修改其中的数据。情报机构也有权干扰目标电脑，并通过不是监控对象的第三方电脑，潜入目标电脑。新法案还规定，任何人包括记者、告密者或博客，若“不慎泄露与特别情报行动相关的信息”，将面对长达10年的监禁。暴露安全情报组织特工身份的人，最高刑期将从目前的1年延长至10年。另外，安全情报组织将在某些情况下获得刑事与民事豁免权。

许多人担心，安全情报组织会因此滥用其监控权。对新法案投反对票的澳洲绿党批评新措施过于极端，将导致情报机构的“权力不断扩张”。不过澳洲司法部长布兰迪斯回应说，在这个“新危险时代”，赋予保护国家的机构所需的权力和能力是至关重要的。澳洲越来越担忧“伊斯兰国”等极端组织所构成的威胁。澳洲警方最近在悉尼和布里斯班展开有史以来最大规模的反恐突击行动，粉碎了“伊国”组织准备挟持澳洲平民并将其斩首的恐怖阴谋。

（2）澳大利亚6年来首次全面复核网络安全

2014年11月27日，澳大利亚总理阿博特（Tony Abbott）宣布对网络安全进行复核，以更好地保护澳大利亚的政府及企业免受网络攻击。这是澳大利亚6年来首次进行网络安全问题的复核。据悉，澳大利亚包括澳讯（Telstra）在内的一些大公司、澳大利亚商会（BCA）和位于美国的计算机安全公司思科（Cisco）等，将和澳大利亚政府的技术专家合作以检视澳大利亚抵抗网络攻击的能力。阿博特表示，在越来越多人的日常生活都和网络休戚相关之际，数据安全及其运行的IT网络对澳大利亚人的生活至关重要。他还称，“澳大利亚确实面临（网络攻击的）威胁，而且威胁变得越来越多，越来越严重。”阿博特在进一步解释澳大利亚所面临的网络攻击威胁时，还援引了澳大利亚信号局（ASD）的数据指出，2013年该部门处理了940宗重大的网络安全“事件”，较此前一年增加了37%。澳大利亚政府此次复核的结果将纳入国防白皮书，而且政府目前还在对更广泛领域的国家安全问题进行复核。据政府估计，目前网络犯罪给澳大利亚造成的年损失高达12亿澳元。

（3）东非国家加强网络犯罪管控，加速立法程序成立管理部门

2014年6月，肯尼亚、乌干达和坦桑尼亚等东非国家正加速网络立法程序，该网络法律涵盖数据安全、网络犯罪、信息系统和电子交易。乌干达通信部部长詹姆斯表示，立法已接近尾声。肯尼亚《2014年网络犯罪和计算机相关攻击议案》草案即将提交议会审议。早在2011年，乌干达政府就通过了三部网络法律，目前更严厉的网络犯罪法正在制定中。坦桑尼亚第一部网络犯罪法《数据保护与隐私法》2013年年底启动制定程序，随后还将制定《计算机和系统法》和《电子转账法》等，构成完整的网络法律体系。

与此相对应，东非国家纷纷成立网络管理部门加强管控。肯尼亚通信委员会已经成立了网络安全指导委员会。肯尼亚主持的一个网络犯罪管理工作组正在协调旨在根除东非共同体5国网络犯罪的活动。肯尼亚还带头建立了东非地区的国家计算机应急小组，主持东非通信组织网络安全工作。2014年2月，东非地区打击网络犯罪机构负责人工作组会议在卢旺达首都基加利举行。会议指出，工作组的首要目标是为各国打击网络犯罪执法部门提供一个中央平台，共享信息，讨论打击网络犯罪的联合战略。此外，布隆迪和乌干达也在成立计算机事件应急小组。

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

2014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2014年12月，全国共有586家信息通报工作成员单位（2013年是432家），形成了较稳定的信息通报工作体系。与2013年相比，新拓展安全企业、增值电信企业、域名注册服务机构共154家单位成为信息通报工作成员单位。自2011年1月起，CNCERT/CC建设并启用了网络安全协作平台，试行开展电子化信息报送工作。2012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。2014年，CNCERT/CC建设了网络安全协作平台二期，为通报成员单位报送信息提供更大便利。全国587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（124家）	中国电信集团公司及各省分司、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（20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、北京新网数码信息技术有限公司（湖北）、阿里巴巴通信技术（北京）有限公司[31]、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、

[31] 原北京万网志成科技有限公司。

（续表）

域名注册管理和服务机构（20家）	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、阿里巴巴通信技术（北京）有限公司（湖北）
增值电信业务经营企业（209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、大庆油田信息技术公司、黑龙江省农垦通信有限公司、大庆中基石油通信建设有限公司、大庆卓创多媒体科技有限公司、牡丹江东北亚网络技术有限公司、蓝天科技公司、哈尔滨工程大学科技园发展有限公司、佳木斯海讯网络科技有限公司、广东世纪龙信息网络科技有限公司、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、厦门鑫飞扬信息系统工程有限公司、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）、河北省中誉通信有限公司、润泽科技发展有限公司、河北朗为数据通信科技有限公司、华北石油通信公司、河北广电信息网络集团股份有限公司、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、江西缴费通信息技术有限公司、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、

（续表）

增值电信业务经营企业（209家）	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、江西嘀嘀叭叭科技有限公司、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、大连正迅网络科技有限公司、大连一海通科技有限公司、哈尔滨市假日旅游咨询服务有限公司、哈尔滨朗新科技发展有限公司、黑龙江龙采科技有限公司、农垦北大荒数据有限公司、哈尔滨三雷科技有限公司、牡丹江易联网络科技服务有限公司、黑龙江亿林网络技术有限公司、黑龙江省公众信息产业有限公司、哈尔滨工程大学三金高新技术有限责任公司、哈尔滨国裕数据技术服务有限公司、上海北信源信息技术有限公司、杭州海康威视数字技术股份有限公司、厦门易企网络科技有限公司、泉州万紫千红文化传播有限公司、漳州市众为网络服务有限公司、福州慧林网络科技有限公司、三明市新艺技术贸易有限公司、厦门好景科技有限公司、福州天寻网络科技有限公司、莆田市逐日网络有限公司、厦门中瑞互联科技有限公司、福建省力天网络科技有限公司、福建光通互联通信有限公司、福建省普集网络科技有限公司、英特易信息科技（厦门）有限公司、江西永天信息产业有限公司、南昌瀚天科技有限公司、江西锌瑞文实业有限公司、江西赢家网络文化传播有限公司、南昌东方信息服务有限公司、南昌彩视信息科技有限公司、南昌诺霖信息科技有限公司、江西圣翔元科技有限公司、南昌驰顺网络科技有限公司、江西腾亿科技通信有限公司、南昌市创亚科技有限公司、南昌市思锐广告有限公司、江西盛世腾龙信息技术有限公司、江西图讯信息科技有限公司、江西互联科技有限公司、南昌惊蛰网络科技有限公司、江西云顶通科技有限公司、南昌畅速网络科技有限公司、江西天胜传媒发展有限公司、江西如石网络科技有限公司、南昌市益智信息有限公司、南昌天峰信息科技有限公司、南昌金启软件有限公司、南昌易速科技有限公司、江西行知教育在线有限公司、江西家秀网络科技服务有限公司、江西赣源科技有限公司、郑州鼎达科贸有限公司、河南省金时通电子商务有限公司、河南瑞博科技有限公司、郑州易方科贸有限公司、中原网、湖北兆升凯莱科技有限公司、湖北五五互联科技有限公司、襄阳市佰网信息科技有限公司、湖北众远信息科技有限公司、武汉长城宽带网络服务有限公司、湖北长江时代通信有限公司、武汉商启网络信息有限公司、深圳市安之天信息技术有限公司、西宁网联电子信息有限公司、青海亿网网络有限公司、青海省通信服务公司、乌鲁木齐众维信息产业有限公司、乌鲁木齐路桥信息有限公司、乌鲁木齐中科网网络有限公司、新疆欧凯网络服务有限公司、新疆轩驰网络技术有限责任公司、乌鲁木齐新科德软件有限公司、新疆天山智汇信息科技有限公司

