

2015年 中国互联网 网络安全报告



分类建议：计算机/网络安全
人民邮电出版社网址：www.ptpress.com.cn

2015年
中国互联网
网络安全报告

人民邮电出版社

CNERT|CC
国家互联网应急中心

2015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



中国工信出版集团



人民邮电出版社
POSTS & TELECOM PRESS

CNERT|CC
国家互联网应急中心

2015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

人民邮电出版社
北京

图书在版编目 (C I P) 数据

2015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,
2016.6

ISBN 978-7-115-42291-0

I. ①2… II. ①国… III. ①互联网络—安全技术—
研究报告—中国—2015 IV. ①TP393.408

中国版本图书馆CIP数据核字 (2016) 第081451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”, 英文缩写为“CNCERT”或“CNCERT/CC”) 发布的2015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数据和通信行业相关单位报送的数据, 具有鲜明的行业特色和重要的参考价值。内容涵盖我国互联网网络安全态势分析、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。其中, 本书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, 并对2015年开展的网络安全威胁治理行动等重要活动或网络安全事件做专题分析。此外, 本书对2015年国内外网络安全监管动态、国内网络安全组织发展情况和国内外网络安全重要活动等情况做了阶段性总结, 并预测了2016年网络安全热点问题。

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。

2015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: 14 2016年5月第1版
字数: 150千字 2016年5月北京第1次印刷

ISBN 978-7-115-42291-0

定价: 79.00元

读者服务热线: (010) 81055488 印装质量热线: (010) 81055316

反盗版热线: (010) 81055315

《2015 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	丁 丽	李 佳	纪玉春	
委 员	狄少嘉	徐 娜	徐 原	何世平	
	温森浩	赵 慧	李志辉	姚 力	
	张 洪	朱芸茜	郭 晶	朱 天	
	高 胜	胡 俊	王小群	张 腾	
	吕利锋	何能强	李 挺	陈 阳	
	李世淙	王适文	刘 婧	饶 毓	
	肖崇蕙	贾子骁	张 帅	吕志泉	
	韩志辉	马莉雅			

互联网在我国政治、经济、文化以及社会生活中发挥着举足轻重的作用。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 10 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网络安全环境、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的基础上,《CNCERT/CC 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,在工业和信息化部网络安全管理局(原通信

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。

《2015 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数据,具有鲜明的行业特色和重要的参考价值。报告涵盖我国互联网网络安全态势分析、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,并对 2015 年开展的网络安全威胁治理行动等重要活动或发生的典型网络安全事件做专题分析。此外,报告对 2015 年国内外网络安全监管动态、国内网络安全组织发展情况和国内外网络安全重要活动等情况做了阶段性总结。最后,报告预测了 2016 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

2016 年 4 月

《2015 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（以下简称“CNCERT/CC”）网络安全工作实践。CNCERT/CC 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《2015 年中国互联网网络安全报告》撰写过程中，CNCERT/CC 向恒安嘉新（北京）科技有限公司、北京网秦天下科技有限公司、哈尔滨安天科技股份有限公司、北京奇虎科技有限公司、微软公司、腾讯公司、卡巴斯基技术开发（中国）有限公司、深信服科技有限公司、北京猎豹移动科技有限公司等单位征集并采用了网络安全数据和专题文章素材^[1]，特此致谢。

2015 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。北京新网数信息技术有限公司、阿里云计算有限公司、厦门商中在线科技有限公司、上海美橙科技信息发展有限公司、成都西维数码科技有限公司、厦门纳网科技有限公司、成都飞数科技有限公司、厦门市资源网络服务有限公司等单位对 CNCERT/CC 事件处置要求及时响应，配合积极；恒安嘉新（北京）科技有限公司、北京神州绿盟信息安全科技股份有限公司、哈尔滨安天科技股份有限公司

[1] 《2015 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，CNCERT/CC 未做验证。

公司、北京奇虎科技有限公司、北京猎豹移动科技有限公司、北京瑞星信息技术有限公司等单位向 CNCERT/CC 报送了大量有价值的信息通报，起到了很好的预警效果；中国移动 MM、木蚂蚁、OPPO 软件商店、百度手机助手、小米应用商店、91 助手、应用汇、360 手机助手、安智市场、安卓市场积极配合开展移动互联网恶意程序下架等工作；北京启明星辰信息技术有限公司、北京神州绿盟科技有限公司、北京奇虎科技有限公司（补天平台）、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、乌云平台、漏洞盒子，在漏洞信息报送方面表现突出；中国教育和科研计算机网、上海交通大学网络信息中心、北京信息安全测评中心、中国电信集团公司网络运行维护事业部、中国移动通信集团公司信息安全管理与运行中心、中国联合网络通信集团有限公司运行维护部、中国科技网、北京知道创宇信息技术有限公司等单位在漏洞处置和全局响应方面表现突出。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，《2015 年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，CNCERT/CC 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 CNCERT/CC 的发展。CNCERT/CC 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。

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

国家互联网应急中心的主要业务能力如下。

事件发现。CNCERT/CC 依托“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。CNCERT/CC 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，CNCERT/CC 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，作为我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 为著名网络安全合作组织 FIRST 正式成员以及亚太应急组织 APCERT 的发起人之一。截至 2015 年，CNCERT/CC 与 66 个国家和地区的 165 个组织建立了“CNCERT/CC 国际合作伙伴”关系。

联系方式

CNCERT/CC 建立了 7×24h 的网络安全事件投诉机制，国内外用户可通过网站、电子邮件、热线电话、传真 4 种主要渠道向 CNCERT/CC 投诉网络安全事件。

网 址：<http://www.cert.org.cn/>

电子邮件：cncert@cert.org.cn

热线电话：+86 10 82990999（中文）

+86 10 82991000（English）

传 真：+86 10 82990399

CONTENTS 目录

01	2015 年我国互联网网络安全状况	15
	1.1 总体状况	15
	1.2 数据导读	23
02	网络安全专题分析	26
	2.1 网络安全威胁治理专项行动（来源：CNCERT/CC）	26
	2.2 广告平台传播恶意扣费 APP 专题分析（来源：CNCERT/CC）	35
	2.3 工业互联网安全分析（来源：CNCERT/CC）	44
	2.4 一例针对中方机构的准 APT 攻击分析（来源：安天公司）	56
	2.5 Dorkbot 僵尸网络分析（来源：微软公司）	63
	2.6 社保系统泄密“风波”安全事件分析（来源：深信服公司）	75
	2.7 DNS DDoS 攻击事件分析（来源：绿盟公司）	87
03	计算机恶意程序传播和活动情况	97
	3.1 木马和僵尸网络监测情况	97
	3.2 “飞客”蠕虫监测情况	105
	3.3 恶意程序传播活动监测	107
	3.4 通报成员单位报送情况	110
04	移动互联网恶意程序传播和活动情况	120
	4.1 移动互联网恶意程序监测情况	120
	4.2 移动互联网恶意程序传播活动监测	122
	4.3 通报成员单位报送情况	124

05	——	网站安全监测情况	141
		5.1 网页篡改情况	141
		5.2 网站后门情况	145
		5.3 网页仿冒情况	148
06	——	信息安全漏洞公告与处置	150
		6.1 CNVD 漏洞收录情况	150
		6.2 CNVD 行业漏洞库收录情况	153
		6.3 漏洞报送和通报处置情况	157
		6.4 高危漏洞典型案例	159
07	——	网络安全事件接收与处理	166
		7.1 事件接收情况	166
		7.2 事件处理情况	168
		7.3 事件处理典型案例	170
08	——	网络安全信息通报情况	177
		8.1 互联网网络安全信息通报	177
		8.2 行业外互联网网络安全信息发布情况	178
09	——	国内外网络安全监管动态	180
		9.1 2015 年国内网络安全监管动态	180
		9.2 2015 年国外网络安全监管动态	185

10	安全组织发展情况	192
	10.1 网络安全信息通报成员发展情况	192
	10.2 CNVD 成员发展情况	198
	10.3 ANVA 成员发展情况	201
	10.4 CNCERT/CC 应急服务支撑单位	203
11	国内外网络安全重要活动	207
	11.1 国内重要网络安全会议和活动	207
	11.2 国际重要网络安全会议和活动	209
12	2016 年值得关注的热点问题	216
13	网络安全术语解释	218

2015年

网络安全大事记

◆ 2015年1月5日，机锋论坛的2300万用户数据在网上疯传，引发公众的广泛关注。360补天漏洞响应平台负责人赵武对此表示：“经调查，网上流传的2300万数据是机锋2013年的老数据。但机锋论坛还有多个高危漏洞没有完全修复，其2700万最新用户数据也暴露在黑客枪口下。”

机锋论坛
存在高危漏洞或导致
2700万最新用户数据泄露

社保系统
漏洞曝光涉及
30余省数千万
用户数据

◆ 2015年4月，“补天漏洞响应平台”发布信息称：30余个省市的社保、户籍查询、疾控中心等系统存在高危漏洞；仅社保类信息安全漏洞涉及数据就达到5279.4万条，包括身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

50家单位
入选第六届
CNCERT/CC
网络安全应急服
务支撑单位

◆ 2015年5月25日，国家互联网应急中心在湖北省武汉市举行第六届CNCERT/CC网络安全应急服务支撑单位评选活动，评选产生了8家国家级应急服务支撑单位和42家省级应急服务支撑单位。

2015年中国
网络安全技术
对抗赛和
中国计算机
网络安全大会
成功举办

◆ 2015年5月26日，在工业和信息化部指导下，国家互联网应急中心（CNCERT/CC）在湖北省武汉市举办了2015中国网络安全技术对抗赛。2015年5月27-28日，以“智能网络·安全护航”为主题的2015中国计算机网络安全大会（第12届）在湖北省武汉市召开，来自政府和重要信息系统、企业、行业协会、科研院所等单位以及来自CNCERT/CC国际合作伙伴的代表共七百余参加了本次大会。

◆ 2015年6月19日，国内32家单位在北京共同签署了《中国互联网协会漏洞信息披露和处置自律公约》，这是首次以行业自律的方式共同规范漏洞信息的接收、处置和发布方面的行为。

《中国互联网
协会漏洞信息披露
和处置自律公约》
在京签署

◆ 网络安全法草案7月6日起在中国人大网上全文公布，并向社会公开征求意见一个月。2015年6月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。

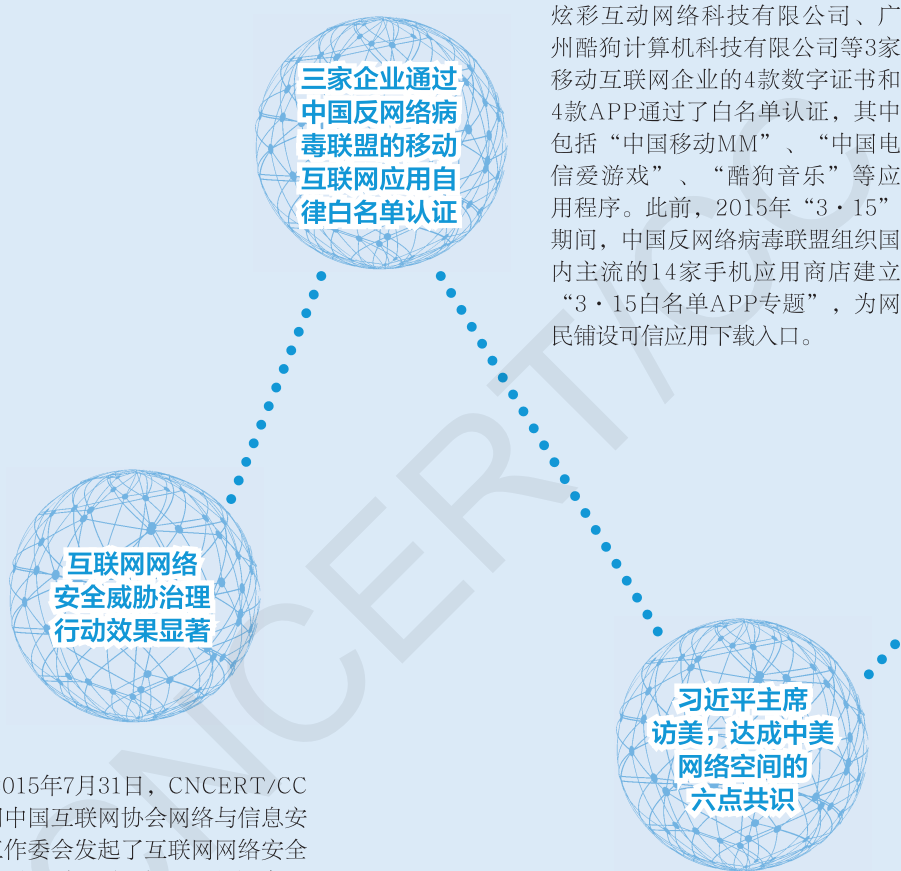
网络安全法
草案全文公布并
征求社会意见

“海莲花”
APT组织被曝光
长期攻击我国
海事机构等
重要部门

◆ 2015年5月29日，360“天眼实验室”发布的报告，首次披露一起针对中国的国家级黑客攻击细节。该境外黑客组织被命名为“海莲花(OceanLotus)”。自2012年4月起，“海莲花”针对中国的海事机构、海域建设部门、科研院所和航运企业，使用木马病毒攻陷和控制政府人员、外包商、行业专家等目标人群的电脑，甚至操纵电脑自动发送相关情报，很明显是一个有国外政府支持的APT行动。

《国家安全法》
公布施行

◆ 2015年7月1日，十二届全国人大常委会第十五次会议表决通过了新的国家安全法。国家主席习近平签署第29号主席令予以公布。法律对政治安全、国土安全、军事安全、文化安全、科技安全等11个领域的国家安全任务进行了明确，首次以法律形式提出“维护国家网络空间主权”。



三家企业通过
中国反网络病
毒联盟的移动
互联网应用自
律白名单认证

◆ 2015年8月19日，中国移动、炫彩互动网络科技有限公司、广州酷狗计算机科技有限公司等3家移动互联网企业的4款数字证书和4款APP通过了白名单认证，其中包括“中国移动MM”、“中国电信爱游戏”、“酷狗音乐”等应用程序。此前，2015年“3·15”期间，中国反网络病毒联盟组织国内主流的14家手机应用商店建立“3·15白名单APP专题”，为网民铺设可信应用下载入口。

互联网网络
安全威胁治理
行动效果显著

◆ 2015年7月31日，CNCERT/CC会同中国互联网协会网络与信息安全工作委员会发起了互联网网络安全威胁治理专项行动，重点打击以DDoS攻击、网页篡改为代表的制造、销售、传播网络攻击工具以及实施网络攻击行为的地下黑色产业链，效果显著。

习近平主席
访美，达成中美
网络空间的
六点共识

◆ 2015年9月，习近平主席访美，与美方在网络议题相关的领域达成了六点共识，包括网络安全审查、商业领域加强信息通讯技术网络安全的一般措施、恶意网络活动提供信息及协助、反对网络窃取知识产权、制定和推动国际社会网络空间国家行为准则，以及建立两国打击网络犯罪及相关事项高级别联合对话机制。

苹果
XcodeGhost恶
意程序出现为应
用供应链安全问
题敲响警钟

◆ 2015年9月13日，CNCERT/CC接到报告称，使用非苹果公司官方渠道的Xcode开发工具开发APP时，非官方Xcode会向正常的APP中植入恶意代码“XcodeGhost”，且被植入恶意程序的苹果APP可以在App Store正常下载并安装使用，感染国内用户达2140万。CNCERT/CC已在9月14日发布预警通报，提醒开发者切勿使用非苹果官方渠道的Xcode工具，以维护广大用户的个人信息安全。

第二届
世界互联网
大会召开

◆ 2015年12月16日，第二届世界互联网大会在浙江省桐乡市乌镇举行。本届大会的主题是“互联互通·共享共治——共建网络空间命运共同体”。开幕式上，中共中央总书记、国家主席、中央军委主席习近平发表主旨演讲。

Java
反序列化
漏洞

◆ 2015年12月，CNCERT/CC通报Java反序列化漏洞情况，该漏洞影响多款应用广泛的Web容器软件。远程攻击者利用漏洞可在目标系统上执行任意代码，危害较大的可以取得网站服务器控制权。CNCERT/CC对相关Web应用的分布情况和受漏洞影响进行了探测，发现境内主机IP中Jboss、Weblogic、Jenkins受到漏洞影响的未修复比例分别是13.9%、50.4%、33.4%。



2015年我国互联网 网络安全状况

1.1 总体状况

2015年，党中央、国务院加大对网络安全的重视，我国网络空间法制化进程不断加快，网络安全人才培养机制逐步完善，围绕网络安全的活动蓬勃发展。我国新《国家安全法》正式颁布，明确提出国家建设网络与信息安全保障体系；《刑法修正案（九）》表决通过，加大打击网络犯罪力度；《反恐怖主义法》正式通过，规定了电信业务经营者、互联网服务提供者在反恐中应承担的义务；《网络安全法（草案）》向社会各界公开征求意见；高校设立网络空间安全一级学科，加快网络空间安全高层次人才培养；政府部门或行业组织围绕网络安全举办的会议、赛事、宣传活动等丰富多样。

2015年是我国“十二五”规划收官之年，我国实现了半数中国人接入互联网，网民规模达6.88亿，手机网民规模达6.2亿，域名总数为3102万个^[2]。2015年，我国陆续出台“互联网+”行动计划、“宽带中国2015专项行动”等，加快建设网络强国。我国不断完善网络安全保障措施，网络安全防护水平进一步提升。然而，层出不穷的网络安全问题仍然难以避免。基础网络设备、域名系统、工业互联网等我国基础网络和关键基础设施依然面临着较大的安全风险，网络安全事件多有发生。木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、安全漏洞、网页仿冒、网页篡改等网络安全事件表现出新的特点：利用分布式拒绝服务攻击（以下简称“DDoS攻击”）和网页篡改获得经济利益现象普遍；个人信息泄露引发的精准网络诈骗和勒索事件增多；智能终端的漏洞风险增大；移动互联网恶意程序的传播渠道转移到网盘或广告平台等网站。

[2] 数据来自《第37次中国互联网络发展状况统计报告》。



1.1.1 网络基础设施

（1）基础通信网络安全防护水平进一步提升

基础电信企业逐年加大网络安全投入，加强通信网络安全防护工作的体系、制度和手段建设，推动相关工作系统化、规范化和常态化。2015年，工业和信息化部以网络安全管理、技术防护、用户个人电子信息和数据安全保护、应急工作、网络安全问题整改等为检查重点，对电信和互联网行业落实网络安全防护工作进行抽查。根据抽查结果，各基础电信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2014年下降20.5%。

（2）我国域名系统拒绝服务攻击能力显著提升

CNCERT/CC监测发现，2015年针对我国域名系统的DDoS攻击流量进一步增大。4月，我国某重要新闻网站的域名服务器多次遭受DDoS攻击，峰值流量达8Gbit/s，经分析发现此次攻击主要为利用NTP^[3]和UPnP^[4]进行的反射攻击，主要攻击源均来自境外；8月，我国顶级域名系统先后遭受两次大流量DDoS攻击，峰值流量超过10Gbit/s。2015年发生的多起针对重要域名系统的DDoS攻击均未对相关系统的域名解析服务造成严重影响，反映出我国重要域名系统普遍加强了安全防护措施，抗DDoS攻击能力显著提升。

（3）工业互联网面临的网络安全威胁加剧

新一代信息技术与制造业深度融合，工业互联网成为推动制造业向智能化发展的重要支撑。近年来，国内外已发生多起针对工业控制系统的网络攻击，攻击手段也更加专业化、组织化和精确化。2015年，国家信息安全漏洞共享平台（以下简称“CNVD”）共收录工控漏洞125个，发现多个国内外工控厂商的多款产品普遍存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险，可被攻击者利用实现远程访问。据CNCERT/CC监测，2015年境外有千余个IP地址对我国大量使用的某款工控系统进行渗透扫描，有数百个IP地址对我国互联网上暴露的工控设备进行过访

[3] NTP（Network Time Protocol，即网络时间协议）。

[4] UPnP（Universal Plug and Play，即通用即插即用）协议。

问。2015年12月，因遭到网络攻击，乌克兰境内近三分之一的地区发生断电事故。据分析，此次网络攻击利用了一款名为“黑暗力量”的恶意程序，获得对发电系统的远程控制能力，导致电力系统长时间停电。此次事件的发生，再次对我国提出警示，我国工业互联网也可能面临着严峻的网络安全威胁。

（4）针对我国重要信息系统的高强度有组织攻击威胁形势严峻

据CNCERT/CC监测，2015年我国境内有近5000个IP地址感染窃密木马，存在失泄密和运行安全风险。针对我国实施的APT^[5]攻击事件也在不断曝光，例如境外“海莲花”黑客组织多年以来针对我国海事机构实施APT攻击；国内安全企业发现一起名为APT-TOCS的长期针对我国政府机构的攻击事件。2015年7月发生的Hacking Team公司信息泄露事件，揭露了部分国家相关机构雇佣专业公司对我国重要信息系统目标实施网络攻击的情况。

1.1.2 公共互联网

1.1.2.1 公共互联网网络安全环境

2015年，根据CNCERT/CC自主监测数据，我国公共互联网网络安全状况总体平稳，位于境内的木马和僵尸网络控制端数量保持下降趋势，主流移动应用商店安全状况明显好转，但个人信息泄露、网络钓鱼等方面的安全事件数量呈上升趋势。

（1）木马和僵尸网络

我国境内木马和僵尸网络控制端数量再次下降，首次出现境外木马和僵尸网络控制端数量多于境内的现象。据抽样监测，2015年共发现10.5万余个木马和僵尸网络控制端，控制了我国境内1978万余台主机。其中，位于我国境内的控制端近4.1万个，较2014年下降34.1%，并继续保持下降趋势。以上情况的出现主要与行业内相关单位近年来持续开展木马和僵尸网络治理有关。2015年，在工业和信息化部指导下，按照《木马和僵尸网络监测与处置机制》的有关规定，CNCERT/CC组织基础电信企业、

[5] APT（Advanced Persistent Threat，高级持续性威胁）：利用先进的攻击手段对特定目标进行长期持续性网络攻击的形式。



域名服务机构等成功关闭678个控制规模较大的僵尸网络，累计处置690个恶意控制服务器和恶意域名，成功切断黑客对154万余台感染主机的控制。随着我国境内持续开展木马和僵尸网络治理工作，大量木马和僵尸网络控制端向境外迁移。2015年抽样监测发现，境外有6.4万余个木马和僵尸网络控制端，较2014年大幅增长51.8%，占全部控制端数量的61.2%，首次出现境外木马和僵尸网络控制端多于境内的现象。

（2）个人信息泄露

个人信息泄露事件频发。2015年我国发生多起危害严重的个人信息泄露事件，例如某应用商店用户信息泄露事件、约10万条应届高考考生信息泄露事件、酒店入住信息泄露事件、某票务系统近600万用户信息泄露事件等。针对安卓平台的窃取用户短信、通信录、微信聊天记录等信息的恶意程序爆发。安卓平台感染此类恶意程序后，大量涉及个人隐私的信息被通过邮件发送到指定邮箱。2015年，CNCERT/CC抽样监测发现，恶意程序转发的用户信息邮件数量超过66万封。CNCERT/CC在判定此类恶意程序的恶意行为后，立即协调处置涉及的URL、域名和邮箱，有效防止影响范围进一步扩大。此外，个人信息泄露事件频繁被媒体报道，反映出社会对此类事件的关注度不断提升。

个人信息泄露引发网络诈骗和勒索等“后遗症”。2015年发生多起因网购订单信息泄露引发的退款诈骗事件，犯罪分子利用遭泄露的收件地址和联系方式等用户购物信息，向用户发送虚假退款操作信息，迷惑性很强，造成财产损失。由于许多网民习惯在不同网站使用相同账号密码，个人隐私信息易被“撞库”^[6]等黑客行为窃取，进而威胁到网民财产安全。2015年，CNCERT/CC多次接到网民投诉苹果手机被锁遭敲诈勒索事件。据查，此类事件大多因用户个人隐私泄露，攻击者利用用户账户密码等信息结合苹果手机的防遗失功能，对用户进行锁机勒索，勒索不成则远程删除用户手机数据，给用户带来严重损失。

（3）移动互联网恶意程序

移动互联网恶意程序数量仍大幅增长。2015年，CNCERT/CC通过自主捕获和厂

[6] 撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登录其他网站后，得到一系列可以登录的用户。

商交换获得移动互联网恶意程序数量近148万个，较2014年增长55.3%，主要针对安卓平台。按恶意行为进行分类，排名前三位的恶意行为分别是恶意扣费类、流氓行为类和远程控制类，占比分别为23.6%、22.2%和15.1%。CNCERT/CC发现移动互联网恶意程序下载链接30万余条，同比增长7.2%，涉及的传播源域名4万余个、IP地址近两万个，恶意程序传播次数达8384万余次，较2014年增长了9.8%。

主流移动应用商店安全状况明显好转，大量移动恶意程序的传播渠道转移到网盘或广告平台等网站。在工业和信息化部的指导下，经过连续三年的治理，国内主流应用商店积极落实安全责任，不断完善安全检测、安全审核、社会监督举报、恶意程序下架等制度，积极参与处置响应与反馈，恶意APP下架数量连续保持下降趋势，2015年较2014年下降了57.3%。2015年，CNCERT/CC累计向302家应用商店、云盘、网盘或广告宣传网站等平台通报恶意APP事件1.7万余起，要求对通报的恶意APP进行下架，全年下架率达97.2%。按各平台接到通报的数量来看，排名前6的平台接到的通报次数占全年总通报次数的50.2%。经确认发现，这6家主要是提供云盘、网盘、广告宣传等业务的网站，反映出大量的恶意程序传播源已发生转移。

应用软件供应链安全问题凸显。2015年先后曝出多起应用软件开发工具被植入恶意代码，导致使用这些工具开发的应用软件出现安全问题的事件。9月，CNCERT/CC监测发现，苹果开发工具Xcode被植入XcodeGhost恶意代码，导致使用该工具开发的苹果APP被植入恶意代码。国内数百款知名的APP均受到感染，这些恶意APP绕过苹果AppStore安全审核机制供用户下载。截至9月18日，全国受感染用户达2140万。10月，网上披露了“WormHole”漏洞，该漏洞存在于国内某公司开发的一款公共开发套件中，影响集成此套件的该公司系列APP及其他20余款APP。CNCERT/CC及时完成了事件的样本分析、处置和预警，要求涉事单位及时修复相关APP并通知用户更新，有效遏制了恶意代码传播蔓延势头。

（4）拒绝服务攻击

DDoS攻击仍然是我国互联网面临的严重安全威胁之一。近年来，DDoS攻击的方式和手段不断发生变化。自2014年起，利用互联网传输协议的缺陷发起的反射型DDoS攻击日趋频繁，增加了攻击防御和溯源的难度。几乎不需要技术基础即可使用的DDoS攻击服务平台在互联网上大量出现，DDoS攻击以服务形式在互联网上公开叫



卖，这些平台的出现极大地降低了DDoS攻击技术门槛，使攻击者可以轻易发起大流量攻击。2015年前三季度，攻击流量在1Gbit/s以上的DDoS攻击次数近38万次，日均攻击次数达到1491次。为遏制DDoS攻击事件数量继续增长，减少DDoS攻击带来的危害，CNCERT/CC于2015年第四季度组织电信和互联网行业单位集中开展互联网网络安全威胁治理行动，日均DDoS攻击数量明显下降。

（5）安全漏洞

网络安全高危漏洞频现，网络设备安全漏洞风险依然较大。2015年，CNVD共收录安全漏洞8080个，较2014年减少11.8%。其中，高危漏洞收录数量高达2909个，较2014年增长21.5%；可诱发零日攻击的漏洞1207个（即收录时厂商未提供补丁），占14.9%。2015年曝出了Juniper Networks ScreenOS后门漏洞^[7]、Java反序列化远程代码执行漏洞^[8]、Redis未授权执行漏洞^[9]、HTTP.sys远程代码执行漏洞^[10]和GNU Glibc函数库缓冲区溢出漏洞^[11]（又称为“Ghost”幽灵漏洞）等多个涉及基础软件的高危漏洞。基础软件广泛应用在我国基础应用和通用软硬件产品中，若不及时修复，容易被批量利用，造成严重危害。从CNVD行业漏洞收录数量统计分析发现，电信行业漏洞库收录漏洞数量为657个，其中网络设备（如路由器、交换机等）漏洞占54.3%，可见网络设备安全风险依然较大。值得注意的是，如果骨干路由器等关键节点网络设备的漏洞被攻击利用，可能导致网络设备或节点被操控、破坏网络稳定运行、窃取用户信息、传播恶意代码、实施网络攻击等问题，需引起高度重视。2015年，CNVD共向基础电信企业通报2447份漏洞风险通报，较2014年增长61.9%；通报涉及的基础电信企业门户网站及业务系统漏洞风险事件2530起，较2014年增长60.3%。

涉及重要行业和政府部门的高危漏洞事件持续增多，修复进度未跟上步伐。政府机构和重要信息系统的网络系统上承载大量有价值的数据信息，广泛被漏洞挖掘者关注。2015年，CNCERT/CC通报了涉及政府机构和重要信息系统部门的事件型漏洞近

[7] 编号CNVD-2015-08306、CNVD-2015-08307，CVE-2015-7756。

[8] 编号CNVD-2015-07556。

[9] 编号CNVD-2015-07557。

[10] 编号CNVD-2015-02422，CVE-2015-1635。

[11] 编号CNVD-2015-00719，CVE-2015-0235。

2.4万起，约是2014年的2.6倍，继续保持快速增长态势。然而，部分通报漏洞未及时修补，为相关系统带来严重安全隐患。CNCERT/CC抽取2015年12月通报的安全漏洞事件进行修复验证，发现政府部门网站系统漏洞隔月修复率仅为52.7%，涉及网络基础设施的漏洞隔月修复率为81.3%，可见部分漏洞修复不及时。

智能联网设备暴露出的安全漏洞问题严重。乘着“互联网+”的新机遇，各行业与互联网深度融合，智能联网设备也逐渐在各行业广泛使用，漏洞威胁也在逐步增加。2015年，CNVD共收录739个移动互联网设备或软件产品漏洞；通报了多款智能监控设备、路由器等存在被远程控制高危风险漏洞的安全事件。2015年年初，政府机关和公共行业广泛使用的某型号监控设备被曝存在高危漏洞，并已被利用植入恶意代码，导致部分设备被远程控制并可对外发动网络攻击。CNCERT/CC核查发现，我国主要厂商生产的同类型设备，普遍存在类似安全问题，亟需进行大范围整改。

（6）网页仿冒

网页仿冒事件数量暴涨。CNCERT/CC监测发现，2015年针对我国境内网站的仿冒页面数量达18万余个，较2014年增长85.7%。其中，针对金融支付的仿冒页面数量上升最快，较2014年增长6.37倍；针对娱乐节目中奖类的网页仿冒页面数量也较2014年增长1倍。大量仿冒银行或基础电信企业积分兑换的仿冒网站链接由伪基站发送。2015年，CNCERT/CC共处置各类网络安全事件近12.6万起，其中网页仿冒事件数量位居第一，达7.5万余起，同比增长近3.2倍。由于我国加大了对网页仿冒的打击力度，大量的网页仿冒站点迁移到境外。在针对我国境内网站的仿冒站点中，83.2%位于境外，其中位于中国香港的IP地址承载的仿冒页面最多，有6万余个。

（7）网页篡改

植入暗链^[12]是网页篡改的主要攻击方式。CNCERT/CC监测发现，2015年我国境内近2.5万个网站被篡改，其中被篡改政府网站有898个，较2014年减少49.1%。从网页篡改的方式来看，我国被植入暗链的网站占全部被篡改网站的比例高达83%，在被篡改的政府网站中，超过85%的网页篡改方式是植入暗链。植入暗链已成为黑客地下产

[12] 暗链就是页面上看不见网站链接，主要指向博彩、私服等非法网站链接。



业链牟利方式之一，2015年CNCERT/CC处置参与网页篡改攻击的博彩、私服等非法网站链接6320个，通知5609个被植入暗链网站用户单位对网站进行修复。

1.1.2.2 公共互联网网络安全合作

网络空间具有开放互联等特性，网络安全问题涉及面广。首先，网络安全威胁往往是涉及多行业、多领域的交叉问题，需要跨部门、跨行业、跨地域的多方力量共同协作才能有效应对。其次，跨境网络安全事件频发，需要加强国际对话合作，建立高效的网络安全信息共享和跨境网络安全事件处置协作机制。2015年，我国网络安全领域的国内外合作均进一步加强。在国内，电信和互联网行业积极发挥行业自律作用，共同应对网络安全威胁；在国际合作方面，协作处置的跨境网络安全事件数量显著增加。

（1）互联网网络安全威胁治理行动

2015年7月31日，CNCERT/CC联合中国互联网协会网络与信息安全工作委员会组织开展互联网网络安全威胁治理行动。共56家企业参与此次行动，包括基础电信企业、互联网企业、域名注册服务机构、应用商店等。该行动以加强行业自律为目的，通过投诉举报、信息共享、威胁认定、协同处置、信息发布等多项措施环环相扣，取得了显著治理效果。此次行动重点针对DDoS攻击、网页篡改等与互联网黑产密切相关的事件进行处置。截至2015年年底，CNCERT/CC共接到广大网民举报的网络安全事件54937起，处置网络安全事件52950起，发布URL黑名单地址47061条。DDoS攻击事件次数由行动启动前的日均1491起下降到日均358起，大幅下降76.7%；境内被篡改网站相比行动启动前月均下降8.6%，其中被篡改政府网站月均下降了44%，国内主流浏览器、搜索引擎对共享的URL黑名单地址进行拦截或提示次数达千万余次。

（2）安全漏洞披露和处置规范

为方便涉事单位在漏洞披露前得到通知并及时修复漏洞，避免漏洞信息描述不准确或漏洞披露信息夸大其词造成社会恐慌，或漏洞披露信息过于详细而被黑客利用等，CNCERT/CC与乌云、补天、漏洞盒子等多家民间漏洞平台建立工作联系，并于2015年6月，组织国内32家单位在北京共同签署了《中国互联网协会漏洞信息披露和处置自律公约》，首次以行业自律的方式共同规范漏洞信息的接收、处置和发布方面的行为。协议签署后，相关单位漏洞披露、处置方式的规范性得到有效提升。

（3）网络安全国际合作

2015年，CNCERT/CC继续与国际网络安全组织加强合作，完善跨境网络安全事件协作处置机制。截止到2015年年底，已与66个国家和地区的165个组织建立联系机制，与其中的16个国家或地区的CERT、7个网络安全组织签署网络安全合作谅解备忘录，全年协调境外安全组织处置涉及我国境内的安全事件近1.9万起，比2014年增长1倍多。CNCERT/CC还推动落实中国-东盟国家计算机应急响应组织合作机制的行动计划、加强中日韩区域网络安全协作，积极发挥在FIRST、APCERT等国际组织中作用，并支撑开展上合组织、APEC-TEL、ITU及双边网络安全对话国际合作活动。

1.2 数据导读

以下是2015年CNCERT/CC对我国网络安全宏观状况抽样监测的主要数据分析结果。

（1）木马和僵尸程序监测

2015年，木马或僵尸程序控制服务器IP地址总数为105056个，较2014年上升0.8%。其中，境内木马或僵尸程序控制服务器IP地址数量为40782个，较2014年下降34.1%；境外木马或僵尸程序控制服务器IP地址数量为64274个，较2014年增长51.8%。

2015年，受控主机IP地址总数为28728402个，较2014年大幅上升105.3%。其中，境内共有19781858个IP地址的主机被植入木马或僵尸程序，较2014年增长78.4%；境外共有8946544个IP地址的主机被植入木马或僵尸程序，较2014年增长208.1%。

（2）“飞客”蠕虫监测

2015年，全球互联网月均感染“飞客”蠕虫的主机IP地址数量为391万个，较2014年下降58.5%。其中，我国境内感染的主机IP地址数量月均近48万个，较2014年下降53.4%。

（3）移动互联网安全监测

2015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1477450个，较2014年增长55.3%。

按行为属性统计，恶意扣费类的恶意程序数量仍居首位，为348859个，占



23.61%，流氓行为类328092个（占22.21%）、远程控制类222941个（占15.09%）分列第二、三位。

按操作系统分布统计，针对Android平台的移动互联网恶意程序占99.6%；其次是Symbian平台，占0.19%。

（4）网站安全监测

2015年，我国境内被篡改的网站数量为24550个，较2014年的36969个下降33.6%。其中，境内政府网站被篡改数量为898个，较2014年的1763个减少49.1%。

2015年CNCERT/CC共监测到境内75028个网站被植入后门，其中政府网站有3514个。向我国境内网站实施植入后门攻击的IP地址中，有31348个位于境外，主要位于美国（13.9%）、中国香港（6.5%）和韩国（6.0%）等国家和地区。

2015年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面184574个，涉及到境内外20488个IP地址。其中，83.2%的IP地址位于境外，中国香港（27.1%）、美国（9.4%）和韩国（2.2%）居前三位。从钓鱼站点使用域名的顶级域分布来看，以.com最多，占67.4%，其次是.cc和.pw，分别占12.3%和5.5%。

（5）安全漏洞公告与处置

2015年，CNVD收录新增通用软硬件漏洞8080个，包括高危漏洞2909个（占36.0%）、中危漏洞4553个（占56.4%）、低危漏洞618个（占7.6%）。

与2014年相比，2015年CNVD收录的漏洞总数下降11.8%，其中高危漏洞增长21.5%，中危漏洞减少24.5%，低危漏洞减少16.1%。

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62.0%），Web应用漏洞（占14.4%）和网络设备漏洞（占12.5%）。

2015年，CNVD共收录漏洞补丁6835个。

（6）网络安全事件接收与处理

2015年，CNCERT/CC共接收境内外报告的网络安全事件126916起，较2014年增长了125.9%。其中，境内报告的网络安全事件126424起，较2014年增长了128.6%，境外报告的网络安全事件数量为492起，较2014年下降了43.9%。接收的网络安全事件中，数量排前三位的分别是网页仿冒事件（占59.8%）、漏洞事件（占20.2%）和网页

篡改事件（占9.8%）。

2015年，CNCERT/CC共成功处理各类网络安全事件125815起，较2014年的56072起增长124.4%。其中，处理数量排名前三的分别是网页仿冒事件（占59.7%）、漏洞事件（占20.2%）和网页篡改事件（占9.8%）。

（7）网络安全信息通报情况

2015年，CNCERT/CC共收到各单位报送的月度信息369份，事件信息和预警信息497份，全年共编制并向各单位发送《互联网网络安全信息通报》23期。

2015年，CNCERT/CC通过发布网络安全周报、月报、专报、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254份。



网络安全专题分析

2.1 网络安全威胁治理专项行动（来源：CNCERT/CC）

2.1.1 行动背景

2.1.1.1 地下黑色产业链严重危害互联网生态安全

随着信息技术的快速发展和互联网应用的日益普及，特别是近年来互联网新技术、新应用的成熟应用，人民群众的日常工作、生活对互联网的依赖程度越来越高。受经济利益驱动，以分布式拒绝服务攻击（以下简称“DDoS攻击”）、网页篡改为代表的黑客活动呈快速增长趋势，并形成地下黑色产业链，严重危害互联网用户和企业的切身利益。

地下黑色产业链庞大且分工精细化，大致分为：组织者、恶意程序开发者、恶意程序传播和贩卖者、网络攻击入侵和网络欺骗的实施者、“肉鸡”、用户信息和攻击服务的贩卖商等多个环节。其中，组织者处于整个链条的顶端，对产业链的各个环节进行分工和协调。根据组织者的要求，由专门编写恶意程序的人员开发出各种木马程序、钓鱼网页程序等。

（1）DDoS攻击危害公共互联网秩序和基础网络安全

CNCERT/CC抽样监测发现，2015年1-6月1Gbit/s以上的DDoS攻击事件日均数量为1558起，与2014年全年的日均1283起相比，日均增长275起，增长了21.4%。近三年来CNCERT/CC重点分析的30起大流量DDoS攻击事件中，查明其中75%以上的攻击与地下黑色产业链有关，查实其中约40%的攻击是由于游戏私服网站之间的争斗发起的，涉黑产典型DDoS攻击事件清单见表2-1。例如，2015年8月25日凌晨，针对传奇私服发布网站www.rfinfo.cn的大规模域名请求攻击，造成我国国家顶级域.CN的域名解析出现异常，从而引起了部分地区.cn域名出现大规模访问故障。

表2-1 CNCERT/CC近5年监测处置的部分涉黑产典型DDoS攻击事件列表

时间	事件	峰值流量	攻击性质
2015年6月16日	某博彩网站被攻击事件	15Gbit/s	对博彩网站的攻击
2015年5月29日	某游戏私服被攻击事件	10Gbit/s	对游戏私服网站的攻击
2015年5月21日	某色情网站被攻击事件	4Gbit/s	对色情网站的攻击
2015年3月2日	某色情网站被攻击事件	20Gbit/s	对色情网站的攻击
2015年2月11日	浙江宁波某IDC机房被攻击事件	40Gbit/s	对托管游戏网站的攻击
2014年12月20日	阿里云被攻击事件	453Gbit/s	对托管游戏的攻击
2014年10月28日	浙江宁波某IDC机房被攻击事件	40Gbit/s	对托管游戏网站的攻击
2014年6月13日	某游戏私服DNS服务器被攻击事件	3Gbit/s	对游戏私服DNS服务器的攻击
2014年6月8日	人民网DNS服务器被攻击事件	1Gbit/s	为他人发动攻击获经济利益
2014年5月25日	云服务商UCLOUD被攻击事件	120Gbit/s	对托管游戏的攻击
2014年1月20日	浙江宁波某IDC机房被攻击事件	30Gbit/s	对托管游戏网站的攻击
2013年10月18日	浙江宁波某IDC机房被攻击事件	20Gbit/s	对托管游戏网站的攻击
2013年8月31日	爱民网被攻击事件	50Gbit/s	对游戏私服DNS服务器的攻击
2013年8月25日	825CN顶级域名服务器被攻击事件	13Gbit/s	对游戏私服网站的攻击
2013年3月29日	某游戏私服被攻击事件	3Gbit/s	对游戏私服网站的攻击
2013年3月17日	浙江宁波某IDC机房攻击事件	32Gbit/s	对托管游戏网站的攻击
2012年7月10日	工业和信息化部网站流量异常事件	350Gbit/s	游戏私服网站www.hlt3.com转嫁
2012年5月17日	美国DNS MADE EASY公司 投诉攻击事件	40Gbit/s	对游戏私服的DNS放大攻击
2012年5月1日	广东湛江电信机房DDOS攻击事件	40Gbit/s	对托管游戏网站的攻击
2012年2月10日	某游戏私服网站被攻击事件	3Gbit/s	对游戏私服网站的攻击
2012年2月10日	广东省公安厅网站流量异常	4Gbit/s	私服外挂网站www.52blt.com转嫁
2012年2月7日	多省DNS流量异常事件	80Gbit/s	对游戏私服网站权威服务器的攻击
2011年12月8日	美国NEUSTAR公司投诉攻击事件	40Gbit/s	对游戏私服的DNS放大攻击
2011年8月26日	浙江某游戏网被攻击事件	30Gbit/s	对游戏网站的攻击
2011年8月18日	新疆电信DNS流量异常事件	800Mbit/s	对游戏私服网站权威服务器的攻击
2011年5月17日	工业和信息化部网站流量异常事件	1Gbit/s	私服网站www.cnlipan.com转嫁
2011年3月24日	北京市公安局网站流量异常事件	200Mbit/s	卖药网站www.hbgroujian.com转嫁
2010年8月4日	某游戏网站被攻击事件	64Gbit/s	对游戏网站的攻击
2010年7月30日	某棋牌网站被攻击事件	112Gbit/s	对游戏网站的攻击
2010年7月1日	某游戏充值网站被攻击事件	1Gbit/s	对游戏充值网站的攻击



（2）网页篡改危害网站声誉及正常业务的开展

2014年CNCERT/CC抽样监测发现，我国境内被恶意篡改的网站36969个，较2013年增长54%，主要表现为篡改网页内容、植入暗链。2015年6月16-30日期间被篡改网站7660个，其中政府网站223个。在被篡改的网站中，约40%的网站（其中不乏政府网站）被植入了博彩相关的内容或暗链。此类篡改行为既违反了国家禁止赌博的法律，又严重影响了被篡改网站的声誉及网站正常业务的运行。

（3）DDoS攻击工具及服务、网页挂链服务在互联网上公然叫卖

游戏私服等行业之间的恶性竞争、违法广告与灰色推销等现象导致DDoS攻击工具及服务、网页挂链服务在互联网上公然叫卖和泛滥成灾，这些不法工具和服务降低了网络攻击的成本和技术门槛，进一步加剧了公共互联网的安全风险。图2-1~图2-5展示了部分网络攻击服务的搜索结果。

[ddos攻击器|DDoS攻击者下载 1.5 绿色中文版 - 新云软件下载](#)



[↓ 下载地址](#) 22 KB - 免费软件 - 简体中文

简介：本软件是一个**DDoS攻击**工具，程序运行后自动驻入系统，并在以后随系统启动，在网上时自动对事先设定好的目标进行**攻击**。可...

[www.newasp.net/soft/...](#) 2013-07-16 - [快照](#)

[暴风DDOS DDOS攻击 DarkShell DDOS攻击器 NbDdos DDOS软件 -...](#)

暴风DDOS是一款超级牛B的**DDOS攻击**软件,在广大用户群中一直享有较好的口碑!本站提供免费**DDOS攻击器**下载,可以试用一个月,暴风DDOS工作室还为您提供NbDdos,DarkS...

[www.yddos.com](#) 2015-07-10 - [快照](#)

[DDOS攻击|DDOS攻击器|DDOS攻击教程|DDOS攻击软件-鬼影工作室](#)

鬼影工作室专注于**DDOS攻击器**开发,提供**DDOS攻击**教程,DDOS攻击工具及DDOS攻击软件下载等,并手把手教您彻底解决DDOS攻击困扰,为您的服务器保驾护航!

[www.gyddos.com](#) 2015-07-10 - [快照](#)

图2-1 DDoS攻击搜索引擎搜索结果



图2-2 DDoS攻击社交网络搜索结果



图2-3 DDoS攻击售卖平台

黑链,买黑链,挂黑链,黑链交易网

我们支持淘宝交易,加入消费者保障服务计划,让您无忧**购买**,无数的客户对我们表扬,让我们做的更好 淘宝店铺: **黑链交易**淘宝旺旺:点击这里给我发消息 最新更新文章 May...

www.heilianwang.com/ - 百度快照 - 评价

黑链买卖网 - 低成本高效优化网站



黑链买卖网,缔造行业旗舰品牌,**黑链**低成本快速优化网站。... **黑链**的模式主要是随机链接不予挑选,很多客户不理解认为因该区分PR,因为我们并不是明链,所以请不要用挑...

www.tw747.com/ - 百度快照 - 评价

第一黑链网

1.以上所有套餐可以按季度支付价格更优惠,链接买卖的站属于隐藏链接(**黑链**) 2....**黑链** 黑帽 **黑链**购买 **黑链**出售 **黑链**交易 **黑链**买卖 优质**黑链** 探索**黑链**的秘密...

www.diyiheilian.com/ - 百度快照 - 评价

黑链购买 百度知道

1个回答 - 提问时间: 2011年10月09日

问题描述: 请问**购买黑链**做排名怎么样?

1:**黑链**是外链中最容易获得的一种,网站优化外链为皇,网站的权重靠内容外链支撑,外链的提高有助于被收录内页的排名 2:**黑链**比手动发论坛签名回复/博客群建权重高...

更多关于**黑链** 购买的问题>>

zhidao.baidu.com/link?... - 百度快照 - 80%好评

黑链交易网 - 廉价网站优化首选



黑链交易网,打造全国最大的**黑链**行业门户!... 最近学习了排名优化,**购买**了友情链原来有排名自己做老板真好...一直苦于给用户加友情链接高昂的成本,现在有了**黑链**交易网...

www.8888y.com/ - 百度快照 - 评价

图2-4 暗链搜索引擎搜索结果

第一黑链网

在线客服: 2180917399 (点击咨询) QQ交谈

首页 黑链代码 挂黑链 黑链SEO 黑链资讯 网站推广 其他技术 购买黑链

中文客服时间: 在线客服: 2180917399 (点击咨询) QQ交谈

方案名称	PR值	网站数量	月付	季付	续费
A套餐	PR1 PR2	PR1=10个PR2=10个共20个站	30元	60元	续费
B套餐	PR2 PR3	PR2=10个PR3=10个共20个站	50元	100元	续费
C套餐	PR3 PR4	PR3=10个PR4=10个共20个站	70元	140元	续费
D套餐	PR3	PR3=10个共10个站	35元	70元	续费
E套餐	PR4	PR4=10个共10个站	45元	90元	续费
F套餐	PR1 PR2 PR3 PR4	PR1=10个PR2=10个PR3=10个PR4=10个共40个站	80元	160元	续费
G套餐	PR1 PR2 PR3 PR4	PR1=20个PR2=20个PR3=20个PR4=20个共80个站	150元	300元	续费
H套餐	PR1 PR2 PR3 PR4	PR1=30个PR2=30个PR3=30个PR4=30个共120个站	220元	440元	续费
J套餐	PR1 PR2 PR3 PR4	PR3-PR4随机 共500个站	390元	780元	续费

包月套餐价格: 在线客服: 2180917399 (点击咨询) QQ交谈

方案名称	PR1	PR2	PR3	PR4	PR5	PR6	套餐说明	新报价	续费
包月套餐一	3	3	4	3	-	-	持续增加链接30日共390个站	300元	续费
包月套餐二	-	-	8	5	-	-	持续增加链接30日共390个站	525元	续费
包月套餐三	-	-	6	5	2	-	持续增加链接30日共390个站	675元	续费
包月套餐四	-	-	5	4	2	2	持续增加链接30日共390个站	780元	续费
包月套餐五	-	-	-	8	5	-	持续增加链接30日共390个站	840元	续费
包月套餐六	7	7	-	-	-	-	持续增加链接30日共420个站	225元	续费
包月套餐七	-	-	-	-	-	-	每天随机增加PR2-PR6链接 35条 持续增加链接30日共1050个站	630元	续费

中文客服时间: 在线客服: 2180917399 (点击咨询) QQ交谈

图2-5 暗链售卖平台

（4）黑客向年轻化发展，黑客团队向黑社会化发展

根据对网络攻击犯罪嫌疑人的年龄统计，网络攻击背后的黑客呈现年轻化趋势，相当比例的网络攻击犯罪嫌疑人在20~30岁，有不少嫌疑人甚至只有14、15岁。黑客通过社交媒体公然联络鼓动攻击，其沟通语言、行为方式、组织管理模式效仿黑社会。

一方面地下黑色产业链危害了公众的信息数据安全和财产安全，影响了互联网秩序，另一方面黑客地下团伙之间的恶性争斗、相互倾轧对公共互联网的安全运行构成威胁。有效防范治理网络安全威胁及地下黑色产业链将对保障网络信息安全、公众信息财产安全和互联网治理发挥积极重要的作用。

2.1.1.2 发挥行业自律作用，共治互联网安全环境

网络安全的本质是网络攻防对抗，互联网网络安全威胁治理的基础是要具备应对网络安全威胁和网络攻击的技术分析能力和处置能力。在国家层面提升对网络攻击和网络威胁的监测发现、分析追溯、处置恢复和预警防范的技术能力和业务水平，这是改善我国网络安全状况的重要核心。随着互联网的快速发展和电信企业、互联网企业体量的快速增长，需要将电信运营企业、域名服务企业、互联网企业等全面纳入我国网络安全防护体系，让相关机构企业和互联网用户在我国网络安全治理工作中充分发挥作用。

（1）引导行业自律，规范行业行为，成立行业联盟

网络攻击活动涉及多个环节，例如黑客团伙需要连接互联网、注册域名、购买入侵服务器、发布推广攻击工具服务，涉及基础电信企业、域名注册管理商、IDC、搜索引擎和社交媒体互联网企业等。因此，网络安全威胁的治理单靠行业主管部门是不够的，需要多方的共同参与，发挥各自的技术和资源优势，规范各自的行为并承担相应的社会责任，引导建立互联网行业自律机制和成立网络安全威胁治理联盟。

（2）鼓励企业投诉、群众举报，共同维护互联网安全

网络安全是国家、组织和个人的共同责任，通过鼓励企业投诉、群众举报，有效补充网络安全威胁治理的数据来源和线索证据，提升网络安全威胁治理的效率。



2.1.2 开展情况

2.1.2.1 启动互联网网络安全威胁治理行动

2015年7月31日，CNCERT/CC会同中国互联网协会网络与信息安全工作委员会发起了互联网网络安全威胁治理专项行动，对危害互联网用户和企业的切身利益、威胁我国基础网络设施和重要信息系统运行安全、影响我国互联网健康发展的地下黑色产业链进行专项整治。行动一经发起，就得到行业内广大企事业单位的积极响应。行动期间，先后有54家单位签订了行动承诺书，表示愿意同其他单位一起，以行业自律的方式，以“保护他人，即保护自己”的态度，共同打击以DDoS攻击、网页篡改为代表的制造、销售、传播网络攻击工具以及实施网络攻击行为的地下黑色产业链，共筑安全生态环境。

建立互联网网络安全威胁治理行动邮件列表和微信群，能够快速进行信息共享和事件的协同处置。同时，行动对外发布接收互联网网络安全威胁举报的热线电话和邮箱，接收广大群众的举报。图2-6展示某互联网公司发送的威胁举报邮件示例。



图2-6 某互联网公司网络安全威胁举报邮件示例

2.1.2.2 互联网网络安全威胁治理行动阶段总结

2015年9月25日，CNCERT/CC会同中国互联网协会网络与信息安全工作委员会在京召开专门研判会，出席会议的有80多位企业代表和专家。会议就前一段时间的工作进行总结，分析当前的形势，布置下一阶段的工作任务。

行动开展两个月以来，通过公开设立的举报电话及邮箱，共接到广大网民举报的网络安全事件29658起。经验证分析后，重点针对DDoS攻击、网页暗链篡改等与互联网黑产密切相关的事件进行重点处置。通过行动参与单位的密切配合，处置网络安全事件13573起，包括处置DDoS攻击服务售卖平台14个，DDoS攻击控制服务器51个，参与网络攻击的博彩、私服等网站链接3382个；关停未备案网站37个；通知1706个被篡改和916个被植入后门的网站用户单位对网站进行修复。此外，还组织了国内主流浏览器厂商对18502条恶意网站黑名单进行访问拦截或提示。行动取得初步成效，DDoS攻击事件次数由行动启动前的日均1491起下降到日均397起，大幅下降73.37%；8月境内被篡改网站相比7月下降了9.85%，其中境内被篡改政府网站数量下降了25.56%；浏览器拦截提示黑名单次数近千万次。

会议对行动取得的阶段性成果给予充分肯定，并对网络安全威胁治理行动参与单位提出希望：要继续支持和深化治理行动各项工作，探索建立威胁治理长效工作机制。

2.1.2.3 互联网网络安全威胁治理行动2015年年终总结

2015年12月底，CNCERT/CC对互联网网络安全威胁治理行动进行了年终总结。行动自启动以来，举全行业之力，通过投诉举报、情报共享、威胁认定、协同处置、信息发布等多项措施环环相扣，取得了显著治理效果。互联网黑产已经成为影响我国互联网正常运行的重要原因之一，如博彩或私服等网站链接通过向政府网站或知名网站植入暗链提高网络搜索排名，通过采用DDoS攻击对竞争对手发起网络攻击导致网络不能正常提供服务等。此次行动重点针对DDoS攻击、网页篡改等与互联网黑产密切相关的事件进行重点处置。行动期间共接到广大网民举报的网络安全事件109972起，处置网络安全事件71220起，包括处置DDoS攻击服务售卖平台14个，DDoS攻击和僵尸控制服务器668个，参与网络攻击的博彩、私服等网站链接6320个，通知7499个被篡改和2051个被植入后门的网站用户单位对网站进行修复等，发布黑名单地址54614条。DDoS攻击事件



次数由行动启动前的日均1491起下降到现在的日均265起，大幅下降82.2%；境内被篡改网站相比行动启动前下降21.4%，其中被篡改政府网站相比下降了56.2%。此次行动，直面互联网黑产背后存在巨大的利益链条，不惧触动链条上利益群体，行动参与单位排除顾虑，积极行动，对于发现的网上DDoS攻击售卖和传播等互联网黑产行为进行了坚决处置。2015年1-12月DDoS攻击事件数量按月统计如图2-7所示。

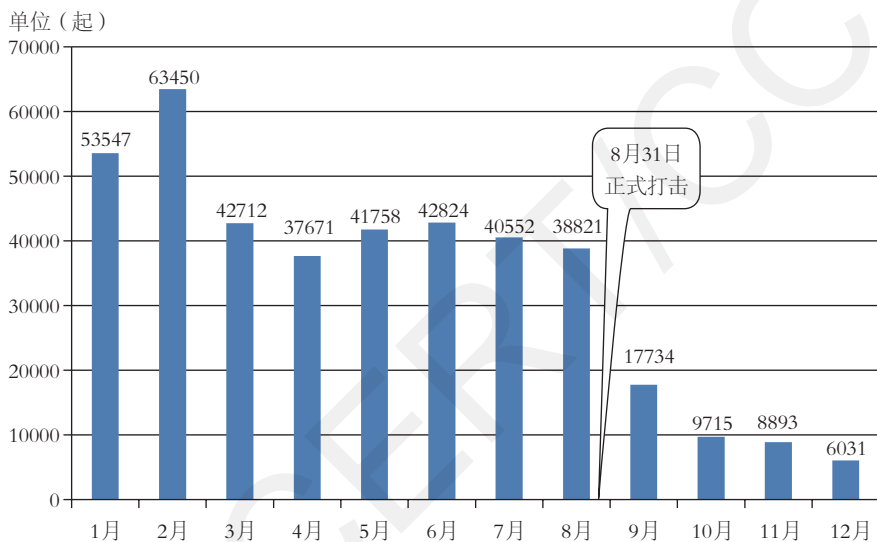


图2-7 2015年1-12月DDoS攻击事件数量按月统计

2.1.3 总结与展望

通过开展互联网网络安全威胁治理行动，积累了一条很重要的经验：依靠全行业的力量，网络安全可以做得更好。行动不能永远不结束，但是行动积累的经验可以固化保留。中国互联网网络安全威胁治理联盟的成立，为有关各方提供了一个行业内公共沟通交流的平台，以行业自律为主导，联合网络安全领域上下游各方面的力量，充分发挥联盟成员单位的作用，加强互联网网络安全威胁的情报共享、相互协作，对与互联网黑产密切相关的各类威胁进行整治，有效净化网络安全环境，维护用户网络安全和利益，树立我国负责任网络大国的良好形象。

2.2 广告平台传播恶意扣费APP专题分析（来源：CNCERT/CC）

2.2.1 背景分析

目前，政府部门对于应用商店的管理逐渐完善，应用商店建立手机APP的安全审核机制，具有恶意扣费行为的APP很难通过应用商店的安全审核，无法在应用商店上架，使得灰产从业者很难直接利用应用商店向用户推送恶意扣费APP。

但现实中，灰产从业者利用一种恶意APP的嵌套方法可以绕过应用商店的安全审核机制，那就是在没有恶意行为的APP中嵌入广告推送插件。利用广告推送插件，灰产从业者可以在云端向用户远程推送正常内容的同时，也推送恶意扣费APP，诱骗用户下载安装。当应用商店在审核APP时，如果APP中的广告内容无恶意内容，那么这些APP就会通过审核进行上架发布。

通过“内容时变”的广告推送方式，在正常的广告内容中掺杂恶意APP，导致这些掺杂恶意广告内容的APP能够通过应用商店的安全检测。正是利用这种方法，灰产从业者可以选择时下热门的APP嵌入“恶意广告”，一方面利用“热门APP”作为幌子诱骗用户下载安装，另一方面通过植入“恶意广告”达到牟利目的。

2.2.2 恶意扣费APP分析

以2015年年底出现大量恶意“抢票软件”为例，这些“抢票软件”通过应用内的插屏广告平台推送大量带有低俗内容的广告，诱骗用户点击安装，其中大部分都有恶意扣费行为。以一款名为“智能火车票抢票刷票软件”为例，如图2-8所示，在主流的应用市场都可以找到。



图2-8 应用商店中上架的“智能火车票抢票刷票软件”（来源：CNCERT/CC）

这款名为“智能火车票抢票刷票软件”除了查询火车票的功能外，主要行为是采用插屏广告方式推送其他应用，其中包含大量带有低俗内容的APP，如图2-9所示。



图2-9 安装使用“智能火车票抢票刷票软件”过程中弹出的广告内容
(来源: CNCERT/CC)

用户点击这类广告会自动安装相应的APP, 该类APP普遍具有信息窃取、恶意扣费等恶意行为。如图2-10所示, 以CNCERT/CC捕获的一款带有低俗内容的“爱爱视频”APP为例, 该程序窃取用户信息, 拦截提示短信, 私自替用户发送回复短信, 达到恶意扣费的目的。其恶意行为具体如下。



图2-10 “爱爱视频”私自上传用户信息并获取扣费SP端口和扣费指令
(来源: CNCERT/CC)

- (1) 恶意程序运行后, 私自上传用户手机固件、地理位置等信息到远程服务器。
- (2) 如图2-11所示, 恶意程序从服务器获取电话号码、短信内容, 私自向该号码发送短信订购扣费业务, 从服务器端获取的电话号码为10655598201, 短信内容为“3317567”和“3217123”, 后台私自发送短信。



图2-11 “爱爱视频”私自向指定SP端口发送带有扣费指令的短信
(来源: CNCERT/CC)

- (3) 如图2-12所示, 恶意程序私自拦截、屏蔽电话号码为“10086、10010、10000”或以“1062、1065、1066、182231”开头的短信, 即SP业务订购回执短信, 解



析短信内容，发送回复确认短信，并删除该短信。



图2-12 “爱爱视频”软件中存在拦截短信和自动回复短信的代码
(来源: CNCERT/CC)

过滤是否为指定条件的短信。“爱爱视频”软件中拦截手机号如图2-13所示。



图2-13 “爱爱视频”软件中拦截手机号 (来源: CNCERT/CC)

(4) 如图2-14、图2-15所示，恶意程序私自推广其他APP，创建桌面快捷图标，诱骗用户点击下载、安装。

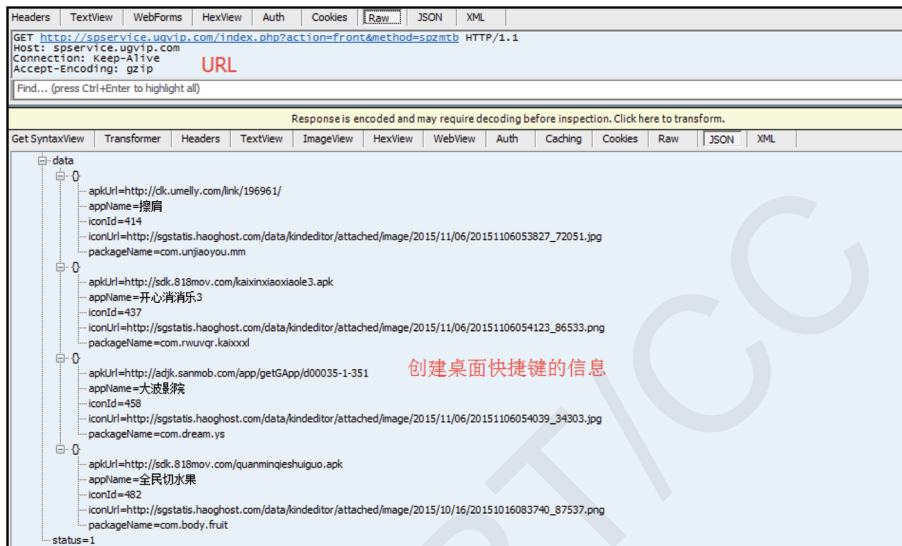


图2-14 “爱奇艺”软件推送其他APP的数据（一）（来源：CNCERT/CC）

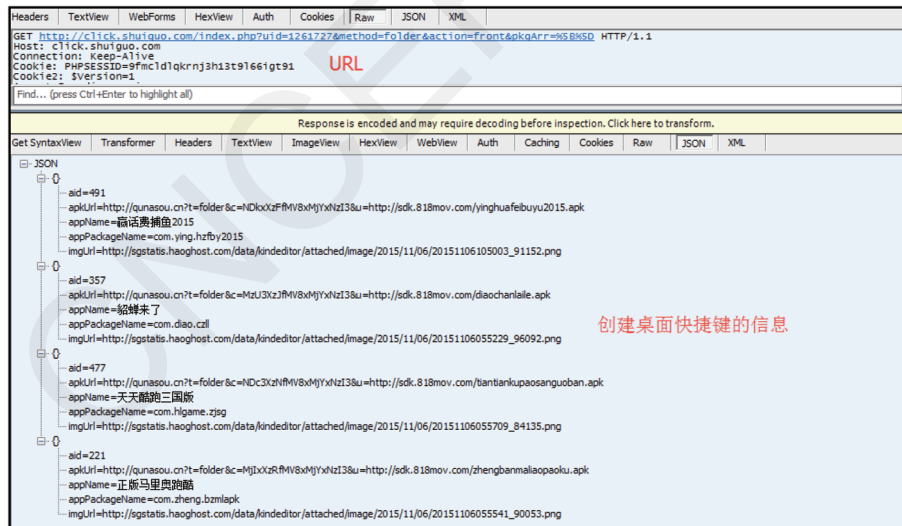


图2-15 “爱奇艺”软件推送其他APP的数据（二）（来源：CNCERT/CC）

（5）如图2-16所示，恶意程序私自联网获取其他APP信息列表，在后台下载并安装。

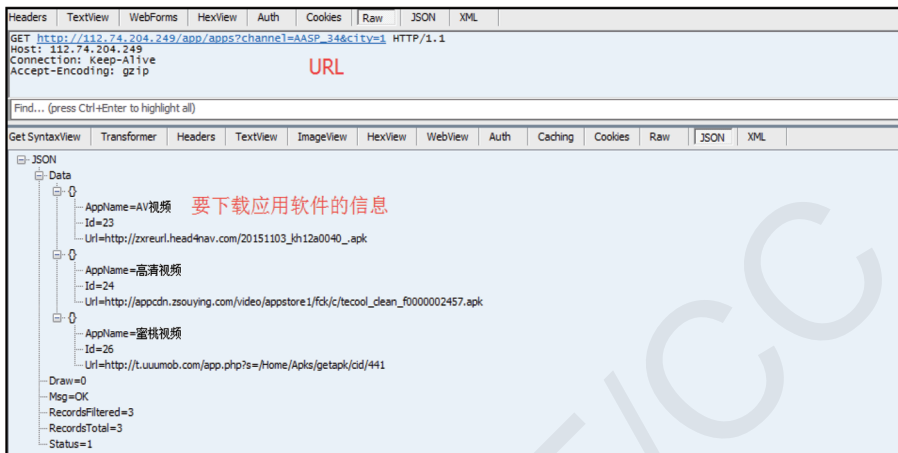


图2-16 “爱爱视频”软件后台下载其他APP（来源：CNCERT/CC）

（6）如图2-17所示，恶意程序病毒弹窗诱导用户下载、安装恶意插件。

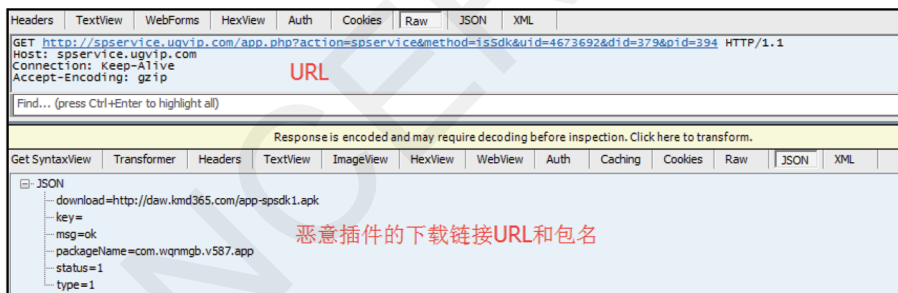


图2-17 “爱爱视频”软件弹窗诱导用户安装插件的数据（来源：CNCERT/CC）

如图2-18所示，弹窗提示，诱导用户点击下载、安装恶意插件。

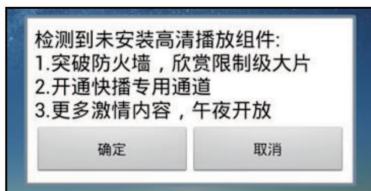


图2-18 “爱爱视频”软件弹窗界面（来源：CNCERT/CC）

(7) 如图2-19所示, 恶意插件安装后, 运行后通过弹窗、创建桌面快捷图标等方式诱骗用户点击下载、安装其他应用软件。

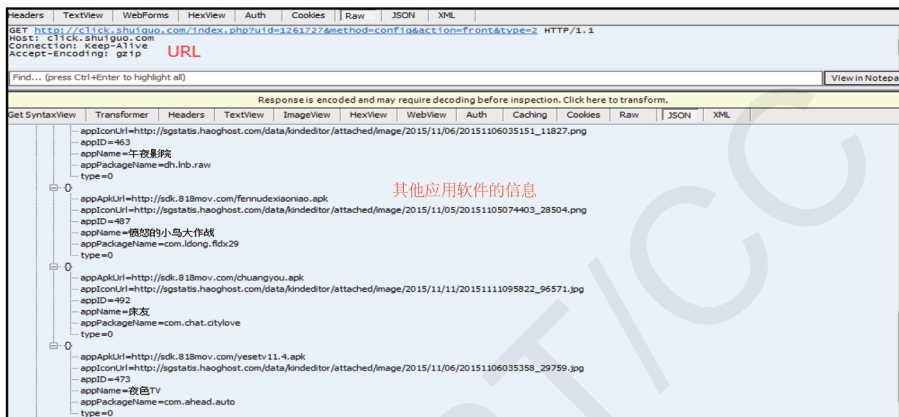


图2-19 “爱爱视频”软件诱导用户安装插件后推广其他APP的数据
(来源: CNCERT/CC)

根据CNCERT/CC对“爱爱视频”的监测结果, 全国感染“爱爱视频”恶意程序的用户超过120万。经过CNCERT/CC对工商部门提供的取证数据进行分析, 2015—2016年间“爱爱视频”恶意程序累计扣取用户话费超过2000万元。

2.2.3 恶意扣费APP传播方式分析

由于高额商业利益的驱使, 国内出现大量从事APP推广的公司和人员, 使得APP在传播渠道上乱象丛生, 存在大批不合规的APP推广方式。由于恶意扣费APP无法在正规的应用商店进行发布, 使得不法分子通过各种渠道去应用商店外的其他渠道推广恶意APP。在QQ群中搜索“APP推广渠道”, 可看到大量用于讨论手机APP推广的QQ群, 如图2-20和图2-21所示。



图2-20 用于讨论“APP推广渠道”的QQ群列表一（来源：CNCERT/CC）



图2-21 用于讨论“APP推广渠道”的QQ群列表二（来源：CNCERT/CC）

如图2-22和图2-23所示，从QQ群中的聊天内容可以看到“明扣”、“静默产品”、“诱导量”等字眼。例如，“一手静默产品，月初通道好，转化高，三网，实

时，日结，寻量大渠道，欢迎渠道拿包上线测试！”。



图2-22 用于讨论“APP推广渠道”的QQ群聊天记录一（来源：CNCERT/CC）

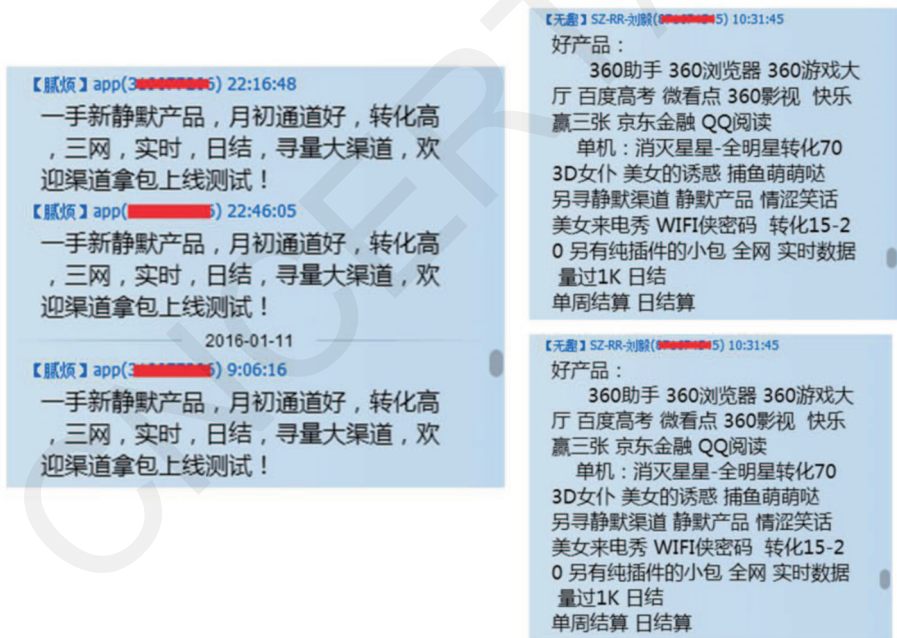


图2-23 用于讨论“APP推广渠道”的QQ群聊天记录二（来源：CNCERT/CC）

2015年CNCERT/CC累计协调应用商店、网盘、广告平台等302家网站下架恶意APP达1.7万个，未来CNCERT/CC将继续做好移动恶意程序传播源打击治理工作，切断移动恶意程序的传播途径。



2.3 工业互联网安全分析（来源：CNCERT/CC）

2015年12月23日，乌克兰发生了一次影响很大的通过有组织、有预谋的定向网络攻击致使乌境内近三分之一的地区持续断电的安全事件。此次事件表明：关键基础设施已经成为网络攻击的对象，而且一旦被攻击导致瘫痪，将给国家安全、社会稳定造成不可估量的伤害。此外，攻击主体已经上升到黑客组织乃至国家层面，攻击手段也日益专业化、组织化、精确化。

“乌克兰电力系统被攻击事件”对我国极具警示意义，CNCERT/CC利用技术手段对我国关键基础设施网络安全形势开展初步调研和分析，其结果不容乐观，加强相关安全技术保障能力建设已是我国“工业转型升级”、“两化融合”背景下的当务之急。

2.3.1 事件分析及趋势推断

2.3.1.1 乌克兰电力系统被攻击事件简析

据知名安全公司ESET分析验证，乌克兰国家电力系统所感染的是一款名为“黑暗力量（BlackEnergy）”的恶意软件。如图2-24所示，在乌克兰电力系统被攻击事件中，其攻击路径如下。

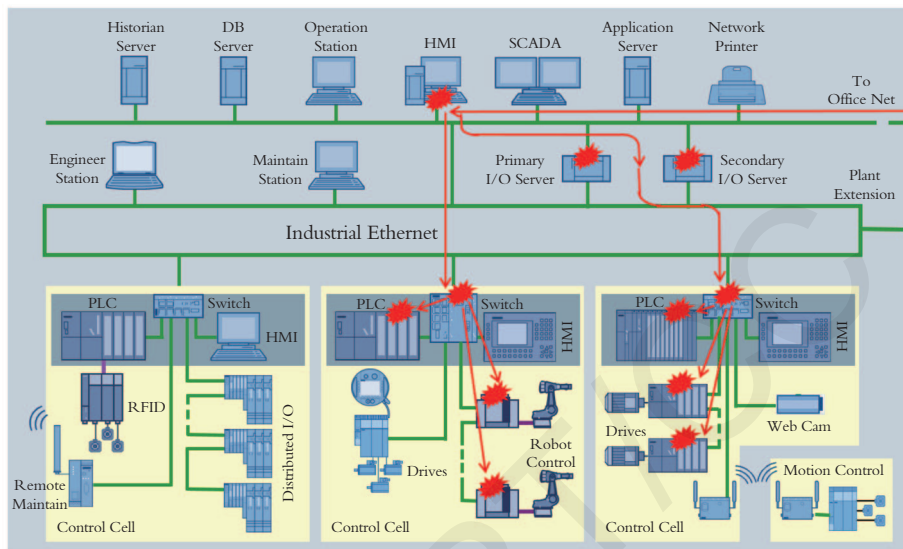


图2-24 BlackEnergy的攻击路径示意

(1) 黑客先收集目标用户邮箱，然后向其定向发送携带恶意文件的鱼叉钓鱼邮件，疏于安全防范的用户在SCADA系统中打开了带宏病毒的Office文档（或利用Office漏洞的文档）即可运行Installer（恶意安装程序），Installer则会释放并加载Rootkit内核驱动，之后Rootkit使用APC线程注入系统关键进程svchost.exe（注入体main.dll），main.dll会开启本地网络端口，使用HTTPS协议主动连接外网主控服务器，一旦连接成功，开始等待黑客下发指令就可以下载其他黑客工具或插件。

(2) 黑客利用BlackEnergy作为后门，利用感染的主机进行进一步的入侵，包括搜集情报、添加SSH后门、下载KillDisk组件等。

(3) 黑客远程控制被劫持的SCADA系统下达断电指令，并利用KillDisk摧毁SCADA系统的上位机以阻滞电力系统的恢复，并清除入侵痕迹。与此同时，利用拨号DDoS阻塞电力公司的服务电话，最终实现目标电力系统的长时间停电。

2.3.1.2 伊朗核设施被攻击事件简析

震网病毒（Stuxnet）是全球首款专门针对工控系统的APT网络武器，它的设计思想和实现机制都非常精巧，并成功实施对伊朗核设施的攻击。如图2-25所示，其攻击



路径如下。

- Stuxnet首先通过其恶意传播组件广泛感染大量联网主机，并最终实现对目标U盘或便携式终端的感染；
- 当被感染的U盘或便携式终端接入到工业控制网络中，Stuxnet就会在整个工控网络内部传播，如感染到HMI（上位机）；
- 注入在HMI中的Stuxnet通过WinCC与PLC通信，向其植入恶意程序或直接发送控制指令，从而实现对生产设备的操控而导致物理损伤。

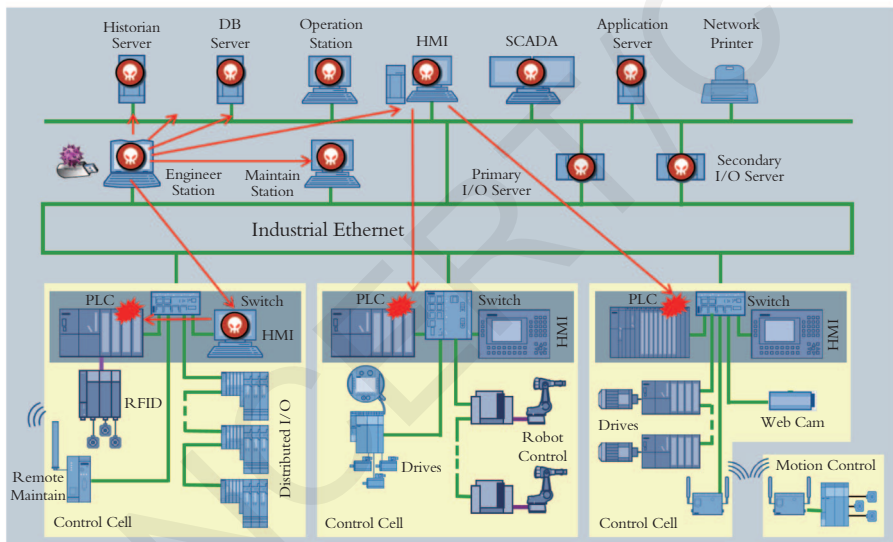


图2-25 Stuxnet的攻击路径示意

2.3.1.3 事件对比分析及趋势推断

两次典型安全事件的对比分析，见表2-2。

表2-2 两次典型安全事件的对比分析

	震网（Stuxnet）	黑色能量（BlackEnergy）
攻击目标	伊朗核设施	乌克兰发电站（电力系统）
攻击源	美国政府	黑客组织（俄政府背景）
目标属性	军工，高度警戒	民用，重点防护
联网与否	隔离，非联网	直接或间接联网
攻击方法	摆渡攻击、自动扩展	协同攻击、远程操控
核心部件	HMI、PLC	HMI、PLC
攻击效果	精确攻击、定向清除	大面积瘫痪

由此，我们可以得出以下基本推断。

（1）针对国家关键基础设施的网络攻防对抗研究将成为各国政府、安全界乃至暴恐组织的关注重点，相关的安全事件将持续增加。主要依据如下：

- 从震网和乌克兰电站两次安全事件来看，美俄两个主要大国均已具备很强的针对关键基础设施的网络攻击能力，并持续增强其网络攻击能力。可以想见，世界主要的信息强国必将加强研究，发展其相应的攻防能力。

- 无论是从攻击效果，还是攻击成本、攻击隐蔽性乃至攻击可控性来看，针对国家关键基础设施的网络攻击将有可能逐步取代传统的军事战争，成为各国政府的优先选择手段之一。

- 与传统的物理攻击方式相比，网络攻击对攻防双方具有较强的不对称性（远程、普适、隐匿、经济），未来必将成为暴恐组织的优先选择手段之一。

（2）对绝大多数关键基础设施而言，无论联网与否，都不是保证其安全的充分条件。特别地，随着互联网与信息技术的应用不断拓展，开放互联是大势所趋，因此关键技术设施将面临更为严峻的网络安全威胁。

（3）对绝大多数关键基础设施而言，SCADA/HMI和PLC两个产品处于信息化与自动化的结合环节，它们因此也成为网络攻击的主要对象和核心环节。其他的某些非关键主机，在面临普通病毒侵袭时也是非常脆弱的。



2.3.2 我国关键基础设施网络安全形势

2.3.2.1 电力行业网络安全形势

根据发改委2014年发布的第14号令《电力监控系统安全防护规定》^[13]，电力监控系统安全防护的总体策略可简单归纳为16字方针，即：“安全分区、网络专用、横向隔离、纵向认证”，如图2-26所示。

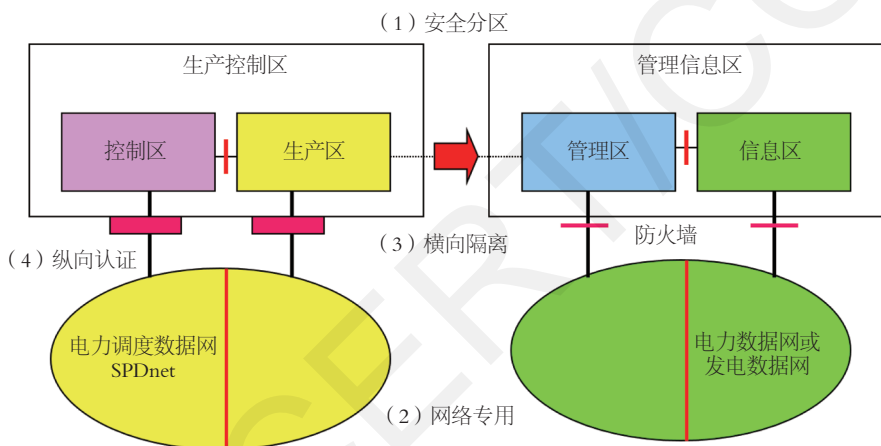


图2-26 电力监控系统的总体安全策略

(1) 发电侧

实际应用中，传输环节（即电网，主要为国家电网和南方电网两家企业垄断）对安全比较重视，防护措施及运维管理均较为严格。发电侧的情况则较为复杂，除5大发电集团之外，还存在着许多大大小小的民营发电企业（尤其是新能源领域），这些企业的安全意识相对较为薄弱。

多数情况下，各发电企业拥有的发电厂站与电网调度控制中心（生产控制区）的连接如图2-27所示。

[13] 由电监会2009年发布的《电力二次系统安全防护规定》演变而来。

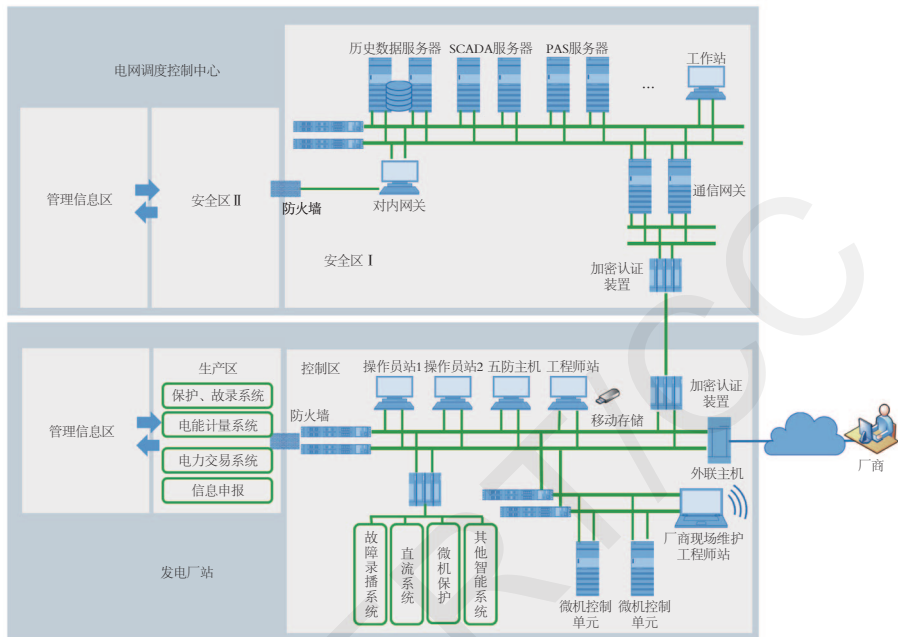


图2-27 发电厂站与调控中心的连接示意

据了解，目前我国发电厂站普遍存在运维人员技术水平不高、安全意识薄弱的问题。尽管电力行业全面推行《电力监控系统安全防护规定》，但在发电厂站层面，两种违规行为仍相当普遍：第一，系统集成商派工程师驻场提供调试维护服务，调试人员违反安全规定使用联网调试终端，或者调试终端自身的安全性并未达到电力系统的安全要求；第二，设备厂商为降低成本而采用远程维护方式，通过互联网（以ADSL/3G/4G等方式）远程接入电厂监控系统。无论哪一种行为，都相当于将电力的生产控制区直接或间接地接入互联网。此外，近年来兴起的各种新能源发电，如风电、光伏发电等及其并网也加剧了此种安全风险。

（2）用电侧

用电侧的安全风险同样不可忽视。近年来，用电侧开始大量接入智能电表、电动汽车充电桩等智能终端设备，同时利用IT构建用电信息采集和计费管理系统（如图2-28所示），并接入到电力监控系统。这些智能终端设备/系统一方面在地理



上高度分散，无法用物理防护措施防止攻击者的访问；另一方面大量的设备需要借助于电信网或3G/4G等公共网络与系统主站通信，从而直接或间接地与互联网相连接。这就给电力监控系统带来新的安全威胁。

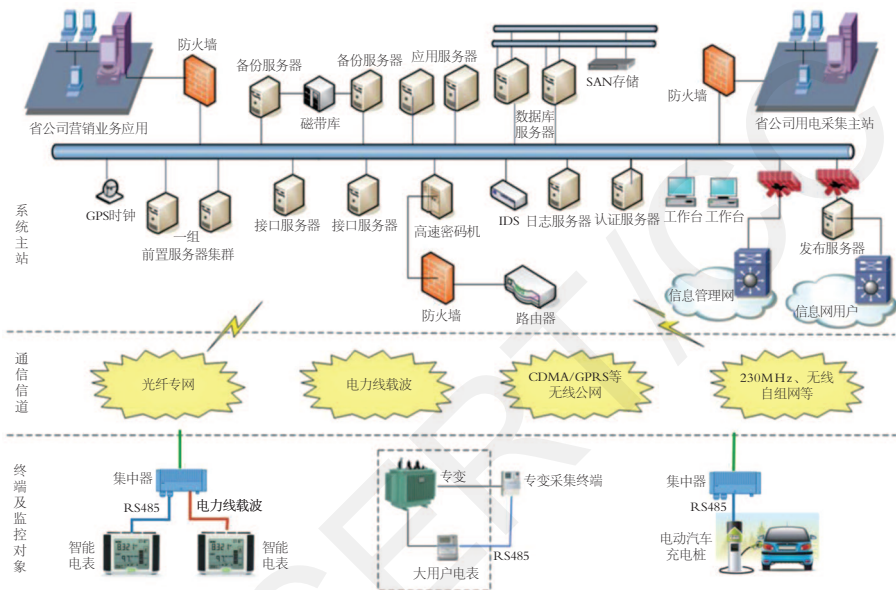


图2-28 用电信息采集与计费管理系统

事实上，早在2009年与2013年的Blackhat大会上，就有安全人员在讨论攻击智能电表。2014年，在荷兰阿姆斯特丹举行的Blackhat欧洲大会上，研究人员公布他们发现西班牙所使用的智能电表中存在安全漏洞，该漏洞可以导致电费欺诈甚至进入电路系统导致大面积停电。据统计，西班牙三家主要的电力公司——Endesa、Iberdrola和E.ON大约安装有800万台存在漏洞的智能电表，占全国总数近30%。一旦该漏洞被黑客利用实施攻击，肯定会影响国家安全与社会稳定。

2.3.2.2 关键基础设施行业网络安全总体形势

在“乌克兰事件”中遭受攻击的电力系统属于关键基础设施的范畴。依据国际社会的界定，关键基础设施涵盖一系列关系国计民生的基础性行业，集中于电力、供水、石油、天然气、通信、交通、化工、核设施等领域。关键基础设施通常包括信息

网络和控制网络两大部分。其中信息网络是指企业的业务网，大多可访问互联网；控制网络通常又称为工业控制系统。

CNCERT/CC针对国内关键基础设施及其工业控制系统的网络安全总体形势开展了初步调研和分析，其结果不容乐观。

(1) 国外工控产品占据国内市场份额的主导，且大多存在安全漏洞风险。

工业控制系统的核心软硬件产品主要包括SCADA/HMI监控软件和PLC，据《2014年中国工业控制系统信息安全蓝皮书》的调研数据，在国内工控HMI监控软件市场，国外产品的市场份额约为74%，占主导地位；在国内PLC市场，95%以上产品来自国外公司。然而，这些软硬件产品大多存在安全漏洞风险，如图2-29所示，自2010年“震网”事件后，CNVD每年收录的工控产品漏洞数量始终处于高位，如图2-30所示，2015年共收录公开工控漏洞125个，涉及多个国内外工控厂商的多款产品。

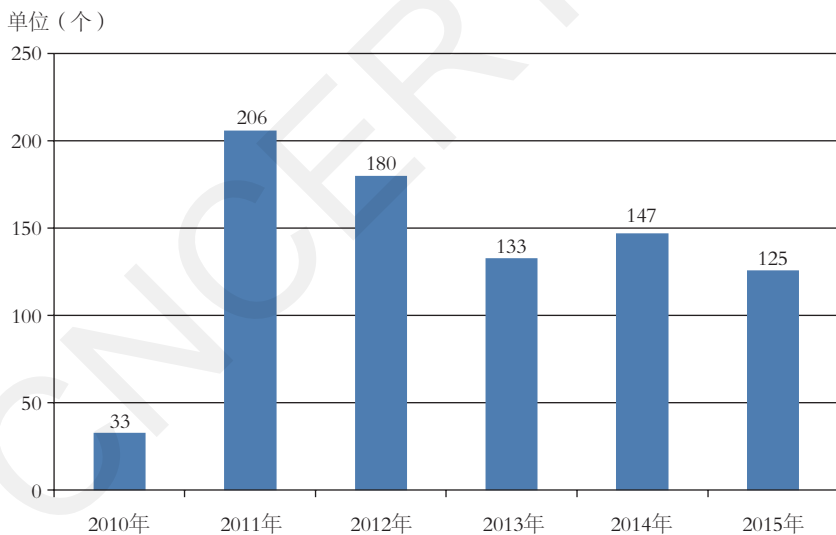


图2-29 2010-2015年CNVD工控漏洞收录情况

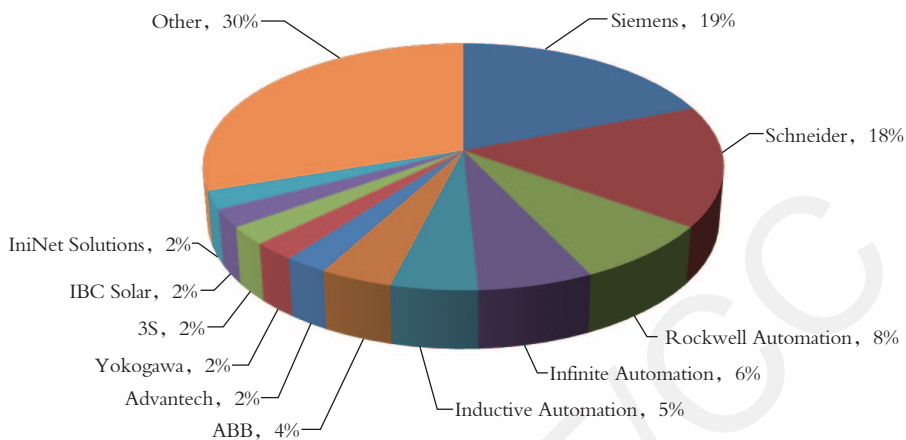


图2-30 2015年CNVD收录工控漏洞按厂商分布

对于SCADA/HMI监控软件，由于其通常承载在Windows或Linux系统上，采用C/S或B/S架构，攻击者可利用传统IT对其渗透，进而操控PLC，实现对物理设备的控制与损伤。2015年10-11月期间，安全中心针对国内外部分工控系统开展安全测试，成功渗透了30多个系统，涉及生产制造、燃气、污水处理、水利设施、智能楼宇等多个领域。