（续表）

非经营性互联单位（5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、中国科技网、河南省教育科研计算机网网络中心、
安全企业（187家）	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）、北京瑞星信息技术有限公司（贵州）、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安徽分公司、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、北京神州绿盟科技有限公司贵州分公司、北京神州绿盟信息安全科技公司青海分公司、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黑龙江分公司、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科技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、北京天融信科技有限公司山西分公司、北京网秦天下科技有限公司、北京网秦天下科技有限公司（北京）、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（北京）、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）、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）、北京知道创宇信息技术有限公司（青海）、北京知道创宇信息技术有限公司（湖南）、北京知道创宇信息技术有限公司（贵州）、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南京分公司、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（北京）、哈尔滨安天信息技术有限公司（天津）、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（安徽）、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）、哈尔滨安天科技股份有限公司（四川）、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、猎豹移动公司[32]、浪潮集团有限公司、北京网御星云信息技术有限公司、

[32] 原金山网络科技有限公司。

（续表）

安全企业（187家）	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（安徽）、奇虎360软件（北京）有限公司（北京）、奇虎360软件（北京）有限公司（天津）、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）、奇虎360软件（北京）有限公司（四川）、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）、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（安徽）、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（贵州）、恒安嘉新（北京）科技有限公司（青海）、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、南京铱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）、中国电信集团系统集成有限责任公司（江苏）、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（青海）、深圳市深信服电子科技有限公司（新疆）、深圳市深信服电子科技有限公司（北京）、深圳市深信服电子科技有限公司（安徽）、深圳市深信服电子科技有限公司（河北）、深圳市深信服电子科技有限公司（上海）、深圳市深信服电子科技有限公司（江苏）、深圳市深信服电子科技有限公司（湖北）、深圳市深信服电子科技有限公司（湖南）、深圳市深信服电子科技有限公司（广东）、深圳市深信服电子科技有限公司（四川）、深圳市深信服电子科技有限公司（广西）、深圳市深信服电子科技有限公司（贵州）、深圳市深信服电子科技有限公司（甘肃）、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）、杭州安恒信息技术有限公司（北京）、杭州安恒信息技术有限公司（天津）、杭州安恒信息技术有限公司（河北）、杭州安恒信息技术有限公司（贵州）、杭州安恒信息技术有限公司（甘肃）、杭州安恒信息技术有限公司（辽宁）、杭州安恒信息技术有限公司（广西）、杭州安恒信息技术有限公司（青海）、江苏国瑞信安科技有限公司、趋势科技中国有限公司、趋势科技中国有限公司（江苏）、上海众人网络安全技术有限公司、上海韶武信息技术有限公司、南京欧奥信息科技有限公司、北京亚鸿世纪科技发展有限公司、西安瑞天信息安全科技公司、甘肃海丰信息科技有限公司、北京山石网科信息技术有限公司、中电长城网际系统应用有限公司

（续表）

其他（10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、上海市计算机软件评测重点实验室、电信科学技术第一研究所、河南省互联网协会、四川省互联网协会、四川省通信行业协会

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安全漏洞信息共享知识库，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。

2014年年初，CNVD完成成员单位改选，新增17家，成员单位共计41家。CNVD成员单位分为技术合作组和用户支持组两类。在用户支持组中新建政府高校、基础电信企业、网络设备、工业控制、邮件系统、电子政务、增值电信7个用户组，同时CNVD继续向CNVD成员单位开放漏洞库数据共享接口。2014年CNVD全年新增信息安全漏洞9163个，较2013年的7854个增加16.7%，其中高危漏洞2394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1300余次漏洞分析和验证工作。2014年，CNVD继续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、分析验证和处置工作。CNVD网站共发展1430余个白帽子注册用户以及109个行业单位用户，协调处置9000余起涉及国务院部委、地方省市级部门、证券、金融、民航、保险、税务、电力等重要信息系统以及基础电信企业的漏洞事件，有力地支撑了国家网络信息安全监管工作。依托CNCERT/CC国家中心和分中心的处置渠道，有效降低了上述单位信息系统被黑客攻击的风险，挽回的潜在经济损失以千万元计（按信息泄露和服务器肉鸡价值估计）。此外，CNVD官方微博账号发布100余条重要漏洞预警信息,并对一些重大漏洞事件作出积极回应。

截至2014年12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技术合作单位（15家）	CNCERT/CC 国家信息技术安全研究中心 北京信息安全测评中心 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 北京天融信网络安全技术有限公司 北京奇虎科技有限公司 沈阳东软系统集成工程有限公司 恒安嘉新（北京）科技有限公司 哈尔滨安天科技股份有限公司 北京知道创宇信息技术有限公司 杭州安恒信息技术有限公司 北京数字认证股份有限公司 看雪安全网站 上海交通大学网络信息中心
CNVD用户支持组（26家）	政府高校组： 中国工程物理研究院计算机应用研究所 中国教育和科研计算机网 中国科技网 基础电信企业组： 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 网络设备组： 华为技术有限公司 北京网康科技有限公司 杭州华三通信技术有限公司 深圳市深信服电子科技有限公司 工业控制组： 北京首钢自动化信息技术有限公司 北京力控华康科技有限公司 北京三维力控科技有限公司 北京亚控科技发展有限公司 西门子中国研究院

（续表）

CNVD用户支持组（26家）	邮件系统组： 北京安宁创新网络科技有限公司 北京亿中邮信息技术有限公司 电子政务组： 北京拓尔思信息技术股份有限公司 增值电信组： 上海巨人网络科技有限公司 上海盛大网络发展有限公司 网之易信息技术(北京)有限公司 北京搜狐互联网信息服务有限公司 新浪网技术（中国）有限公司 百度在线网络技术（北京）有限公司 北京暴风网际科技有限公司 腾讯控股有限公司