PLC主要涉及嵌入式系统漏洞挖掘利用，在过去一年中，施耐德的Quantum和M340两款主流PLC连续被安全界挖掘出一系列低级安全漏洞。以M340系列PLC为例，2015年被发现存在缓存区溢出漏洞（CVE-2015-7937），不但可以导致设备崩溃，还可能被利用，从而在设备内存中远程执行任意代码。以Quantum系列PLC的以太网模块为例，早在2011年就被发现存在固件后门的高危漏洞（CVE-2011-4859）；但直到两年之后，施耐德官方才通过升级设备固件的方式进行修复。即使如此，2015年8月的联网设备漏洞探测结果表明：暴露在互联网的Quantum相关设备，仍有超过20%没有进行固件升级以修复其安全漏洞，可以轻易进行远程访问。

（2）外国工业产品广泛分布在我国各个地区的重要关键领域。

根据MIR睿工业的市场调研统计，作为最早进入中国的工控企业之一，西门子WinCC的市场占有率稳居首位，达到24%，主要应用在钢铁、烟草、水处理、石油石

化、电力等行业；通用电气的Cimplicity紧随其后，市场占有率为14%，主要应用在汽车、石油石化、水处理、轨道交通等行业；而研华科技的WebAccess利用其价格优势，主要应用在智能楼宇、船舶、石油石化、水处理等行业中，市场占有率大约为2.3%。

（3）主动巡检发现全国各地工业设备及系统连接互联网现象普遍，且主要集中在北京、上海等经济发达地区。

由于工业控制系统（包括通信协议、软硬件系统）从设计到实现都先天性缺乏对网络安全因素的考虑，因此它抵御网络攻击的能力特别薄弱，一旦暴露在互联网中，将面临严重的网络安全威胁。

CNCERT/CC利用主动探测技术，发现中国境内联网工控系统设备及组件共2737个，其中大陆地区1267个，台湾地区1470个。如图2-31所示，设备类型包括PLC（306个）、Modbus子站（1039个）、Web-SCADA（600个）、OPC服务器（26个）、HMI主机（24个）、串口转换器（499个）、通信处理器（3个）、远程I/O（37个）、内嵌Web（32个）和其他未识别设备（85个）。按设备生产厂商统计排名如图2-32所示。

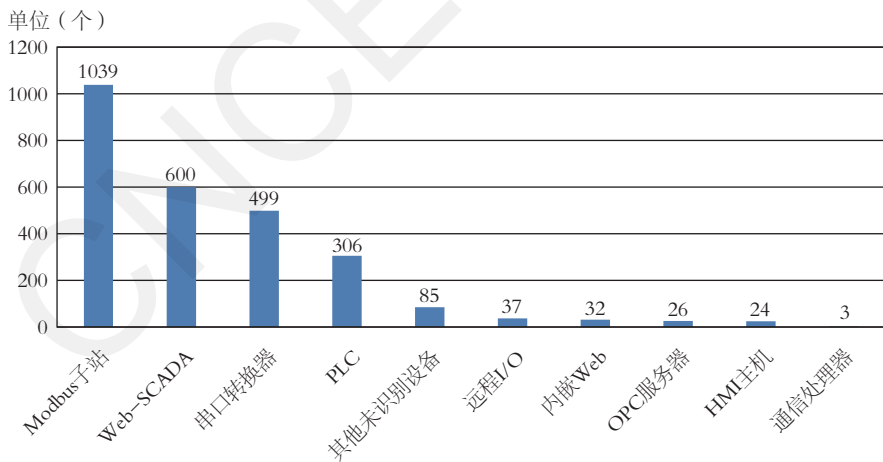


图2-31 按设备类型统计排名

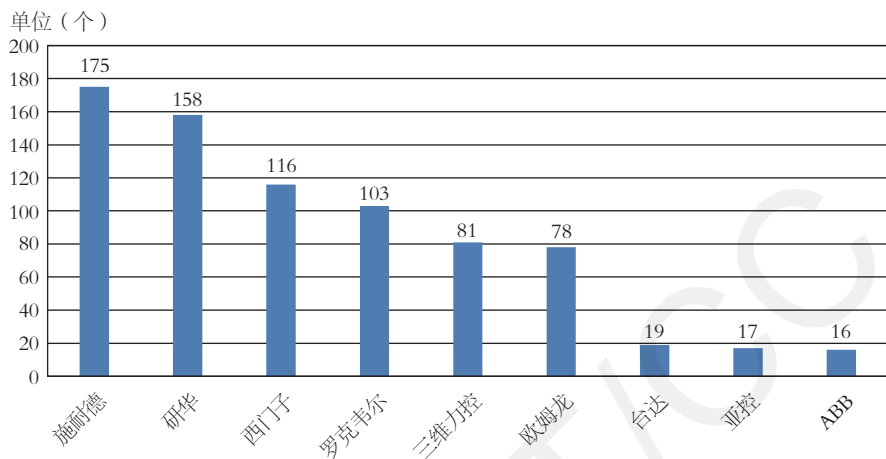


图2-32 按设备生产厂商统计排名

根据CNVD及CVE漏洞库的公开信息，许多设备及系统存在缓冲区溢出、拒绝服务、缺乏访问控制机制、弱密码、目录遍历等漏洞，攻击者可轻易对其进行远程访问，窃取信息或进行恶意操作。

从图2-33可以看出，相关的联网工控系统或设备主要分布在北京、浙江、上海、江苏、广东、山东、河北、辽宁等经济或工业较为发达的省份，它们一旦遭到网络攻击，将会带来非常严重的经济损失、设备损伤乃至人员伤亡，必将严重影响当地的社会稳定。

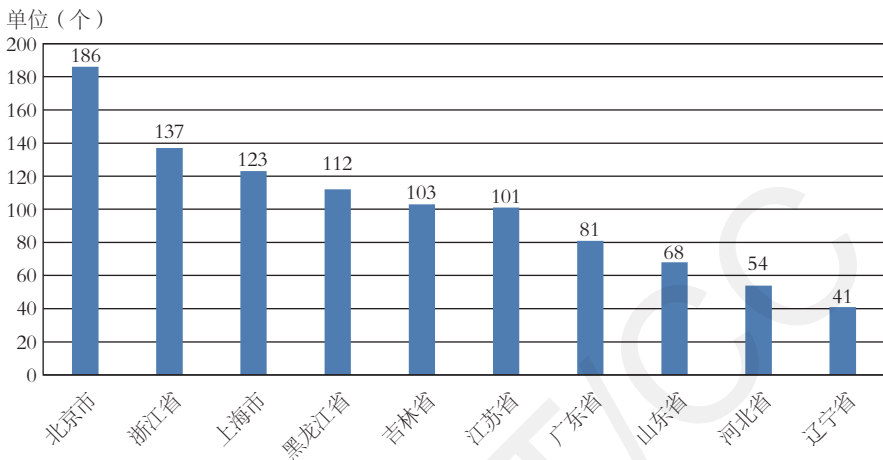


图2-33 联网工控设备的地域分布情况

(4) 互联网流量监测分析表明,大量境外组织机构持续对我国关键基础设施的工控系统进行扫描渗透^[14]。

德国西门子S7系列PLC在国内工控领域应用最为广泛。CNCERT/CC在2015年年初开展了针对境内联网的西门子S7系列PLC的初步流量监测和分析工作,发现有境外势力正在对我国关键基础设施工控系统扫描渗透。据统计,共有来自国外1123个IP地址(包括来自美国的428个IP地址)对境内西门子工控系统进行连接通信,其中,Shodan^[15]搜索引擎等境外机构进行过高频次、大范围的探测扫描。此外,还有数百个境外IP地址对我国互联网上暴露的工控设备进行访问,尚待进行更深入的威胁情报溯源分析。

2.3.3 加强国家关键基础设施网络安全技术保障的对策及建议

2.3.3.1 设立关键基础设施安全防护的专项研究基金

开展战略规划研究与安全标准编制、关键技术攻关及产业化应用、前沿基础理论研究等

[14] 本次监测主要针对西门子S7系列PLC,该组件广泛应用于工控领域。根据《2015中国PLC市场研究报告》,西门子在国内市场占有率超过38%,应用范围涵盖冶金、汽车、市政、交通、化工、电力等领域。

[15] Shodan是一个用于帮助发现主要的互联网系统(包括路由器、交换机、工控系统等)漏洞的搜索引擎。



相关工作。以美国为例，美国国家科学基金会长期支持网络安全研究，近期通过“安全可靠的网络空间”项目拨款7450万美元，投资257个新项目，资助37个州的研究人员。该项目旨在加强网络安全的实践和技术，将网络安全研究转化为实际项目等，该做法值得我国借鉴。

2.3.3.2 建立关键基础设施领域设备测评的技术和认证体系

加强关键基础设施领域核心设备的测评技术研究、测评工具开发、测评环境建设等能力提升，制定信息安全规范和标准指南，逐步形成我国独具特色的信息安全测评技术、认证以及网络安全审查体系。推动国产高端制造业的发展，实现生产设备和安全设备的国产化替代。

2.3.3.3 实施关键基础设施入口环节的有效防护

首先，面向各行业实现关键基础设施的互联网统一接入，在接入口加强网络信息安全检测系统部署，持续做好网络安全被动监测，及时发现木马和病毒，并采取针对性措施；其次，加强主动巡查，开展日常的运行监测、安全审计、漏洞预警和整改加固。

2.3.3.4 建立关键基础设施的安全年检制度，开展跨部门网络安全应急演练

由关键基础设施保护主管部门牵头，各行业主管部门组织实施，聘请第三方专业技术机构对关键基础设施运营企业的信息网络、控制网络进行风险评估，对其中的关键设备和重要的信息系统进行安全检测和检查。此外，还应以行业为单位每两年组织一次跨部门的网络安全攻防演练模拟，加强网络安全应急协同能力。

2.4 一例针对中方机构的准APT攻击分析（来源：安天公司）

2015年5月27日，安天分析人员发现一例准APT攻击事件，目标为中国政府机构。在攻击场景中，攻击者依托自动化攻击测试平台Cobalt Strike生成的、使用信标（Beacon）模式进行通信的Shellcode，实现对目标主机进行远程控制。这种攻击模式在目标主机中体现为“无恶意代码实体文件”，每60s发送一次网络心跳数据包，使用Cookie字段发送数据信息等行为，这些行为在一定程度上可以躲避主机安全防护检测软件的查杀与防火墙的拦截。鉴于这个攻击与Cobalt Strike平台的关系，分析人员暂时将这一攻击事件命名为APT-TOCS（APT Threat on Cobalt Strike）。

传统意义上的APT攻击更多地让人联想到精干的作业团队、强大的用于攻击的基础设施、专业的0day漏洞挖掘小组以及专门的恶意代码编写小组等。因此，多数的APT研究者愿意把更多目光放在具有这些特点的事件上。但APT-TOCS则用一种新的方式，为一些技术能力和资源相对有限的国家和组织提供了另一种选择。该事件也说明，随着攻击平台、商用木马和开源恶意工具的使用，网络武器被更加广泛的使用可能成为一种趋势。

2.4.1 技术分析

2.4.1.1 攻击方式

如图2-34所示，APT-TOCS攻击的步骤是，加载Shellcode的脚本通过命令行调用Powershell.exe，将一段加密数据加载到内存中执行。解密后的数据是一段可执行的Shellcode，该Shellcode由Cobalt Strike生成。分析人员根据加载Shellcode的脚本进行关联，发现一个可能在类似攻击中的作为脚本前导执行文件的PE程序，但由于相关脚本可以通过多种方式执行，并不必然依赖前导PE程序加载，且其是Cobalt Strike生成的标准攻击脚本，因此无法判定该前导PE文件与本例攻击的关联。

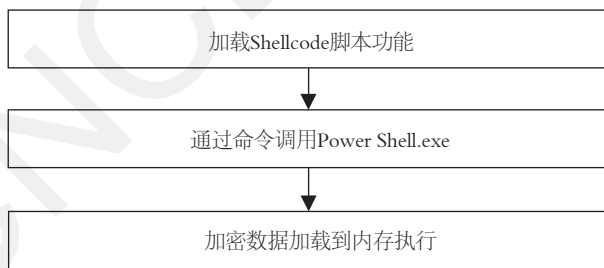


图2-34 APT-TOCS攻击核心步骤

这种基于脚本+Shellcode方式的特点在于：注入内存执行，不需要进行硬盘写入操作，在信标（Beacon）模式下可以同时和多个信标通信。这种攻击方式可以不依赖实体文件进行攻击，并可以依靠网络投放能力和内网横向移动按需投放，这将会给取证工作带来极大的困难。同时，目前的一些沙箱检测产品也对这种攻击无效。



APT-TOCS攻击尽管看起来已经具备接近APT水准的攻击能力，但并非依赖攻击团队自身的能力，而是依托商业的自动化攻击测试平台达成攻击目的。

分析人员对此事件的样本进行关联与分析，发现曾被用于类似攻击的前导文件，之后通过对关键机理的研究，得出各模块之间的衍生关系和模块的主要功能，在攻击来源验证的过程中，判断出这是一个系列化的攻击事件，攻击者可能采用社工邮件、文件捆绑、系统和应用漏洞利用、内网横向移动等方式，最终实现对目标主机的控制。分析人员通过分析攻击者所采用的技术来源，最后证明此次事件确实利用自动化测试平台Cobalt Strike。

2.4.1.2 攻击特点

攻击特点如下：

- 依托自动化攻击测试平台；
- 无恶意代码实体文件；
- 注入内存执行、没有硬盘写入操作；
- 使用信标（Beacon）模式进行通信。

2.4.1.3 事件样本分析与关联

分析人员通过对此事件中病毒名称为Trojan/Win32.MSShell的样本进行关联分析，发现二进制攻击前导文件（以下简称Sample A）曾被用于类似攻击，PE样本中嵌入的脚本，与分析人员获取到的Shellcode脚本功能代码完全相同，但加密数据存在差异，该PE样本曾在2015年5月2日被首次上传到Virus Total。该“前导文件”可以作为类似攻击的前导，但在当前研究情况下，并不能确定这一前导文件与本起APT事件具有关联关系。其依托系统和应用程序漏洞，不依赖类似文件，依然可以实现脚本的执行与最终的控制。

APT-TOCS的攻击者掌握多种脚本加载权限的远程注入手段，如利用安全缺陷或漏洞直接在主机上执行脚本。其中，攻击核心部分依托PowerShell加载的加密数据脚本（以下简称Sample B），该脚本与各模块的功能与衍生关系如图2-35所示。

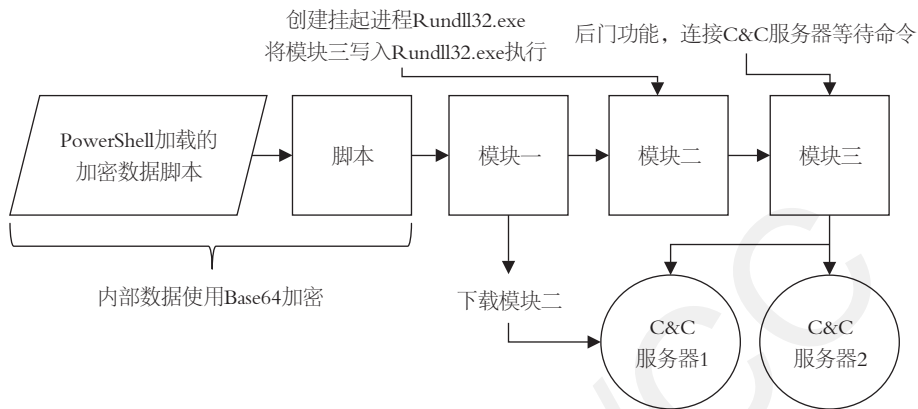


图2-35 数据脚本与各模块的功能与衍生关系

脚本与模块说明如下。

Sample B的功能是将Base64加密过的内容进行解密，再使用Gzip进行解压缩，得到模块一，并使用PowerShell加载执行。

脚本的功能是将经过Base64加密的数据解密，得到模块一，写入到Powershell.exe进程内，然后调用执行。

模块一的主要功能是调用函数，进行连接网络，下载模块二的操作，并加载到内存中执行。

模块二创建并挂起系统进程Rundll32.exe。

模块三的数据并非为PE文件，而是具有后门功能的Shellcode。该模块会连接两个罗马尼亚地址。该模块为后门程序，会主动向指定的地址发送Get请求，使用Cookie字段发送心跳包，间隔时间为60s。心跳包数据包括：校验码、进程ID、系统版本、IP地址、计算机名、用户名、是否为64bit进程。心跳包数据使用RSA、Base64加密及编码。

2.4.1.4 攻击技术来源的验证分析

分析人员关联的PE前导文件Sample A和Sample B利用PowerShell的方法完全相同，但正因为相关脚本高度的标准化，并不排除Sample A与本次攻击没有必然联系。而基于其他情况综合分析，依然判断该事件是一个系列化的攻击事件，攻击者可能采用社工邮件、文件捆绑、系统和应用漏洞利用、内网横向移动等方式实现对目标主机的控制。



而在分析“模块一”时，分析人员发现“Beacon”等字符串，依托过往分析经验，怀疑该Shellcode与自动化攻击测试平台Cobalt Strike密切相关。于是，分析人员对使用Cobalt Strike生成的Beacon进行对比分析，验证两者之间的关系。

分析人员将模块一与使用Beacon生成的Payload进行比较，发现只有三处数据不同，分别为：Get请求时发送的Head数据、请求的文件名称和IP地址。

分析人员将模块二与Beacon相关的文件进行比较，发现两者的反汇编指令除了功能代码不同之外，其他指令完全一致。

分析人员将模块三与Beacon生成模块的Get请求进行比较，发现两者都是使用Cookie传输信息，该信息进行加密，每间隔60s主动发送请求，该数据为上线包/心跳包。

利用Cobalt Strike的攻击可以在目标系统中执行多种操作，如下载文件、上传文件、执行指定程序、注入键盘记录器、通过PowerShell执行命令、导入PowerShell脚本、通过CMD执行命令、利用mimikatz抓取系统密码等。

Cobalt Strike 是一款以metasploit（一个渗透测试平台）为基础的GUI框架式渗透工具，Cobalt Strike的商业版具有集成服务扫描、自动化溢出、多模式端口监听、多种木马（DLL木马、内存木马、Office宏病毒和Beacon通信木马等）生成方式、钓鱼攻击、站点克隆、目标信息获取，浏览器自动攻击等功能，如图2-36所示。



Cobalt Strike具有以下特点：

- 穿透沙箱
- 躲避白名单机制与云检测
- 内网渗透
- 持久化攻击
- 攻击多种平台

Cobalt Strike作者：Raphael Mudge（美国）
Strategic Cyber LLC（战略网络有限责任公司）创始人

图2-36 Cobalt Strike特点及作者

在对Cobalt Strike及其作者的背景的研究中发现，其作者Raphael Mudge在2012-2014年均参加黑客大会，并且在软件开发、信息安全、社工学领域都十分擅长。值得

注意的是，他曾是某国空军安全研究员，具有军事背景。从对本次事件的分析以及分析人员的监控情况来看，商用木马、标准化的渗透平台等已经被广泛用于各种定向持续攻击中，特别是针对中国的攻击。Cobalt Strike平台能力展示如图2-37所示。

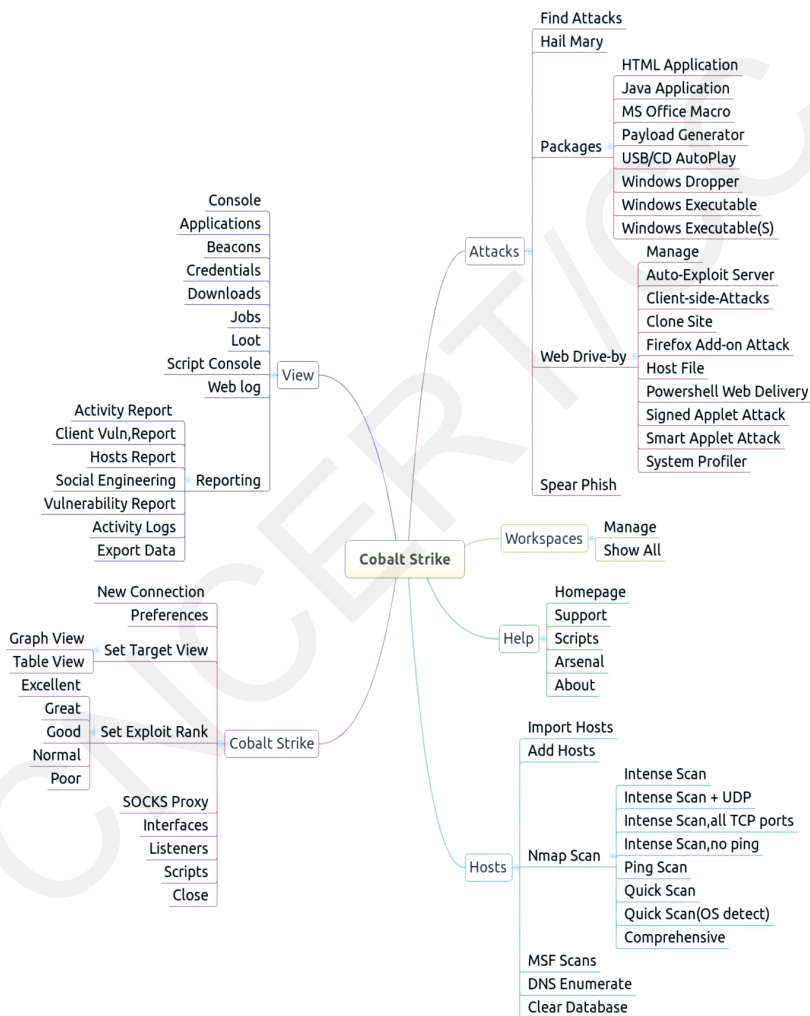


图2-37 Cobalt Strike平台能力展示



2.4.2 防范措施

从过去的跟踪来看，这种威胁已经存在近5年之久，但依然缺乏有效检测类似威胁的产品和手段。对于APT的防御，首先要建立专业事件响应团队，及时查看告警信息，及时处理发现威胁，安全厂商之间应互通协作，对抗威胁。众所周知，APT防御是一个综合的解决方案，需要在黑客的研究、渗入、数据发现、数据捕获和数据传出等阶段进行全面的防护，这样就需要多个产品之间的协同配合。同时，用户在工作过程中，不要随意打开来历不明的邮件，提高安全意识，上网行为要进行规范化的管理。政府企业等应安装威胁检测系统或设备对全网流量到终端进行安全检测与监控，发现各类已知与未知的威胁，并进行统计分析，及时处置威胁。

2.4.3 事件总结

分析人员之所以将APT-TOCS事件定位为准APT事件，是因为该攻击事件一方面符合APT攻击针对高度定向目标作业的特点，同时隐蔽性较强，具有多种反侦察手段。而使用自动化攻击测试平台Cobalt Strike进行攻击渗透方式具有穿透防火墙的能力，其控制目标主机的方式非常隐蔽，难以被发现；同时具备攻击多种平台的能力，如Windows、Linux、Mac等；同时与可信计算环境、云检测、沙箱检测等安全环节和手段均有对抗能力。

但APT-TOCS与我们过去所熟悉的很多APT事件中，进攻方具备极高的成本承担能力与巨大的能力储备不同，其成本门槛并不高。事件的恶意代码并非由攻击者自身进行编写构造，商业攻击平台使事件的攻击者不再花费高昂的恶意代码开发成本，相关攻击平台亦为攻击者提供了大量可选注入手段，为恶意代码的加载和持久化提供了配套方法。这种方式降低了攻击的成本，使得缺少雄厚资金、也没有精英黑客的国家和组织依托现有商业攻击平台提供的服务即可接近APT级水准。而这种高度“模式化”攻击也会让攻击缺少鲜明的基因特点，从而更难追溯。

在这里，引用信息安全前辈Bruce Schiner的观点，“一些重大的信息安全攻击事件发生时，都认为它们是网络战的例子，我认为这是无稽之谈。我认为目前正在发生而且真正重要的趋势是：越来越多战争中的战术行为扩散到更广泛的网络空间环境中，这一点非常重要。通过技术可以实现能力的传播，特别是计算机技术可以使攻击

行为和攻击能力变得自动化。”显然，高度自动化的商业攻击平台使这种能力扩散速度已经超出了我们的预测。

需要提醒各方关注的是，鉴于网络攻击技术存在极低的复制成本的特点，当前已经存在严峻的网络军备扩散风险。商业渗透攻击测试平台的出现，一方面成为高效检验系统安全的有力工具，但对于缺少足够的安全预算、难以承担更多安全成本的国家、行业和机构来说，会成为一场噩梦。在这个问题上，一方面需要各方面建立更多的沟通和共识；而另一方面毫无疑问的是，当前在攻防两端均拥有全球最顶级能力的超级大国，对于有效控制这种武器级攻击手段的扩散，应该负起更多的责任。

同时，APT-TOCS与之前发现的诸多事件一样，体现了一个拥有十三亿人口、正在进行大规模信息化建设的国家所面对的严峻的网络安全挑战；当然，也见证了中国用户与安全企业为应对这种挑战所做的努力。

2.5 Dorkbot僵尸网络分析（来源：微软公司）

在微软安全研究人员的协助下，全球各执法机构于2015年12月2日成功摧毁由恶意软件Win32/Dorkbot组成的大型僵尸网络。该僵尸网络影响范围非常广泛，已感染190多个国家的一百多万台个人电脑。

Dorkbot主要通过USB闪存、即时通信软件和社交网络进行传播。它不仅盗取用户凭证和个人信息，关闭安全保护软件，而且还会传播其他多种流行的恶意软件。

微软恶意软件防护中心（MMPC）和微软数字安全研究中心（DCU）作为牵头方，与安全厂商ESET公司和波兰互联网应急响应中心（波兰CERT、NASK）联手对Dorkbot恶意软件进行分析。

经过全面的调查和研究，波兰互联网应急响应中心（CERT）、ESET、加拿大广播电视和电信委员会（CRTC）、美国互联网应急响应中心（DHS/USCERT）、欧洲刑警组织、美国联邦调查局（FBI）、国际刑警组织和加拿大皇家骑警（RCMP）等各国执法机构和技术支持机构互相合作，联合打击和清理分布在全球各地的Dorkbot僵尸网络及其相关基础设施。

微软恶意软件防护中心自2011年4月发现Dorkbot以来就对其开展密切监测，并发



布以下研究报告：

- 2012年3月恶意软件删除工具：除恶务尽^[16]；
- Dorkbot感染分析报告（第一部分）^[17]；
- Dorkbot感染分析报告（第二部分）^[18]。

微软的实时安全防护软件，如Windows 10上的Windows Defender软件、微软安全扫描工具以及微软恶意软件移除工具，都可以查杀Dorkbot。

2.5.1 Dorkbot监测数据

如图2-38所示，在2015年5-10月，微软每月平均监测到有10万台设备感染Dorkbot。图2-39显示了排名前10位的Dorkbot受害国，这些国家受感染的设备占全球总量的61%。2015年8-10月受Dorkbot感染设备热点如图2-40所示。

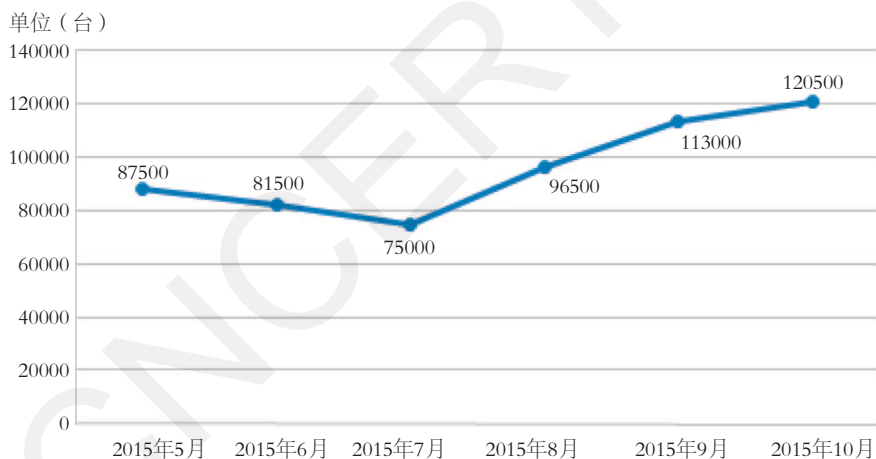


图2-38 2015年5-10月受Dorkbot感染的设备数量

[16] <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32/Dorkbot>。

[17] <https://blogs.technet.microsoft.com/mmpc/2012/03/12/msrt-march-2012-breaking-bad/>。

[18] <https://blogs.technet.microsoft.com/mmpc/2012/11/14/an-analysis-of-dorkbots-infection-vectors-part-1/>。

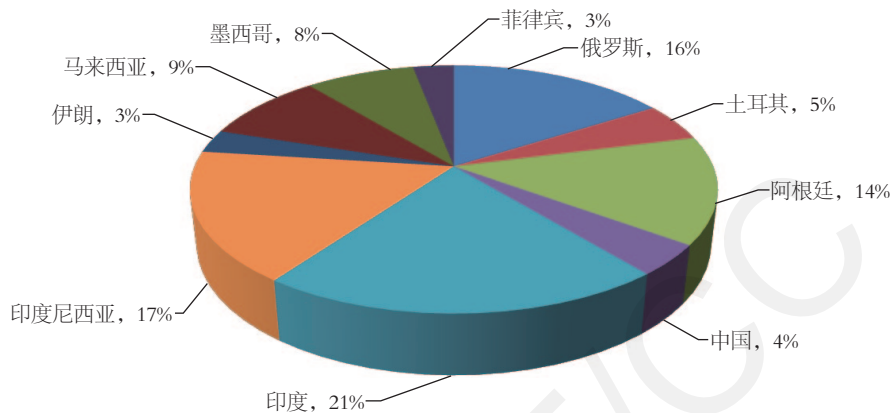


图2-39 2015年5-10月受Dorkbot感染的国家比例

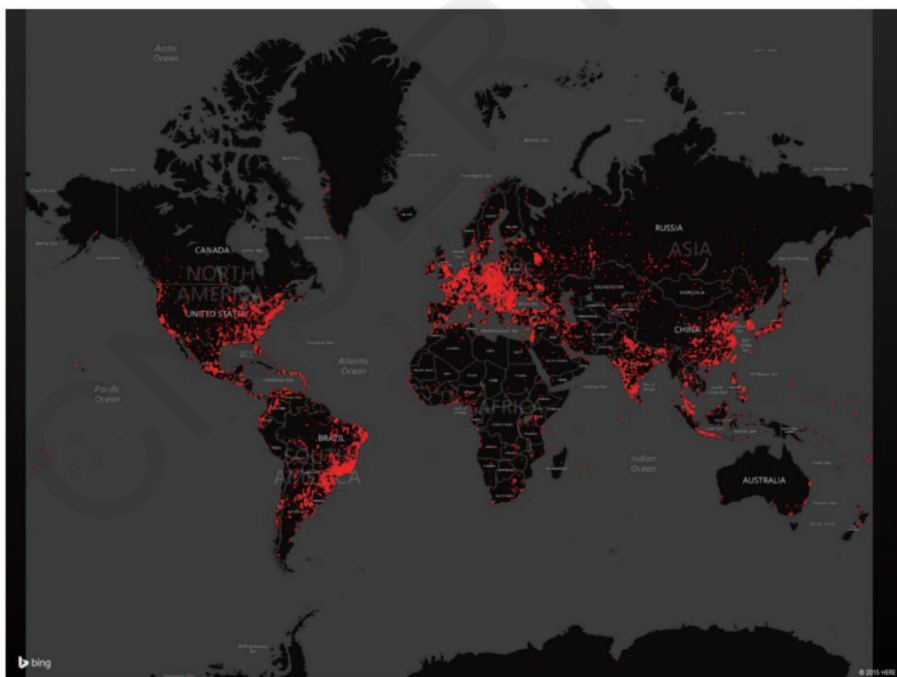


图2-40 2015年8-10月受Dorkbot感染设备的热点分布

Dorkbot是一种基于互联网中继聊天（Internet Relay Chat，IRC）协议的僵尸网络



程序。要创建一个Dorkbot僵尸程序只需要在一些黑客论坛上购买NgrBot工具包，按照工具包中的说明文档，在僵尸程序生成器上简单操作即可完成。图2-41和图2-42展示了其中一种Dorkbot僵尸程序生成器界面，通过NgrBot工具包可对多项功能进行配置，包括IRC服务器设置和命令设置。

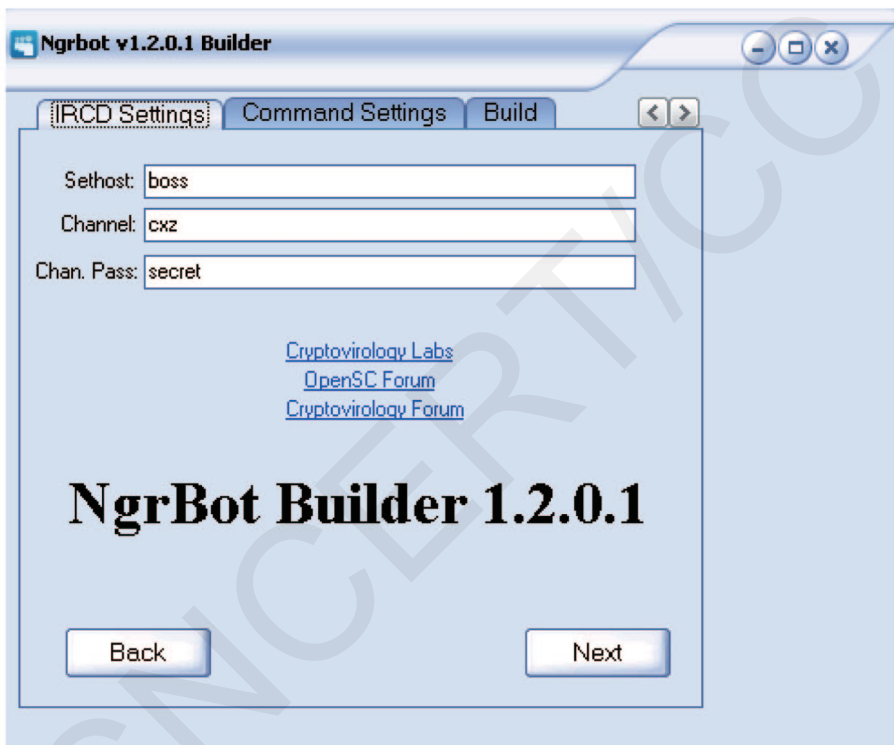


图2-41 Dorkbot僵尸程序生成器IRC服务器配置界面

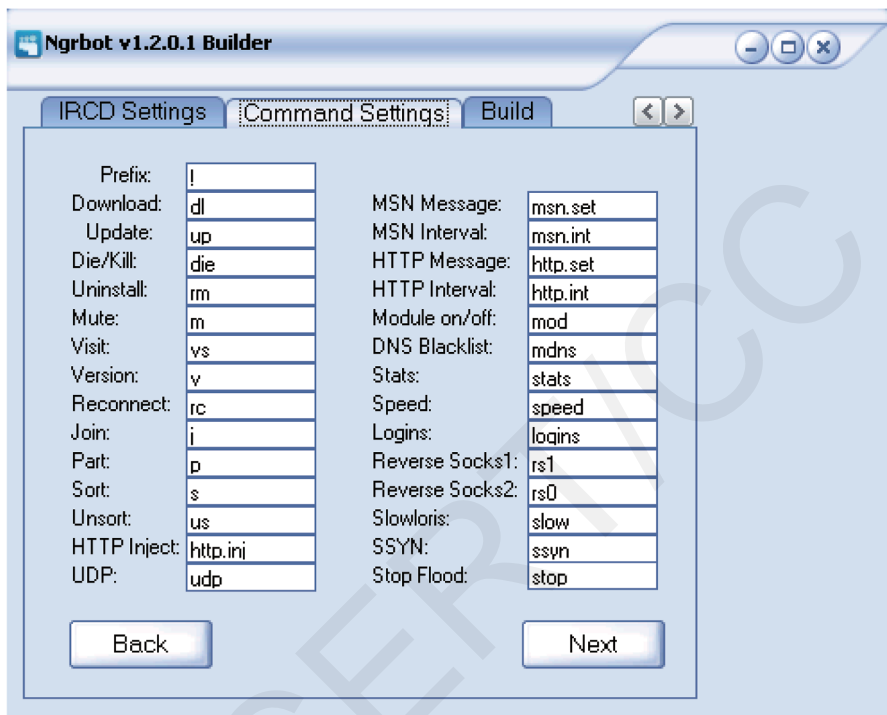


图2-42 Dorkbot僵尸程序生成器命令设置界面

2.5.2 传播方式

如图2-43所示，Dorkbot恶意软件可以通过多种途径传播，包括：

- 可移动磁盘（USB闪存）；
- 即时通信软件；
- 社交网络；
- 隐蔽式下载（Drive-by Downloads）^[19]/漏洞攻击工具包（Exploit Kits）；
- 垃圾邮件。

[19] 在用户没有察觉的情况下，将恶意程序隐蔽地下载到用户的电脑中。

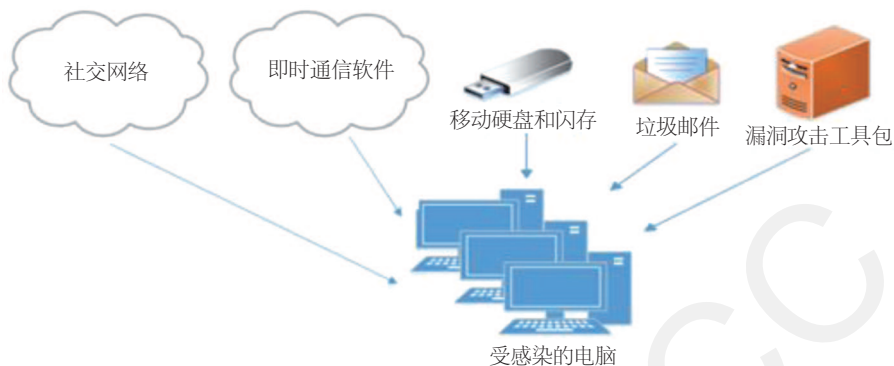


图2-43 Dorkbot传播方式

漏洞攻击工具包可以利用用户电脑上的软件漏洞，在用户访问网站时感染用户的电脑。隐蔽式下载感染是指黑客将漏洞攻击工具包放置在网站上，这些网站被称为漏洞攻击网站（也被称作挂马网站）。一部分漏洞攻击网站是僵尸网络的控制者为扩散恶意软件创建的，另外一些则是被黑客侵入后篡改的合法网站。

当一台电脑访问漏洞攻击网站时，漏洞攻击工具包会试图攻击未打补丁的软件以安装Dorkbot。电脑一旦受到感染，Dorkbot可以通过可移动磁盘（USB闪存）、即时通信软件和社交网络自动传播。

2.5.3 行为分析

Dorkbot的首要目标是盗用网络用户账户和密码以及其他身份识别信息。

2.5.3.1 Dorkbot加载程序

根据研究发现，有许多僵尸网络控制者都利用Dorkbot。如图2-44所示，Dorkbot加载程序有自己的代码用于更新和传播其他恶意软件，此外通过修改IRC协议的配置信息和禁用自检程序的方法，Dorkbot加载程序可以让僵尸程序连接到指定的命令与控制（Command and Control, C&C）服务器地址。

```

v4 = CreateThread(0, 0, Dorkbot::DestructivePayload, 0, 0, 0);
MessageBox(
    0,
    "This binary is invalid.\r\n"
    "\r\n"
    "Main reasons:\r\n"
    "- you stupid cracker\r\n"
    "- you stupid cracker...\r\n"
    "- you stupid cracker?! \r\n",
    "Bot Error",
    0x30u);
WaitForSingleObject(v4, 0xFFFFFFFF);
ExitProcess(0);

```

图2-44 原始Dorkbot具有自检功能，但已被篡改

2.5.3.2 Dorkbot加载程序自动更新并下载其他恶意软件

如图2-45所示，Dorkbot加载程序模块中包含一组加密的下载链接，这些下载地址中包含Dorkbot恶意软件、更新程序以及其他恶意软件。

```

http://api1.wipr.../api1.gif
http://api2.wipr.../api2.gif
http://api3.wipr.../api3.gif
http://api4.wipr.../api4.gif
http://api5.wipr.../api5.gif
http://api6.wipr.../api6.gif
http://api7.wipr.../api7.gif
http://api8.wipr.../api8.gif
http://api9.wipr.../api9.gif
http://api.wipma...i.gif
http://api.wipma...api.gif
http://api.wipma...api.gif
http://api.wipma...u/LkwAxD.gif
http://api.wipma...oJAi.gif
http://api.wipma...fjTMe.gif
http://api.wipma...oSPHv.gif
http://api.wipma...xmcHM.gif
http://api.wipma...u/frflec.gif
http://api.wipma...zwFMwD.gif
http://update.w...t.ru/logo.gif

```

图2-45 Dorkbot加载程序模块中解密后的下载链接

感染了Dorkbot的电脑会继续接收指令，下载并安装其他恶意软件。经过



CNCERT/CC监测发现，通过Dorkbot会感染以下的恶意软件。

Win32/Gingplog.A	Win32/Mustrat.A
Win32/Fleercivet.D	Win32/Kasidet.A
Win32/Tolouge	Win32/Neurevt.A
Win32/Gamarue.A	Win32/Leenstic
Win32/Lethic.I	Win32/Crowti
Win32/Kelihos	Win32/Necurs
Spammer:Win32/Emotet	Win32/Waledac

微软恶意软件移除工具具有检测Dorkbot以及相关恶意软件的功能。

2.5.3.3 指定IRC模块连接其他C&C地址

自2011年年中以来，Dorkbot的IRC模块基本没有变化，只有某些字节被更新过。IRC模块内部对于C&C服务器地址有长度限制，僵尸网络控制者通过在Dorkbot加载程序模块中植入代码的方法，指定IRC模块连接到其他的C&C服务器地址。

如图2-46～图2-48所示，Dorkbot加载程序会创建一个陷阱触发进程（Trap Process），例如mspaint.exe，并在域名解析接口（DNSQuery_A，DNSFree）上安装劫持代码（Hook Code）。Dorkbot通过DNS查询C&C服务器地址时，查询的返回值就会被篡改，重定向到僵尸网络控制者指定的地址。

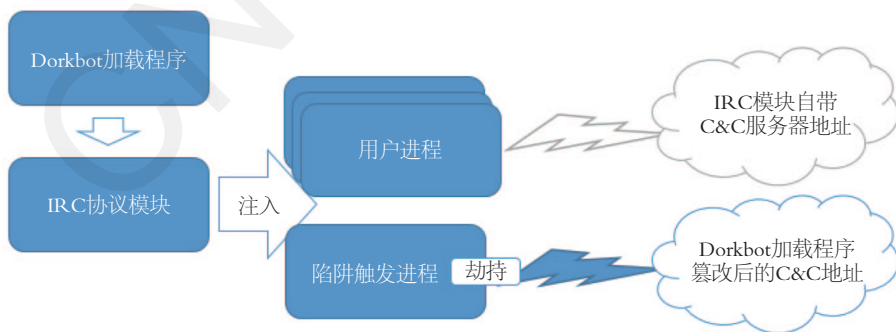


图2-46 篡改C&C服务器地址的示意

```

v9 = 0;
if ( lpstrName
&& (!strcmp(lpstrName, ".org") || !strcmp(lpstrName, ".biz") || !strcmp(lpstrName, ".ne")) )
{
    if ( strcmp(lpstrName, dword_40FD90) )
    {
        if ( strcmp(dword_40FD90, "impossible") )
        {
            if ( !gDomains[++domain_index] )
                domain_index = 0;
        }
    }
    memset((BYTE *)dword_40FD90, 0, 0x80u);
    strcpy(dword_40FD90, lpstrName);
    v9 = 1;
    v8 = lpstrName;
    v10 = gDomains[domain_index];
}
RestoreLastError(0);
org_DnsQuery_handler();
if ( v9 == 1 && !result )
{
    v7 = *(_DWORD *)ppQueryResultsSet;
    dword_40FD8C = *(_DWORD *)(*(_DWORD *)ppQueryResultsSet + 4);
    *(_DWORD *) (v7 + 4) = v8;
}
return result;

```

图2-47 覆盖原始C&C服务器地址

a.aip	axyblack42.com
a.ajj	x42.com
a.ado	rstandme42.com
n.lot	
n.jnt	
n.hmi	
a.naj	elema1.com
a.naj	elema2.com
g.roo	.com
g.roo	.com
g.roo	.com
g.roo	.com
g.so1	
a.aip	axyblack42.com
a.ajj	x42.com
a.ado	rstandme42.com

图2-48 C&C服务器地址列表

Dorkbot成功连接到C&C服务器后，IRC模块就会开始接收指令。

2.5.3.4 Dorkbot的IRC模块（即NgrBot）

Dorkbot在感染电脑后，将尝试连接事前设定好的C&C服务器。利用SSL加密后的IRC协议，Dorkbot的配置信息可以自动更新。在首次通信时，Dorkbot首先向C&C