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了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。

2014年，ANVA组织基础电信企业、安全企业、应用商店等联盟成员，支撑2014年工业和信息化部、公安部和工商总局三部委联合开展的移动互联网恶意程序专项治理工作，持续开展黑白名单信息共享，移动应用程序开发者第三方数字证书签名与验证试点等工作。2014年，ANVA对外发布移动恶意程序黑名单38372条，放马恶意地址黑名单90419条，移动恶意程序传播源地址黑名单1187条，与中国信息通信研究院、中国互联网协会等单位共享黑名单数据，并要求应用商店接入ANVA网站查看并及时下架黑名单中的移动恶意程序。另一方面，ANVA于2013年启动了移动应用自律白名单的工作，旨在建立安全的移动互联网生态，2014年ANVA持续进行白名单工作，组织

包括11家主流安全企业在内的白名单工作组对中国农业银行、搜房网等近百余家移动互联网公司的白名单申请进行了审查，并通过中国农业银行、百度理财、搜房网、奇虎360共4家企业的4款数字证书进入白名单。截至2014年，移动互联网白名单生态系统已初步建立，包括中国移动MM商城、360手机助手、腾讯应用宝、百度应用中心等20余家主流应用商店均已对白名单应用进行标识，并设立白名单专区，引导用户安装使用安全可靠的白名单应用。

在2014年移动恶意程序专项治理工作期间，ANVA支撑工业和信息化部通信保障局开展移动应用程序开发者第三方数字证书签名与验证试点工作，协调联盟中12家应用商店、5家手机安全软件厂商参与工作，组织数字证书认证服务机构、应用商店和安全企业等单位论证移动签名技术方案，参与制定《Android应用程序开发者第三方数字证书签名、验证和标识规范（试行）》，并于2014年10月24日组织召开“移动互联网应用程序开发者第三方数字证书签名与验证试点宣介会”。专项行动期间，百度手机助手、360手机助手、移动MM商城、联通沃商店等知名应用商店已经实现了对上架试点应用程序的签名验证和标识功能，数十款经过第三方数字证书签名的应用程序在参与试点的应用商店上架并标识。

在联盟成员发展方面，2014年ANVA积极吸纳南京翰海源、北京CA等网络安全领域企业加入联盟，总计新增3家企业，截至2014年12月，ANVA联盟成员单位数量已达40家，成员单位具体情况见表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

（续表）

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
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（原信息产业部）批准，

2004年CNCERT/CC首次面向社会公开选拔了一批国家级、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分别举办了第二届、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了积极贡献，在国家重大活动期间为保障网络安全发挥了重要的技术支撑作用。

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启动了第五届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，受到了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。评选工作有效促进了各单位间的了解和沟通，增强了各单位的竞争和服务意识，推动了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。

2014年，各应急服务支撑单位依托自身技术力量，积极拓展网络安全业务，支撑CNCERT/CC开展日常监测分析、信息通报、恶意代码分析和事件应急处置工作。9月，国家级支撑单位及部分省级支撑单位，协助CNCERT/CC顺利完成了对部分重要政府网站的网络安全专项检测工作。应急服务支撑单位的工作，对健全公共互联网网络安全事件应对能力，强化公共互联网网络安全应急技术体系建设，提高社会各部门各行业网络安全意识，起到了积极作用。

第五届CNCERT/CC网络安全应急服务支撑单位见表10-4（有效时限为2013年7月3日至2015年7月3日）。

表10-4　第五届CNCERT/CC网络安全应急服务支撑单位列表（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

（续表）

单位名称	级别	证书编号
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[33]	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
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
南京铱迅信息技术股份有限公司[34]	省级	CNCERT-2013-150703SJ020
青岛速科评测实验室有限公司	省级	CNCERT-2013-150703SJ021

[33] 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”。
[34] 原南京铱迅信息技术有限公司，2014年9月19日更名为“南京铱迅信息技术股份有限公司”。

（续表）

单位名称	级别	证书编号
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）CNVD 2014年春季工作会议在京召开

2014年2月26日，CNVD在北京组织召开CNVD 2014年春季工作会议。会议由CNCERT/CC和中国互联网协会网络与信息安全工作委员会联合主办，工业和信息化部通信保障局相关领导莅临指导，国内网络安全研究机构、基础电信企业、网络安全企业以及软硬件厂商共40余家单位的近百名代表受邀参加本次会议。

工业和信息化部通信保障局刘伯超副处长为会议致辞，他指出，网络安全业界各方和相关厂商要进一步加强自律，配合行业主管部门和国家互联网应急中心的工作，逐步规范漏洞信息发布和应急处置流程。国家互联网应急中心王明华处长作了题为 “漏洞的价值”的发言。CNCERT/CC对2013年CNVD工作情况作了整体介绍。

同时，CNVD对各成员单位及安全研究者为平台的建设和发展提供的支持表示感谢。北京启明星辰信息安全技术有限公司、哈尔滨安天科技股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、恒安嘉新（北京）科技有限公司5家单位荣获 “CNVD 2013年漏洞信息报送突出贡献单位”称号；北京奇虎科技有限公司、北京知道创宇信息技术有限公司、上海交通大学网络信息中心、乌云网站4家单位荣获 “CNVD 2013年原创漏洞发现突出贡献单位”称号。

（2）CNCERT/CC发布《2013年我国互联网网络安全态势综述》

2014年3月28日，CNCERT/CC在京举办了“2013年我国互联网网络安全态势综述”（简称“态势综述”）发布会，对2013年我国互联网网络安全的总体形势和主要特点进行了发布和说明。来自政府机构、重要信息系统运行部门、电信运营企业、域

名注册管理和服务机构、行业协会、互联网企业和安全厂商等47家单位的专家和代表出席了发布会。CNCERT/CC运行部王明华主任对态势综述进行了详细地阐述和讲解，并回答了媒体提问。

态势综述从CNCERT/CC视角出发，依据CNCERT/CC和通信行业相关单位在日常工作中积累的数据和资料总结编撰而成，分别从基础信息网络、公共互联网、移动互联网、经济信息安全、政府网站、境外攻击威胁6个方面，总结概括了2013年我国互联网网络安全威胁的特点，展望了2014年值得关注的威胁热点，提出了若干对策建议，具有较为鲜明的行业特色和技术特点。

当前我国互联网发展迅速，网络化和信息化水平不断提高，网络安全保障工作的重要性日益凸显。CNCERT/CC希望该态势综述能够帮助政府机构、重要信息系统部门、各相关行业和广大网民了解、掌握我国互联网网络安全面临的主要威胁和发展趋势，进一步提高对网络安全的重视，加强自身网络信息系统安全管理和防护，共同维护我国互联网网络安全。