服务器发送其地理位置、运行的Windows版本以及唯一的电脑设备识别码。然后，Dorkbot就可以随时执行僵尸网络控制者发送的指令，详细的指令如图2-49所示。

通常，在连接C&C服务器后，被感染的电脑会被控制下载其他恶意软件或将恶意软件传染给其他电脑。

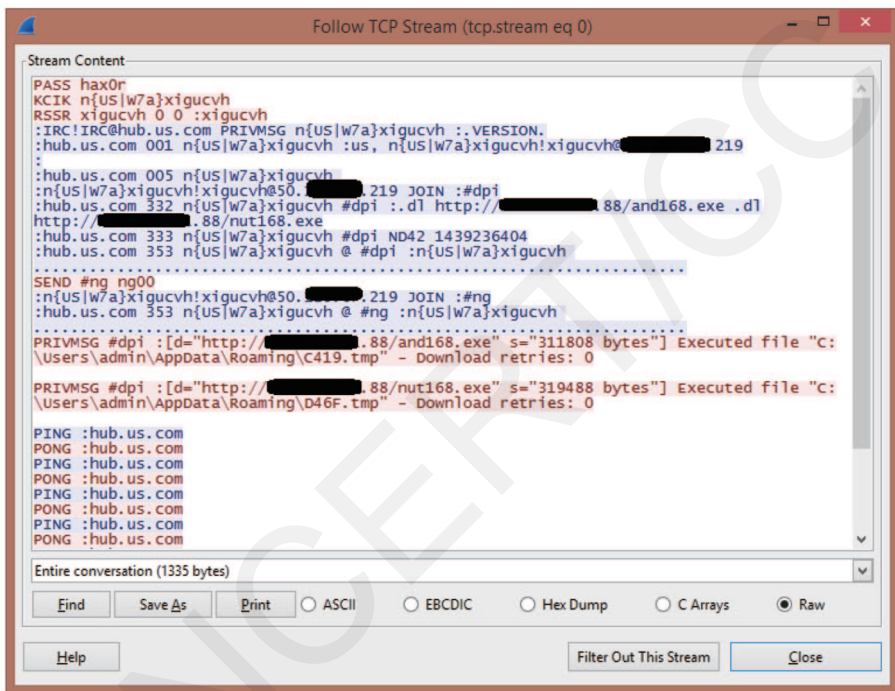


图2-49 Dorkbot与C&C服务器通过IRC协议通信

僵尸网络控制者还会不断升级Dorkbot程序，例如修改IRC协议的命令（USER、PASS、NICK、PRIVMSG等）或电脑设备识别码的格式。Dorkbot的新旧版本比较如图2-50所示。

172e419351f78ba82dfca3e3442eae816a7acfd8.exe.d																
0001	4A50:	55	53	45	52	20	25	73	20	30	20	30	20	3A	25 73 0D	USER %s 0 0 :%s.
0001	4A60:	0A	00	00	00	4E	49	43	4B	20	25	73	0D	0A	00 00 00 00	NICK %s.....
0001	4A70:	4A	4F	49	4E	20	25	73	20	25	73	0D	0A	00	00 00 00 00	JOIN %s %s.....
0001	4A80:	50	41	52	54	20	25	73	0D	0A	00	00	00	50	52 49 56	PART %s.PRIV
0001	4A90:	4D	53	47	20	25	73	20	3A	25	73	0D	0A	00	00 00 00 00	MSG %s : %s.....
0001	4AA0:	51	55	49	54	20	3A	25	73	0D	0A	00	00	50	4F 4E 47	QUIT :%sPONG
0001	4AB0:	20	25	73	0D	0A	00	00	00	50	49	4E	47	00	00 00 00 00	%s..... PING....
0001	4AC0:	50	52	49	56	4D	53	47	00	5B	76	3D	22	25	73 22 20	PRIVMSG. [v="%s"
2371adeb2ffc42109a05e241ea288a43a1e499b0.bot																
0001	4910:	53	44	52	52	20	25	73	20	30	20	30	20	3A	25 73 0D	SDRR %s 0 0 :%s.
0001	4920:	0A	00	00	00	4B	43	49	4B	20	25	73	0D	0A	00 00 00 00	KCIK %s.....
0001	4930:	53	45	4E	44	20	25	73	20	25	73	0D	0A	00	00 00 00 00	SEND %s %s.....
0001	4940:	50	41	52	54	20	25	73	0D	0A	00	00	00	50	50 50 50	PART %s.PPPP
0001	4950:	4D	53	47	20	25	73	20	3A	25	73	0D	0A	00	00 00 00 00	MSG %s : %s.....
0001	4960:	51	55	49	54	20	3A	25	73	0D	0A	00	00	50	50 4E 47	QUIT :%sPONG
0001	4970:	20	25	73	0D	0A	00	00	00	50	49	4E	47	00	00 00 00 00	%s..... PING....
0001	4980:	50	50	50	50	4D	53	47	00	5B	76	3D	22	25	73 22 20	PPPPMSG. [v="%s"

图2-50 Dorkbot旧版本（上）和新版本（下）比较

2.5.3.5 盗用网络用户凭证

通过劫持以下三个与网络相关的应用程序接口（API），Dorkbot会监控网页浏览器的通信，并且拦截网页浏览器与部分网站间的通信。

- HttpSendRequestA/W
- InternetWriteFile
- PR_Write

当用户登录以下网站时，Dorkbot可以盗取以下用户账号和密码。

- AOL
- eBay
- Facebook
- Gmail
- Godaddy
- OfficeBanking
- Mediafire
- Netflix
- PayPal
- Steam
- Twitter
- Yahoo
- YouTube



2.5.4 Dorkbot的自我保护措施

2.5.4.1 屏蔽网站

与C&C服务器建立连接以后，Dorkbot通过劫持IRC协议模块中的DNSQuery接口，阻止用户访问包含以下关键字的安全防护网站。这样做的主要目的是阻止受感染的电脑更新杀毒软件的病毒库，避免Dorkbot被查杀。

- | | | |
|-----------------|------------------------|-------------------|
| • avast | • heck.tc | • precisecurity |
| • avg | • iseclab | • sophos |
| • avira | • jotti | • sunbeltsoftware |
| • bitdefender | • kaspersky | • symante |
| • bullguard | • lavasoft | • threatexpert |
| • clamav | • malwarebytes | • trendmicro |
| • comodo | • mcafee | • virscan |
| • emsisoft | • onecare.live | • virus |
| • eset | • norman | • virusbuster |
| • fortinet | • norton | • nprotect |
| • f-secure | • novirusthank | • viruschief |
| • garyshood | • onlinemalwarescanner | • virustotal |
| • gdatasoftware | • pandasecurity | • webroot |

2.5.4.2 反沙盒技术

当Dorkbot加载程序在系统上运行时，它会在“%TEMP%\c731200”文件夹中创建一个文件，记录首次执行时间（时间格式为转换成秒的UTC时间）。在下载最新Dorkbot指令和其他恶意软件之前，Dorkbot加载程序将检查当前系统时间是否超过首次执行时间48h。通过这种方式，Dorkbot加载程序可在杀毒软件后台分析系统中隐匿真实的下载地址。

2.5.5 防范措施及建议

为防止感染Dorkbot或其他恶意软件，可以采取以下措施。

- 在打开来自未知用户的邮件或社交网络信息时应格外谨慎；
- 在非官方网站上下载软件时应保持警惕；
- 定期使用反恶意软件工具进行扫描。

此外，还可以使用Windows 10操作系统上的安全防护软件Windows Defender，微软安全扫描工具和微软恶意软件移除工具查杀Dorkbot。微软还将继续与有关方面开展合作，保护电脑用户免受恶意软件侵害。

2.6 社保系统泄密“风波”安全事件分析（来源：深信服公司）

随着互联网+、大数据时代的到来，互联网用户的个人信息数据每时每刻都在进行交互、存储、转发。在这样一个全民网络化的时代，互联网安全正在面临着一个前所未有的挑战，2015年我国互联网个人信息泄露问题成高发态势，研究报告^[20]显示，仅2011—2014年年底已被公开并被证实的泄露中国公民的个人信息就多达11.27亿条。这个庞大的数据告诉我们，在信息化的时代几乎每一个上网的人，自己的个人信息可能早已经在不知不觉中被窃取利用。其中，社保系统泄露用户数据事件备受关注。以下将对此事件做重点分析。

2.6.1 事件回顾

如图2-51所示，2015年4月22日，据多家媒体报道，超过30个省份的社保系统存在高危漏洞，漏洞涉及千万人，泄露内容包括身份证、社保参保信息、个人薪酬、房屋等重要敏感信息。事件至少包括上海、广东、河北、江苏、四川、浙江等30个省份受到严重影响，危害多个行业的社会信息系统，对国家、社会造成严重危害。

[20] 《2015年第一季度网络诈骗犯罪数据研究报告》。



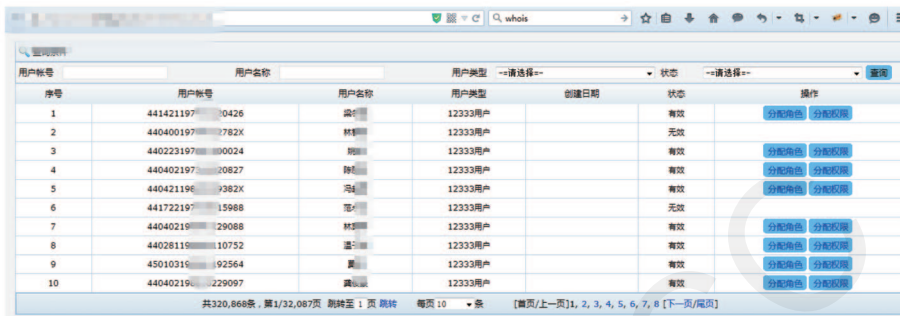
	带头大哥 发布 台州市社会保险某站漏洞可获取大量社保人员身份证、卡号以及社保... ¥100	查看详情
	带头大哥 发布 宁波市社保局某系统存在注入漏洞	查看详情
	带头大哥 发布 山西省社保局某漏洞	查看详情
	带头大哥 发布 合肥市劳动和社会保障局某系统漏洞可泄露大量职工社保信息	查看详情
	带头大哥 发布 贵州省社保局某系统漏洞泄露大量事业单位职工敏感信息	查看详情
	带头大哥 发布 沈阳社保局某系统SQL注入或可泄漏用户信息	查看详情
	带头大哥 发布 山西省社保卡应用统计报表系统存在IIS写权限漏洞	查看详情
	带头大哥 发布 某社保管理信息系统通用SQL注入漏洞 ¥300	查看详情
	i3esn0w 发布 某市社保局网站被入侵，泄露百万社保信息	查看详情
	carry_your 发布 茂名市社会保险基金管理局某站点存在漏洞，可getshell泄...	查看详情

图2-51 “补天”漏洞响应平台（来源：深信服公司）

事件发生当天，深信服安全实验室就接到多家民计、民生类行业客户的应急响应与安全服务工作。在提供安全服务的整个过程中，发现了多起高危安全泄露事件，涉及行业包括社会保险基金管理局、人力资源市场管理平台、人力资源和社会保障局、人才网等多个领域。下面列举针对深信服公司发现的事件型安全漏洞。

案例一：某市人力资源与社会保障局用户越权漏洞导致30万条个人信息泄露

首先，登录某市人力资源与社会保障局，注册任意账号。使用注册的账号登录后发现存在大量未授权访问的信息，例如可以查看任意用户账号（身份证）、用户名称、用户类型，效果如图2-52所示。



序号	用户帐号	用户名称	用户类型	创建日期	状态	操作
1	441421197	0426	12333用户		无效	分配角色 分配权限
2	440400197	782X	12333用户		无效	分配角色 分配权限
3	440223197	00024	12333用户		无效	分配角色 分配权限
4	440402197	20827	12333用户		无效	分配角色 分配权限
5	440421196	7382X	12333用户		无效	分配角色 分配权限
6	441722197	15988	12333用户		无效	分配角色 分配权限
7	440402196	29088	12333用户		无效	分配角色 分配权限
8	440281196	10752	12333用户		无效	分配角色 分配权限
9	450103196	92564	12333用户		无效	分配角色 分配权限
10	440402196	229097	12333用户		无效	分配角色 分配权限

图2-52 某市人力资源与社会保障局用户越权漏洞示意一（来源：深信服公司）

其次，如图2-53所示，利用当前网站存在的越权漏洞给任意角色分配权限；成功利用漏洞后，当前用户就成为了“管理员”；再使用分配过管理权限的账号登录，成功登录后，可以对单位情况、工资情况、社保业务情况一览无遗。

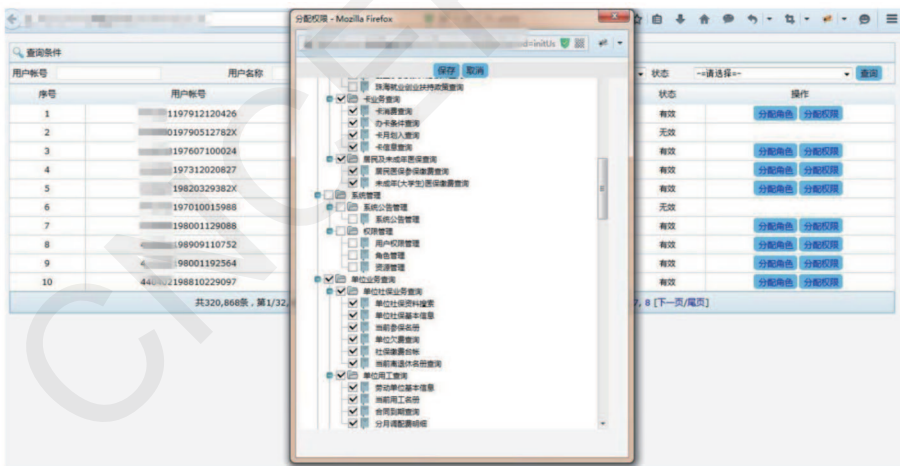


图2-53 某市人力资源与社会保障局用户越权漏洞示意二（来源：深信服公司）

最后，攻击者利用该漏洞，可以对该系统的30万条个人信息数据进行查看、篡改，效果如图2-54所示。



由于对参数过滤不严，某市人才网存在SQL注入漏洞，攻击者成功利用该漏洞，获取该人才网的240万条个人信息数据。图2-55为攻击者利用SQLMap注入攻击获取个人信息数据。

[illegible]

图2-55 某市人才网SQL注入漏洞（来源：深信服公司）

2.6.2 事件分析

2015年4月事件发生以来，深信服公司在对大量行业客户的社保系统进行无公害化验测的过程中，发现超过半数以上的社保系统存在高危安全威胁。

如图2-56所示，统计分析表明，从2014年以来，涉及居民社保信息泄露的问题在补天、乌云等漏洞报告平台被层出不穷地曝光，整个漏洞分布以高危风险漏洞为主。对漏洞进行分析整理，得出如下结论。

从风险类别来看，SQL注入风险威胁占据核心主导作用，约有70%的风险威胁均为SQL注入导致，统计发现MySQL、Oracle数据库为本次事件受影响最为严重的数据库类型。

从地域分布来看，北京、上海、广东、湖北、浙江、山东为事件高发地域，以上地域民生类信息系统防护能力较差。

从黑客攻击来看，攻击者采用的攻击方法普遍简单、低级，对敏感数据的获取也以自动化黑客工具居多。这些工具往往在互联网上就可以下载，只要稍微有技术基础的人利用黑客工具就可以实施网络攻击，通过统计发现本次事件中SQLMap注入工具使用量最多。

从漏洞修复来看，整体修复率不到30%，成为该行业又一个显著特点。统计分析发现，多地社保部门在漏洞发现后的数月间，没有采取任何行动，有的至今未对漏洞进行修复。



搜索关键词： 人力资源和社会 (共 213 条记录) 按未公开漏洞的入侵搜索结果

十堰市人力资源和社会保障局SQL注入漏洞

十堰市人力资源和社会保障局SQL注入漏洞...http://**.**.**.* 可能会有注入 Test 好像可以 ... 加强过滤

提交日期: 2015-04-09 作者: Sndav

鹤壁市人力资源和社会保障局养老保险查询存在用户信息泄露

鹤壁市人力资源和社会保障局养老保险查询存在用户信息泄露, 姓名身份证没有进行匹配...http://**.**.**.*cx/yjcx.aspx 鹤壁市人力资源和社会保障局养老保险查询存在用户信息泄露, 姓名身份证没有进行匹配 ... 修改代码

提交日期: 2015-04-04 作者: 天之天威

菏泽市人力资源和社会保障局网站统计弱口令

菏泽市人力资源和社会保障局网站统计弱口令...http://**.**.**.*counter/ 用户名: admin 密码: admin ... 修改密码

提交日期: 2015-04-04 作者: 路人甲

山西省人力资源和社会保障厅#sql两处打包#大量数据泄露

山西省人力资源和社会保障厅#sql两处打包#大量数据泄露...山西省人力资源和社会保障厅#sql两处打包#大量数据泄露...山西省人力资源和社会保障厅#sql两处打包#大量数据泄露...http://**.**.**.*inurl?id=http://**.**.**.*fingerprint/Detail.aspx?ID=14855 ... 你懂得。

提交日期: 2015-04-02 作者: 路人甲

济南市人力资源和社会保障局验证码绕过可爆破用户账号密码

你猜你猜...验证码绕过可被pkav大神器完美识别...- burp抓包丢进去就可以爆破哦 只需要生成个字典遍历下后6位就知道用户不存在, 账号为身份证号, 默认密码为身份证号后6位, 设置payload 用一个字典一起爆破 再用pkav大神器的验证码识别绕过验证码。。。你懂得 经验证, 返回的包的长度为以下: 账号不存在: 11281 密码正确: 10907 密码错误: 11262 可以根据返回的长度来判断爆破成功与否 ... 用老弱...

提交日期: 2015-04-01 作者: Mr.R

云浮市人力资源和社会保障局存在SQL注射

...注入点 http://**.**.**.*ForJobDetail.aspx?ID=425 扔SQLMAP Database: XOCMS [53 tables] +-----+ | ARTICLES || ARTICLES_BAK || AZ01B || BULLETINS || CHATINFO || COLUMNS || COMMENTS || DRUGSTORE || EMPLOYMENT || FLINKS || FLINKSTYPE || GROUPOWER || GROUPS || GUESTBOOK || GUESTBOOKTYPE |...

图2-56 乌云漏洞报告平台对社保泄露事件的披露 (来源: 深信服公司)

通过上述分析不难发现,我国民生类信息系统安全问题具备一些共性:首先,攻击漏洞简单、低级的角度,可以看出系统的整体防护能力非常差,并且这些漏洞的存在就好比是给攻击者敞开一个进出的大门,让攻击者可以轻松地获取到重要的信息数据;其次,从影响范围来看,几乎涵盖全国所有省,事件直接威胁国家安全;最后,从整体泄露的数据量来看,涉及数据5000万条,对社会造成一定程度的恐慌,危害极大。

事件发生后,深信服安全实验室对诱发本次社保泄密“风波”的原因进行盘点总结,发现外部因素、内部因素将成为诱发个人信息数据泄露事件的核心问题。

(1) 外部因素

首先,系统安全漏洞方面,研究统计表明,2015年44%的数据泄露事件的发生是由于系统长期存在安全隐患,有的甚至有2~4年之久。因此针对该类问题,定期更新补丁非常必要。其次,是由于其他系统数据泄露带来的风险。针对以上威胁风险,单一的网络安全产品很难做好防御工作,要做好以大数据为基石的安全防护。最后,是

企业级APT攻击方面。更高级别的攻击者利用APT攻击方式进入网络之后，他们会渗透更多的内部主机，收集信息，提升权限，实现持久控制。针对信息窃取APT攻击往往以窃取系统中更具价值的信息为目的。正因为该类攻击具有隐蔽、持续、目的性强的特点，这也将成为未来信息泄露问题将要面临的最为严峻的挑战。

（2）内部因素

即使系统的防护能力非常强悍，但如果忽视内部员工带来的安全风险，依然会酿成危害。首先，员工安全意识方面，要加强公司员工的信息安全教育，例如告知他们不要被诱骗安装未知应用程序，并让他们意识到未知的、流行的、免费的软件通常充斥着大量的恶意程序。其次，开发人员安全意识薄弱也会造成泄露风险，2015年由于开发人员安全意识薄弱造成安全泄露风险的情况屡见不鲜。最后，要对员工上网行为进行严格管控，规避“内鬼”带来的严重泄露风险。

社保系统包含个人非常隐私的信息，同时也是国家宏观调控的重要信息和数据来源，一旦系统信息被不法分子进行篡改，后果不堪设想。社保泄露将会带来的危害包括：首先，身份证号、单位、账户金额可推算出个人工资水平，内容涵盖我国大量宏观调控数据，一旦被境外黑客组织利用，将会对国家造成巨大损失。其次，会发生个人账户资金异常，社保缴纳账号资金异常、公积金账户资金异常等事件，造成个人经济损失。最后，身份伪造诈骗，不法分子可利用获取的个人信息数据通过电话、短信实施诈骗。

2.6.3 黑产交易

近些年来，随着互联网的快速发展，黑色产业也在朝着规模化的方向进行蜕变，个人信息数据一旦流入黑色市场，带来的危害将会是永久的。这也与个人身份信息几乎是永久性息息相关，至少可以断定数据泄露带来的影响短时间内很难消除。

为了追查本次泄密事件的影响和危害，在对地下黑色产业交易进行排查时发现，社保重要信息数据库的买卖其实早已开始。

案例一：如图2-57所示，某黑色产业论坛从2014年8月就开始对社保泄露的个人信息数据进行买卖交易。



上海地区的社保信息，信息很全 - [售价 2 库币] ... 2 3 4 5 6 ... 9	jaelr 2014-9-27	82 976	sjp154030451 10 分钟前
送几个传烂了的数据库 - [售价 2 库币] ... 2 3 4 5 6 ... 293	hundan 2014-8-11	2924 17075	jealy535210 11 分钟前
广东社保38W [售价 2 库币] - [阅读权限 20] - [售价 2 库币] ... 2 3	amair 2014-8-22	29 107	sjp154030451 13 分钟前

图2-57 地下黑色产业论坛交易（来源：深信服公司）

案例二：如图2-58所示，通过社交媒体出售、收购各种社保、医保信息。

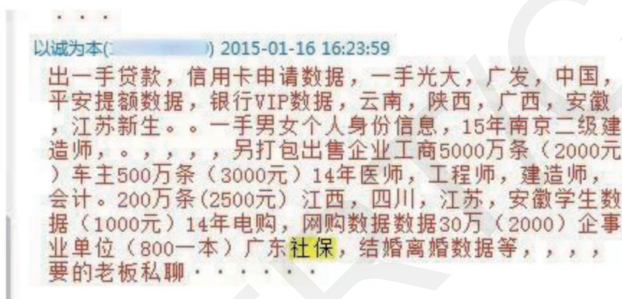


图2-58 地下黑色产业数据交易（来源：深信服公司）

分析发现，大部分泄露的数据都是在被攻击者充分利用、经过多手转卖后才会曝光。可以说，黑色产业数据的交易其实早已开始。

除了社保系统的数据外，发现近些年包括社保数据、医保数据、银行卡数据、学生信息，在黑色市场交易也非常活跃。被泄露的个人信息无论从数量还是种类上都只是“冰山一角”，实际泄露的数据比我们看到的、想象的还要多。

2.6.4 安全建议

一直以来，我国很多部门和产业都存在“重建设轻运维”、“重管理轻安全”的情况，无论是资金还是技术和人才方面的投入都大大低于欧美国家。如果这个趋势不改变，随着互联网经济的爆发性发展，类似的事件将会继续曝光出来。

结合社保泄密事件，针对如何保护个人信息安全，要从国家、企业、个人三个层面加强防护能力。

2.6.4.1 国家主管单位要加强网络治理和监管

(1) 国家立法建设方面。当今世界各国都高度重视网络安全立法, 提倡用法治的方式为网络安全运行保驾护航。虽然在2015年6月, 第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法(草案)》, 使我国网络安全立法取得了阶段性的成果。但是面对多变的网络环境、隐蔽的网络犯罪、复杂的网络攻击, 针对公民个人信息泄露的法律依据依然略显单薄无力。

(2) 黑色产业打击方面。正是由于利益链条的驱使, 才使得个人信息数据在互联网上贩卖成为可能。值得庆幸的是, 2015年7月31日CNCERT/CC启动了为期半年的互联网网络安全威胁治理行动, 整个行动过程中对黑产产业治理取得阶段性的成果。但互联网黑产背后存在巨大的利益链条, 要有效治理好黑色产业, 依然任重而道远。

(3) 黑客工具治理方面。长期以来, 针对DDoS工具、SQL注入工具公开在互联网上售卖或任意下载屡禁不止, 没能够找到合理的方式进行有效制止。社保信息泄露事件给我们的启迪是, 大量攻击者自身攻击水平较低, 正是由于黑客工具的泛滥才使得事件复杂化、严重化。因此对黑客工具的治理也是对个人信息的有效防护。

(4) 安全人才培养方面。网络安全人才培养战略要从“培养人才、发现人才、使用人才和管理人才”进行考虑, 提前布局信息安全产业。从加大安全人才投入的角度, 杜绝信息泄露等一系列安全事件的发生。

2.6.4.2 存储个人重要信息数据的企业要加强持续检测与纵深防御的能力

开展系统网络安全建设。加强系统的自我持续检测与纵深防御能力, 开展安全建设的过程中, 建议参考《信息安全等级保护》, 并且需要有专业的安全人员对系统进行防护, 做专业的指导, 从而规避常见的安全风险。

提高系统的漏洞修复能力。互联网中重大网络安全问题要及时修复, 加强信息系统漏洞紧急修复与处置能力。同时, 在防护的过程中要考虑到主机、网络、数据库等信息系统的诸多方面, 并且采取有针对性的防控措施。

建立信息安全责任制。当前我国缺乏对信息安全泄露的问责机制, 缺少法律依据, 因此把信息安全责任落实到相关部门和企业的负责人已迫在眉睫。

加强网络管理人员的安全意识。例如, 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。

加强系统开发人员的安全意识。例如，在Github上不要泄露系统源码或系统登录的账号、密码信息。

2.6.4.3 提高网民安全意识

(1) 增加密码的复杂度，密码长度不少于8位，同时不使用弱口令，如123456、Password等。

(2) 分级管理账号密码，对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，每隔一段时间修改自己的账号密码，可以有效避免数据库泄露影响自身账号安全。

2.6.5 几点思考

随着物理网、车联网、移动互联网等新兴技术的兴起，个人信息数据也开始向各个领域迁移蔓延。2015年数据显示，超半数以上的企业、单位在追求快速发展的同时，忽略了自身安全隐患问题。

今天计算机技术快速发展，物联网技术成为新时代技术的宠儿，技术在大量应用的同时，也将承载大量的个人信息数据。安全专家指出，移动设备和可穿戴设备大量的应用，为网络犯罪分子提供新的、潜在的入侵方式。

如图2-59所示，近日，央视《焦点访谈》栏目曝光儿童智能手表成为隐形“窃听器”的严重安全问题。家长给孩子买智能手表的初衷是为了获得一份安全感，但智能手表上的漏洞却成为不法分子的“窃听器”。

在给孩子购买智能手表的风潮下，却隐藏着巨大的安全风险。对智能手表的安全分析表明，攻击者利用儿童智能手表的安全漏洞，导致儿童被黑客实时监控，获取儿童的日常行走轨迹以及实时环境声音，同时漏洞还会造成与父母有关的关键信息数据泄露。



图2-59 《焦点访谈》栏目（来源：深信服公司）

目前国家对于儿童安全手表等智能穿戴设备还没有统一规范，这类产品在信息安全方面的质量参差不齐。手表厂商因不注重信息的加密技术，技术力量薄弱，形成安全隐患。新型技术的兴起可能会带来一些商业机会，但在技术高速发展、产品不断迭代的今天，要注意的是，敏感数据传输是要加密的，访问必须受到限制。

2015年诈骗短信成为导致用户个人信息泄露的重要因素。数据显示，2015年冒充熟人的诈骗短信最多，占28.5%，其次是虚假中奖类诈骗短信，占25.6%，冒充银行的诈骗短信，占19.9%。2015年利用短信进行精准的钓鱼欺诈案例层出不穷，如图2-60所示。

图2-60 钓鱼欺诈导致个人信息泄露（来源：深信服公司）

随着互联网的普及与各类应用的不断使用，用户基本个人信息也在以各种各样的形式在互联网上被采集、存储和传输。未来黑色产业也会利用互联网的特点，届时将看到黑客行为更为组织化、产业化、规模化。在这样的背景以及环境下，如何保证个人关键信息不被泄露、篡改、伪造将会成为未来一段时间内的热点。社保信息泄露事件给我们带来太多的启示，也为我们敲响警钟。

2.7 DNS DDoS攻击事件分析（来源：绿盟公司）

2.7.1 事件概述

某运营商枢纽节点DNS网络中防火墙的会话数接近饱和(in Use Count达到900万), 绿盟科技ADS产品报警有DDoS攻击告警, 监测发现域名解析延时增大, 严重影响了DNS业务的正常运行。

2015年6月15日上午, 接到某运营商网管中心互联网室的通知, 其枢纽节点DNS服务器疑似遭受DDoS攻击。绿盟科技服务团队启动应急响应, 并协调绿盟科技云安全运营中心协助处理, 响应工作随即启动。

2.7.2 事件处理过程

2.7.2.1 检测过程

2015年6月15日9:30, 绿盟科技DDoS防护系统发出DDoS攻击告警, 同时接到某运营商网管中心互联网室通知其DNS疑似遭受DDoS攻击, 域名解析延时增大, 成功率低于90%, 随即绿盟科技运营商服务团队启动了应急响应工作。从15日凌晨至19日, 攻击一直在持续, 初步统计此次攻击流量至少在10GB以上, 其持续时间之长, 攻击流量之大, 当属近几年该运营商之最。

通过样本分析发现, 此次攻击主要是通过控制肉鸡对美国黑客网站(Defcon.org)和僵尸网络(router.bittorrent.com、router.utorrent.com)域名进行ANY查询请求和随机查询请求, 导致该运营商DNS遭受拒绝服务攻击。攻击在短时间内发起了峰值大于6Gbit/s的查询请求, 造成该运营商枢纽DNS递归服务器延迟增大, 核心解析业务受到严重影响。

使用ADS自带的抓包工具捕获数据包样本, 并对捕获到的攻击样本进行分析, 如图2-61所示。



Filter: dns.qry.name == 'defcon.org'		Expression... Clear Apply Save				
No.	Time	Source	Destination	Protocol	Length	Info
75	0.050501	192.168.1.1		DNS	81	Standard query 0x98ad ANY defcon.org
86	0.057863			DNS	81	Standard query 0x98ad ANY defcon.org
104	0.069894			DNS	81	Standard query 0x98ad ANY defcon.org
108	0.072561			DNS	81	Standard query 0xc12 ANY defcon.org
109	0.073228			DNS	81	Standard query 0xc12 ANY defcon.org
118	0.079260			DNS	83	Standard query 0x0d56 ANY defcon.org
129	0.086615			DNS	81	Standard query 0xb405 ANY defcon.org
136	0.091296			DNS	81	Standard query 0xc12 ANY defcon.org
140	0.093975			DNS	76	Standard query 0x11b2 ANY defcon.org
142	0.095312			DNS	81	Standard query 0x98ad ANY defcon.org
145	0.097326			DNS	72	Standard query 0x1df5 ANY defcon.org
147	0.098665			DNS	77	Standard query 0x508c ANY defcon.org
202	0.135120			DNS	81	Standard query 0xc12 ANY defcon.org
224	0.149688			DNS	81	Standard query 0xdf79 ANY defcon.org
227	0.151680			DNS	81	Standard query 0x34ff ANY defcon.org
233	0.155651			DNS	81	Standard query 0xc12 ANY defcon.org
261	0.174200			DNS	86	Standard query 0xffc8 ANY defcon.org
272	0.181487			DNS	81	Standard query 0xc12 ANY defcon.org
274	0.182809			DNS	81	Standard query 0xc12 ANY defcon.org
276	0.184172			DNS	76	Standard query 0xf86b ANY defcon.org
278	0.185496			DNS	108	Standard query 0x6954 ANY defcon.org
282	0.188149			DNS	81	Standard query 0xdf79 ANY defcon.org
302	0.201660			DNS	81	Standard query 0xc12 ANY defcon.org
316	0.210917			DNS	81	Standard query 0xdf79 ANY defcon.org
362	0.241585			DNS	76	Standard query 0x0a48 ANY defcon.org
364	0.242908			DNS	77	Standard query 0x15c0 ANY defcon.org
393	0.262144			DNS	77	Standard query 0x23a0 ANY defcon.org
401	0.267471			DNS	81	Standard query 0xc1a0 ANY defcon.org
416	0.277702			DNS	71	Standard query 0x69e2 ANY defcon.org
417	0.278363			DNS	74	Standard query 0x4282 ANY defcon.org
482	0.321474			DNS	80	Standard query 0xae4b ANY defcon.org
492	0.328122			DNS	88	Standard query 0xc5d4 ANY defcon.org

图2-61 捕获到的攻击样本分析

在ADS上监控到defcon.org这个域名的查询数量一直排在第一位，且查询数量较多，属于异常现象，如图2-62所示。

域名查询排名统计	
域名	查询数量
defcon.org	822990
eventlog.beacon.qq.com	371777
loc.map.baidu.com	268726
monitor.uu.qq.com	257050
a.root-servers.net	241203
www.baidu.com	236246
...	...

图2-62 域名查询排名统计

查询数量最多的域名是一个国外的黑客网站，如图2-63所示。

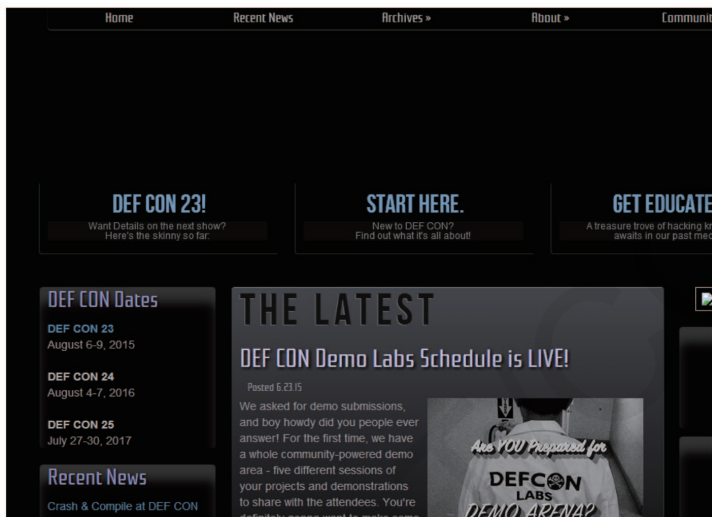


图2-63 一个国外的黑客网站

2.7.2.2 攻击原理

攻击者控制大量肉鸡发起针对多个域名（主要域名为defcon.org）的ANY放大查询（DNS Amplification Attack，DNS反射攻击）和随机查询攻击，极大地消耗了防火墙的性能。这种攻击由来已久，如图2-64所示，2014年12月10-19日，国内出现大规模针对运营商DNS网络的恶性DDoS攻击事件，当时的攻击者就是通过肉鸡对国外游戏厂商的域名（arkhamnetwork.org、arkhamnetwork.com、getfastinstagramfollowers.net）随机查询进行拒绝服务攻击，造成各省的DNS递归服务器延迟增大，核心解析业务受到严重影响。这种攻击模式成本低、效果好，追踪溯源困难。

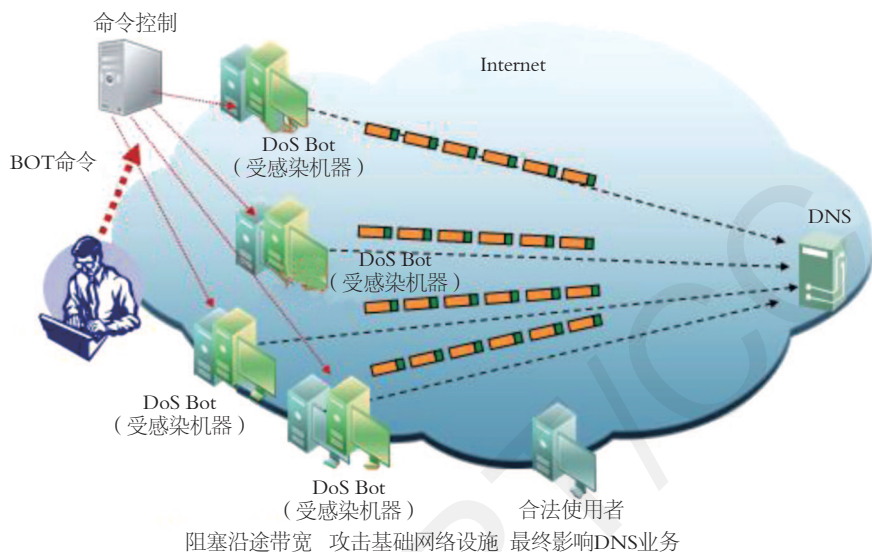


图2-64 大规模针对运营商DNS网络的恶性DDoS攻击

攻击特点如下：

- 攻击开始时都是采用ANY查询进行放大攻击，放大倍数在50倍左右，基本特征不变，目前没有产生新的变种；
- 基本上的攻击都是肉鸡、无线路由器，监控设备，也有一些源IP地址本身是DNS；
- 攻击时间不固定，下午多一些；
- 最高流量峰值达到10GB。

2.7.2.3 分析过程

通过结合域名专项防护系统ADS的告警日志和抓包分析发现，有大量对defcon.org的ANY查询，分析发现此次攻击事件的攻击源90%来自省内IP地址，部分肉鸡存在弱口令，相对于过去的攻击，此次攻击的攻击源更加多样化，其中智能监控设备和商用无线路由器（如某厂商的路由器带有dnsmq服务）成为主力。

大量对defcon.org的ANY查询的恶意请求如图2-65所示。



No.	Time	Source	Destination	Protocol	Length	Info
9	0.071649			DNS	81	Standard query 0x47a7 AAAA router.bittorrent.com
78	0.125530			DNS	81	Standard query 0xf92a A router.bittorrent.com
80	0.126887			DNS	81	Standard query 0x42b2 AAAA router.bittorrent.com
82	0.128238			DNS	81	Standard query 0x983a AAAA router.bittorrent.com
88	0.132311			DNS	81	Standard query 0xf92a A router.bittorrent.com
95	0.137091			DNS	81	Standard query 0xb15 AAAA router.bittorrent.com
96	0.137734			DNS	81	Standard query 0xcff AAAA router.bittorrent.com
97	0.138415			DNS	81	Standard query 0xeal AAAA router.bittorrent.com
179	0.194772			DNS	81	Standard query 0xd1db AAAA router.bittorrent.com
269	0.257159			DNS	81	Standard query 0x41b1 AAAA router.bittorrent.com
286	0.268858			DNS	81	Standard query 0x9292 AAAA router.bittorrent.com
341	0.306628			DNS	81	Standard query 0x08cc AAAA router.bittorrent.com
345	0.309378			DNS	81	Standard query 0x1139 AAAA router.bittorrent.com
346	0.310066			DNS	81	Standard query 0x93e8 AAAA router.bittorrent.com
420	0.360894			DNS	81	Standard query 0x2cef AAAA router.bittorrent.com
501	0.416442			DNS	81	Standard query 0x8aed AAAA router.bittorrent.com
540	0.443524			DNS	81	Standard query 0x1444 AAAA router.bittorrent.com
592	0.479195			DNS	81	Standard query 0x0863 A router.bittorrent.com
633	0.507127			DNS	81	Standard query 0xbd66 A router.bittorrent.com
637	0.509817			DNS	81	Standard query 0xc00f AAAA router.bittorrent.com
639	0.511154			DNS	81	Standard query 0xabae A router.bittorrent.com
641	0.512504			DNS	81	Standard query 0xefae A router.bittorrent.com
642	0.513191			DNS	81	Standard query 0x377d A router.bittorrent.com
643	0.513886			DNS	81	Standard query 0x6901 AAAA router.bittorrent.com
644	0.514583			DNS	81	Standard query 0x74fe A router.bittorrent.com
645	0.515274			DNS	81	Standard query 0xab0c A router.bittorrent.com
647	0.516641			DNS	81	Standard query 0x2a01 AAAA router.bittorrent.com
648	0.517338			DNS	81	Standard query 0xd9e6 AAAA router.bittorrent.com
651	0.519655			DNS	81	Standard query 0xd07b AAAA router.bittorrent.com
653	0.521032			DNS	81	Standard query 0xd07b AAAA router.bittorrent.com

图2-67 大量对bittorrent.com的随机域名查询

域名专项防护系统ADS上defcon.org的查询统计，查询数量一直排在第一位，如图2-68所示。

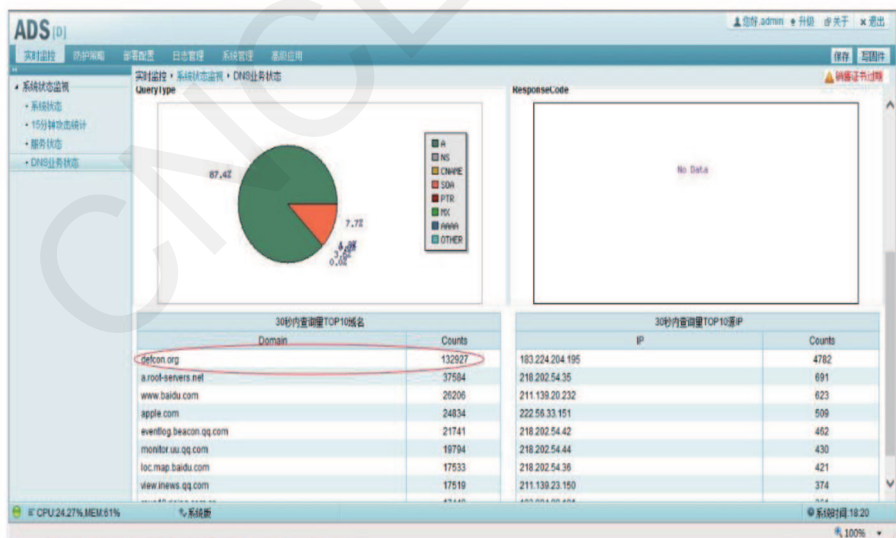


图2-68 域名专项防护系统ADS上defcon.org的查询统计

2.7.2.4 处置阶段

根据告警情况，结合DNS防火墙的会话性能适用占比情况，及时调整域名专项防护设备的UDP检测阈值（其UDP阈值调整在8万~15万pps）对攻击流量进行清洗。同时在域名专项防护系统开启模式匹配策略（7层丢弃），对查询Defcon.org的域名源IP地址的请求进行丢弃，这样有效地保障DNS的高可用性，截至2015年6月19日下午，在流量清洗和模式匹配的防护下，该运营商DNS域名解析正常。

调整防护策略，UDP检测阈值调整范围在8万~15万pps，如图2-69所示。

启用	检测SYN Flood	6000 (pps)	40000 (pps)	双向保护	1-SafeConnect
启用	检测ACK Flood	100000(pps)		双向保护	
启用	检测UDP Flood	80000 (pps)		双向保护	
启用	检测ICMP Flood	6000 (pps)		双向保护	
禁用	流量控制		2000(kbps)	不保护	

图2-69 UDP检测阈值

开启流量牵引，将访问DNS的流量牵引到域名专项防护系统ADS进行清洗，同时启动模式匹配，对恶意查询包进行丢弃，如图2-70所示。

实时监测	防护策略	日志管理	系统管理	高级应用
- 新包验证 - 新包验证控制 - 模式匹配 - 模式匹配控制 - 模式匹配规则 - 模式匹配工具 - DNS服务器性能测试工具	- 高级模式 - 高级模式控制 - 高级模式规则 - 高级模式工具 - DNS服务器性能测试工具			
	源IP地址	255.255.255.0		
	源端口			
	协议类型	UDP		
	访问控制	丢弃		
	是否启用	是		
	接口范围			
	包长度范围			
	TOS	--		
	TTL			
	UDP校验			
	ICMP类型	--		
	TCP选项	--		
	TCP标记	☐ SYN ☐ ACK ☐ FIN ☐ RST ☐ URG ☐ PSH		
	流量量	0(字节)		
	深度	1480(字节)		
	大小端匹配	否		
	特征字符串	"\x06\x64\x65\x66\x63\x67\x6e\x03\x6f\x72\x67\x00"		

图2-70 启动模式匹配，对恶意查询包进行丢弃

被清洗的流量日志如图2-71所示。



策略应用 • 模式匹配 • 模式匹配规则

模式匹配规则

目标IP	目标子网掩码	目标端口范围	源IP	源子网掩码	源端口范围	协议	访问控制	状态	操作
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.252		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.0		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.255		UDP	禁止	启用	 
	255.255.255.255	53		255.255.255.255		UDP	禁止	启用	 
255.255.255.255	53	255.255.255.255		UDP	禁止	启用	 		

添加

图2-71 被清洗的流量日志

如图2-72所示，在防护措施实施以后，DNS业务解析状态逐渐恢复正常。

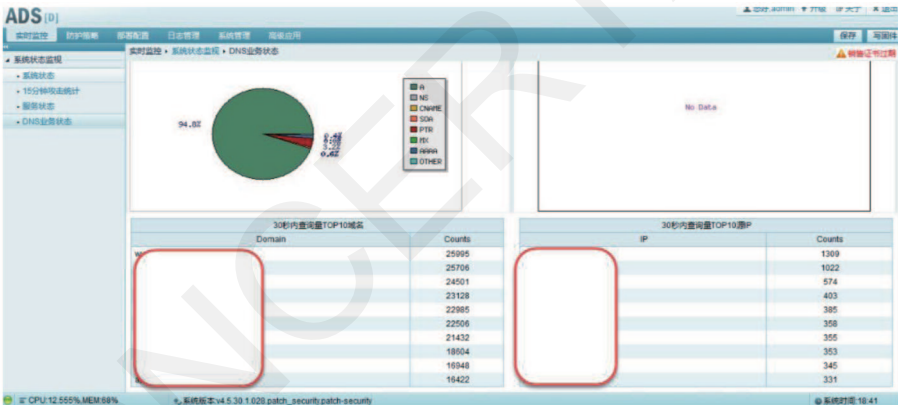


图2-72 防护措施实施后DNS业务恢复正常

2.7.3 攻击源回溯

通过抓包分析，大部分攻击源头如图2-73所示。

```
*.*82.138 区域 1 *.*82.27 区域 1 ***.*83.202 区域 1
*.*99.51 区域 2 *.*82.107 区域 1 ***.*82.136 区域 1
*.*85.35 区域 1 *.*84.65 区域 1 ***.*75.137 区域 1
*.*82.122 区域 1 *.*83.19 区域 1 ***.*82.96 区域 1
*.*219.17 区域 3 *.*82.121 区域 1 ***.*87.194 区域 1
*.*86.66 区域 1 *.*85.90 区域 1 ***.*20.231 区域 1
```

图2-73 大部分攻击源头

如图2-74所示，通过查询其IP地址分配发现，大部分攻击源头来自于某银行互联网专线，对其专线进行渗透测试发现，该专线均开放了如下端口。

```
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.62
80/tcp open http LuCI Lua http config
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
389/tcp filtered ldap
443/tcp open ssl/https?
444/tcp filtered snpp
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
1025/tcp filtered NFS-or-IIS
1434/tcp filtered ms-sql-m
2222/tcp open ssh Dropbear sshd 2011.54 (protocol 2.0)
4444/tcp filtered krb524
5800/tcp filtered vnc-http
6129/tcp filtered unknown
10000/tcp open snet-sensor-mgmt?
Service Info: OS: Linux
```

图2-74 对专线进行渗透测试发现开放端口

如图2-75所示，登录80和443端口发现该系统属于无线路由器，通过集成商的配合调查，发现其Web登录存在弱口令，该设备AP是某厂商无线接入网关，目前的登录账号属于弱口令。

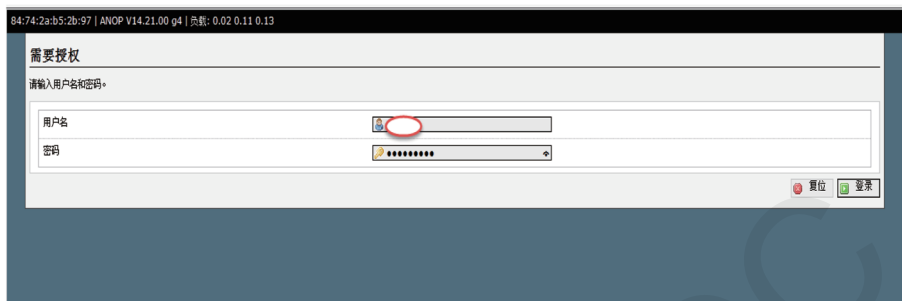


图2-75 Web登录存在的口令

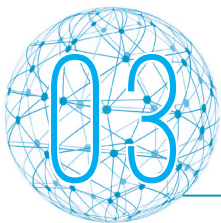
由于维护方不提供ssh登录账号密码和网关登录的账号密码，另外针对defcon.org的恶意查询已经消失，故无法继续深入调查。根据调查分析确认，本次攻击来自于肉鸡、商业无线路由器，监控设备。

2.7.4 事件总结

本次攻击事件从2015年6月15日开始，至2015年6月19日未发现攻击。在此期间，该运营商网管中心互联网室协调绿盟科技等对攻击事件进行持续监控和分析，并采取有效的防护措施，最终有效地抵御了攻击，目前该运营商DNS业务恢复了正常。

从2014年开始DDoS攻击方式出现了新的反射式放大攻击形式，该类攻击基于SSDP利用一些智能设备进行反射式攻击，攻击带宽放大倍数最高可达75倍，攻击方技术不断演进，将“以大欺小”（流量型攻击）与“以小博大”（资源耗尽型）两种攻击方式组合起来，利用逐渐提高的网络带宽增强攻击力等。

此次攻击事件持续时间长、攻击流量大、攻击技术复杂，对该运营商DNS业务的正常运行造成严重影响。虽然采取一系列的防护措施，达到预期的效果，但是，安全工作是一个长期持续性而非阶段性的工作，需要时刻保持警觉，认真总结这次攻击事件的应急处理过程，提升安全监控人员和管理维护人员面对突发事件的应急处理能力，同时不断完善安全技术防护手段，不断更新安全制度，落实安全管理，从而能更有力地保障系统稳固健康运行。



计算机恶意程序传播和活动情况

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。

2015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105056个，较2014年上升0.8%，受控主机IP地址总数为28728402个，较2014年大幅上升105.3%。其中，境内木马或僵尸程序受控主机IP地址数量为19781858个，较2014年上升78.4%，境内控制服务器IP地址数量为40782个，较2014年下降34.1%。连续三年我国境内木马或僵尸程序控制服务器数量出现下降，体现了近三年来我国持续开展木马和僵尸网络专项治理工作和日常处置工作所取得的良好效果。

3.1.1 木马或僵尸程序控制服务器分析

2015年，境内木马或僵尸程序控制服务器IP地址数量为40782个，较2014年大幅下降34.1%；境外木马或僵尸程序控制服务器IP地址数量为64274个，较2014年有所增长，增幅为51.8%，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。

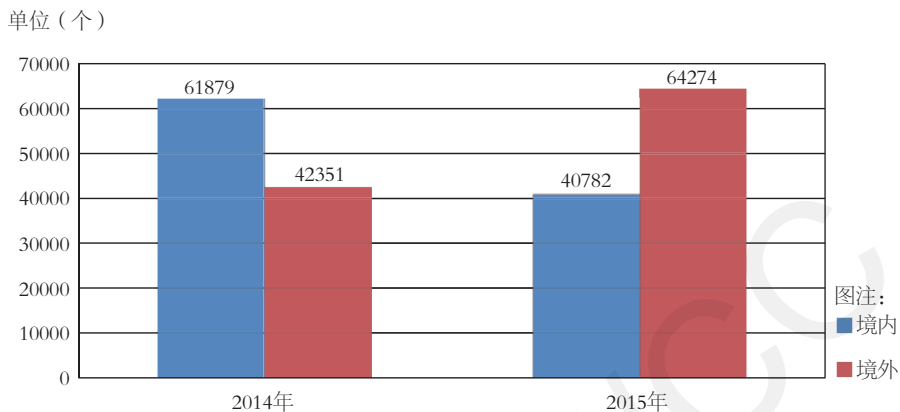


图3-1 2015年与2014年木马或僵尸程序控制服务器数据对比（来源：CNCERT/CC）

2015年，在发现的因感染木马或僵尸程序而形成的僵尸网络中，规模100~1000的占70.6%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2014年相比分别增加530个、160个、112个、20个、19个。2015年僵尸网络规模分布情况如图3-2所示。

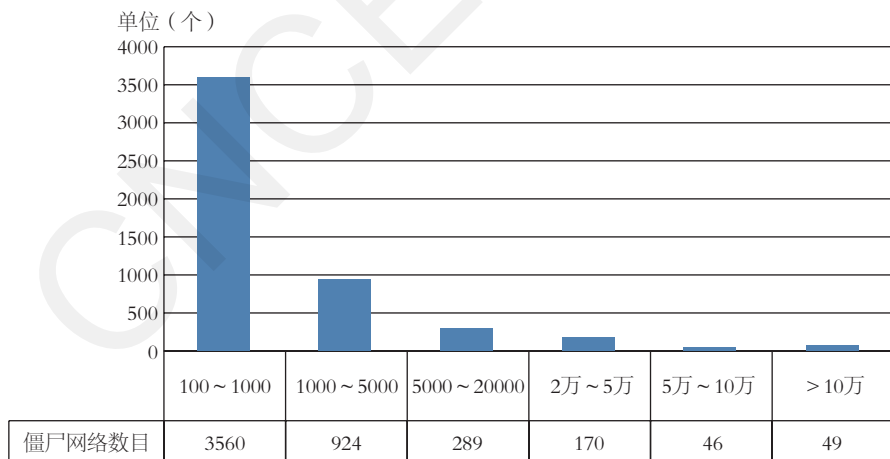


图3-2 2015年僵尸网络规模分布（来源：CNCERT/CC）

2015年木马或僵尸程序控制服务器IP地址数量的月度统计如图3-3所示，全年呈波动态势，1月达到最高值28777个，5月为最低值7410个。

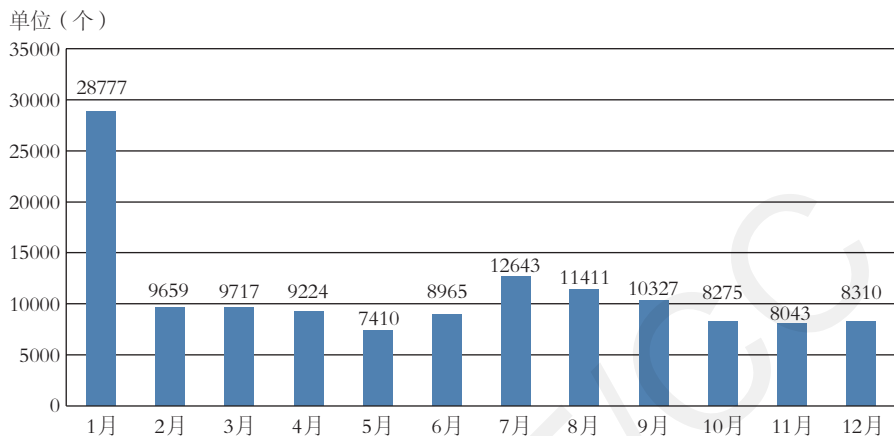


图3-3 2015年木马或僵尸程序控制服务器IP地址数量月度统计（来源：CNCERT/CC）

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、北京市居于木马或僵尸程序控制服务器IP地址绝对数量前三位，云南省、广东省、江苏省居于木马或僵尸程序控制服务器IP地址相对数量的前三位。

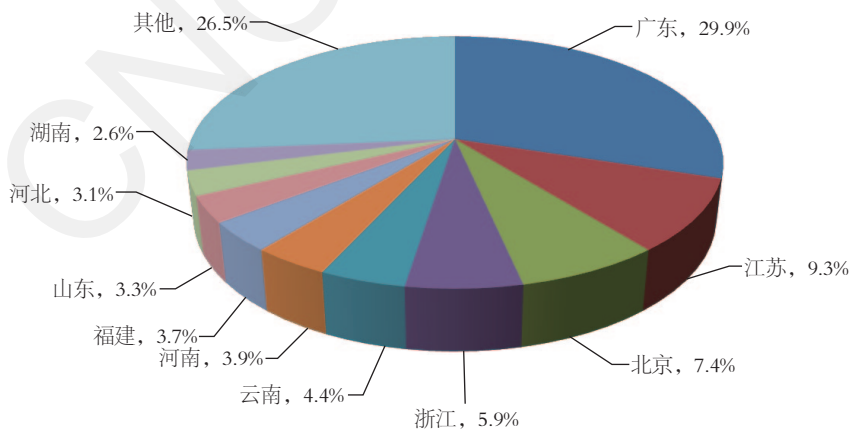


图3-4 2015年境内木马或僵尸程序控制服务器IP地址按地区分布（来源：CNCERT/CC）

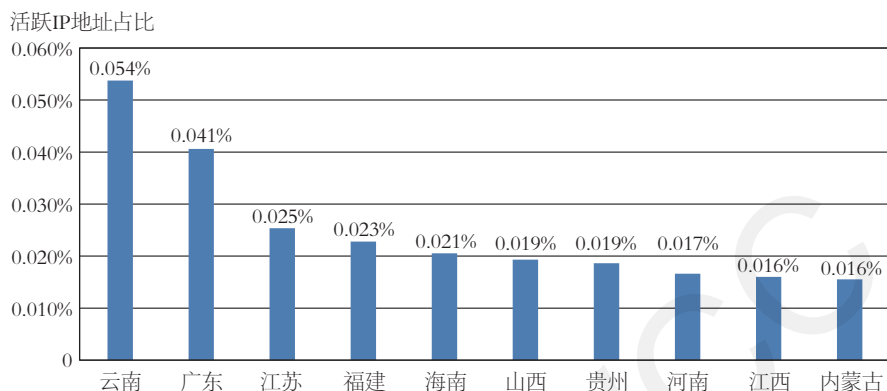


图3-5 2015年境内木马或僵尸程序控制服务器IP地址
占所在地区活跃IP地址比例TOP10（来源：CNCERT/CC）

图3-6和图3-7为2015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地址数量约占境内控制服务器IP地址数量的2/3。

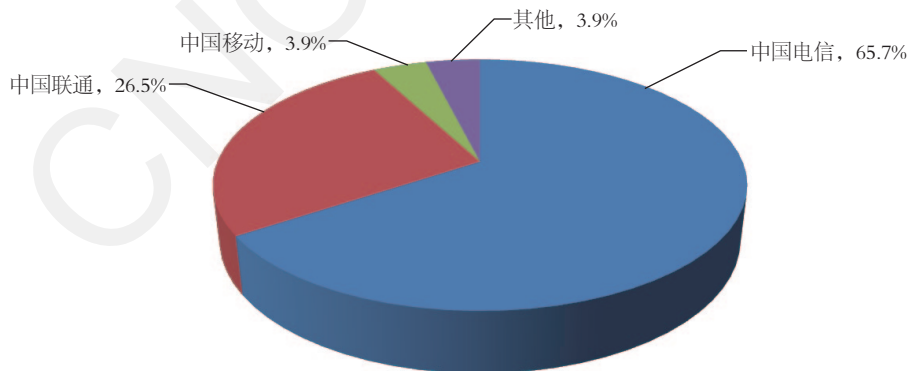


图3-6 2015年境内木马或僵尸程序控制服务器IP地址按基础电信企业分布
（来源：CNCERT/CC）

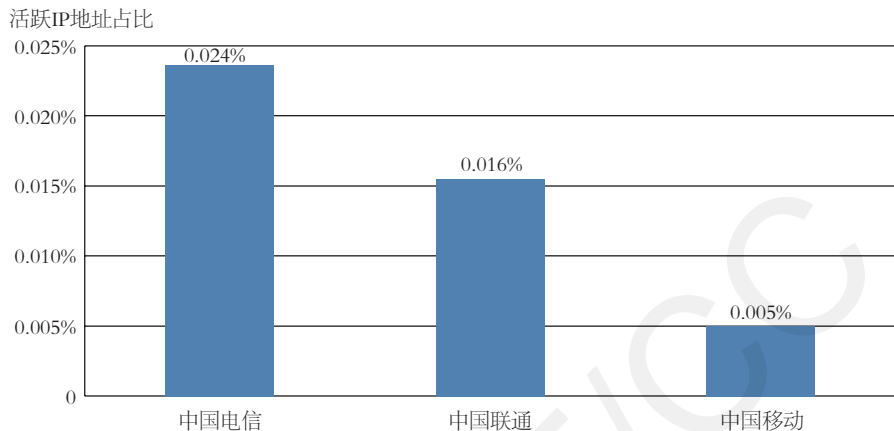


图3-7 2015年境内木马或僵尸程序控制服务器IP地址占所属基础电信企业活跃IP地址比例（来源：CNCERT/CC）

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26.8%，中国台湾和德国分列第二、三位，占比分别为22.4%和3.8%。

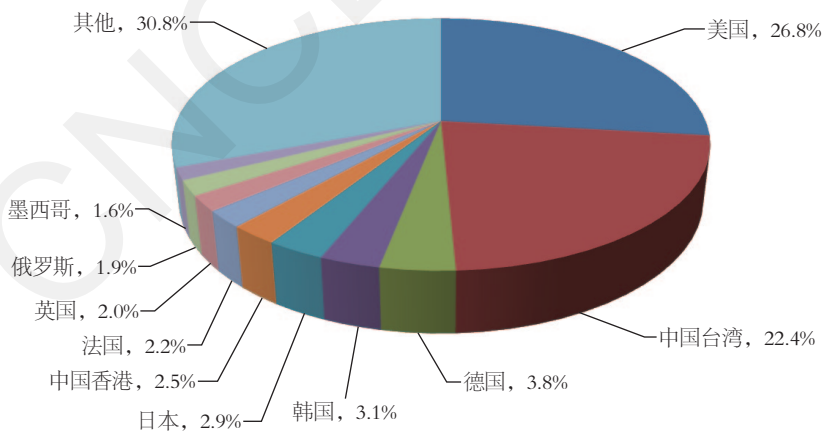


图3-8 2015年境外木马或僵尸程序控制服务器IP地址按国家和地区分布（来源：CNCERT/CC）



3.1.2 木马或僵尸程序受控主机分析

2015年，境内共有19781858个IP地址的主机被植入木马或僵尸程序，境外共有8946544个IP地址的主机被植入木马或僵尸程序，数量较2014年有所增加，增幅分别达到了78.4%和208.1%，具体如图3-9所示。

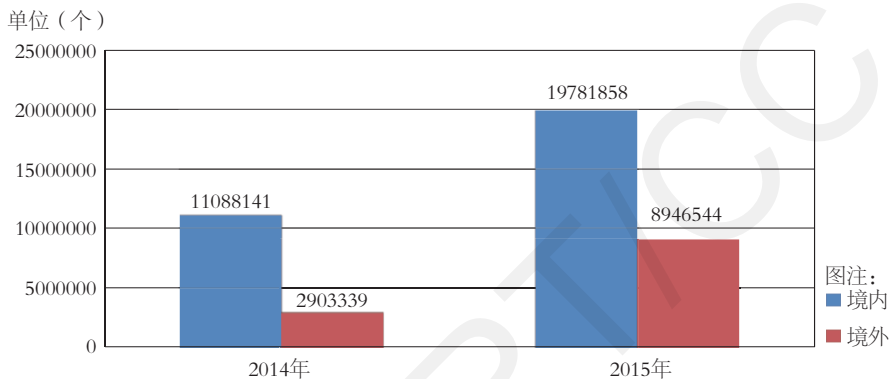


图3-9 2015年和2014年木马或僵尸程序受控主机数量对比（来源：CNCERT/CC）

2015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，1月达到最高值5307660个，12月为最低值2332874个。2015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。

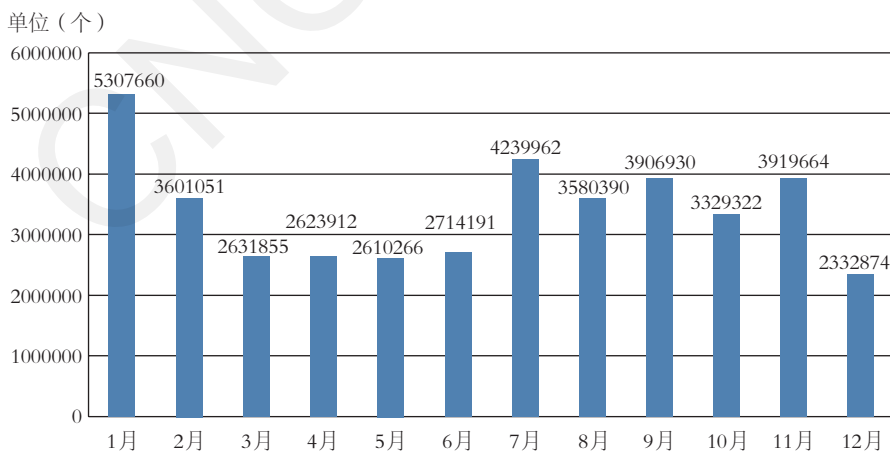


图3-10 2015年木马或僵尸程序受控主机IP地址数量月度统计（来源：CNCERT/CC）

境内木马或僵尸程序受控主机IP地址绝对数量和相对数量（即各地区木马或僵尸程序受控主机IP地址绝对数量占其活跃IP地址数量的比例）前10位地区分布如图3-11和图3-12所示，其中，广东省、江苏省、山东省居于木马或僵尸程序受控主机IP地址绝对数量前三位。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。青海省、海南省、辽宁省居于木马或僵尸程序受控主机IP地址相对数量的前三位。

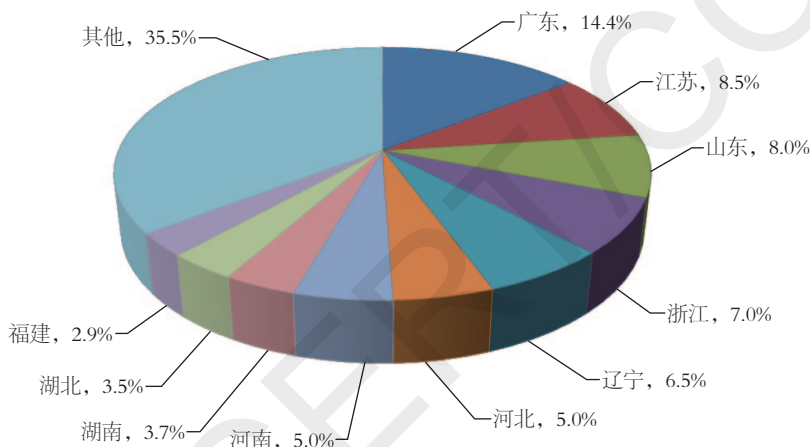


图3-11 2015年境内木马或僵尸程序受控主机IP地址数量按地区分布
(来源: CNCERT/CC)

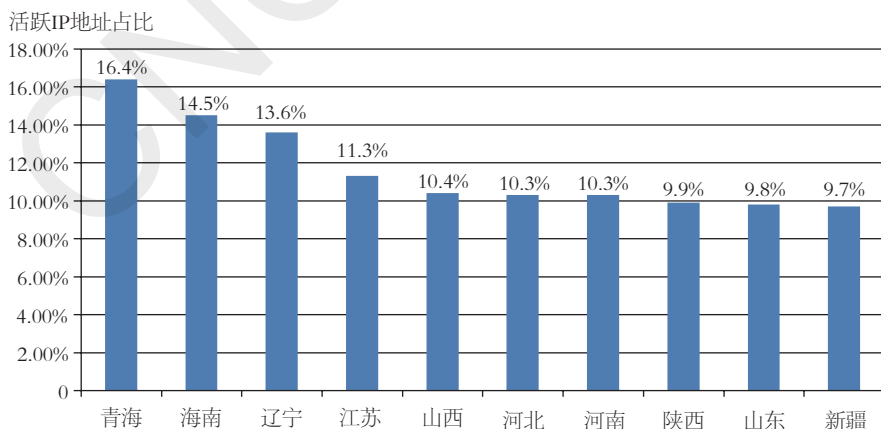


图3-12 2015年境内木马或僵尸程序受控主机IP地址数量占
所在地区活跃IP地址比例TOP10 (来源: CNCERT/CC)



图3-13和图3-14为2015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近2/3。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%。

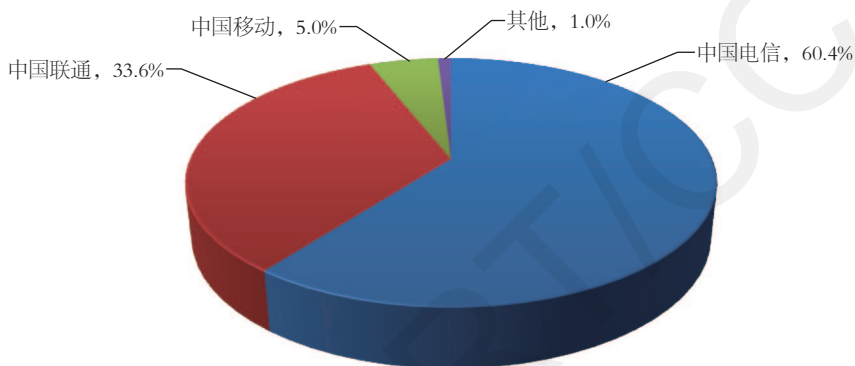


图3-13 2015年境内木马或僵尸程序受控主机IP地址数量按基础电信企业分布
(来源: CNCERT/CC)

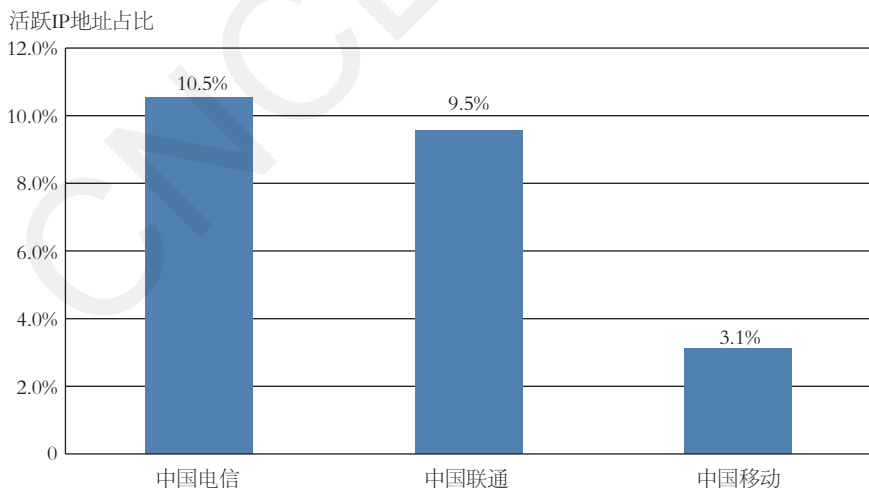


图3-14 2015年境内木马或僵尸程序受控主机IP地址数量占所属基础电信企业活跃IP地址数比例 (来源: CNCERT/CC)

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，埃及、泰国、越南居前三位。

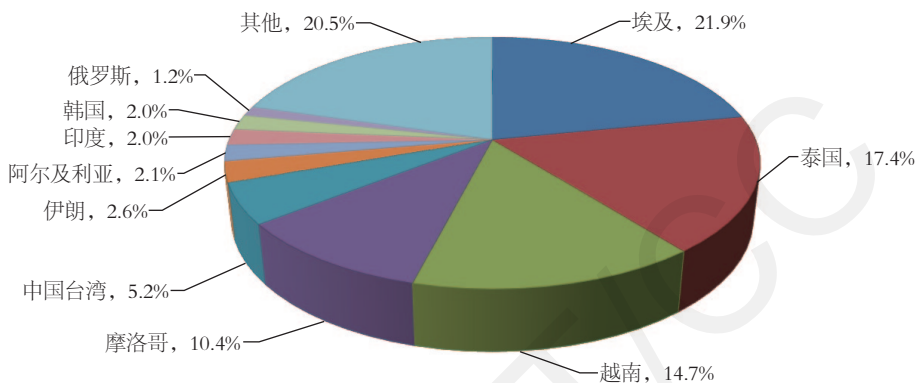


图3-15 2015年境外木马或僵尸程序受控主机IP地址数量按国家和地区分布
(来源: CNCERT/CC)

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，构建一个庞大的攻击平台，不仅能够用于大范围的网络欺诈和信息窃取，而且能够被利用发动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和通报处置。监测数据显示，全球互联网月均感染“飞客”蠕虫的主机IP地址数量持续减少，2010年12月超过6000万个IP地址，2011年月均3500万个IP地址，2012年月均2800万个IP地址，2013年月均1722万个IP地址，2014年月均943万个IP地址，2015年月均391万个IP地址。

据CNCERT/CC监测，2015年感染“飞客”蠕虫的主机IP地址数量排名前三的国家或地区分别是中国大陆（12.4%）、印度（7.1%）和巴西（7%），具体分布情况如



图3-16所示。图3-17为2015年境内主机IP地址感染“飞客”蠕虫的数量月度统计，月均数量近48万个，总体上稳步下降，较2014年下降了53.4%，但2015年9月起“飞客”蠕虫在境内又呈现活跃态势。

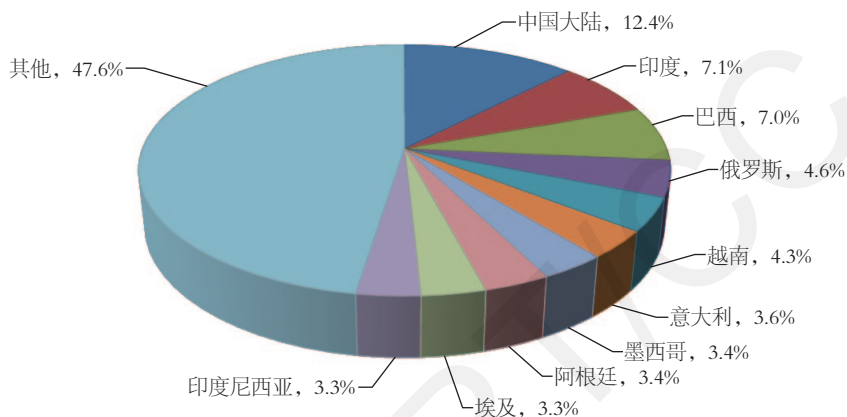


图3-16 2015年全球互联网感染“飞客”蠕虫的主机IP地址数量按国家和地区分布
(来源: CNCERT/CC)

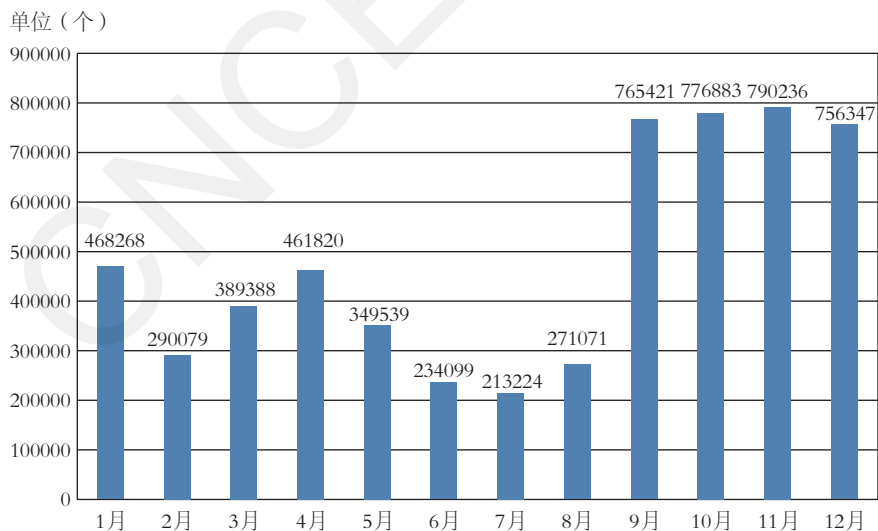


图3-17 2015年中国境内感染“飞客”蠕虫的主机IP地址数量月度统计
(来源: CNCERT/CC)

3.3 恶意程序传播活动监测

如图3-18所示, 2015年1-4月恶意程序传播活动频次相对较低, 5-7月恶意程序传播活动频次进入全年最低谷, 8月的恶意程序传播事件数量较前7个月出现暴增, 8-10月恶意程序传播事件数量出现持续增长, 始终保持在水准, 11-12月的恶意程序传播事件数量较10月有所下降但仍然维持在较高水准。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, 还要提高广大用户的安全意识。

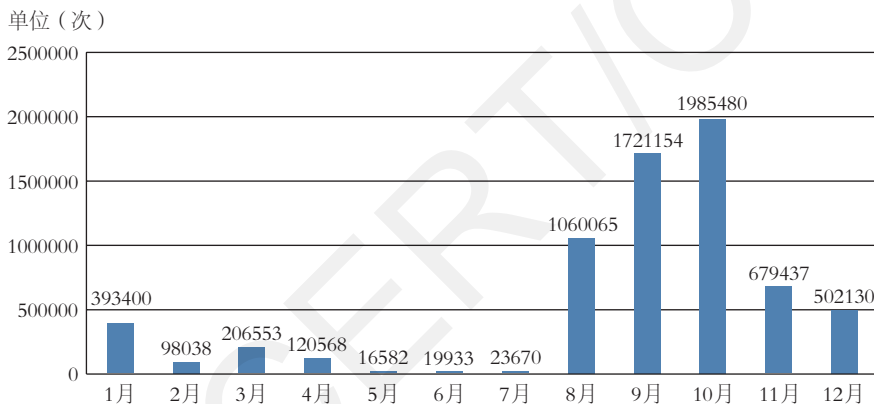


图3-18 2015年已知恶意程序传播事件次数月度统计 (来源: CNCERT/CC)

2015年, CNCERT/CC共监测到5524个(去重后的数量)放马站点, 图3-19是中国大陆地区放马站点数量月度统计情况, 可以看到, 放马站点数量在2015年呈现波动趋势, 1月达到峰值, 12月为全年最低值。

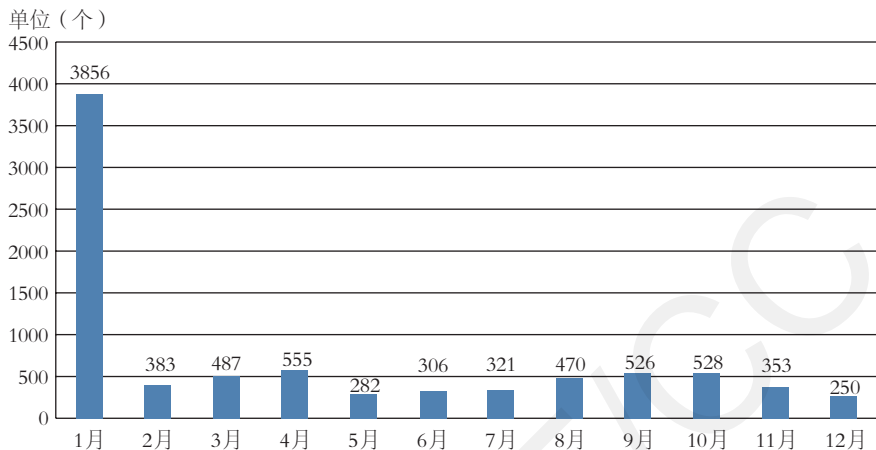


图3-19 2015年放马站点数量月度统计(来源: CNCERT/CC)

CNCERT/CC监测发现2015年中国大陆地区放马站点按省份分布情况如图3-20所示, 列前5位的省份是广东省(13.7%)、江苏省(11.4%)、浙江省(10.5%)、北京市(7.5%)和山东省(6.4%)。放马站点多集中在人口稠密、经济发达的省份。

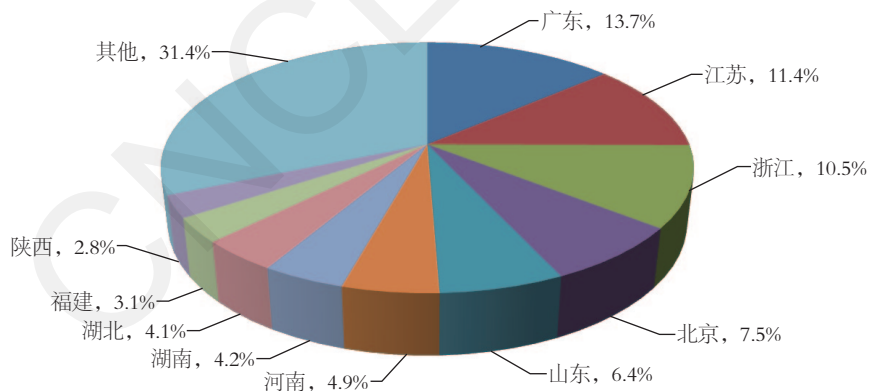


图3-20 2015年中国大陆地区放马站点按省份分布(来源: CNCERT/CC)

CNCERT/CC监测发现2015年中国大陆地区放马站点按域名分布情况如图3-21所示。其中, 排名前三位的是.com域名(55.9%)、.cn域名(25.2%)和.net域名(11.8%)。

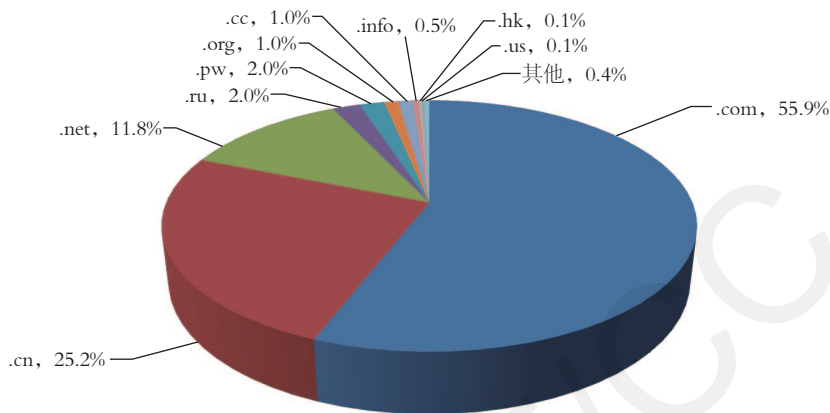


图3-21 2015年中国大陆地区放马站点按域名分布（来源：CNCERT/CC）

CNCERT/CC监测发现，2015年恶意程序传播主要使用5505和80端口，其中以5505端口最多。CNCERT/CC全年监测发现，恶意程序传播大量使用域名down01.kuaibo8.com:5505承载多种恶意程序，该域名上承载的恶意程序主要为Trojan/Win32.Reconyc家族与Trojan/Win32.StartPage家族，传播与感染数量非常大。放马站点使用的端口分布统计如图3-22所示。

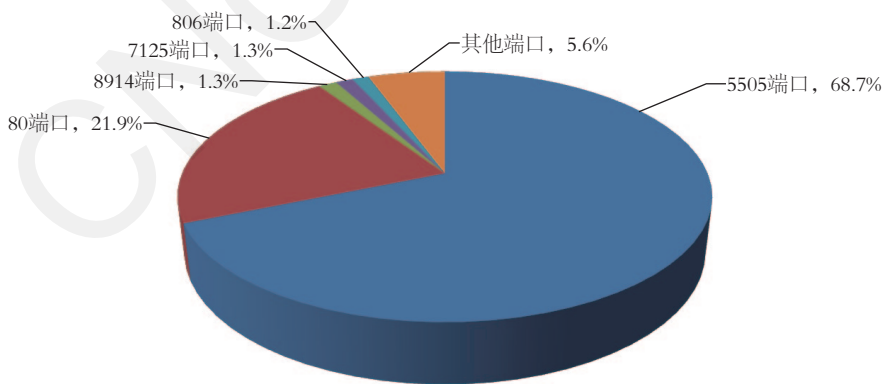


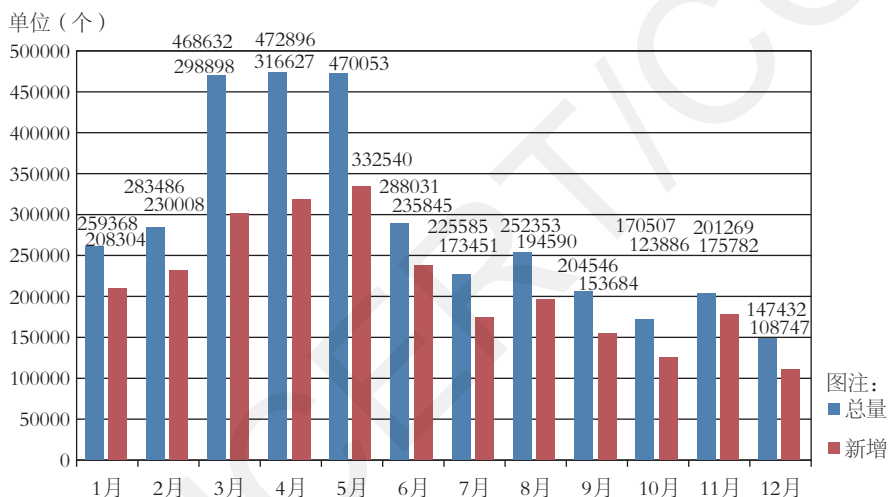
图3-22 放马站点使用的端口分布统计（来源：CNCERT/CC）



3.4 通报成员单位报送情况

3.4.1 安天公司恶意程序捕获情况

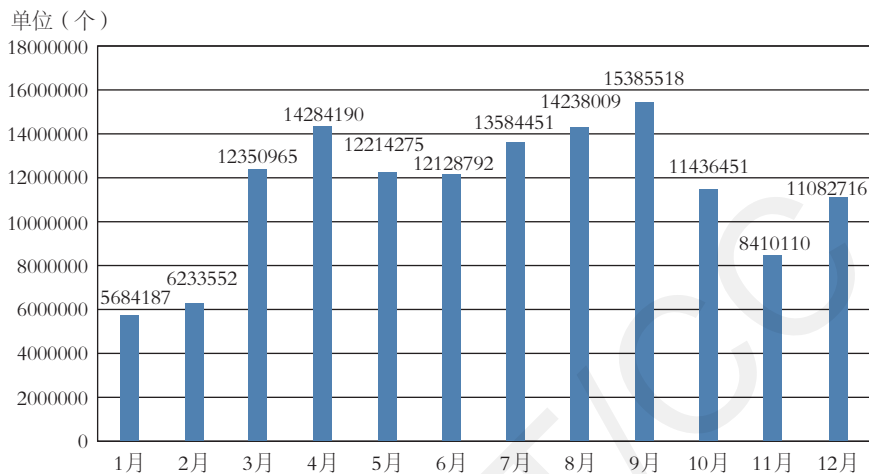
根据安天公司的监测结果，2015年全年捕获恶意程序总量为2871658个（按恶意程序名称统计），比2014年的3516450个下降18.3%。2015年各月捕获数量如图3-23所示，其中4月达到全年最高值（472896个），12月达到全年最低值（147432个）。



注：由于安天公司记录的恶意程序月度统计数据有重复，所以每月恶意样本之和大于统计的恶意程序总量

图3-23 2015年捕获恶意程序数量月度统计（来源：安天公司）

2015年全年捕获恶意程序样本总量为137033216个（按MD5值统计），比2014年的40346645个增长239.6%。2015年各月捕获数量如图3-24所示，其中9月达到全年最高值（15385518个），1月达到全年最低值（5684187个）。



注：由于安天公司只记录统计新增恶意样本，所以每月恶意样本之和即为本公司每月新增恶意样本总数

图3-24 2015年捕获恶意程序样本数量月度统计（来源：安天公司）

3.4.2 猎豹移动公司报送的恶意程序情况

根据猎豹移动公司的监测结果，2015年全年捕获病毒样本总量为104674316个（去重后的数量），比2014年的134202997个减少22%。2015年各月捕获数量如图3-25所示，其中12月达到全年最低值（4848472个），5月达到全年最高值（11623702个）。

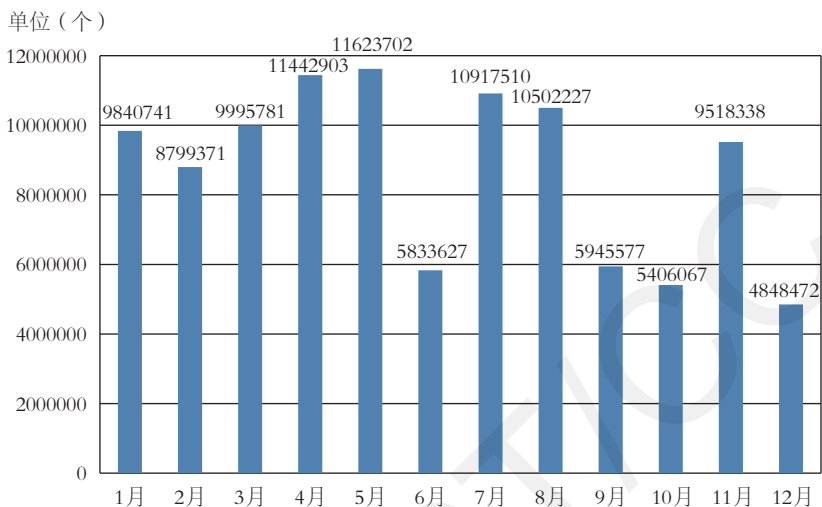


图3-25 2015年捕获病毒样本月度统计(来源:猎豹移动)

2015年全年捕获新增病毒特征总量为41176376个(去重后的数量),比2014年的30145726个上升36.6%。2015年各月捕获数量如图3-26所示,其中12月达到全年最低值(2816995个),8月达到全年最高值(4106443个)。

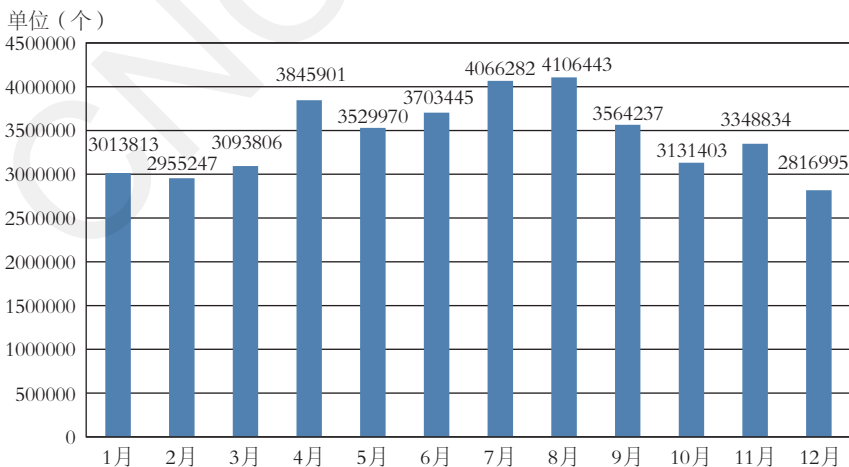


图3-26 2015年捕获新增病毒样本月度统计(来源:猎豹移动)

2015年全年监测到感染恶意程序的主机129284060台，比2014年的143392990个下降9.8%。感染恶意程序的主机数量为下降趋势，其中感染主机数量12月为全年最低点（8455008个），8月达到全年最高值（12204286个），如图3-27所示。

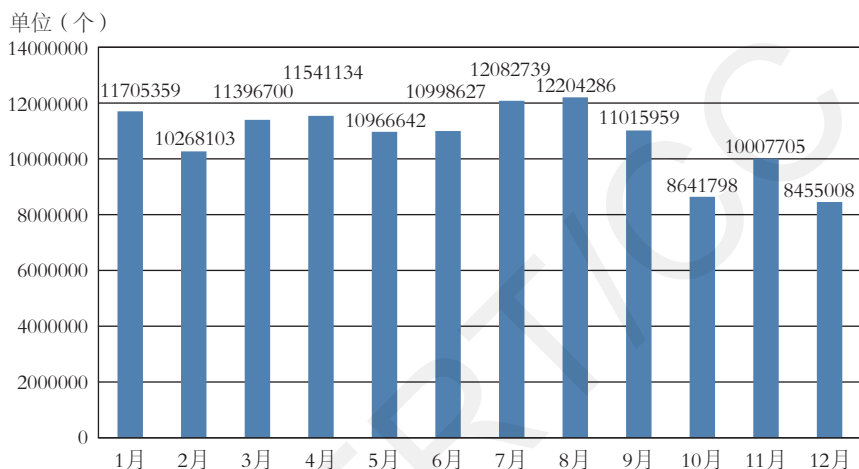


图3-27 2015年感染主机数量月度统计（来源：猎豹移动）

2004-2015年捕获恶意程序数量（去重后的数量）走势如图3-28所示。

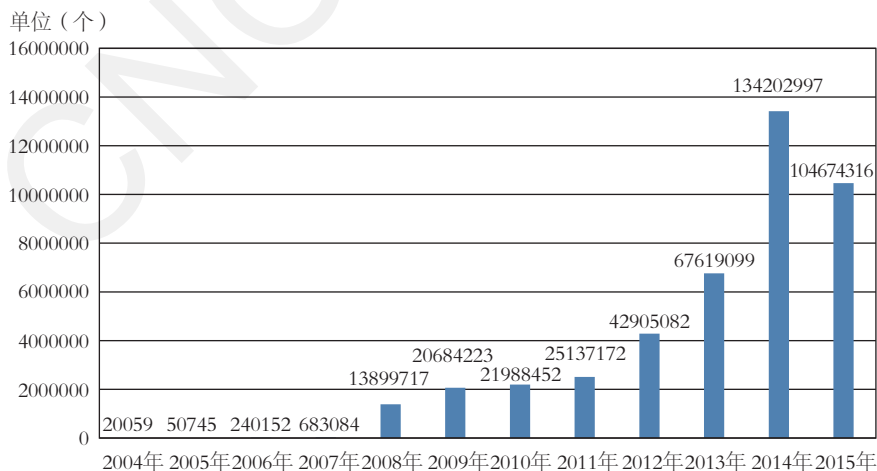


图3-28 2004-2015年捕获恶意程序数量走势（来源：猎豹移动）



3.4.3 奇虎360公司报送的恶意程序情况

2015年全年，360互联网安全中心共截获PC端新增恶意程序样本3.56亿个，和2014年相比增长9.9%；平均每天截获新增恶意程序样本97.7万个。360安全卫士、360杀毒共为全国用户拦截恶意程序攻击855.4亿次，相比2014年大幅增长49.4%；平均每天为用户拦截恶意程序攻击约2.3亿次。