（3）首都网络安全论坛在京举行

由北京市公安局、中国电子信息产业发展研究院、公安部第一研究所联合主办，《中国经济和信息化》杂志社和《警察技术》杂志社共同承办的首都网络安全论坛于2014年4月28日在北京举行。作为“4.29首都网络安全日”系列活动中的一项重要内容，本次论坛以“网络安全就是国家安全”为主题，以首都重要网络和系统安全需求交流为核心内容，以“需求梳理与对接”为工作方法加强信息安全建设，旨在从个人、企业、产业、法律4个层面全方位整合、发动、利用好各方的社会资源，提升全民网络安全意识，引导行业企业不断创新，提高网络安全防护技术能力，展示网络安全最新技术和成果。

（4）2014年中国计算机网络安全年会在广东汕头召开

2014年5月28日，2014年中国计算机网络安全年会（第11届）在广东省汕头市召开。工业和信息化部总工程师张峰出席大会并作主旨报告。张峰在报告中指出，2014年是我国接入国际互联网20周年，如今我国已成为名副其实的网络大国，然而，互联网的发展给经济社会带来一系列挑战，网络安全问题日益复杂，云平台、社交网络、

移动互联网等新技术新业务快速发展，不断带来新的安全风险。前不久，中央网络安全和信息化领导小组已正式成立，要深刻领会习近平总书记关于“没有网络安全就没有国家安全”、“网络安全和信息化是一体之两翼，驱动之双轮，必须要统一谋划、统一部署、统一推进、统一实施”的重要讲话精神，从保障国家安全，维护公众利益，促进信息化发展的高度，充分认识新形势下做好网络安全工作的重要性和紧迫性，为把我国建设成为网络强国而努力奋斗。随后，张峰简要回顾了近年来工业和信息化部网络安全工作的总体情况，并进一步提出网络安全领域的5点工作要求：一是积极应对网络安全威胁，大力加强关键信息基础设施安全保障；二是增强自主创新能力，提高信息技术和服务的安全可控水平；三是开展移动互联网恶意程序治理，营造健康的移动生态环境；四是加强业界合作，健全网络安全事件协调联动处置机制；五是加强国际合作，努力提高我国在网络空间国际治理中的话语权。张峰代表工业和信息化部对本次年会的成功召开表示祝贺，并希望参会代表利用年会信息共享和技术交流的平台，畅所欲言，交流思想。

中国工程院邬贺铨院士、倪光南院士分别应邀以《大智移云时代网络安全新挑战》、《智能终端操作系统与信息安全》为题作大会报告。来自国家计算机网络应急技术处理协调中心、广东省通信管理局、亚太地区计算机应急响应联盟的领导、专家以及多个网络安全企业的技术专家，分别围绕大数据、互联网环境治理等网络安全热点议题发表了看法。

年会由CNCERT/CC主办，历经11年发展，目前已成为国内外网络安全领域技术、业务交流的重要平台。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600余人参加了本次会议。会上还举行了汕头大数据产业发展咨询专家聘请仪式。

（5）中国网络安全法制建设研讨会召开

2014年6月13日，根据我国网络安全立法和司法实际需要，经最高人民法院批准，最高人民法院中国应用法学研究所与新华社·望智库在京共同举办中国网络安全法制建设研讨会。最高人民法院副院长李少平出席会议。李少平指出，党中央高度重视网络安全问题，网络安全和信息化问题已经上升到了国家战略，事关国家安全、国家发

展和广大人民群众工作生活，需要运用法律手段予以解决。人民法院要不断总结新形势下应对网络安全、处理涉及网络犯罪的司法经验，通过司法解释或提出立法建议来完善我国网络安全法制，实现“司法反哺立法”，为我国建设网络强国提供有力的司法保障。会议主要围绕新时期我国网络安全形势、网络基础设施保护、防止网络泄密、打击网络恐怖主义、惩治网络谣言、网络色情、网络信息滥用与欺诈等违法犯罪行为，以及强化网络知识产权保护制度建设等几项议题展开。与会专家结合国际安全环境和我国实际，就我国网络安全立法方向和制度构建提出了若干建设性意见。

（6）首届“中国网络安全与媒体责任”活动启动

由中国报业协会、中国互联网协会共同主办的2014首届“中国网络安全与媒体责任”公益活动于2014年6月30日在京启动。据介绍，首届活动以“自警、自律、自信”为主题，旨在深入探讨传统媒体、新媒体如何应用网络安全与信息发展技术，提升传统媒体的版权维护意识与能力，以及在新媒体融合发展中如何进行风险防范。中国互联网协会副理事长高新民称，中国互联网发展势头迅猛，到2020年网民普及率有望达到70%，网络安全成为面临的一大挑战，主要表现在：网络攻击手段愈发隐蔽，网络谣言防不胜防，网络诈骗、欺诈时有发生，网络色情、暴力则对青少年构成危害，此时媒体应承担起网络安全责任，提升公众网络安全防范意识和能力。中国报业协会驻会副会长石国雄指出，此活动是在国家提出重视网络安全的大背景下展开的，通过社会调研、网络技术与经验交流等活动，提出新媒体时代下网络安全对策、建议及安全防范路径。该活动持续3个月，发布《中国传媒网络安全与社会责任倡议书》，探索成立“中国传媒网络安全联盟”。

（7）中国互联网协会互联网工业应用委员会成立大会在京召开

2014年8月12日，中国互联网协会互联网工业应用委员会成立大会在北京召开。全国政协常委、工业和信息化部原部长李毅中以及工业和信息化部党组成员、总工程师朱宏任到会指导，中国互联网协会副理事长高新民，工业和信息化部信息中心主任孙蔚敏、中国家用电器协会秘书长徐东生出席会议并讲话。来自委员会首批成员单位、相关行业协会和企业，以及新闻媒体的百余名代表参加了会议。会议审议通过了《中国互联网协会互联网工业应用工作委员会工作规则》，选举产生了第一届委员会领导机构。互

联网工业应用委员会是由国内从事互联网工业应用推广、产品技术研发、发展政策研究、科研机构和社会团体组成的中国互联网协会下属专业组织。委员会将致力于凝聚和引导互联网及工业行业的社会力量，制定支持互联网与工业融合发展的标准规范，推动互联网与工业融合创新，深化互联网技术在工业企业和行业管理中的应用，探索工业全产业链与互联网结合的新业态，助力工业生产的网络化、智能化转变，推进互联网与工业的产用互动和协调发展，为我国抢占产业革命先机，从工业大国向工业强国迈进积极贡献力量。截至目前，已申请加入“中国互联网协会互联网工业应用委员会”的成员单位有50余家，涵盖装备制造、电子制造、家电、软件等领域诸多企业，以及基础电信企业、大型互联网企业和有关行业协会、行业媒体等诸多领域。