图3-29和图3-30分别给出2015年各月PC端恶意程序新增量和拦截量月度统计情况。

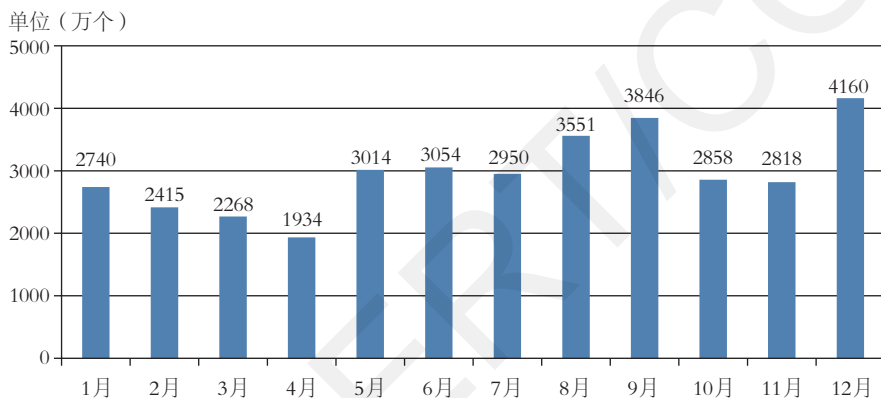


图3-29 2015年PC端各月新增恶意程序样本数（来源：360互联网安全中心）

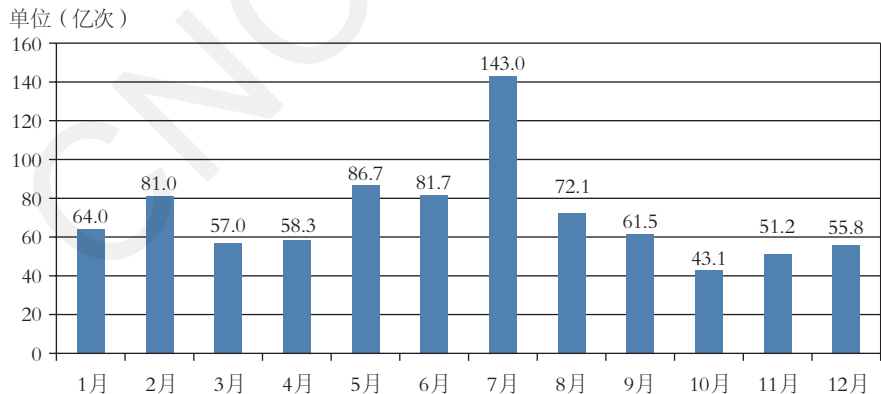


图3-30 2015年PC端各月恶意程序云查询拦截量（来源：360互联网安全中心）

图3-31给出了最近两年PC端恶意程序新增量和云查询拦截量的对比情况。

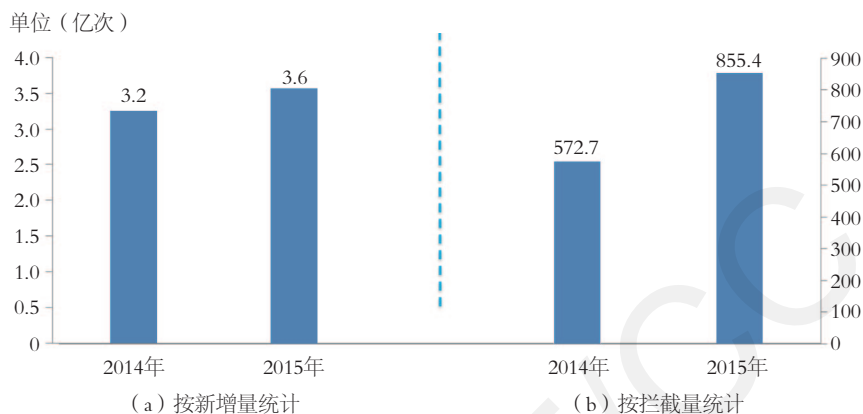


图3-31 2014–2015年PC端恶意程序情况对比（来源：360互联网安全中心）

3.4.4 卡巴斯基公司报送的恶意程序情况

根据卡巴斯基监测结果，2015年全年捕获恶意程序总量为112589个（按恶意程序名称统计），比2014年的105717个增长6.5%。2015年各月捕获数量如图3-32所示，其中9月达到全年最高值（12402个），1月达到全年最低值（5908个）。

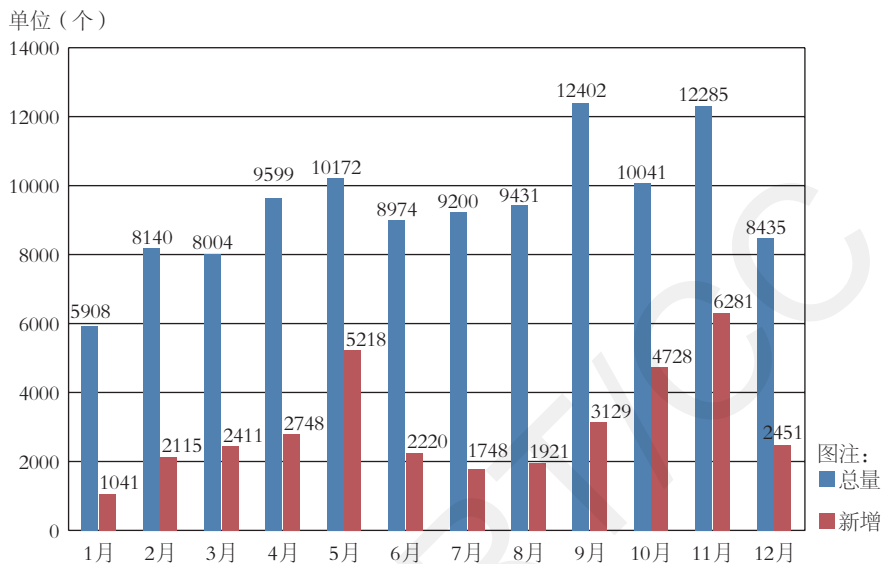


图3-32 2015年捕获恶意程序数量月度统计(来源:卡斯基)

2015年全年捕获恶意程序样本总量为826379978个(按MD5值统计),比2014年的753143542个增长9.7%。2015年各月捕获数量如图3-33所示,其中7月达到全年最高值(83592346个),2月达到全年最低值(61111869个)。

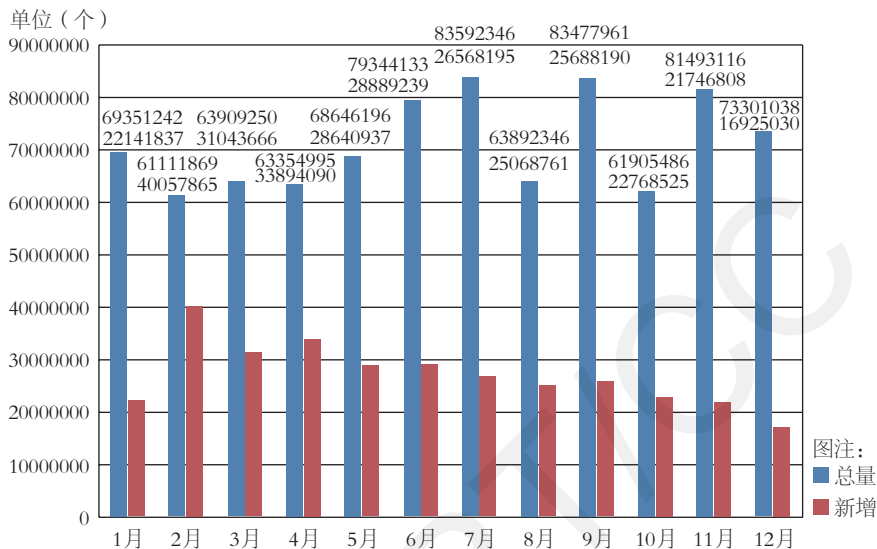


图3-33 2015年捕获恶意程序样本数量月度统计(来源:卡巴斯基)

2015年全年监测到感染恶意程序的主机862658314台,较2014年的745447561个增长15.7%。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1月为全年最高点(110742105个),10月达到全年最低值(54066608个),如图3-34所示。

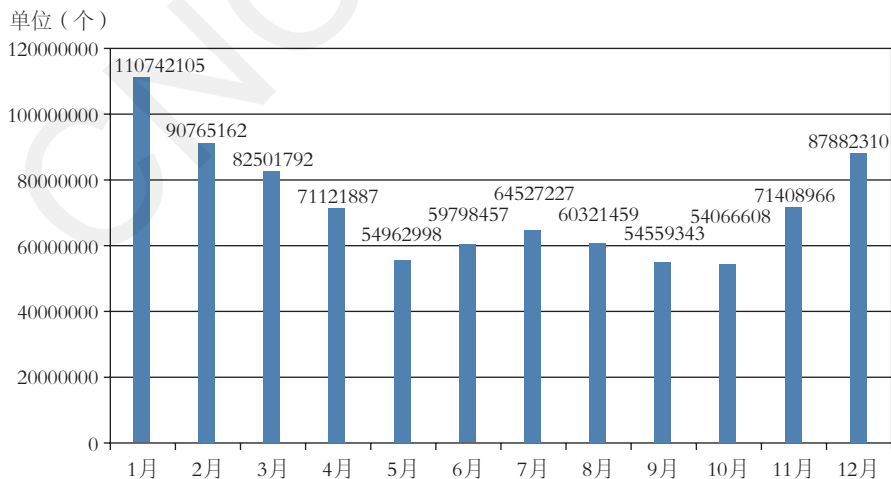


图3-34 2015年感染恶意程序主机数量月度统计(来源:卡巴斯基)



3.4.5 深信服公司报送的恶意程序捕获情况

根据深信服公司的监测结果，2015年全年捕获恶意程序总量为4727个，比2014年的4236个增长11.6%。2015年各月捕获数量如图3-35所示，其中6月达到全年最高值（623个），11月达到全年最低值（132个）。

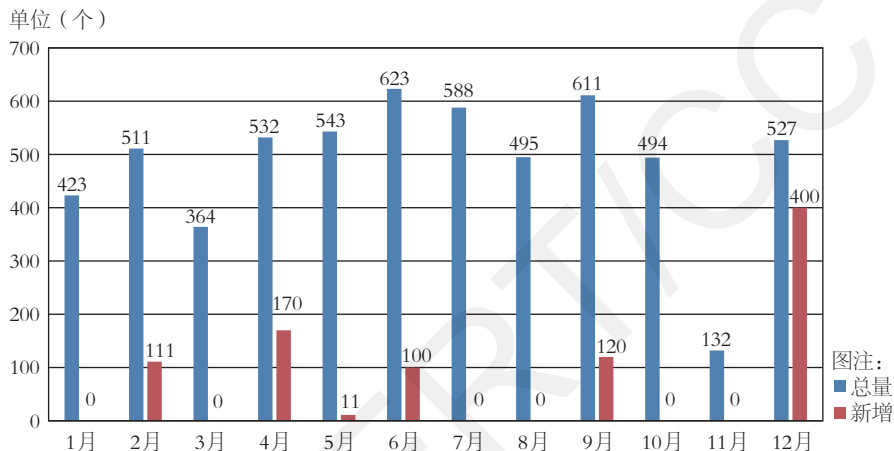


图3-35 2015年捕获恶意程序数量月度统计（来源：深信服公司）

2015年全年捕获恶意程序样本总量为78221个（按MD5值统计），比2014年的74424个增长5.1%。2015年各月捕获数量如图3-36所示，其中9月达到全年最高值（7924个），12月达到全年最低值（3732个）。

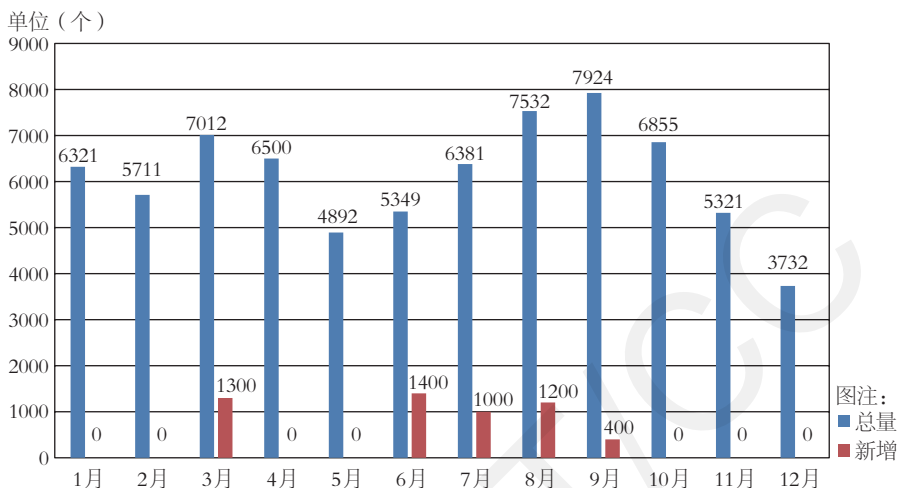


图3-36 2015年捕获恶意程序样本数量月度统计（来源：深信服公司）

2015年全年监测到感染恶意程序的主机84219台，较2014年的68435个增长23.1%。其中感染主机数量10月为全年最高点（10245个），11月达到全年最低值（4763个），如图3-37所示。

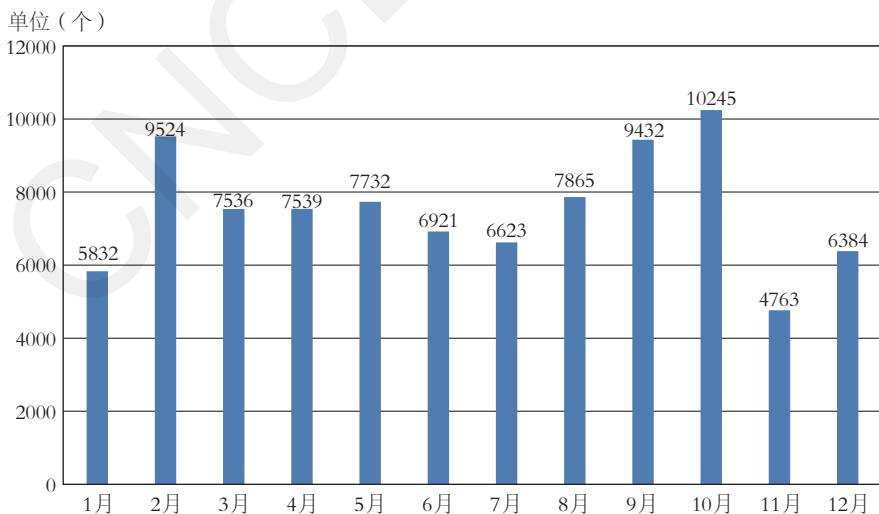


图3-37 2015年感染恶意程序主机数量月度统计（来源：深信服公司）



移动互联网恶意程序 传播和活动情况

2015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,2015年移动互联网恶意程序的数量继续保持增长趋势,较2014年的数量增长速度有所回升。

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。2015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1477450个。

2015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348859个,占23.61%,流氓行为类328092个(占22.21%)、远程控制类222941个(占15.09%)分列第二、三位。2015年,CNCERT/CC组织通信行业开展了12次移动互联网恶意程序专项治理行动,着重针对影响范围大、安全风险较高的恶意程序进行治理,恶意扣费类恶意程序的治理效果显著,样本数量减少近20万个,其比例由2014年的54.98%下降至2015年的23.61%。

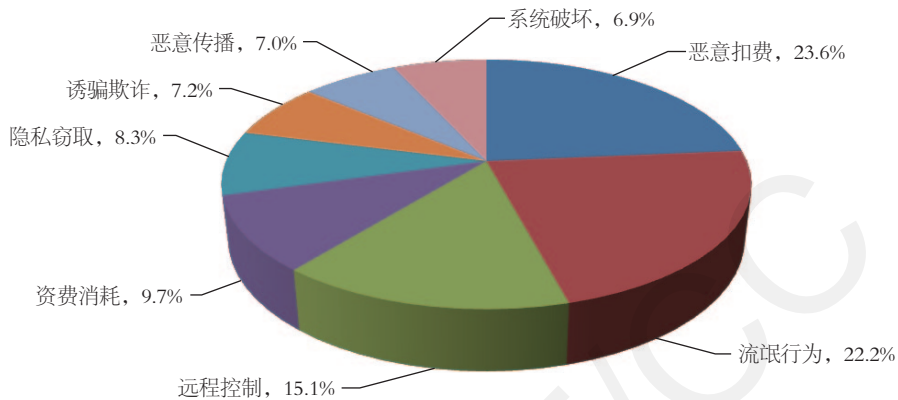


图4-1 2015年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

按操作系统分布统计，2015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1472381个，占99.6%以上，位居第一。其次是Symbian平台，共有2917个，占0.19%。此外，iOS平台和J2ME平台的恶意程序数量分别为8个和4个。继2014年出现的苹果iOS平台“Wirelurker”等恶意程序后，2015年出现更大规模感染的iOS恶意程序“XcodeGhost”，标志着iOS平台恶意程序的制作和传播链条更加成熟。2015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。

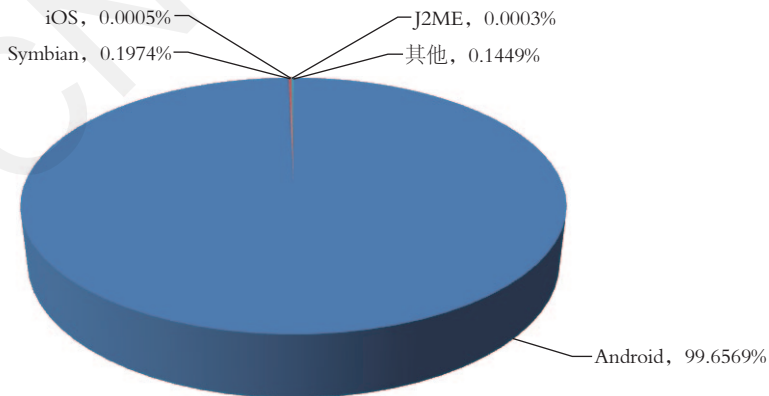


图4-2 2015年移动互联网恶意程序数量按操作系统分布（来源：CNCERT/CC）



如图4-3所示,按危害等级统计,2015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,高危的有30927个,占2.1%;中危的有253749个,占17.2%;低危的有1192774个,占80.7%。相对于2014年,高危移动互联网恶意程序的分布情况略有提升,中危移动互联网恶意程序所占比例下降7%,低危移动互联网恶意程序所占比例增加7%。

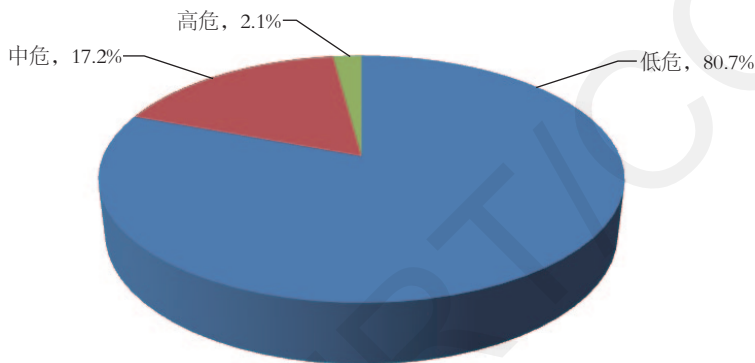


图4-3 2015年移动互联网恶意程序数量按危害等级统计(来源:CNCERT/CC)

4.2 移动互联网恶意程序传播活动监测

2015年,CNCERT/CC监测发现移动互联网恶意程序传播事件83839598次,较2014年同期81747407次增长2.6%,较2014年6倍的增长速度,继续呈现出大幅度下降的趋势。移动互联网恶意程序URL下载链接303810个,较2014年同期的296080个增长2.6%。进行移动互联网恶意程序传播的域名41249个,较2014年同期增长70.4%;进行移动互联网恶意程序传播的IP地址18017个,较2014年同期大幅度下降68.6%。

随着政府部门对应用商店的监督管理愈加完善,通过正规应用商店传播移动恶意程序的难度不断增加,传播移动恶意程序的阵地已经转向网盘、广告平台等目前审核措施还不完善的APP传播渠道。移动互联网恶意程序传播事件的月度统计如图4-4所示,结果显示2015年1-6月移动恶意程序传播活动呈逐月下降趋势,7月后传播事件数量总体呈上升趋势。

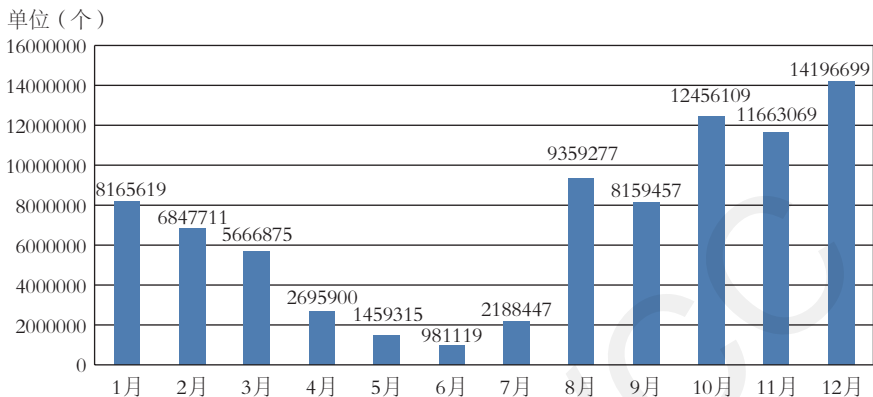


图4-4 2015年移动互联网恶意程序传播事件次数月度统计（来源：CNCERT/CC）

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2015年1-6月传播恶意程序的域名和IP数量呈逐渐减少趋势，7-12月传播恶意程序的域名和IP数量呈逐渐增加，12月的恶意域名数量达到全年最大值，单月出现的恶意域名数量达2.4万个。

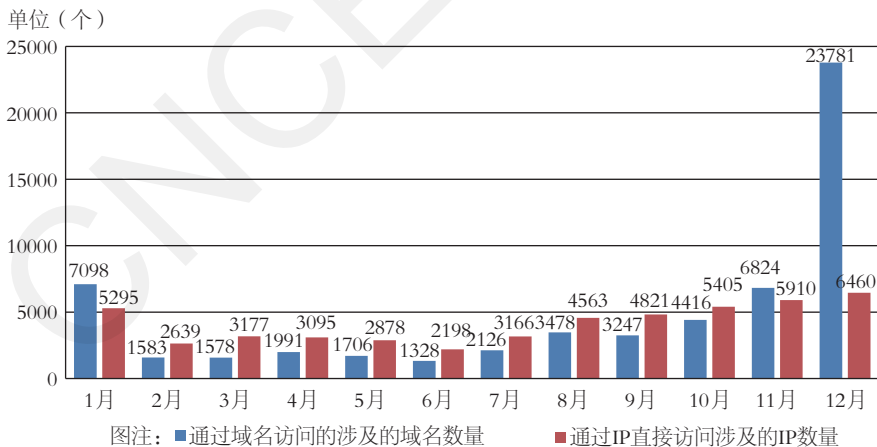


图4-5 2015年移动互联网恶意程序传播源域名和IP地址数量月度统计（来源：CNCERT/CC）



4.3 通报成员单位报送情况

4.3.1 安天公司报送的移动互联网恶意程序捕获情况

根据安天公司的监测结果，截至2015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）400045个，其中2015年新发现116864个。截至2015年年底，累计捕获移动互联网恶意程序样本5610537个（按照MD5值统计），其中2015年新捕获样本2499436个。按照《移动互联网恶意程序描述格式》的8类分类标准，2015年发现的移动互联网恶意程序分类统计数据为：恶意扣费142407个；信息窃取166186个；远程控制188874个；恶意传播47188个；资费消耗142407个；系统破坏21176个；诱骗欺诈55352个；流氓行为1017871个。

2015年各月捕获移动互联网恶意程序数量（按恶意程序名称统计）如图4-6所示，其中6月达到全年最高值（23459个），2月达到全年最低值（10378个）。

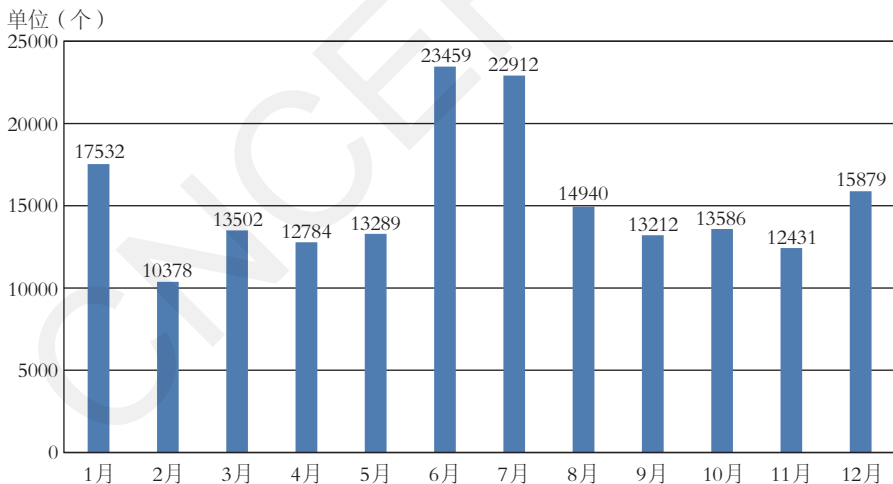


图4-6 2015年捕获移动互联网恶意程序数量月度统计（来源：安天公司）

2015年各月捕获移动互联网恶意程序样本数量（按照MD5值统计）如图4-7所示，其中11月达到全年最高值（281645个），9月达到全年最低值（134778个）。

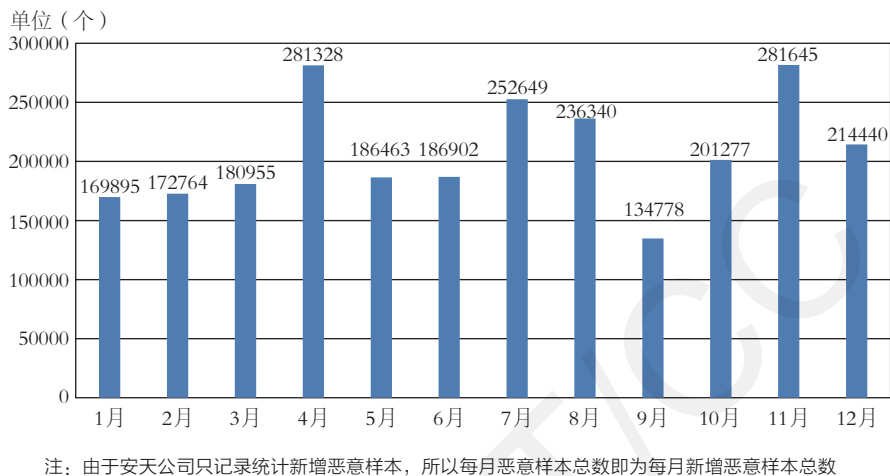


图4-7 2015年捕获移动互联网恶意程序样本数量月度统计（来源：安天公司）

2011-2015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4-8所示。

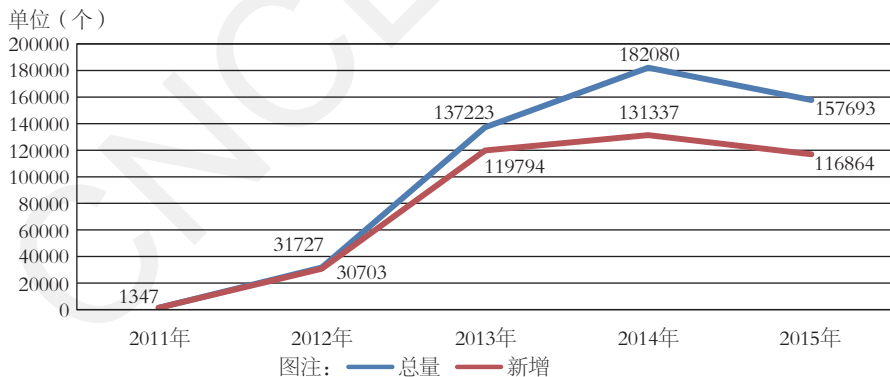


图4-8 2011-2015年移动互联网恶意程序数量走势（来源：安天公司）

2011-2015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4-9所示。

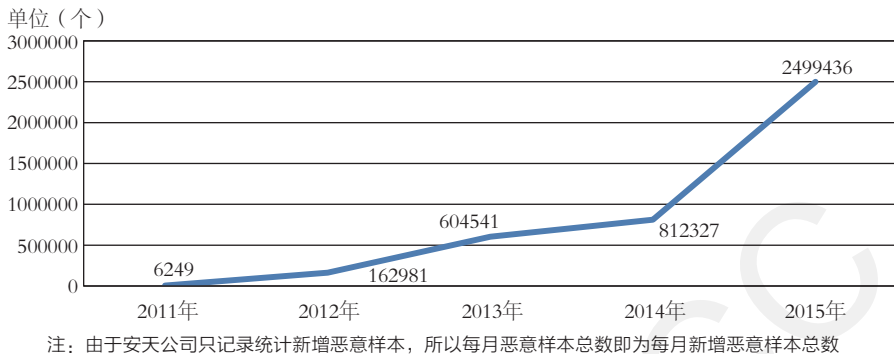


图4-9 2011-2015年捕获移动互联网恶意程序样本数量走势（来源：安天公司）

截至2015年，累计发现移动互联网恶意程序下载链接921072条。其中，2015年共发现移动互联网恶意程序下载链接204870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（个）
down.zuo99.com	219831
kunte.net.cn	218497
cdn.150wz.com	101260
7540.taomike.com	20525
m.shouji.360tpcdn.com	19303
gdown.baidu.com	18109
cdn.1000su.com	16539
download.shininghunter.com	15535
do.djyqsnzx.org	15432
shouji.360tpcdn.com	7003

注：由于缺少各应用商店对应域名信息，所以无法估算共发现多少个手机应用商店，只能统计共涉及22427个域名

4.3.2 奇虎360公司报送的移动互联网恶意程序捕获情况

如图4-10所示，2015年全年，360互联网安全中心累计截获Android平台新增恶意程序样本1874.0万个，分别是2013年、2014年的27.9倍、5.7倍，平均每天截获新增恶

意程序样本也高达51342个。

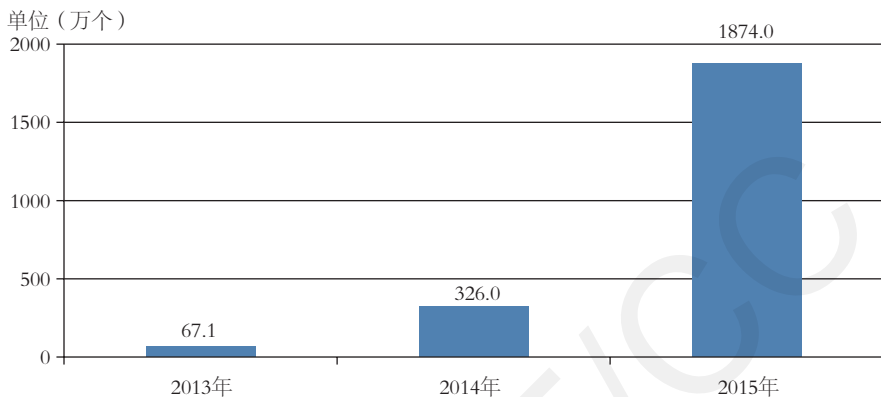


图4-10 2013-2015年Android平台新增恶意程序样本数
(来源: 360互联网安全中心)

2015年各月Android平台新增恶意程序样本量的分布如图4-11所示。新增恶意程序整体呈现中间高、两头低的态势,即上半年各月新增恶意程序量整体呈现上升,在7月达到最高峰;下半年从8月开始逐月下降,12月达到最低。这与2014年12月数量(86.6万)达到最高,形成鲜明对比。

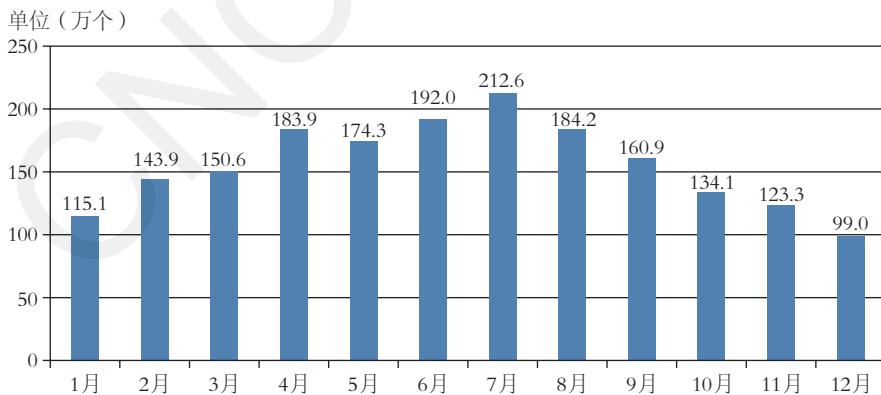


图4-11 2015年Android平台各月新增恶意程序样本数
(来源: 360互联网安全中心)



如图4-12所示, 2015全年, 360互联网安全中心累计监测到Android用户感染恶意程序3.7亿人次, 分别是2013年、2014年的3.8倍和1.1倍, 平均每天恶意程序感染量达到了100.6万人次。

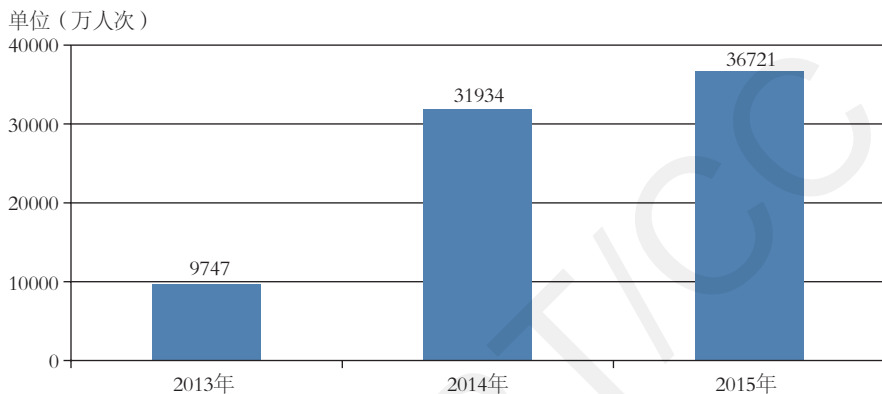


图4-12 2013-2015年Android平台恶意程序感染量 (来源: 360互联网安全中心)

2015年Android平台新增恶意程序感染量的按月分布如图4-13所示, 分析可知, 下半年恶意程序感染量和上半年相比, 基本持平, 但上半年波动较大, 全年最高值和最低值分别出现在1月(5384万)、6月(2015万); 下半年各月感染量略显平均, 11月和12月高于其他各月。

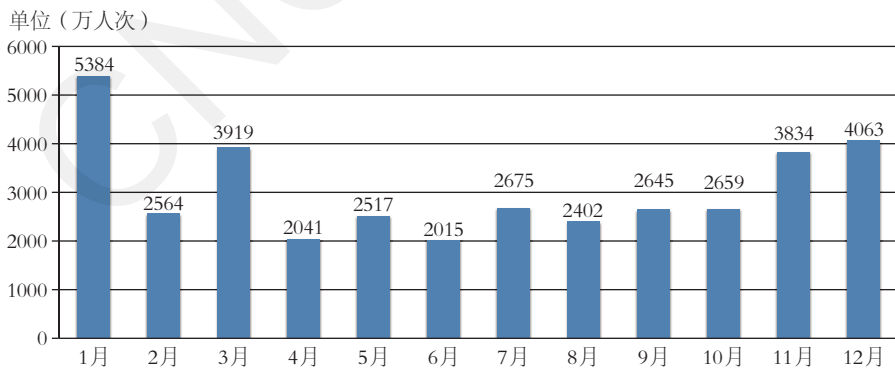


图4-13 2015年Android平台各月恶意程序感染量 (来源: 360互联网安全中心)

2015年, Android平台新增恶意程序的样本量与感染量都有一定幅度的提升, 主要

是因为Android系统、APP的普及与发展带动了Android手机等智能终端用户量的持续攀升，从而导致黑客的攻击目标也逐渐转向移动端。随着技术的发展，Android平台的恶意程序制作成本逐渐降低，并且可以批量生成恶意程序，致使针对移动端的攻击行为逐渐规模化。未来，移动端的安全隐患将更值得被关注。

（1）恶意程序危害分析

根据中国反网络病毒联盟的分类标准，360互联网安全中心在2015全年监测的Android平台恶意程序的分类统计如图4-14所示。从图4-14中可知，2015年Android平台新增恶意程序主要是资费消耗，占比高达73.6%；其次为恶意扣费（21.5%）和隐私窃取（4.1%）。可以看到，已经有90%以上的移动恶意程序是直接冲着用户“钱包”来的，关系到用户的直接经济损失。

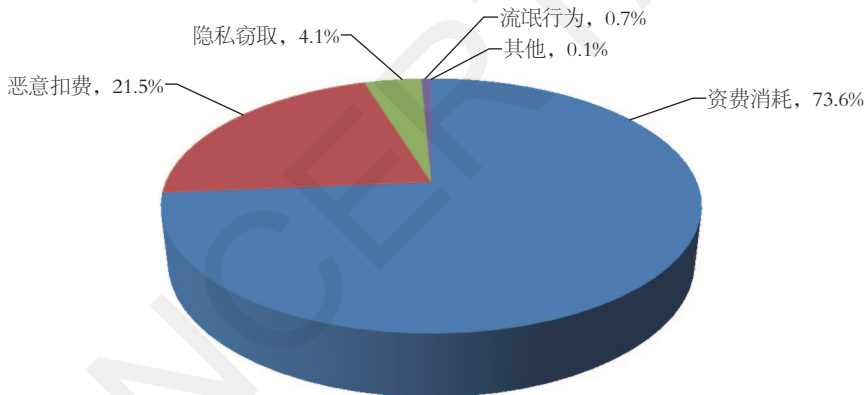


图4-14 2015年Android平台新增恶意程序类型分布（来源：360互联网安全中心）

图4-15给出了2015年4个季度Android平台恶意程序感染类型的比例分布变化情况，其中，恶意扣费、流氓行为这两类恶意程序都在第三季度达到最高峰；而资费消耗类恶意程序在第三季度反而有较大幅度的回落，又在第四季度实现反弹；另外，隐私窃取类恶意程序呈全年缓慢下降趋势。

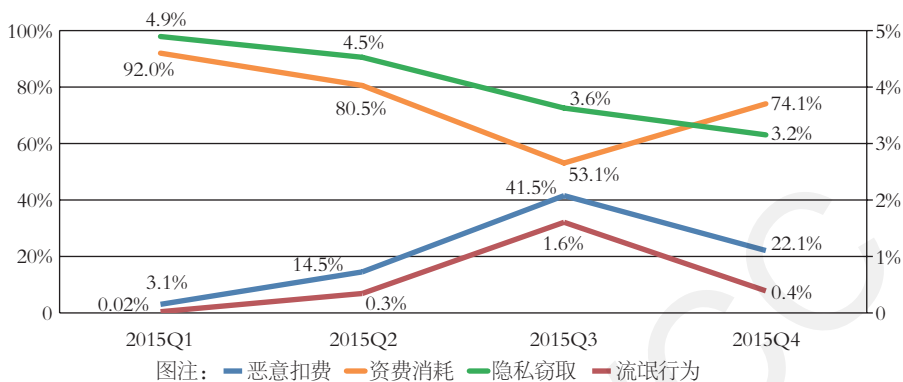


图4-15 2015年Android平台恶意程序感染类型变化趋势
(来源：360互联网安全中心)

(2) 手机木马感染量各季度TOP10

表4-2给出2015年4个季度每个季度感染量最高的10大恶意程序。其中，仿冒版表示该手机木马对原程序进行了篡改，或对原程序的名称、图标进行模仿。

表4-2 2015年各季度手机木马感染量TOP10（来源：360互联网安全中心）

一季度				二季度			
TOP	恶意程序名称	主要危害	感染量 (个)	TOP	恶意程序名称	主要危害	感染量 (个)
1	Android System Service	资费消耗	1097809	1	com.android.system	资费消耗	315061
2	驾考宝典（仿冒版）	资费消耗	1014436	2	我的世界（仿冒版）	资费消耗	294268
3	WifiPassword	隐私窃取	707396	3	午夜直播	恶意扣费	273780
4	com.android.protection	资费消耗	464308	4	成人快播	资费消耗	271247
5	com.android.system	资费消耗	294588	5	com.android.contact	资费消耗	171605
6	Visual Voicemail	恶意扣费	293067	6	超爽诱惑	恶意扣费	126689
7	午夜快播	恶意扣费	261985	7	欲女魅影	恶意扣费	108558
8	Sports Tv	隐私窃取	255218	8	成人小说	恶意扣费	105529
9	ROOT大师（仿冒版）	资费消耗	209987	9	极限快播	资费消耗	99714
10	com.android.avplayer	隐私窃取	182665	10	激情乐播	隐私窃取	98003
三季度				四季度			
TOP	恶意程序名称	主要危害	感染量 (个)	TOP	恶意程序名称	主要危害	感染量 (个)
1	TimeService	资费消耗	1096706	1	AndroidPatch	资费消耗	2590261
2	MonkeyTest	资费消耗	824890	2	MonkeyTest	资费消耗	2356312
3	Adobe air	资费消耗	334376	3	com.android.system	资费消耗	1627306
4	Mont Start	资费消耗	309714	4	EngriIs	资费消耗	856416
5	Sex Position With Sound	资费消耗	233074	5	MobileOcr	资费消耗	849986
6	Native	资费消耗	188359	6	Chajian	资费消耗	666154
7	Dev Engine	资费消耗	178849	7	Measure	资费消耗	468561
8	Mp3 Music Downloader	资费消耗	175188	8	com.android.mic	资费消耗	367113
9	Daemon_app	资费消耗	168393	9	Processor	资费消耗	360714
10	Engine Init	资费消耗	168205	10	Engriks	资费消耗	300172

从全年来看，10大恶意程序见表4-3。



表4-3 恶意应用与流行应用名称对比（来源：360互联网安全中心）

恶意应用名称	危害类型	感染量（个）
MonkeyTest	资费消耗	3181202
AndroidPatch	资费消耗	2590261
com.android.system	资费消耗	2236955
Android System Service	资费消耗	1097809
TimeService	资费消耗	1096706
驾考宝典（仿冒版）	资费消耗	1014436
engrils	资费消耗	856416
mobileOcr	资费消耗	849986
WifiPassword	隐私窃取	707396
chajian	资费消耗	666154

（3）恶意程序感染量地域分布

从地域分布来看，2015年感染手机恶意程序最多的地区为广东省，感染数量占全国感染数量的14.83%；其次为北京（8.57%）、河南（6.31%）、江苏（5.86%）、山东（5.32%）。此外，浙江、四川、河北、广西、湖南的恶意感染数量也排在前列。2015年手机用户恶意程序感染量地域分布如图4-16所示。

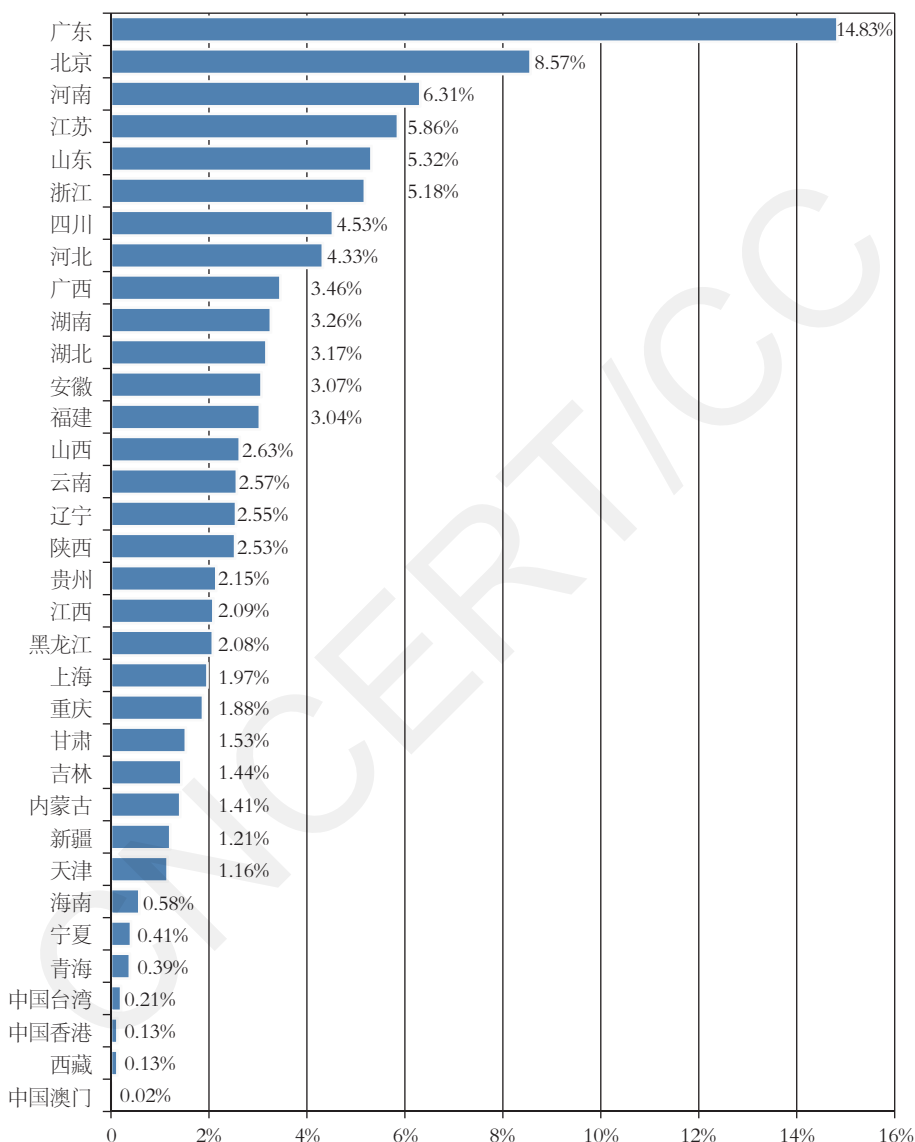


图4-16 2015年手机用户恶意程序感染量地域分布（来源：360互联网安全中心）

图4-17给出了2015年Android平台恶意程序感染量最多的10大城市。其中，北京



用户感染Android平台恶意程序最多，高达3169万人次，居于全国首位；其次是广州（1592万人次）、深圳（991万人次）、成都（819万人次）、郑州（778万人次）；TOP10中还有杭州（768万人次）、上海（729万人次）、重庆（695万人次）、南京（647万人次）和佛山（608万人次）。

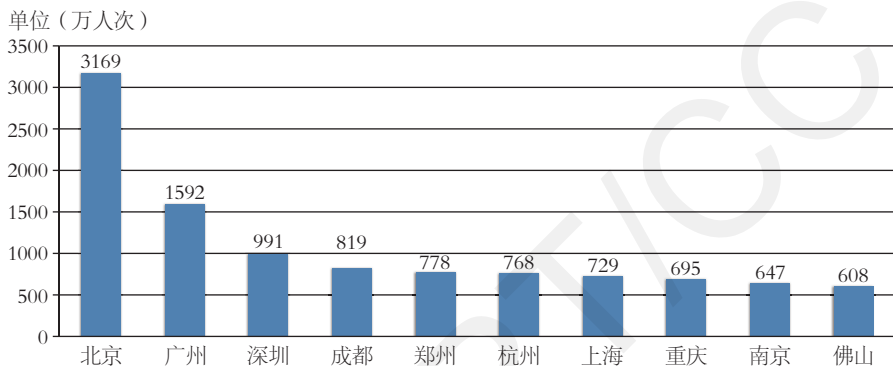


图4-17 2015年Android平台恶意程序感染量TOP10城市
(来源：360互联网安全中心)

4.3.3 恒安嘉新公司报送的移动互联网恶意程序情况

根据恒安嘉新（北京）科技有限公司监测结果，截至2015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）8907个，其中2015年新发现5103个。截至2015年年底，累计捕获移动互联网恶意程序样本12822683个（MD5值不同），其中2015年新捕获样本10026405个。按照《移动互联网恶意程序描述格式》的8类分类标准，2015年发现的移动互联网恶意程序分类统计数据为：恶意扣费1696772个；信息窃取4627560个；远程控制115689个；恶意传播771260个；资费消耗2622284个；系统破坏77151个；诱骗欺诈77126个；流氓行为38563个。

2015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3月达到全年最低值（121个），8月达到全年最高值（1202个）。

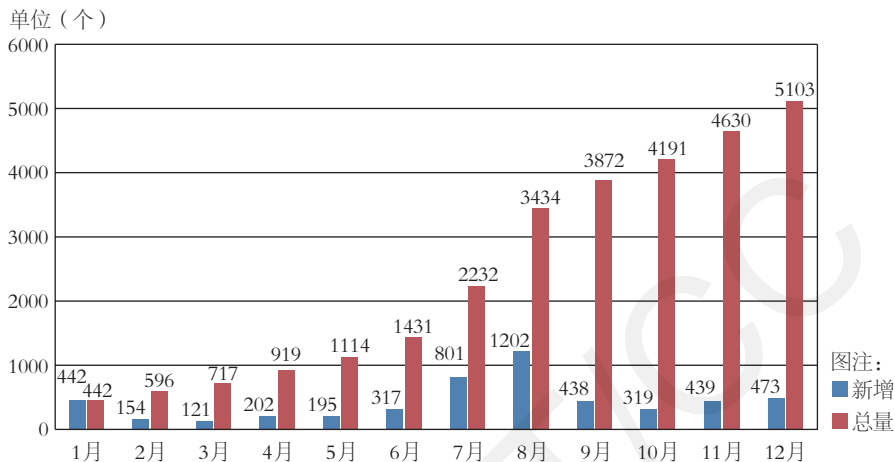


图4-18 2015年移动互联网恶意程序捕获月度统计（来源：恒安嘉新公司）

2015年各月捕获移动互联网恶意程序样本数量（MD5值不同）如图4-19所示，其中3月达到全年最低值（205750个），8月达到全年最高值（2405909个）。

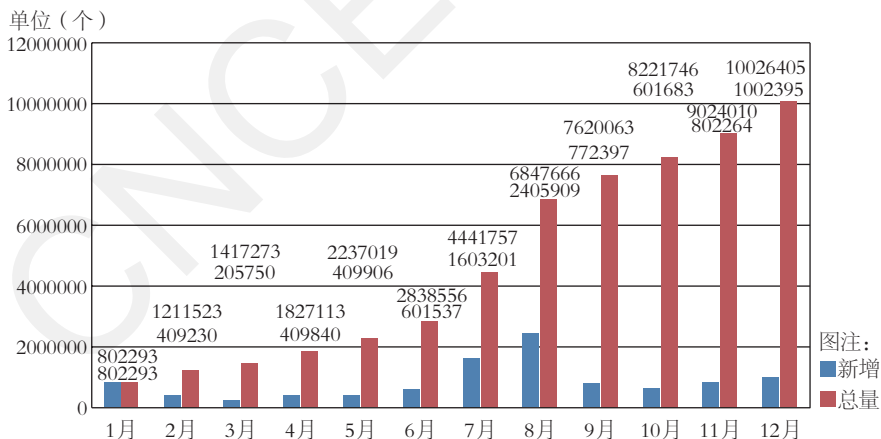


图4-19 2015年移动互联网恶意程序样本捕获月度统计（来源：恒安嘉新公司）

2008-2015年移动互联网恶意程序数量（按恶意程序名称统计）走势如图4-20所示。

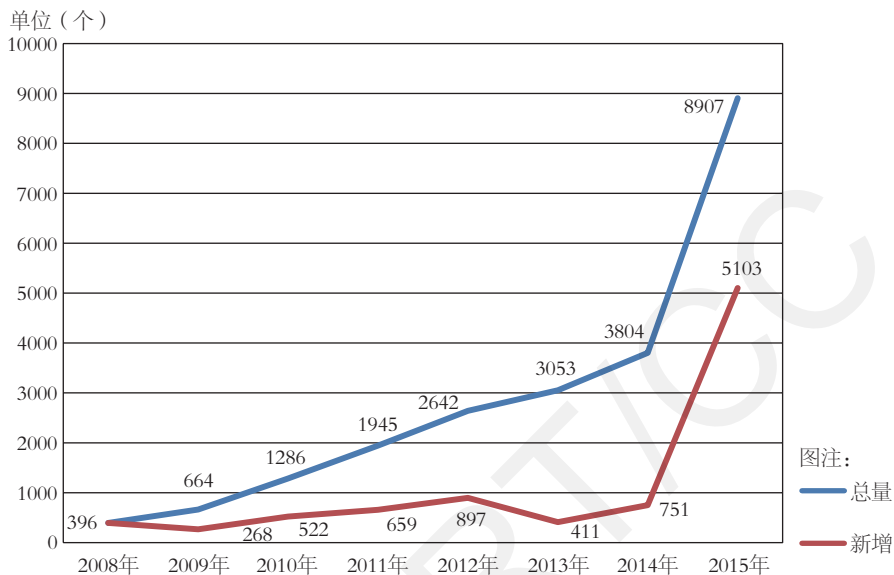


图4-20 2008-2015年移动互联网恶意程序数量走势（来源：恒安嘉新公司）

2008-2015年发现移动互联网恶意程序样本数量（MD5值不同）走势如图4-21所示。

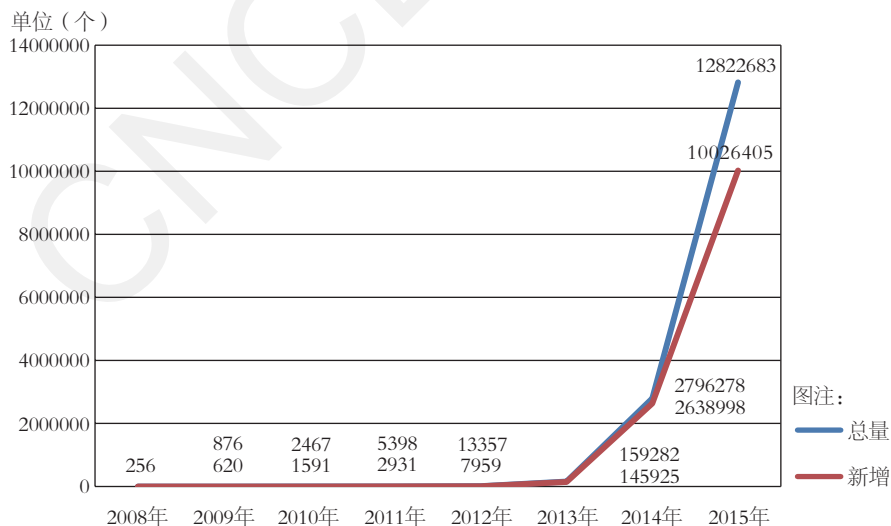


图4-21 2008-2015年移动互联网恶意程序样本数量走势（来源：恒安嘉新公司）

截至2015年，累计发现移动互联网恶意程序下载链接77234条。其中，2015年共发现移动互联网恶意程序下载链接19558条，涉及7149个域名，按恶意程序下载链接数排行前10的域名见表4-4。

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

下载地址域名	恶意程序下载链接数（条）
down.sdzgj.com	1714
down.gongyediping.com.cn:81	836
nm2189cloud.oos-nm2.ctyunapi.cn	594
201412.oss-cn-hangzhou.aliyuncs.com	492
qc.woaixz.com	482
www.7cbox.cn	258
dl.ggmmx.com	257
jscgt.cn:81	221
slink.colefile.net	181
gdown.baidu.com	179

4.3.4 网秦公司报送的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2015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）14199个，其中2015年新发现1194个。截至2015年年底，累计捕获移动互联网恶意程序样本1320601个（按照MD5值统计），其中2015年新捕获样本139012个。按照《移动互联网恶意程序描述格式》的8类分类标准，2015年发现的移动互联网恶意程序分类统计数据为：恶意扣费341个；信息窃取304个；远程控制142个；恶意传播8个；资费消耗351个；系统破坏6个；诱骗欺诈7个；流氓行为35个。

2015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4-22所示，其中3月达到全年最高值（240个），2月达到全年最低值（33个）。

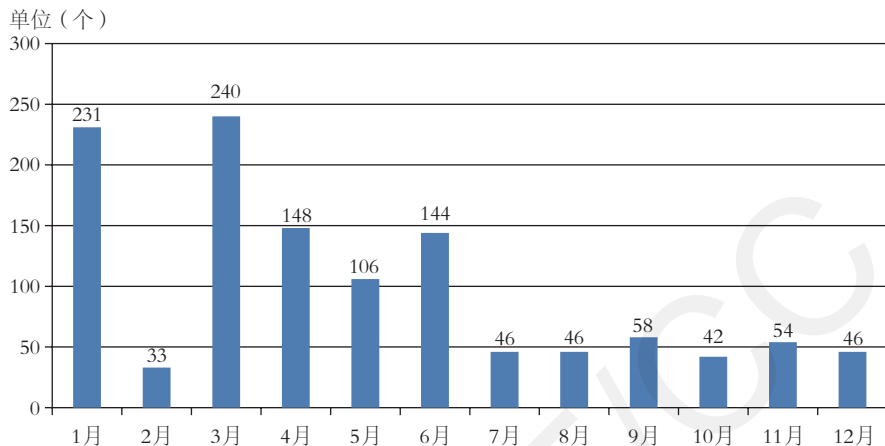


图4-22 2015年捕获移动互联网恶意程序数量月度统计(来源:网秦公司)

2015年各月捕获移动互联网恶意程序样本数量(按照MD5值统计)如图4-23所示,其中5月达到全年最高值(36470个),9月达到全年最低值(4432个)。

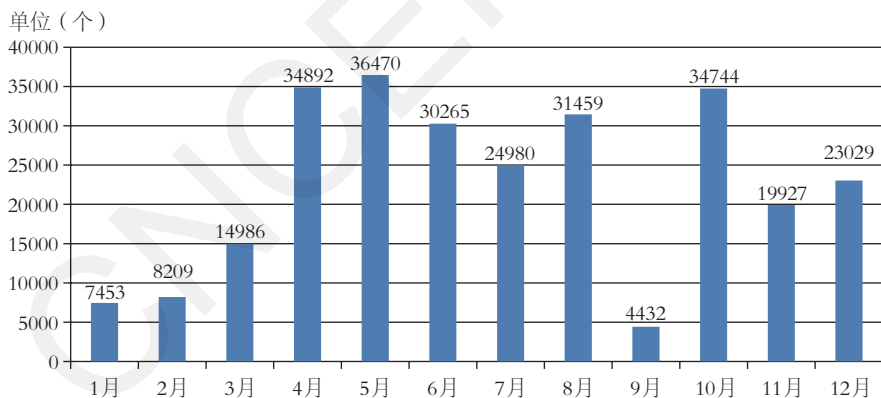


图4-23 2015年捕获移动互联网恶意程序样本数量月度统计(来源:网秦公司)

4.3.5 腾讯公司移动互联网恶意程序捕获情况

如图4-24所示,根据腾讯手机管家监测结果,2015年新发现恶意程序1670.4万个。按照《移动互联网恶意程序描述格式》的8类分类标准,2015年发现的各类移动互

联网恶意程序分类统计数据比例为：恶意扣费病毒占1.72%；信息窃取占5.33%；远程控制占0.35%；恶意传播占0.22%；资费消耗占74.22%；系统破坏占0.28%；诱骗欺诈占9.75%；流氓行为占8.13%。

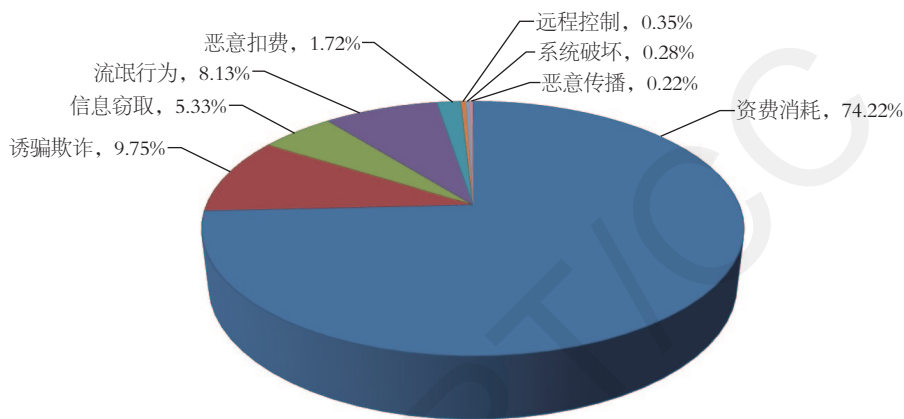


图4-24 2015年手机病毒类型比例（来源：腾讯公司）

2015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4-25所示，其中7月达到全年最高值（3256392个），2月达到全年最低值（359272个）。

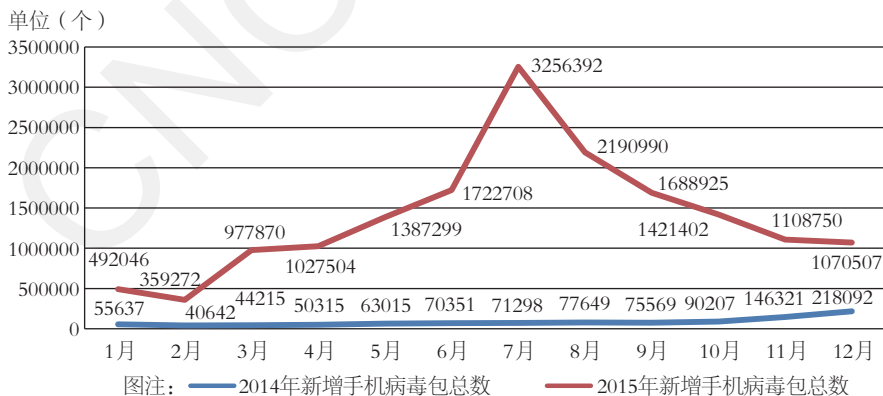


图4-25 2015年捕获移动互联网恶意程序数量月度统计（来源：腾讯公司）



2011–2015年移动互联网恶意程序数量（按恶意程序名称统计）走势如图4-26所示。

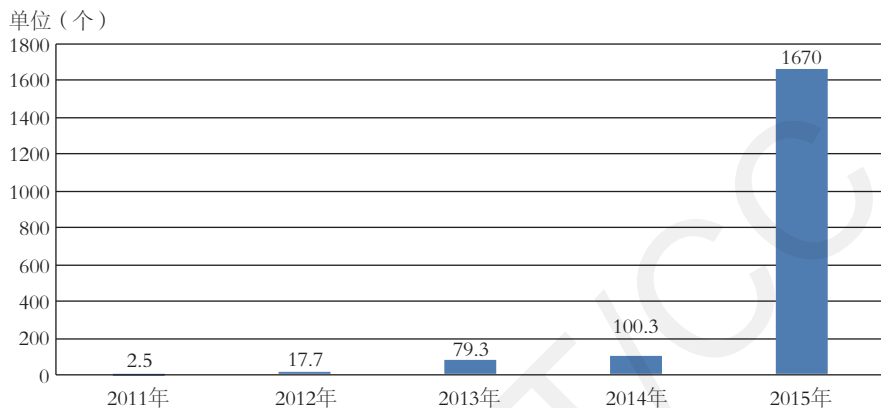


图4-26 2011–2015年移动互联网恶意程序数量走势（来源：腾讯公司）

2015年Android病毒感染人次达到3.08亿，相比2014年，同比增长56.5%。

2011–2015年移动互联网恶意程序感染用户数走势如图4-27所示。从整体增长趋势上看，手机病毒感染人次呈现每月爬坡式增长态势，12月达到增长高峰。

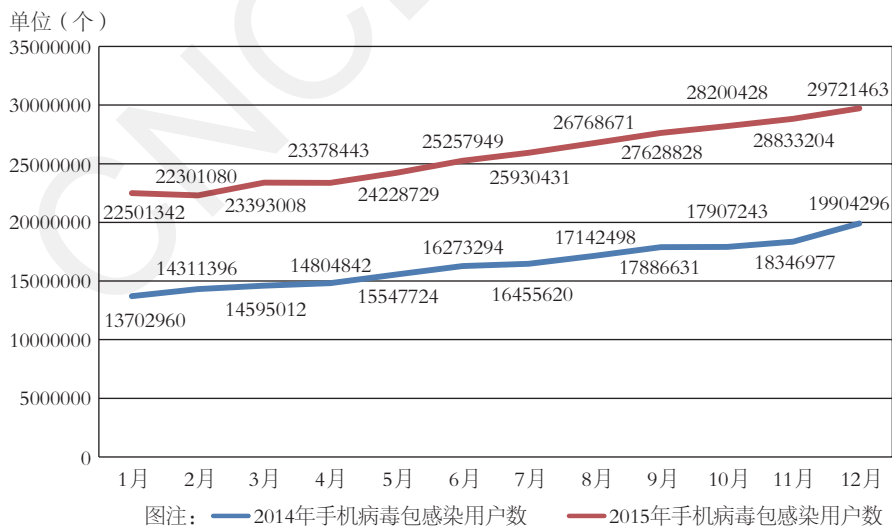
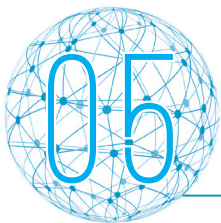


图4-27 2015年手机病毒感染用户数量月度统计（来源：腾讯公司）



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；隐式篡改一般是将被攻击网站的网页植入链接色情、诈骗等非法信息的暗链中，以帮助黑客牟取非法经济利益。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，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

2015年我国境内被篡改的网站数量为24550个，较2014年的36969个下降33.6%。我国境内被篡改网站数量的月度统计情况如图5-1所示。2015年下半年，CNCERT/CC加强了对我国境内网站被植入暗链情况的专项治理，组织全国分中心开展网站暗链、网站篡改以及暗链广告域名治理行动，使得篡改攻击的情况特别是在篡改攻击中占绝大多数（超过85%）的页面广告暗链植入攻击大幅下降。

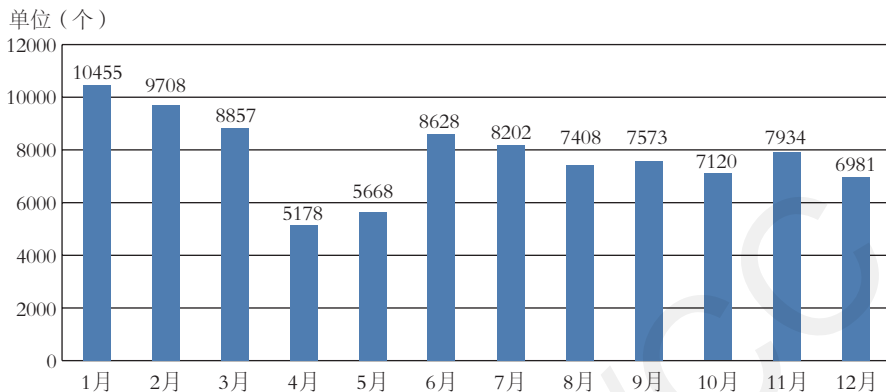


图5-1 2015年我国境内被篡改网站数量月度统计 (来源: CNCERT/CC)

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攻击的超过85%。从域名类型来看,2015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72.3%,其次是网络组织类(.net)网站和政府类(.gov)网站,分别占6.6%和3.7%,非营利组织类(.org)网站占2.0%,如图5-2所示。对比2014年,我国政府类网站被篡改情况有小幅下降,从2014年的4.8%下降至2015年的3.7%。

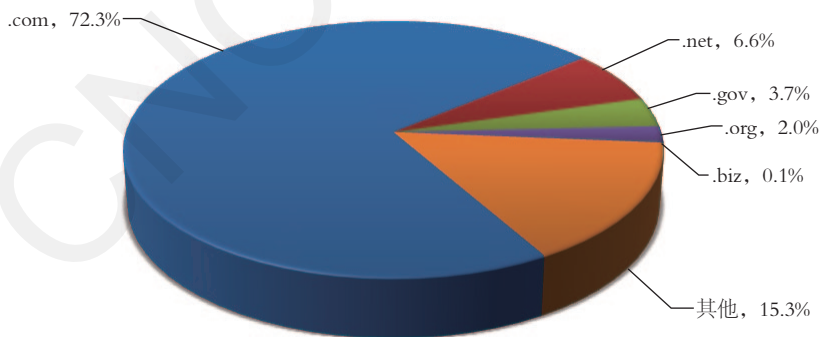


图5-2 2015年我国境内被篡改网站按域名类型分布 (来源: CNCERT/CC)

如图5-3所示,2015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、广东省、河南省、江苏省、福建省、上海市、浙江省、四川省、安

安徽省、天津市。前10位地区与2015年总体一致，只是之间排名略有变化。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。

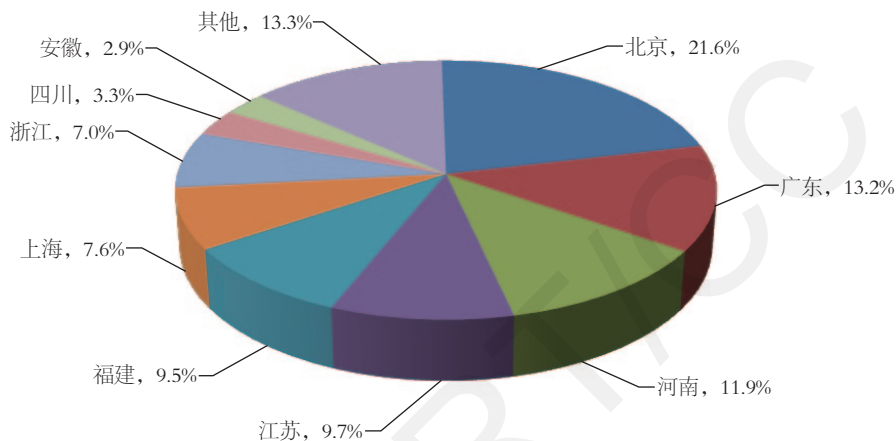


图5-3 2015年我国境内被篡改网站按地域分布（来源：CNCERT/CC）

5.1.2 我国境内政府网站被篡改情况

我国被篡改政府网站数量下降，受到植入暗链攻击威胁大。2015年我国境内政府网站被篡改数量为898个，较2014年的1763个减少49.1%。在2015年的安全威胁治理专项行动中，CNCERT/CC共处置参与网站攻击的博彩、私服等网站链接3382个，通知1706个被篡改的网站用户单位对网站进行修复，这些治理成果的印证就是政府篡改网站数量的下降。2015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，可以看到，下半年政府网站篡改数量及占被篡改网站总数比例呈现下降态势。

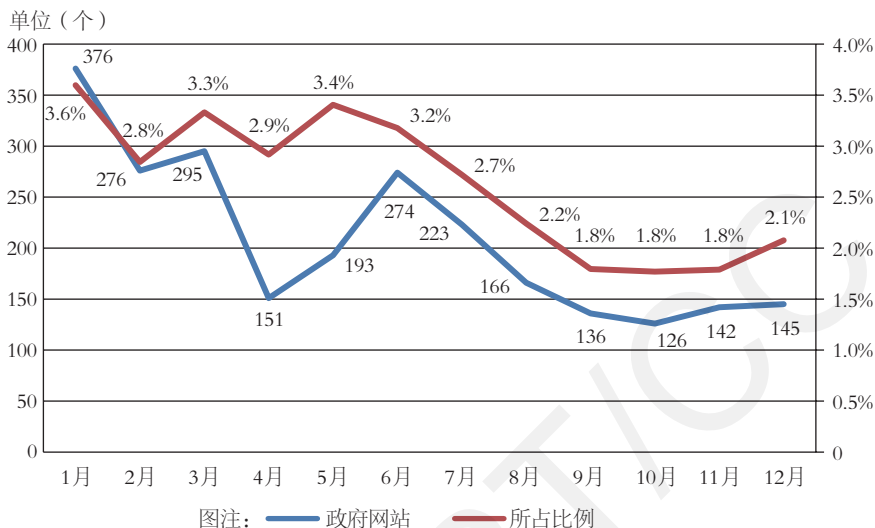


图5-4 2015年我国境内被篡改的政府网站数量和所占比例月度统计
(来源: CNCERT/CC)

表5-1所示为一些被篡改的部分省市级政府部门网站,一些网站管理单位在安全运维和漏洞修复方面投入力量不足,导致篡改页面长时间得不到修复或修复不完全被多次篡改。

表5-1 2015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
江西省委组织部12380举报网站	http://12380jiangxi.gov.cn/index.htm	2015/1/31
河北省物价局	http://www.hebwj.gov.cn//winSec.htm	2015/2/17
湖北省旅游局官方网站	http://hubeitour.gov.cn/naizui.html	2015/2/2
黑龙江省哈尔滨市住房公积金管理中心	http://cs.hrbgjj.gov.cn/ksh.htm	2015/3/4
内蒙古自治区海拉尔市商务局	http://swj.hailar.gov.cn/ina.htm	2015/4/24
邯郸市国土资源局	http://hdgt.hd.gov.cn/bb.html	2015/5/17
第八届跨国零售集团采购会	http://irgsf.gov.cn	2015/7/4
中共天津市滨海新区委员会统一战线工作部	http://bhtz.gov.cn/bb.html	2015/8/9
安徽省科技成果网	http://ahcgw.ahinfo.gov.cn	2015/9/5
山东省淄博市交通局	http://www.zbjt.gov.cn/id.htm	2015/12/6

5.2 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。

2015年CNCERT/CC共监测到境内75028个网站被植入后门，其中政府网站有3514个。我国境内被植入后门网站数量月度统计情况如图5-5所示。

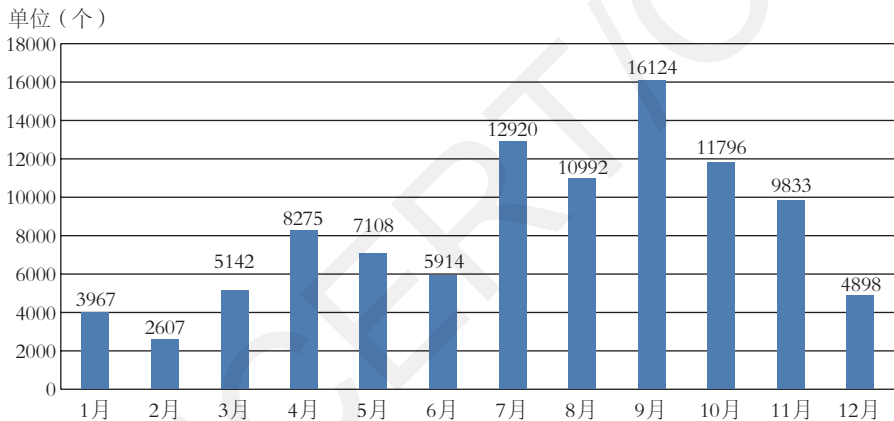


图5-5 2015年我国境内被植入后门网站数量月度统计（来源：CNCERT/CC）

从域名类型来看，2015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57.2%，其次是网络组织类（.net）和政府类（.gov）网站，分别占5.4%和4.7%。2015年我国境内被植入后门的网站数量按域名类型分布如图5-6所示。

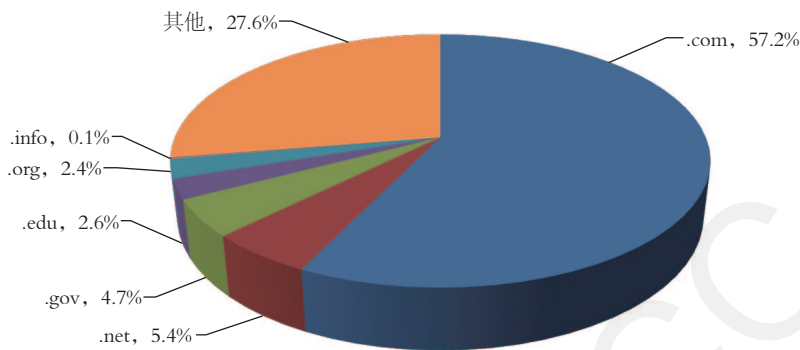


图5-6 2015年我国境内被植入后门网站数量按域名类型分布（来源：CNCERT/CC）

如图5-7所示，2015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：广东省、北京市、江苏省、浙江省、河南省、上海市、山东省、四川省、福建省、江西省。

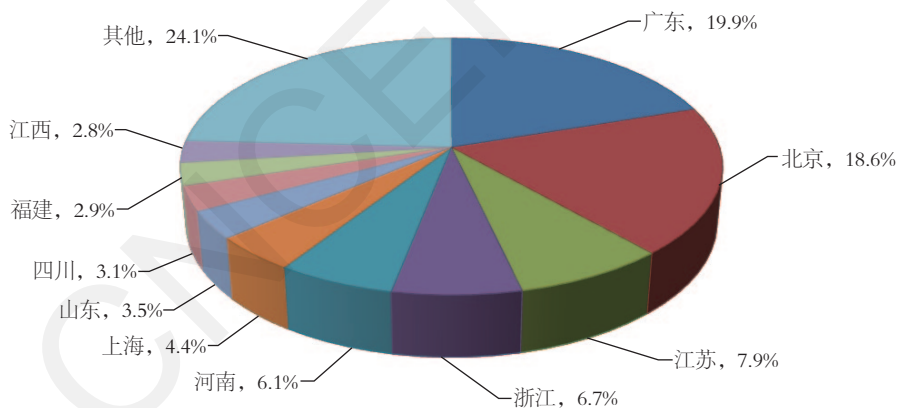


图5-7 2015年我国境内被植入后门网站数量按地区分布（来源：CNCERT/CC）

向我国境内网站实施植入后门攻击的IP地址中，有31348个位于境外，主要位于美国（13.9%）、中国香港（6.5%）和韩国（6.0%）等国家和地区，如图5-8所示。

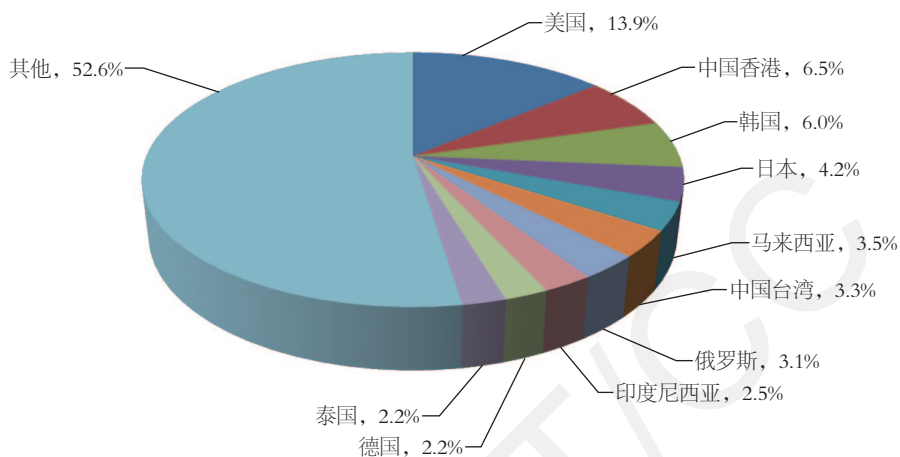


图5-8 2015年向我国境内网站植入后门的境外IP地址按国家和地区分布
(来源: CNCERT/CC)

其中，位于美国的4361个IP地址共向我国境内11245个网站植入后门程序，侵入网站数量居首位，其次是位于中国香港和菲律宾的IP地址，分别向我国境内10100个和5566个网站植入后门程序，如图5-9所示。

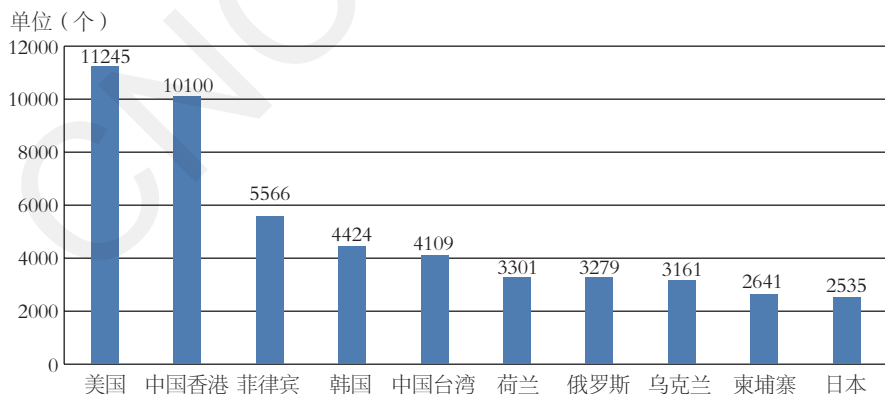


图5-9 2015年境外通过植入后门控制我国境内网站数量TOP10
(来源: CNCERT/CC)



5.3 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。2015年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面184574个，涉及境内外20488个IP地址，平均每个IP地址承载9个钓鱼页面。在这20488个IP地址中，有83.2%位于境外，其中中国香港（27.1%）、美国（9.4%）和韩国（2.2%）居前3位，分别承载60317个、18186个和16031个针对我国境内网站的钓鱼页面。仿冒我国境内网站的IP地址分别如图5-10和图5-11所示。

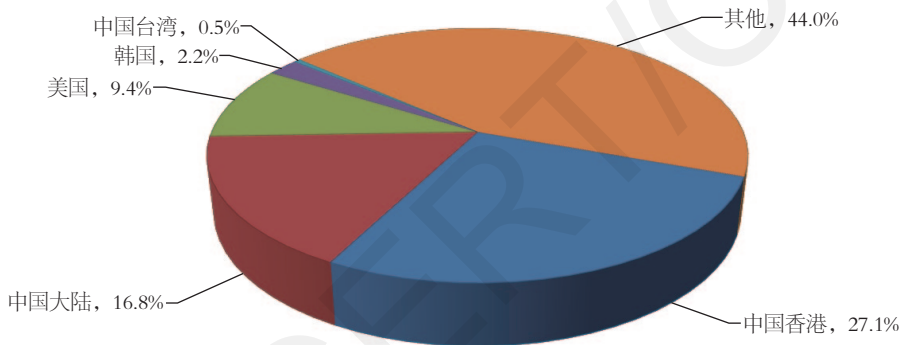


图5-10 2015年仿冒我国境内网站的IP地址按国家和地区分布
(来源: CNCERT/CC)

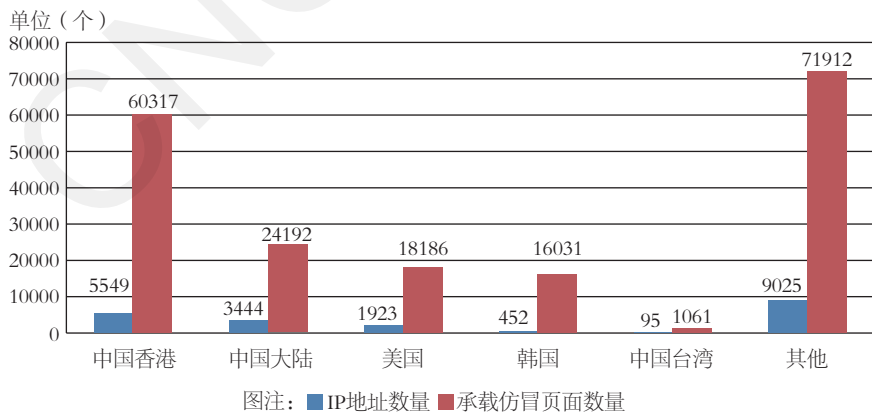


图5-11 2015年仿冒我国境内网站的IP地址及其承载的仿冒页面数量
按国家或地区分布TOP5 (来源: CNCERT/CC)

从钓鱼站点使用域名的顶级域分布来看，以.com最多，占67.4%，其次是.cc和.pw，分别占12.3%和5.5%。2015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5-12所示。

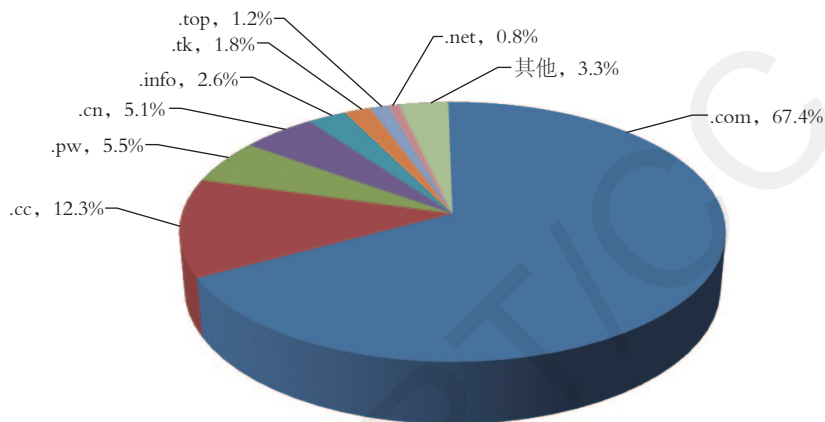
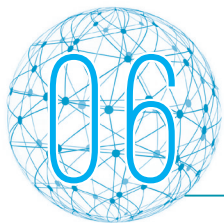


图5-12 2015年抽样监测发现的钓鱼站点所用域名按顶级域分布
(来源: CNCERT/CC)



信息安全漏洞公告与处置

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

国家信息安全漏洞共享平台（CNVD）自成立以来，共收录通用软硬件漏洞9.7万个（含补录漏洞），并接收各方报告的涉及具体行业、具体单位信息系统的漏洞风险信息接近7万条。其中，2015年新增通用软硬件漏洞8080个，包括高危漏洞2909个（占36.0%）、中危漏洞4553个（占56.4%）、低危漏洞618个（占7.6%）。各级别比例分布与月度数量统计如图6-1、图6-2所示。在所收录的上述漏洞中，可用于实施远程网络攻击的漏洞有7185个，可用于实施本地攻击的漏洞有895个。

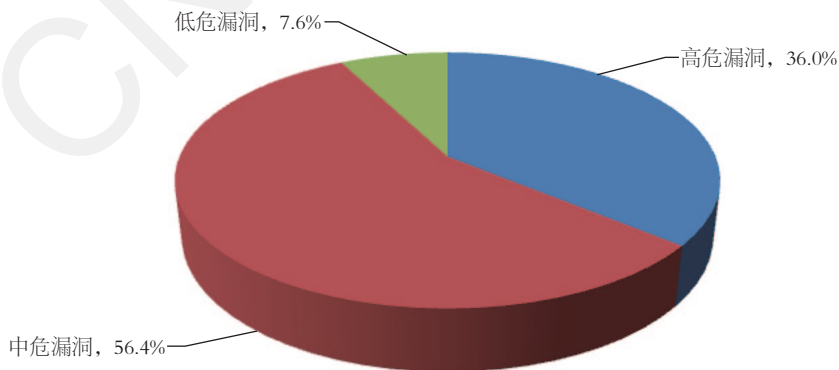


图6-1 2015年CNVD收录漏洞按威胁级别分布（来源：CNVD）

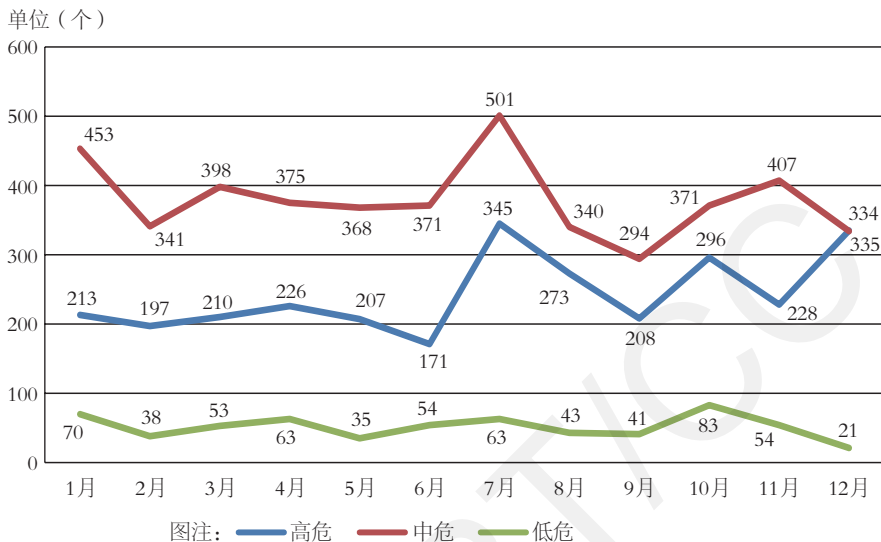


图6-2 2015年CNVD收录漏洞数量月度统计(来源: CNVD)

2015年CNVD共收集、整理了2909个高危漏洞,涵盖Adobe、Microsoft、Apple、Google、Cisco、IBM、Mozilla、Oracle、WordPress、HP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Adobe产品的高危漏洞最多,占全部高危漏洞的14.0%。

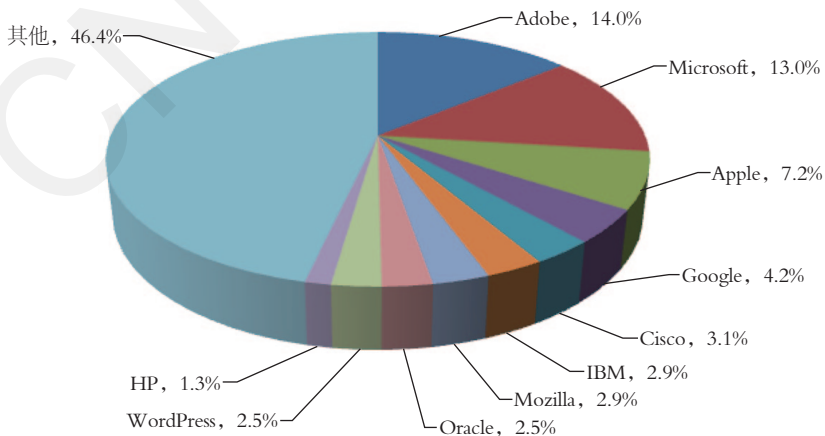


图6-3 2015年CNVD收录高危漏洞按厂商分布(来源: CNVD)



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）和安全产品漏洞（如防火墙、入侵检测系统等）。如图6-4所示，在CNVD2015年收集、整理的漏洞信息中，操作系统漏洞占6.8%，应用程序漏洞占62.0%，Web应用漏洞占14.4%，数据库漏洞占2.3%，网络设备漏洞占12.5%，安全产品漏洞占2.0%。

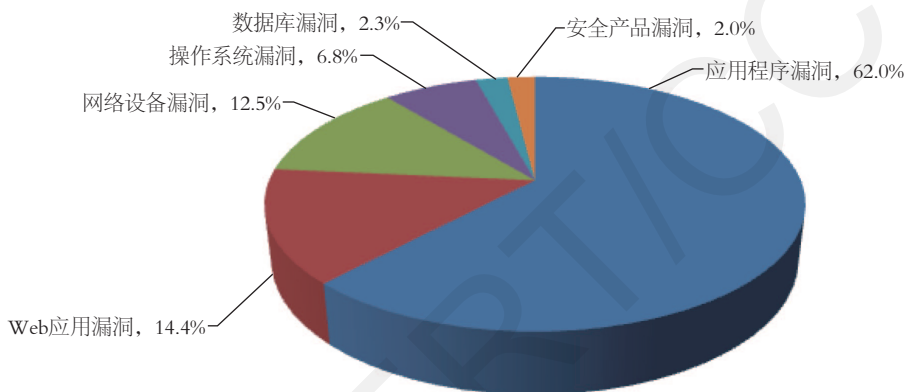


图6-4 2015年CNVD收录漏洞按影响对象类型分类统计（来源：CNVD）

CNVD 通过验证和测试攻击代码，对漏洞带来的危害进行较为全面的分析研判。2015年CNVD 共进行5828次验证，其中比较重要的包括Juniper Networks ScreenOS后门漏洞、Java反序列化远程代码执行漏洞、Redis未授权访问漏洞、HTTP.sys远程代码执行漏洞、多个网站Apache struts远程命令执行漏洞、多款D-LINK路由器产品存在任意文件上传、命令执行、文件包含等多个漏洞等。

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，进而发动大规模网络攻击。2015年CNVD共收录1207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。

2015年CNVD 共收录漏洞补丁6835个，并为大部分漏洞提供可参考的解决方案，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。