（8）中国互联网协会网络安全分论坛在京召开

2014年8月27日，由中国互联网协会主办、CNCERT/CC协办的中国互联网协会网络安全分论坛，以“共筑网络安全空间 助力网络强国建设”为主题在北京召开，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300余人参加了本次会议。

工业和信息化部通信保障局处长付景广在会上表示，在我国互联网高速发展的同时，安全始终是无法回避的重大课题。工业和信息化部将积极维护公共互联网网络安全环境，针对黑客地下产业链、移动恶意程序等危害公共安全和用户利益的问题，采取相关措施，加强综合治理；遏制网络攻击威胁源头，建立移动互联网恶意程序监测处置机制，健全钓鱼网站的监测与惩治机制。来自CNCERT/CC的何能强工程师在大会上介绍了2014年上半年CNCERT/CC移动互联网的治理情况。互联网实验室创始人、董事长方兴东，腾讯高级副总裁丁珂及360公司副总裁谭晓生分别应邀作了大会报告。来自中国科学院研究生院、信息安全国家重点实验室、南京邮电大学、复旦大学的学者，围绕如何建设网络强国发表了看法。

（9）聚焦大数据安全，2014互联网安全大会在京召开

2014年9月24-25日，亚太信息安全领域年度峰会——2014中国互联网安全大会(ISC 2014）在北京召开。作为亚太地区互联网安全行业大会，本届ISC吸引了包括美国首任国土安全部部长汤姆·里奇、计算机病毒之父弗雷德·科恩，以及中国工程院

院士邬贺铨、公安部网络安全保卫局总工程师郭启全、国家计算机网络安全专家云晓春等数百位国内外顶级信息安全专家出席。据了解，中国互联网安全大会是亚太地区规模最大的信息安全主题技术盛会。首届ISC大会于2013年举行，以历时3天、1.2万人次参加的规格与规模，成为轰动国内信息安全界的盛会和安全人员的重要技术交流盛会。2014年中国互联网安全大进一步提升了会议规格、规模和专业性。除保留移动安全、Web安全、企业安全、云与数据、软件安全、APT等热门安全议题外，还首次将视角触及到国家网络空间战略等高端话题，以及工控安全、车联网安全、信息安全立法等新兴热点，共设置12个论坛，另外还增加了攻防挑战赛、安全训练营、车联网系统破解赛等新项目。本届大会超过2万人次参会，超过100场国内外安全专家的精彩演讲和现场交流。ISC 2014大会主题为“互联世界，安全第一”，聚焦在互联网时代、大数据背景下的信息安全所面临的全新挑战和问题，峰会深入探讨了智慧城市、互联网金融、数字医疗、可穿戴计算等业界关心的问题。

（10）首届全国信息安全技术论坛在郑州举行

2014年10月9日，由中国电子学会主办，全国信息安全技能培训考试项目办公室等单位承办的“首届全国信息安全技术论坛”在郑州举行，就安全问题展开激烈讨论。中国工程院院士沈昌祥、河南省工业和信息化厅副厅长刘昱旻等国内多位知名领导和专家参加了此次论坛活动。来自中国互联网网络信息中心发布的报告显示，2014年是中国接入国际互联网20周年，截至2013年年底，中国网民规模突破6亿，其中通过手机上网的网民占80%。中国已是名副其实的“网络大国”，但网络侵犯个人隐私等违法行为时有发生，信息安全问题日益凸显。全国信息安全技能培训考试项目办公室负责人王增利表示，河南省的信息安全产业虽然在全国信息安全产业中所占份额较小，但信息安全技术及政策等相关培训及会议需求却高于信息化建设优势地区。目前，他们已与河南30多所院校建立了网络安全人才培训基地，将培养高素质的复合型人才。

（11）国家信息安全与国产化战略高层论坛在京举行

2014年11月16日，国家信息安全与国产化战略高层论坛在北京举行。中央国家机关、地方政府部门和军队信息化部门领导、科研院所专家、国内知名IT企业代表齐聚一堂，以“大力推进国产化战略，坚决维护国家网络和信息安全”为主题，通过主题

演讲、专题报告、问答互动等形式进行了深入研讨和交流。原国务院信息化领导小组办公室主任、原信息产业部副部长吕新奎、两院院士王越、中国科学院倪光南院士等嘉宾出席会议。会上，王越院士从人类文明、社会文明的独特视角，诠释了信息安全的深刻内涵。他指出，网络信息安全和自主可控核心技术的发展，是复杂、艰巨的系统工程，网络空间是“不战屈人之兵”的空间，应该从系统理论的角度找到信息装备国产化的发展之策，既要弘扬中华优秀文化，又要汲取世界文明智慧。倪光南院士指出，网络安全的内涵就是信息安全，保障网络主权就应保障信息主权；自主可控本质就是：知识产权自主可控、能力自主可控、发展自主可控；另外详细论述了国产操作系统生态环境的主要内涵和以产业基金支持构建的生态环境。

（12）中国首届国家网络安全宣传周11月24日启动

为帮助公众更好地了解、感知身边的网络安全风险，增强网络安全意识，提高网络安全防护技能，保障用户合法权益，共同维护国家网络安全，中央网信办会同中央机构编制委员会办公室、教育部、科技部、工业和信息化部、公安部、中国人民银行、新闻出版广电总局等部门，于11月24–30日举办首届国家网络安全宣传周。首届国家网络安全宣传周是我国第一次举办全国范围的网络安全主题宣传活动，不仅国家有关职能部门共同参与主办，各省、自治区、直辖市也将同期举办相关主题活动，在全国掀起网络安全宣传的高潮。宣传周以“共建网络安全，共享网络文明”为主题，将围绕金融、电信、电子政务、电子商务等重点领域和行业网络安全问题，以及针对社会公众关注的热点问题，举办网络安全体验展等系列主题宣传活动，营造网络安全人人有责、人人参与的良好氛围。从11月24日开始，宣传周分别设置了“启动日”、“政务日”、“金融日”、“产业日”、“电信日”、“青少年日”、“法治日”7个主题宣传日，围绕当前网络安全的重点领域，举办专题宣传活动。活动不仅展示我国网络安全工作的新成功、新进展、新成效，还将围绕网络钓鱼、电信诈骗、网上谣言等关系公众切身利益的常见网络安全风险，普及网络使用安全知识和基本的网络安全防护技能。

（13）中国互联网协会第四届网络与信息安全工作委员会第一次会议在京召开

2014年11月26日，中国互联网协会第四届网络与信息安全工作委员会第一次会议

在北京召开，选举产生中国互联网协会第四届网络与信息安全工作委员会（以下简称网安委员会）领导机构，并组织开展网安委员会工作计划研讨。

会议上，委员们听取了第三届委员会周勇林秘书长所做的工作报告，审议通过委员会组成情况说明、选举办法。会议选举云晓春担任第四届委员会主任委员，选举闫宏强、孙蔚敏、李晓东、杜跃进、吴湘东、周勇林、潘柱廷（按姓氏笔画排名）担任副主任委员，选举严寒冰担任第四届委员会秘书长。同时，经征求方滨兴院士个人意愿，会议提议并通过由方滨兴院士担任第四届网安委员会名誉主任委员的决定。

会上，中国互联网协会秘书长卢卫、新当选的主任委员云晓春做了重要讲话，对做好协会和网安委员会的工作提出要求和展望。同时，与会委员对第四届网安委员会工作献言献策，围绕委员会组织建设、交流研讨活动、重点工作方向、对外合作交流等方面提出了诸多意见和建议，为下一步制定委员会工作计划提供有益的参考。

11.2 国际重要网络安全会议和活动

（1）全球互联网治理委员会成立

2014年2月，在世界经济论坛成立了国际智囊团——全球互联网治理委员会，委员会主席为瑞典现任外长、前任首相卡尔·比尔特。全球互联网治理委员会计划用两年时间，最终实现“在全面协调的基础上促进未来多方利益相关者共同治理互联网”。该委员会表示，将为建立一个持续自由、开放的互联网而努力，并指出当前互联网面对两大威胁：一是专制国家设法对互联网施加更大的控制力；二是近来曝光的大规模监听事件引发的信任危机。该委员会计划解决网上维权等问题，比如为保护人权、隐私和言论自由，打击网络犯罪建立技术中立原则。委员会还对如何更好地规避风险提出建议，包括建立有关国家行为、网络犯罪合作等问题的相关标准。全球互联网治理委员会计划通过政治手段和游说活动影响互联网治理，不过，其必须先对国际互联网域名与地址管理委员会（ICANN）进行有效游说，因为目前ICANN在伦敦的公共关系代表对该委员会的举措尚不了解。ICANN认为，企业、公民与社会组织共同参与决策过程是互联网治理的最佳模式。全球互联网治理委员会的工作将于2014年5

月正式开始，届时ICANN的互联网合作高级别研讨会刚刚结束，相关规划和研究工作已经在进行中。

（2）CNCERT/CC圆满完成2014年APCERT应急演练

2014年2月19日，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2014年亚太地区网络安全应急演练，圆满完成了各项演练任务。

本次演练的主题是“区域协作打击网络攻击行为”。演练的核心内容是，通过区域内及国际间各应急响应组织的协作，有效阻止攻击者计划针对某政府部门信息系统的拒绝服务攻击行为。本次演练旨在检验亚太地区的CERT组织协作应对网络攻击的能力，共有20个CERT组织参加了此次演练，包括：来自16个国家和地区的APCERT成员（澳大利亚、孟加拉、文莱、中国、中国台湾、中国香港、印度尼西亚、日本、韩国、中国澳门、马来西来、缅甸、新加坡、斯里兰卡、泰国和越南），以及特别邀请的3个伊斯兰计算机应急响应合作组织（OIC-CERT）成员（埃及、巴基斯坦和尼日利亚）和1个欧洲政府应急响应合作组织(EGC)成员（来自德国）。这是EGC首次参加APCERT网络安全应急演练。本次演练的事件响应由多个组织协作完成，反映了APCERT各成员在网络安全事件响应方面的高度合作和事件分析处置能力。

（3）第六届中国-东盟网络安全研讨会在汕头召开

2014年5月27-29日，由工业和信息化部国际合作司主办，CNCERT/CC承办的第六届中国-东盟网络安全研讨会在中国汕头召开。来自柬埔寨、印度尼西亚、老挝、缅甸、菲律宾、泰国、越南7个国家的电信政府部门和网络安全应急组织代表出席了本次会议。会上各方充分交流了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，并探讨了如何深入开展中国-东盟国家的网络安全应急合作。

27日的中国-东盟圆桌会议由CNCERT/CC主持，工业和信息化部国际合作司领导首先代表中方致辞，认为随着互联网的快速发展，中国和东盟各国都面临严峻的网络安全挑战。本次中国-东盟网络安全研讨为双方分享经验、增进信任、开展务实合作提供了交流平台。中国东盟在信息通信领域特别是网络安全方面开展了良好的合作并取得丰盛的成果，双方应积极加强合作，共同应对网络安全威胁和跨境网络安全事件。随后，CNCERT/CC向东盟代表介绍了近年来在网络安全应急领域

的发展、管理经验和技术研究，奇虎360公司和安天公司介绍了其网络安全技术研究成果。东盟代表与中方分享了各国近年来在网络安全应急实践的经验和当前东盟国家网络安全发展现状，并表示希望中国能继续开展面向东盟国家的培训，完善相关应急联系机制，提供技术支持，帮助东盟国家提高网络安全意识，共同维护区域内的互联网网络安全环境。

28-29日，CNCERT/CC邀请东盟代表参加了“2014中国计算机网络安全年会”，参观了汕头电子商务高新产业园区。东盟代表积极与参会嘉宾交流，表示这次年会关于网络安全政策、管理和技术方面的新视点极具实践和研究价值。

（4）信息和网络安全国际研讨会在北京召开

外交部与联合国共同举办的信息和网络安全国际研讨会于2014年6月5日在北京开幕，这是中国与联合国首次就网络问题联合举办的国际会议。外交部副部长李保东在致辞中全面阐述了中国在网络安全问题上的立场与实践。李保东表示，中国主张国际社会加强合作，共同维护网络空间的安全、稳定与繁荣。为此，应把握好4点重要原则：一是和平原则，各国应摈弃“零和”思维和冷战时期的意识形态，树立互信、互利、平等、协作的新安全观；二是主权原则，各国对其领土内的信息通信基础设施和信息通信活动拥有管辖权，有权制定符合本国国情的互联网公共政策，任何国家不得利用网络干涉他国内政或损害他国利益；三是共治原则，应遵循多边、民主、透明的原则，努力实现资源共享、责任共担、合作共治；四是普惠原则，应倡导互利共赢理念，开展国际合作，跨越“数字鸿沟”。来自俄、美、英、南非、马来西亚等20余个国家、联合国机构和国内外知名智库的100余名代表与会。在为期两天的会议中，与会代表将就网络空间国际规则制定、互联网治理、联合国作用、区域合作、能力建设等问题展开深入探讨。CNCERT/CC应邀在会上作了题为“加强国际合作，维护网络安全”的演讲。

（5）联合国信息安全政府专家组首次会议举行

联合国信息安全政府专家组首次会议于7月21日在纽约召开。专家组系根据第68届联大有关决议成立，研究网络安全领域现实和潜在威胁，探讨负责任国家行为规范，建立信任措施及国际法相关问题，并将向第70届联大提交报告。该专家组是从国

际安全角度探讨处理网络安全问题的重要机制，旨在制定网络安全领域指导性原则和规范，备受各方关注。此前，联合国曾于2004-2005年、2009-2010年、2012-2013年三度成立信息安全政府专家组，达成了和平利用网络空间、网络空间国家主权原则等重要共识。中国政府专家、外交部网络事务协调员傅聪在会上发言。他说，要确保网络空间的和平性质，深化国家主权原则的内涵，要合作打击网络恐怖主义。他建议推动互联网的全球公平治理。中方认为，互联网治理体系应保证各方共同参与、共同决策，互联网基础资源应由国际社会共同管理、共同监督。傅聪说，2013年以来，大规模网络监听、监控活动不断曝光，侵犯了受害国的国家主权、安全和公民隐私。专家组应从国际安全角度对此进行深入讨论，并制定相应规范、原则和措施，以对此类活动加以约束。

（6）第二届中日韩互联网应急年会在韩国召开

2014年8月21-22日，中日韩三国的国家互联网应急中心（CERT）操作层面代表相聚在韩国首尔，召开了第二届中日韩互联网应急年会。

该年会是根据三方于2011年签订的“国家级计算机安全事件响应小组联合合作备忘录”召开，本届年会由韩国国家互联网应急中心（KrCERT/CC）主办。会议上，三方回顾了重大安全事件的处置和预防工作。三方均派技术人员参与了本届会议，并在会议上交流了网络安全威胁的最新信息。

最后，三方重申，要对重大安全事件的处置案例进行评估，进一步探讨各方事件处置的能力和方法，以继续加强各方的合作。三方一致同意支持建立针对网络风险评估的信息共享协议、范畴和标准，为改善全球网络环境做出贡献。

（7）第九届互联网管理论坛关注网络安全

第九届互联网管理论坛于2014年9月2日在土耳其伊斯坦布尔召开，来自135个国家和地区的约2500名政府官员、网络专家和各界代表出席，网络安全成为此次论坛关注的焦点。当今世界越来越依赖网络，网络安全不仅是普通用户面临的重大问题，各国政府和经济界也面临同样的问题。土耳其交通海事和通信部长卢特菲·埃尔万在会上表示，网络攻击对世界经济构成了威胁，全球每年耗资上万亿美元应对网络攻击。为此，他呼吁国际社会紧密合作研发网络攻击预警系统。联合国官员在会上强调了廉

价互联网接入、网络隐私等的重要性。联合国助理秘书长托马斯·施特尔策在会上表示，每一个网络用户都要学会使用对付网络攻击的必要工具，这事关教育的问题，学校应该提供专门课程。根据论坛上提供的数据，到2014年年底，全球网络用户达到30亿人，2013年全球有5.56亿人成为网络攻击的受害者，平均每天有150万名用户受到网络攻击。互联网管理论坛是前联合国秘书长安南倡议成立的，旨在促进互联网的可持续性、安全性、稳定性。此次会议为期4天，与会代表将围绕网络安全、垃圾邮件、保护儿童、网络隐私等问题进行探讨。一些专家还建议采取多边方式加强对互联网的管理，预防和阻止对政府和经济界的网络攻击。

（8）首届中国–东盟网络空间论坛2014年9月在中国广西南宁举办

中国国家互联网信息办公室主任鲁炜提出倡议：建立中国–东盟信息港。他指出，这既有助于东盟提升信息化水平，缩小乃至逐步消除数字鸿沟，又有利于中国与东盟国家之间的互联互通，建立一条新的“信息丝绸之路”，此举得到与会东盟国家代表的积极响应。中国–东盟信息港的建设是一项系统而又庞大的工程，主要包括基础建设平台、技术合作平台、经贸服务平台、信息共享平台和人文交流平台5个方面。参加网络空间论坛的缅甸嘉宾表示，缅甸希望通过此次网络空间论坛，能够在未来的合作过程中使缅甸获益，缩小缅甸的数字鸿沟。“东盟采取了一系列的措施来实现区域内的互联互通，比如东盟宽带走廊”，新加坡邮政部副总监谢爱铃说。泰国代表强调，在建设中国–东盟信息港、加强信息基础设施建设时，要保护互联网基础设施、域名、网站、电子服务，要保护网民，保护他们的知识产权，保护他们自由发表言论的权利，但又不能影响其他人的隐私。马来西亚的代表说，在东盟区域论坛框架之下，马来西亚和澳大利亚、俄罗斯在泛亚洲和欧亚地区开展了一些打击网络犯罪的工作，同时马来西亚也在与中国通力合作，共同保障网络安全。

（9）中日韩三国首次举行网络攻击对策磋商会

中日韩三国于10月21日在北京举行了有关电脑网络攻击对策的首次工作磋商会议。围绕已成为国家安全新难题的网络攻击问题，中日韩三国展现出共同商谈的姿态。此举是中日韩三国今后将继续进行对话、力争达成相互信任的举动。中日韩三国外交部门网络安全相关负责人出席了此次会谈。日本防卫省及总务省的相关官员出席

了此次会议，并在会上详细说明了日本针对网络攻击的相关对策。与此同时，中方在会议上针对目前的应对措施以及之后的应对策略进行了说明。中日韩三国都表示，今后希望能够多进行类似专业领域之间的商谈，力争互相之间达成信任和合作。

（10）首届世界互联网大会在浙江乌镇召开

经过20年的发展，互联网已经深刻改变了社会生活的每一个层面。为促进全球互联网的发展，打造更加公平和有利于发展的网络环境，由中国主办的首届世界互联网大会于2014年11月19日在浙江乌镇召开，本届大会倡导“互联互通，共享共治”，聚集了全球绝大多数互联网精英和部分政府官员，既强调互联网发展难得的历史机遇，也讨论如何应对风险挑战。中国国务院副总理马凯在大会致辞中表示：“加强互联网领域的交流合作，必须推动基础设施的互联互通。中方愿同世界各国加强合作，加快网络设施、通信设施建设步伐，大力提升宽带水平，推动新一代移动通信技术的研发和推广，架设通达世界的信息高速公路。目前亚洲基础设施投资银行、丝路基金正在积极筹建中，网络基础设施建设也将成为重点投资领域。”

目前，网络经济已经成为世界经济发展速度最快、潜力最大、合作最活跃的领域之一。不过要促进互联网经济的繁荣，离不开对网络环境的治理。爱尔兰前总理伯蒂·艾亨在开幕式中指出：“现在越来越多的消费者正越来越多的使用信息技术来改变他们的生活和工作方式，正如人类历史上的很多发展，我们也要警惕一些危险，因为随着鼠标点击，在客厅就能进行支付和银行业务，所以在互联网领域我们需要更好地治理，推动网络更加安全。”

与会者一致同意，互联网大会永久落户浙江乌镇，每年举办一届。不少专家认为，通过大会对涉及互联网的各项议题进行深入沟通，将有效加强各方合作，更有利地推动行业发展，定位行业方向，也能让中国作为互联网大国发挥更大的建设性作用。

（11）第七届中美互联网论坛在华盛顿举行

为期一天半的第七届中美互联网论坛于2014年12月2日在华盛顿开幕。此次论坛的主题为“对话与合作”。中国国家互联网信息办公室主任鲁炜、美国副国务卿凯瑟琳·诺韦利出席论坛并发表演讲。鲁炜在题为《沟通中互信 合作中共赢》的主旨演讲中指出，新时期的中美网络关系，总体向好、稳步向前，但前进途中时有坎坷，主要呈现两

大特征：一是深度融合、利益攸关；二是存在分歧、时有摩擦。鲁炜还提出中美互联网交流5点主张：一是彼此欣赏而不是互相否定；二是互相尊重而不是对立指责；三是共享共治而不是独善其身；四是沟通互信而不是相互猜疑；五是合作共赢而不是零和博弈。美国副国务卿凯瑟琳·诺韦利说，中美应该在互联网领域合作，两国也正在很多领域进行合作。中美互联网论坛由中国互联网协会和美国微软公司联合举办，已成为中美在互联网领域开展交流合作的最重要的平台之一。来自中美两国知名互联网企业、行业组织、学术机构和政府相关部门的150多名代表参加了本次论坛，围绕大数据和云服务、互联网接入、互联网治理和经济发展与社会利益等议题进行探讨交流。

12 2015年网络安全热点问题

根据对2014年我国互联网网络安全形势特点的分析，我们认为2015年需重点关注的热点问题如下。

（1）拒绝服务攻击威胁将继续升级，影响基础网络稳定运行。分布式反射型攻击将继续是实施拒绝服务攻击的重要形式，攻击者将不断分析、挖掘更多可被利用的网络协议，增加攻击威力，突破防护措施，大量联网智能设备将成为发起攻击的重要工具。随着拒绝服务攻击与防护的对抗日趋激烈，攻击流量规模可能进一步增大，单个攻击事件的峰值流量甚至可能突破1Tbit/s。针对域名系统的攻击将继续呈频繁态势，不仅影响受害目标，而且波及整个基础网络。此外由于网络攻击软件的工具化和平台化，网络攻击服务的商业化等因素，大大降低发起攻击的难度和成本，攻击门槛将越来越低。

（2）移动恶意程序借助“加固”手段对抗安全检测的情况将更加普遍，利用仿冒应用实施钓鱼欺诈的现象将更为猖獗。随着安卓应用免费“加固”服务市场的发展，“加固”技术手段将不断升级，移动恶意程序制作者利用代码加密、加壳等手段对抗安全检测的现象将更加普遍，这将导致经过“加固”处理的恶意程序数量大幅增长，进一步加大移动恶意程序治理工作的难度。由于移动应用制作成本较低、追溯较困难等因素影响，黑客制作假冒手机网银、运营企业客户端、热门游戏等应用程序，通过钓鱼短信或小型网站、社交平台、广告平台等渠道散播，以窃取用户钱财的现象将更加猖獗。

（3）云平台普及加大数据泄露和网络攻击风险，防护措施和管理机制有待完善。一是云平台的数据安全保护问题。云计算技术的发展推动数据的集中化，在大数据时代，海量数据既是企业和用户的核心资产，也成为网络攻击瞄准的目标，以窃取数据为主要目的的攻击事件将越来越多，云平台自身的网络安全防护特别是对海量数据安全的防护将面临挑战。二是云平台的安全审核和管理机制问题。目前大多数云服

务商的安全审核机制并不完善，用户租用后作何用途，云服务商并不清楚，也未作严格审核或周期性检查，因此出现黑客在云平台部署钓鱼网站、传播恶意代码或发动攻击的情况，如不及时加强管理，未来这种现象将继续增多。

（4）针对基础应用、通用软硬件和国产软硬件的漏洞挖掘将增多，应对机制和披露管理面临挑战。2015年，黑客将更加关注应用广泛的网站应用框架、开源软件、集成组件、网络协议等安全问题，随着服务器、芯片、操作系统、数据库、办公软件等信息产业各个领域的自主可控以及深入推进，国产软硬件产品应用增多，其安全问题将受到更多重视。由于基础应用、通用软硬件或国产软硬件的影响范围广泛，一旦漏洞信息提前披露或不客观披露，容易造成社会公众心理恐慌，并引发大面积攻击事件，针对这类应用或产品的漏洞信息披露和应对处置面临挑战。

（5）智能终端将成为新的攻击入口，物联网面临安全挑战。设备智能化的浪潮席卷各行业，智能终端具有带宽较高、全天候在线、系统升级慢、配置较少变动等特点，但由于技术不完善、忽视安全性等原因，大量智能终端设备存在弱口令或安全配置不当等漏洞，安全威胁也随之而来。随着物联网产业的发展和智慧城市的建设，智能生活逐渐推广，连接一切将日益成为现实，智能终端自身安全以及终端间连接或通信的安全问题，都是物联网面临的安全挑战。

（6）智能制造面临的网络攻击威胁将凸显，工业互联网发展面临挑战。以智能制造为主攻方向的“中国制造2025”计划，旨在充分利用信息通信（ICT）技术与制造技术的结合，推动新一轮科技革命和产业变革，实现智能制造、网络制造、绿色制造、服务性制造，促进制造业的数字化、网络化、智能化发展。工业互联网是实现智能制造的必备基础，是智能制造生产体系中必不可少的环节。随着传统工业基础设施加快向工业互联网基础设施演进升级，其所面临的网络攻击威胁也将日益凸显。从近几年的实际案例和统计数据可以看出，针对工业基础设施的网络攻击行为发生频率总体呈逐年增高趋势，攻击手段日益复杂高级，且带有显著APT特征，攻击危害逐渐加大，网络攻击威胁将成为工业互联网发展过程中无法回避的问题。

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，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

- 恶意程序

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

①特洛伊木马（Trojan Horse）

特洛伊木马（简称木马）是以盗取用户个人信息，甚至是以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[35]、网银木马[36]、窃密木马[37]、远程控制木马[38]、流量劫持木马[39]、下载者木马[40]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

[35] 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。
[36] 网银木马是用于窃取用户网银、证券等账号的木马。
[37] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[38] 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。
[39] 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。
[40] 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，我们将按照恶意程序的主要用途参照上述定义进行归类。

- 僵尸网络

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

- 拒绝服务攻击

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

- 网页篡改

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

- 网页仿冒

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

- 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，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

- 路由劫持

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

谢谢您阅读CNCERT/CC《2014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。

国家计算机网络应急技术处理协调中心

2014年
中国互联网
网络安全报告

ISBN 978-7-115-39215-2

ISSN 978-7-115-39215-2

定价：59.00 元

分类建议：计算机／网络安全

人民邮电出版社网址：www.ptpress.com.cn