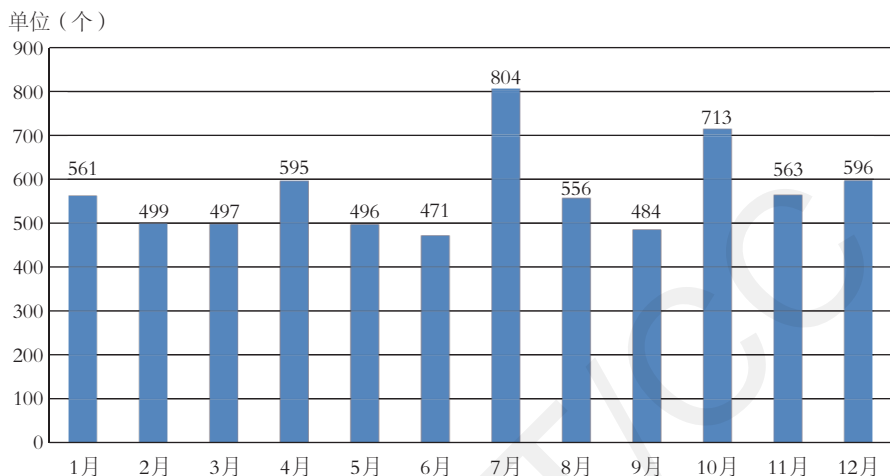


图6-5 2015年CNVD收录漏洞补丁数量按月度统计（来源：CNVD）

6.2 CNVD行业漏洞库收录情况

CNVD对现有漏洞进行深化建设，建立基于重点行业的子漏洞库，目前涉及的行业包括：电信、移动互联网、工业控制系统和电子政务。面向的重点行业客户包括：政府部门、基础电信运营商、工控行业客户等，提供量身定制的漏洞信息发布服务，从而提高重点行业客户的安全事件预警、响应和处理能力。

CNVD行业漏洞通过资产和关键字进行匹配。2015年行业漏洞库资产总数为：电信行业1513类、移动互联网135类、工控系统178类、电子政务165类。CNVD行业库关联热词总数为：电信行业84个、移动互联网42个、工控系统59个、电子政务13个。

CNVD目前共收录电信行业漏洞4938个、移动互联网行业漏洞3719个、工控行业漏洞1223个、电子政务漏洞1273个。近3年各行业漏洞统计数如图6-6所示。

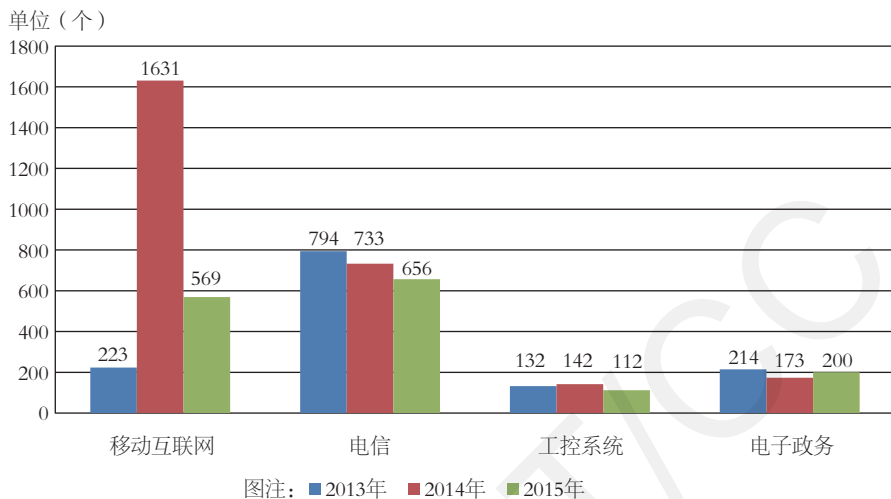


图6-6 2013-2015年CNVD收录行业漏洞对比（来源：CNVD）

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

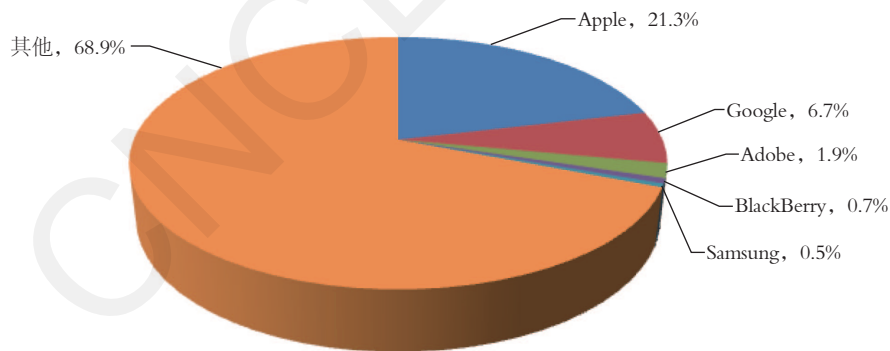


图6-7 2013-2015年CNVD移动互联网行业漏洞厂商分布（来源：CNVD）

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

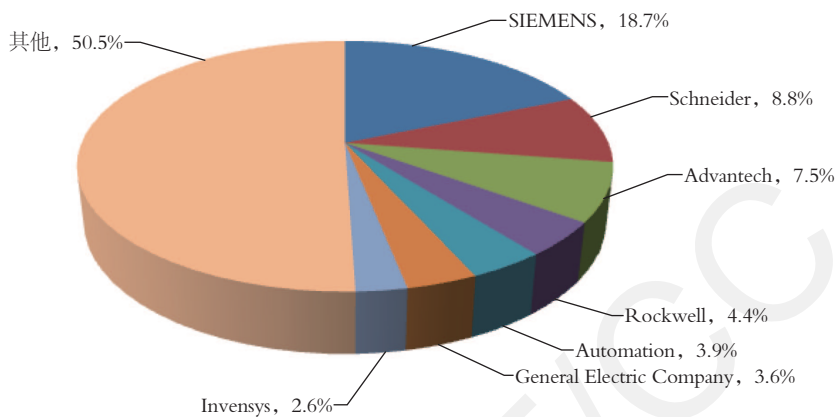


图6-8 2013-2015年CNVD工控行业漏洞厂商分布（来源：CNVD）

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

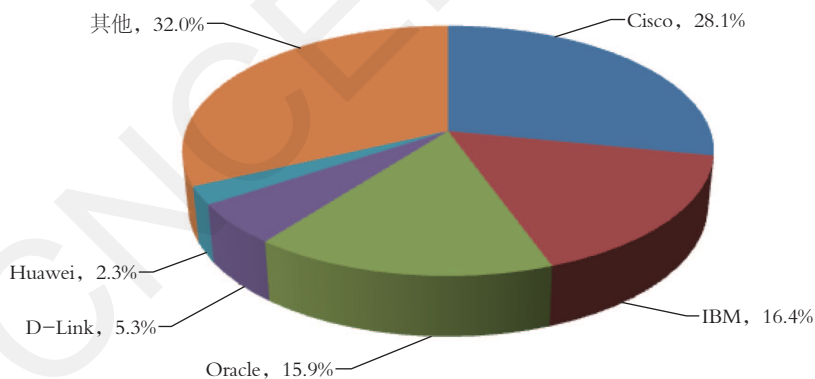


图6-9 2013-2015年CNVD电信行业漏洞厂商分布（来源：CNVD）

电子政务行业漏洞最为相关的厂商包括：Phpmyadmin、IBM(Lotus Domino/Tivoli Monitoring)、DedeCMS、Phpcms、eYou、AspCms，厂商分布如图6-10所示。

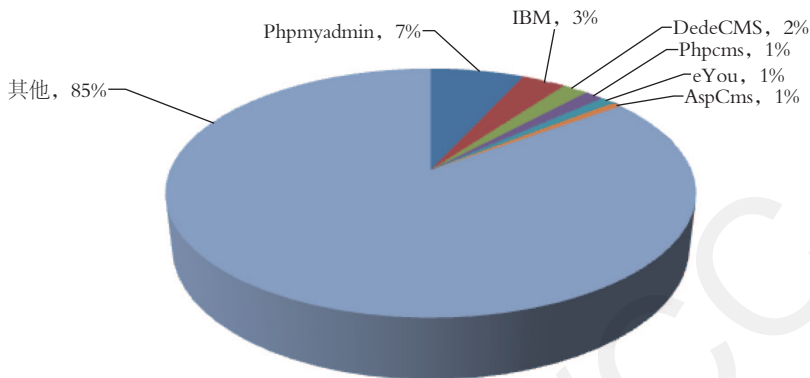


图6-10 2013-2015年CNVD电子政务行业漏洞厂商分布（来源：CNVD）

2015年，CNVD收录的漏洞中影响移动互联网行业的重要漏洞案例包括：Android SystemUI权限提升漏洞（编号：CNVD-2015-08045）、Android任意代码执行漏洞（编号：CNVD-2015-07369）和Apple iOS内核内存破坏漏洞（编号：CNVD-2015-08045）。

Android是基于Linux开放性内核的手机操作系统；Apple iOS是一款运行在苹果iPhone、iPad和iPod touch设备上最新的操作系统。Android 5.1.1 LMY48Z之前版本和6.0 2015-12-01之前版本，SystemUI在实现上存在安全漏洞，远程攻击者利用此漏洞通过构造应用可提升权限。Android 5.1.1 LMY48X之前的5.x版本和2015年之前6.0的版本存在任意代码执行漏洞，允许远程攻击者通过精心编制的媒体文件，执行任意代码或发起拒绝服务攻击。此外，Apple iOS9.0之前版本存在内存破坏漏洞，允许恶意攻击者利用漏洞执行任意代码。

影响电信行业的重要漏洞案例包括：D-Link DIR-645 Wired/Wireless Router操作系统命令注入漏洞（编号：CNVD-2015-01373）、Netcore(Netis)路由器53413/UDP后门服务漏洞（编号：CNVD-2015-00013）、Cisco Secure Access Control System SQL注入漏洞（编号：CNVD-2015-01137）。

D-Link DIR-645是友讯（D-Link）公司的一款可调节无线发射功率的路由器产品；Netcore是深圳市磊科公司，主要产品涉及无线路由器、无线网卡、网卡、集线器、交换机、宽带路由器、二三四层交换机、光终端；Cisco Secure ACS是一款Cisco

网络设备的中央管理平台，用于控制设备的认证和授权。

(1) D-Link DIR-645 Wired/Wireless Router Rev. Ax存在安全漏洞。远程攻击者可利用该漏洞通过对HNAP接口执行GetDeviceSettings操作执行任意代码。目前，DIR-645 firmware 1.04b12之前版本受此漏洞影响。

(2) Netcore/Netis的大量路由器产品在实现上存在可以轻易利用的后门漏洞，攻击者可利用硬编码的后门口令访问该后门服务，可执行任意命令以及上传、下载文件，获取Web登录口令等操作，可完全控制受影响产品。此后门监听53413/UDP端口，可以从受影响设备的WAN端利用此漏洞，即攻击者可从互联网上任何地方利用此漏洞。

(3) Cisco Secure Access Control System由于程序未在SQL查询中充分过滤用户提供的数据，攻击者可以利用漏洞执行任意SQL指令，访问或修改数据。

影响电子政务行业的重要漏洞案例包括：U-Mail邮件系统文件上传漏洞（编号：CNVD-2015-07936）、DedeCMS任意代码执行漏洞（编号：CNVD-2015-03906）、PHPCMS任意代码执行漏洞（编号：CNVD-2015-00304）。

U-Mail是一款专业的邮件服务系统，同时U-Mail也是中国最大的邮件系统供应商之一；DedeCms是一款国内最知名的PHP开源网站管理系统；PHPCMS是一款开源的国内知名内容管理系统。

(1) U-Mail for Windows V9.8.57存在文件上传漏洞，允许攻击者利用漏洞上传后门文件，获取服务器权限。

(2) DeDeCMS 5.7-sp1及之前版本在实现上存在任意代码执行漏洞，攻击者利用此漏洞可在应用上下文中执行任意代码。

(3) PHPCMS前台存在任意代码执行漏洞，允许攻击者利用此漏洞执行任意代码。

6.3 漏洞报送和通报处置情况

2015年国内安全研究者漏洞报告持续活跃，CNVD依托自有报告渠道以及与乌云、补天、漏洞盒子等民间漏洞报告平台的协作渠道，接收和处置涉及党政机关和重要行业单位的漏洞风险事件。CNVD通过各渠道接收到的民间漏洞报告数量统计见表6-1。



表6-1 2015年CNVD接收民间平台或研究者报告情况统计（来源：CNVD）

接收渠道	报告数量（条）
补天平台	26558
乌云平台	14486
CNVD网站	1557
漏洞盒子	1344

CNVD对接收到的事件进行核实验证，并依托CNCERT/CC国家中心、分中心处置渠道开展处置工作，并积极建立与国内其他企事业单位的工作联系机制。2015年CNVD处置涉及我国政府部门以及银行、证券、保险、交通、能源等重要信息系统部门以及电信、传媒、公共卫生、教育等相关行业漏洞风险事件共计23520起，按月度统计情况如图6-11所示。

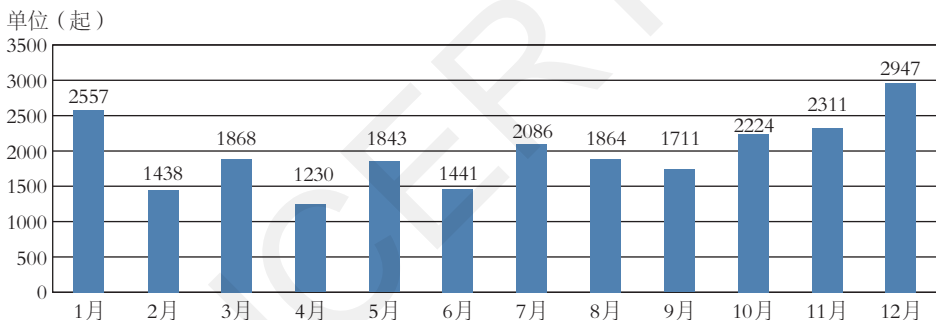


图6-11 2015年CNVD处置漏洞风险事件数量月度统计（来源：CNVD）

2015年CNVD自行开展漏洞事件处置3162次，涉及国内外软件厂商545家（注：不含涉及单个信息系统风险的企事业单位），联系次数最多的厂商见表6-2。

表6-2 2015年CNVD协调处置厂商软硬件产品次数TOP5（来源：CNVD）

厂商	漏洞数（次）
山东浪潮齐鲁软件产业股份有限公司	23
万户网络技术有限公司	15
上海安脉计算机科技有限公司	10
北京久其软件股份有限公司	9
易睦网络科技有限公司	8

其中，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、上海安脉计算机科技有限公司、北京久其软件股份有限公司、易睦网络科技有限公司等多家单位对CNVD的处置积极响应，并能及时回复漏洞修复方案。也有部分厂商未给予配合，如成都星锐蓝海网络科技有限公司、中控科技股份有限公司等。

6.4 高危漏洞典型案例

（1）Juniper Networks ScreenOS后门漏洞

2015年12月，Juniper Networks公司发布公告称其销售的部分型号防火墙产品使用的操作系统ScreenOS存在后门漏洞（CNVD收录编号：CNVD-2015-08306和CNVD-2015-08307，对应CVE-2015-7755和CVE-2015-7756）。CNCERT/CC的CNVD对漏洞进行跟踪监测，并开展案例处置工作。漏洞影响ScreenOS 6.2.0r15-6.2.0r18和6.3.0r12-6.3.0r20版本。由于产品在研发过程中设计不当，导致ScreenOS存在后门访问漏洞。攻击者利用上述漏洞，通过SSH或者Telnet远程管理访问设备，获取管理员权限；或可解密NetScreen设备的VPN流量，改变或删除日志条目，隐藏入侵痕迹。Juniper官方已经为受影响的网络设备发布新的编译版本6.2.0和6.3.0修复上述漏洞。CNVD对该漏洞的综合评级为“高危”。

截至2015年12月25日，CNVD对互联网上NetScreen系列防火墙的分布情况和受漏洞影响情况进行验证探测，结果显示，全球有27172台该系列防火墙设备，其中超过15%的设备受此漏洞直接影响。CNVD已经向基础电信企业、党政机关和重要行业单位通报数10起该漏洞后门案例。

（2）Java反序列化漏洞

2015年12月，CNVD收录Apache Commons Components Invoker Transformer反序列化任意代码执行漏洞（编号：CNVD-2015-07556，又称“Java反序列化漏洞”）。攻击者利用漏洞可借助krbtgt密码绕过身份验证系统，获取管理员访问权限，进而执行一系列管理员操作。

由于Apache Commons Collections组件的Deserialize功能存在设计漏洞，



CommonsCollections组件中对于集合的操作存在可以进行反射调用的方法，且该方法在相关对象反序列化时并未进行任何校验，远程攻击者利用漏洞可发送特殊数据给应用程序或给使用包含Java 'InvokerTransformer.class'序列化数据的应用服务器，在目标服务器当前权限环境下执行任意代码。CNVD对该漏洞的综合评级为“高危”。

截至2015年12月初，CNVD对互联网应用上述4类Web应用的分布情况和受漏洞影响程度进行探测，分别探得全球有40169台主机使用Jboss软件，有9572台主机使用Weblogic软件，有20600台主机使用Jenkins软件，有29975台主机使用Websphere软件。根据对境内主机IP的测试情况，Jboss、Weblogic、Jenkins受到漏洞影响的未修复比例分别是13.9%、50.4%、33.4%；从绝对数量看，Weblogic受到影响的数量最多。CNVD共接收和处置涉及境内党政机关、重要行业单位和企事业单位的该漏洞案例超过1200起。

（3）UPnP中的Libupnp函数库缓冲区溢出漏洞

2015年12月，UPnP的Libupnp函数库存在缓冲区溢出漏洞（编号CNVD-2013-00626，对应CVE-2012-5958），远程攻击者利用漏洞可造成堆栈溢出，导致设备死机，更严重的可在受影响设备上执行任意代码，控制用户手机。

Libupnp是UPnP设备可移植的SDK，提供了API和开源代码，用于实现媒体播放（DLAN）或NAT地址转换（UPnPIGD）。智能手机上的应用程序可利用这些功能播放媒体文件，或利用用户的家庭网络连接到其他设备。该漏洞存在于Libupnp库处理简单服务发现协议（SSDP）包过程中，此协议是Universal Plug N Play（UPnP）标准的部分，在处理进程中会出现堆栈溢出，并且需要UDP1900端口打开。综合利用漏洞，攻击者可使用特制包造成缓冲区溢出，导致设备死机，进一步可在受影响设备上执行任意代码。CNVD对该漏洞的综合评级为“高危”。

（4）Redis未授权访问漏洞

2015年11月，CNVD收录Redis未授权访问漏洞（CNVD-2015-07557）。远程攻击者利用漏洞，在未授权情况下可利用Redis的相关方法写入公钥，进而可以直接取得目标服务器的管理权，发起进一步攻击。

Redis是一套开源的使用ANSIC编写、支持网络、可基于内存亦可持久化的日志型、键值存储数据库，并提供多种语言的API。Redis默认情况下会开启6379端口，

在未开启认证的情况下，可导致任意用户在可以访问目标服务器的情况下未授权访问Redis，读取Redis的数据。该漏洞在较早前就已经被发现，而近期研究者给出更为危险的利用方法。攻击者可利用Redis的相关方法，将自己的公钥写入目标服务器/Root/.ssh文件夹的authorized_keys文件中，进而可以直接登录目标服务器。CNVD对该漏洞的综合评级为“高危”。

根据CNVD成员单位知道创宇公司提供的相关检测结果，存在无验证可直接利用Redis服务的目标在全球有49099个，其中中国有16477个。其中已经被黑的比例分别是全球65%（3.1万个），中国67.5%（1.1万个）。

（5）Xen权限提升漏洞

2015年10月，CNVD收录虚拟机系统软件Xen存在的一处权限提升漏洞（CNVD-2015-07060，对应CVE-2015-7835）。远程攻击者可利用漏洞，提升权限控制整个系统，导致虚拟机逃逸，构成用户主机数据泄露风险。目前，厂商已经发布补丁修补程序。

Xen是一款开源的虚拟机系统软件，是目前云计算服务提供虚拟化的基础系统软件。Xen平台PV模式下运行的虚拟机被披露存在权限提升漏洞。当满足一定条件，用于控制验证Level 2影像页表（Xen Page）的代码可被绕过，导致PV模式下的普通用户（如Guest）可使用超级页表映射权限重新定义可写入的映射。由于漏洞产生原因为页表关联权限绕过，即使在Xen系统配置“allowsuperpage”命令行选项为“否”的情况下也会受到漏洞的影响。综合利用漏洞，可提升普通用户权限，进而控制整个虚拟机系统，构成用户主机数据泄露风险。CNVD对该漏洞的综合评级为“高危”。

（6）ISC BIND 9 TKEY查询拒绝服务漏洞

2015年7月，CNVD收录一个ISC BIND 9 TKEY查询拒绝服务漏洞（CNVD-2015-05040，对应CVE-2015-5477）。远程攻击者可通过构造TKEY查询攻击包，导致服务器拒绝服务。目前，厂商已经发布补丁修补程序。

ISC BIND是美国Internet Systems Consortium（ISC）公司维护的一套DNS域名解析服务软件。该软件被披露存在拒绝服务漏洞，由于TKEY查询的错误可导致BIND服务器发生REQUIRE断言失败并停止服务，攻击者利用漏洞可恶意构造数据包，导致TKEY记录查询错误，进而导致BIND服务器发生REQUIRE断言失败并停止服务。



CNVD对该漏洞的综合评级为“高危”。

目前，漏洞影响BIND 9所有版本（包括BIND 9.1.0至BIND 9.9.7-P1版本、BIND 9.10.0至BIND 9.10.2-P2版本），互联网上对应版本的递归服务器和权威服务器均受到该漏洞影响。

（7）QEMU 'hw/block/fdc.c' VENOM远程内存破坏漏洞

2015年5月，CNVD收录了一个QEMU 'hw/block/fdc.c' VENOM远程内存破坏漏洞（CNVD-2015-03045，对应CVE-2015-3456）。攻击者可以在有问题的虚拟机中逃逸，一定条件下可以在宿主机中获得代码执行的权限。根据评估，“毒液（VENOM）”漏洞有可能使互联网上数以百万计的虚拟机受到威胁，进而影响到全球各大云服务提供商的数据和运行安全。目前，部分Linux厂商已经发布补丁修补程序。

该漏洞影响多款应用广泛的Web容器软件。远程攻击者利用漏洞可在目标系统上执行任意代码，危害较大的可以取得网站服务器控制权。

QEMU是一套由Fabrice Bellard编写的开源模拟处理器软件，主要用于管理多种类型的虚拟机，广泛用于各大GNU/Linux发行版（包括Debian、Gentoo、SUSE、RedHat、CentOS等）。漏洞存在于虚拟软盘驱动器（FDC）代码中，具体位于QEMU的虚拟软驱控制器的模拟代码中。

根据互联网上已公开的情况，漏洞原理可简要描述为：虚拟机操作系统通过FDC（该代码广泛应用于虚拟化平台和设备中）的输入输出端口发送搜索、读取、写入、格式化等指令与FDC进行通信。QEMU的虚拟FDC使用一个固定大小的缓冲区存储这些指令及其相关数据参数。FDC通常会根据一定的算法为指令预留和跟踪存储资源，执行指令并重置缓冲区。攻击者可以从虚拟机系统发送这些指令和精心制作的参数数据到FDC，从而实现缓冲区的堆溢出，从虚拟机系统完成“逃逸”，达到在宿主机监控程序进程环境下执行任意代码的攻击目的。

CNVD对该漏洞的技术评级为“高危”。一旦成功利用，攻击者可以访问宿主机系统以及主机上运行的所有虚拟机，并能够提升相关权限，进而影响到宿主机所在本地和相邻网络。目前，由于虚拟软盘驱动器是当前计算机系统调用较少的一个组成部分，该漏洞又被称为VENOM（毒液）漏洞，是“虚拟环境中被忽视的业务操作”的英文缩写。

（8）HTTP.sys远程代码执行漏洞

2015年4月，微软月度例行安全公告披露一个HTTP.sys远程代码执行漏洞（CNVD-2015-02422，对应CVE-2015-1635），主要威胁到IIS的安全。该漏洞存在于HTTP堆栈（HTTP.sys）中，攻击者可以在系统账户的上下文中执行任意代码或提升权限。目前，互联网已经出现可以使服务器蓝屏的利用代码，不过可导致控制服务器主机被攻击的代码还未出现。CNVD评估认为，一旦可用的远程执行利用代码被披露，有可能造成大规模的针对IIS的攻击。

IIS是微软提供的Web服务程序，全称Internet Information Services，可以提供HTTP、HTTPS、FTP等相关服务，同时支持ASP、JSP等Web端脚本，应用广泛。IIS服务进程依赖HTTP.sys内核驱动程序文件。漏洞产生的原因是HTTP.sys未能正确分析经特殊设计的HTTP请求所致，通过发送特定构造的HTTP请求包（如请求包中相关字段包含类似0xFFFFFFFFFFFFFFFF的大整数值参数），导致整数溢出。成功利用后，攻击者有可能在系统账户的上下文中执行任意代码，导致拒绝服务或提取权限。目前相关分析表明，漏洞的溢出只限于整数型参数，直接构造可执行系统指令的攻击代码还有一定的难度。CNVD对该漏洞的技术评级为“高危”。

（9）SSL/TLS协议加密算法RC4存在漏洞

2015年4月，CNVD收录一个SSL/TLS协议使用的加密算法RC4存在的漏洞（受戒礼）（CNVD-2015-02171）。通过“受戒礼”攻击，攻击者可以在特定环境下只通过嗅探监听就可以还原采用RC4保护的加密信息中的纯文本，导致账户、密码、信用卡信息等重要敏感信息泄露，并且可以通过中间人攻击（Man-in-the-Middle）进行会话劫持。

SSL（Secure Sockets Layer，安全套接层）及TLS（Transport Layer Security，传输层安全）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密，是一个被广泛使用的加密协议。而“受戒礼”攻击能够窃取通过SSL和TLS协议传输的机密数据，如银行卡号码、密码和其他敏感信息。这种攻击利用RC4加密算法中的一个长达13年的漏洞。据统计，互联网上30%的TLS流量加密使用的都是RC4算法。



漏洞的成因主要在于不变性弱密钥是RC4密钥中的一个L型图形，它一旦存在于RC4的密钥中，在整个初始化的过程中将保持状态转换的完整性。这个完整的部分包括置换过程中的最低有效位，在由RPGA算法处理时，决定伪随机输出流的最低有效位。这些偏差的流字节和明文进行过异或，导致密文中会泄露重要明文信息。CNVD对该漏洞的技术评级为“高危”。

(10) Samba组件任意代码执行漏洞

2015年2月，CNVD收录Samba组件存在的一个任意代码执行漏洞（CNVD-2015-01174，对应CVE-2015-0240）。由于Samba组件广泛应用于Linux和UNIX系统，致使主流GNU/Linux发行版受到影响。攻击者成功利用漏洞，使用当前用户权限远程执行代码，导致Samba服务崩溃或控制操作系统主机。目前厂商已经提供修复升级版本，对应Debian、Red Hat发行版本也提供修复措施，同时Red Hat安全团队对漏洞进行较为详细的分析。

Samba是在Linux和UNIX系统上实现SMB协议的一个免费软件，由服务器及客户端程序构成。它使用SMB/CIFS协议提供一个基于互联网、运行在TCP/IP之上的网络文件和打印共享服务，还可以集成动态目录环境，也可以使得服务器主机作为域控制器或作为一个域成员。

Samba存在的任意代码执行漏洞的原因是Samba的守护进程smbd里的一个未初始化指针传递给TALLOC_FREE()功能存在缺陷，即通过使用一个空会话IPC，即可调用ServerPasswordSet RPC api NetLogon端点。允许攻击者利用一个恶意的Samba客户机，发送一个特定构造的畸型netlogon数据包给smbd守护进程，进而直接获得smbd运行的Root权限，导致攻击者以当前用户权限执行任意代码，控制操作系统主机。CNVD对该漏洞的技术评级为“高危”。

(11) GNU Glibc函数库缓冲区溢出高危漏洞

2015年1月，CNVD收录了GNU Glibc ‘__nss_hostname_digits_dots()’ 函数存在的一个缓冲区溢出漏洞（CNVD-2015-00719，对应CVE-2015-0235），互联网上称“Ghost”幽灵漏洞。经过对多个Linux操作系统的本地实例测试，成功利用该漏洞可以以当前用户权限执行任意代码，进而控制操作系统主机。CNVD组织成员单位开展

的进一步测试分析，认为该漏洞影响虽然较为广泛，但从目前披露的利用方式看，要达到远程渗透成功需要一定前提（如系统和网络服务依赖关系和攻击数据包长度要求），短期内出现大规模远程攻击的可能性还很小。GNU官方和部分Linux发行版厂商已经提供修复补丁。

Glibc是GNU发布的Libc库，即C运行库。Glibc是Linux系统中最底层的API，几乎其他任何运行库都会依赖于Glibc。Glibc除了封装Linux操作系统提供的系统服务外，它本身也提供了许多其他一些必要功能服务的实现。

根据国外漏洞研究者公开的情况进行分析，Glibc库中__nss_hostname_digits_dots()函数存在缓冲区溢出漏洞，该漏洞产生的原因是glibc\nss\digits_dots.c 的__nss_hostname_digits_dots函数未加验证使用strcpy(hostname, name)，导致缓冲区溢出。该漏洞可通过gethostbyname*()函数在本地或者远程触发。

触发的一般场景为：应用程序主要使用gethostbyname*()函数发起DNS请求，这个函数会将主机名称转换为IP地址，很多服务程序在调用gethostbyname()之前，会对其做DNS有效性检查，而通常无法满足这个长度要求。因此，当提交一个超长又合法的IP地址类型的字符串给gethostbyname()函数，就会触发一个堆溢出。



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

2015年，CNCERT/CC共接收境内外报告的网络安全事件126916起，较2014年增长了125.9%。其中，境内报告的网络安全事件有126424起，较2014年增长了128.6%，境外报告的网络安全事件数量为492起，较2014年下降了43.9%。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。

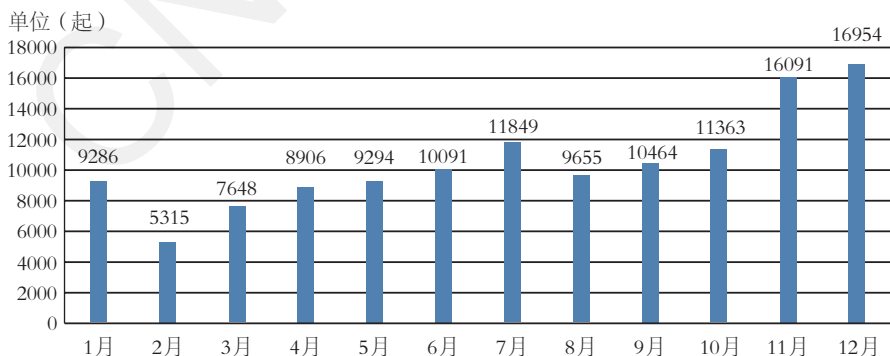


图7-1 2015年CNCERT/CC网络安全事件接收数量月度统计
(来源: CNCERT/CC)

2015年，CNCERT/CC接收到的网络安全事件报告主要来自于政府部门、金融机构、基础电信企业、互联网企业、域名服务机构、IDC、安全厂商、网络安全组织以及普通网民等。事件类型主要包括网页仿冒、漏洞、网页篡改、网站后门、恶意程序等，具体分布如图7-2所示。

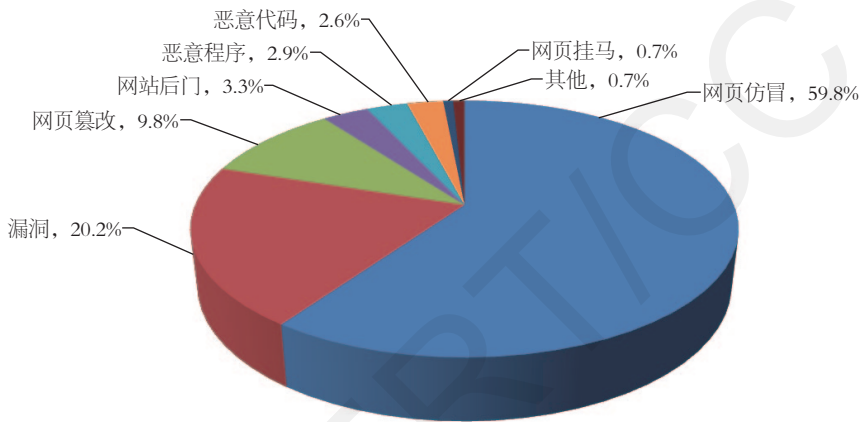


图7-2 2015年CNCERT/CC接收到网络安全事件按类型分布（来源：CNCERT/CC）

2015年，CNCERT/CC接收的网络安全事件数量排前三位的依次是网页仿冒、漏洞、网页篡改，具体情况如下。

网页仿冒事件为75860起，占有所有接收事件的比例为59.8%，位居首位。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，其数量较2014年的17873起增加了324.4%，继续保持增长态势。

漏洞事件数量为25659起，较2014年的20311起增加了26.3%，占有所有接收事件的比例为20.2%，位居第二。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2014年继续保持增长态势。

网页篡改事件数量为12418起，较2014年的9074起增加了36.9%，位居第三，占有所有接收事件的比例为9.8%。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，暗中植入暗链推广游戏、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。2015年，CNCERT/CC共成功处理各类网络安全事件125815起，较2014年的56072起增长124.4%。2015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，12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。

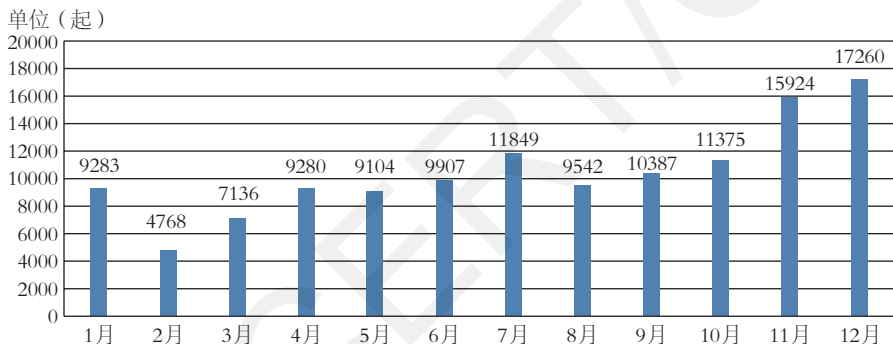


图7-3 2015年CNCERT/CC网络安全事件处置数量月度统计（来源：CNCERT/CC）

CNCERT/CC处理的网络安全事件的类型分布如图7-4所示，其中网页仿冒事件最多，共75135起，占59.7%，较2014年的17926起大幅增长了319.1%。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建设银行、中国工商银行、招商银行、中国移动、中国农业银行、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、浙江卫视、湖南卫视、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。

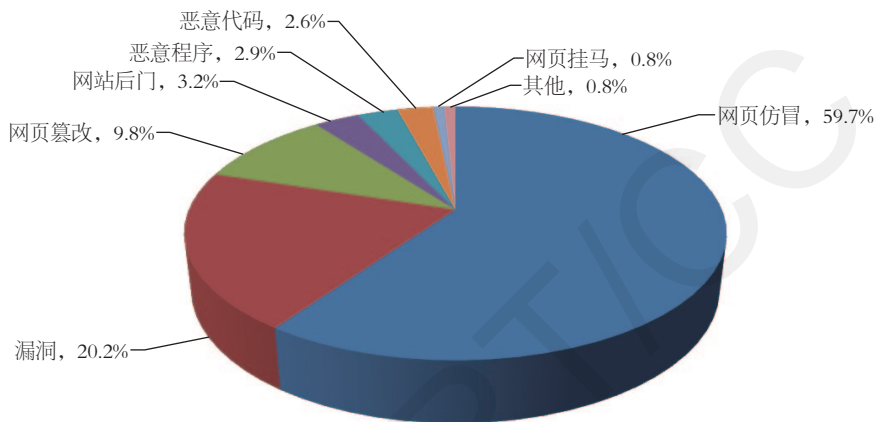


图7-4 2015年CNCERT/CC处理的网络安全事件按类型分布（来源：CNCERT/CC）

漏洞事件处置数量排名第二，全年共处置25451起，占20.2%，主要来源于CNVD收录并处理的漏洞事件。

居第三位的是网页篡改类事件。2015年，CNCERT/CC处理网页篡改类事件12308起，占9.8%，较2014年的8989起增长了36.9%。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2015年CNCERT/CC事件处理工作的重点。

2015年，CNCERT/CC加大公共互联网恶意程序治理力度。在工业和信息化部指导下，CNCERT/CC及各地分中心积极开展公共互联网恶意程序的专项打击和常态治理，加强对木马和僵尸网络等传统互联网恶意程序、移动互联网恶意程序的处置，以打击黑客地下产业链，维护公共互联网安全。

专项打击工作方面，CNCERT/CC组织基础电信企业、互联网接入企业、域名注



册服务机构和手机应用商店先后开展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678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690个,成功切断黑客对近154.1万台感染主机的控制。在移动互联网方面,下架6108个恶意APP程序,处置7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212条恶意程序传播URL链接。

常态治理工作方面,2015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6849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1.7万个。

2015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,公共互联网安全环境逐步好转。

7.3 事件处理典型案例

(1) 处置监控设备存在高危漏洞可被入侵控制并对外发动网络攻击事件

2015年2月27日,监控设备存在高危漏洞可被入侵控制并对外发动网络攻击的安全隐患问题引起社会广泛关注。因涉事监控设备在国内,特别是政府机关和公共行业的应用较广泛,存在风险较为严重。CNCERT/CC对该事件进行了持续关注和有效处置。

2014年3月,有研究机构在互联网上披露“海康威视”某些DVR设备可能通过弱口令漏洞感染了恶意代码,并可能被用于发动僵尸网络攻击。2014年4月,“海康威视”设备可被大规模控制的相关消息在互联网上被大量转载。CNCERT/CC获得相关信息后,立即开始对以“海康威视”监控设备为代表的联网智能设备的漏洞、相关恶意代码、被感染入侵和对外发动攻击等情况展开分析。同时,CNCERT/CC浙江分中心也收到“海康威视”发来的协助处置其产品受到恶意程序攻击的请求。截至2015年4月,CNCERT/CC通过恶意代码样本分析、攻击监测等手段,分析出疑似感染IP地址和控制端IP地址,并分5批次向“海康威视”提供疑似感染的IP地址。“海康威视”对其中4批次的数据进行反馈,并表示已安排修复。同时,CNCERT/CC通过木马和僵尸网络处置机制和国际合作途径,对被感染的IP地址和控制服务器IP地址进行处置。

CNCERT/CC除对“海康威视”设备加强核查分析外,还对可能涉及相关恶意程

序的其他视频监控类产品进行监测，发现至少其他4家国内知名视频监控类设备企业存在类似问题。CNCERT/CC均与相关厂商联系，并要求其提供相关数据，以便对有关情况核查。

（2）处置“相册”系列Android恶意程序导致大面积泄露用户信息事件

2015年5月15日17时，CNCERT/CC接到中国反网络病毒联盟成员单位安天公司举报的“相册”系列Android恶意程序，通过短信内容中的35个dwz.cn短链接在国内26个省、直辖市传播，感染用户超过2000人，泄露用户短信51万条、通讯录联系人信息53万条，造成严重的信息安全威胁。CNCERT/CC第一时间对该系列恶意程序所用的邮箱、传播服务器和控制服务器进行处置，有效控制了恶意程序的影响范围。

“相册”系列恶意程序主要通过短信进行传播，黑客通过发送带有恶意程序下载链接的短信，诱骗用户点击安装。

用户点击安装后，该恶意程序有以下恶意行为：

- 隐藏图标、激活设备管理器，防止用户卸载；
- 上传用户手机号、IMEI、设备型号、手机是否root、是否安装360手机安全软件等信息；
- 上传用户所有短信、通讯录联系人信息到指定的邮箱（a15778352422@vip.163.com）或者服务器（<http://cdn.yunguangli.com/WebApi/Index>），其中服务器域名yunguangli.com在成都飞数注册，服务器主机IP地址位于韩国；
- 能够接收远程控制指令，执行拦截短信、删除短信、删除通讯录以及向指定号码发送指定内容短信等操作。

CNCERT/CC对恶意程序所使用的控制服务器进行取证分析，发现控制服务器后台具备完善的监控功能，该控制服务器监控感染手机超过1500部，邮箱窃取感染用户信息超过500人。

经统计，“相册”恶意程序从5月14日开始通过短信传播，截至5月18日，感染该恶意程序的手机近2000部，且仍有500多部手机处于受控状态，波及全国26个省、直辖市，其中湖南、四川、贵州三省感染用户最多，感染比例分别为19.82%、17.12%、8.56%。

CNCERT/CC分析确认该恶意程序的影响范围后，立即启动针对“相册”系列恶意程序的处置工作，具体如下。



- 协调中国电信、中国移动和中国联通等基础电信运营商对传播恶意程序和接收用户信息的恶意URL地址，包括29个恶意短地址和<http://cdn.yunguangli.com/WebApi/Index>进行阻断处理。

- 协调域名注册商“成都飞数”和网易公司关停了用于接收用户信息的网站域名“yunguangli.com”和邮箱账户a15778352422@vip.163.com。

- 协调“dwz.cn”网站运营者百度公司删除29个恶意短地址，并要求百度公司在转换APK文件下载链接时，拒绝为存在恶意行为的APK文件下载地址进行短地址转换。

（3）处置被越菲两国匿名者组织篡改境内网站事件

2015年5月下旬，越南、菲律宾两国黑客发布声明，准备联合在5月30日中午12:00发起针对中国政府、教育、企业等网络的DDoS和网页篡改攻击。由于事件的升级，网络攻击已提前于5月29日发动。CNCERT/CC对此次攻击行动进行了持续跟踪监测和协调处置。

CNCERT/CC监测发现，截至2015年6月1日18:00，Op China行动黑客共计篡改了境内外175个网站，其中139个为境内或.cn域名网站，其余为中国台湾、中国香港、韩国、印度等国家或地区的网站。

CNCERT/CC第一时间将监测到的境内被攻击网站列表下发给各地分中心，要求分中心加强核实验证，同时积极联系涉事网站管理单位处置。截至2015年5月31日17:00的处置情况显示，涉及的138个境内网站或.cn网站中仍然有72个网站的篡改页面还存在，主要是企业或个人网站。

同时，CNCERT/CC对境外黑客开展攻击溯源获知，从2015年5月25-31日，发起攻击的主要为菲越两国黑客，也有来自中国香港、新加坡以及欧美国家的攻击源IP地址。此外，CNCERT/CC针对境外黑客攻击的手法进行了分析，发现被攻击的境内网站大多存在kineditor后台编辑器上传漏洞以及IIS上传和文件解析漏洞，使得境外黑客可直接上传篡改页面或上传网站后门进而发起篡改攻击。

（4）处置使用非苹果官方Xcode开发APP会被植入恶意代码事件

2015年9月13日，CNCERT/CC广东分中心报告称，使用非苹果公司官方渠道的Xcode开发工具开发APP时，非官方Xcode会在正常的APP中植入恶意代码。

CNCERT/CC第一时间进行技术分析，确认非官方Xcode植入的恶意代码具有信息窃取、远程控制等恶意行为。根据CNCERT/CC的监测结果，国内诸多知名公司由于使用非官方Xcode发布APP，导致官方APP被植入恶意代码，造成严重的安全风险。

通过对比苹果公司官方发布的Xcode开发工具，发现非官方Xcode开发工具中具有名为CoreServices.framework的恶意代码文件，通过该非官方Xcode开发的APP会被植入恶意代码i.privacy.xcodeghost.a。该恶意代码具有信息窃取和远程控制等恶意行为。

根据CNCERT/CC对该恶意代码的监测结果，腾讯、网易等国内知名互联网公司存在使用非官方Xcode开发APP的情况，导致腾讯音乐、网易云音乐、滴滴打车等官方APP被植入恶意代码。目前苹果公司并未发现该恶意代码，以上存在恶意代码的APP可以在App Store正常下载并安装使用。

经测试，截至2015年9月17日，中国联通、语玩、下厨房、我和你、微表情大全、网易云音乐、玩机助手、同花顺至尊版、同花顺、铁友火车票、三国名将、情侣消消乐、平安证券、口语100、卷皮折扣、工银融e联、多屏互动、豆瓣阅读、滴滴打车、保卫萝卜、邦邦熊、G买卖共22款APP被植入恶意代码，并在苹果App Store中可被下载使用。截至2015年9月18日，全国感染该恶意代码的用户达2140万，其中中国移动网内用户787万，中国联通网内用户1121万，中国电信网内用户232万。在全国31个省中，福建省感染用户最多，为186万，其次是安徽省，为180万，再次是浙江省，为147万。

在本次事件发生后，CNCERT/CC第一时间采取以下应急处置措施：

- 将被植入恶意代码的APP列表信息通报中国互联网协会，通过互联网协会通知相应的APP开发者使用苹果官方Xcode更新APP，消除恶意代码的影响；
- 将本次事件结果通报苹果公司，要求苹果公司对在APP Store中出现恶意代码的情况进行书面说明，并尽快采取应急措施消除恶意代码带来的影响。

（5）处置安卓平台窃取用户短信和通讯录的一系列恶意程序

2015年，CNCERT/CC通过自主监测方式，以及与腾讯公司、安天公司等中国反网络病毒联盟成员单位共享方式，累计发现一系列具有窃取用户短信和通讯录的安卓平台恶意程序716款。该系列恶意程序私自读取用户的短信、通讯录信息，并通过邮件发送到黑客指定的恶意邮箱。CNCERT/CC第一时间对该系列恶意程序使用的邮箱进行处置，有效控制了恶意程序的影响范围。



该系列恶意程序通过伪装成“相片”、“资料”、“违章查询”、“成绩单”等正常应用程序，通过伪基站或者手机肉鸡以短信方式进行传播，短信内容都带有恶意程序的下载地址。

该系列恶意程序都具有以下恶意行为：

- 私自读取用户的短信、通讯录信息，并通过邮件发送到指定邮箱，泄露用户隐私；
- 后台私自向指定号码发送短信，消耗用户资费；
- 私自拦截、屏蔽、删除短信，并根据短信指令执行相应的操作，进行远程控制；
- 启动后会隐藏自身图标，诱骗用户激活设备管理器以保护自身不被卸载。

CNCERT/CC对该恶意程序的控制邮箱进行取证分析，涉及网易邮箱、新浪邮箱和中国移动139邮箱等293个恶意邮箱账户，累计接收包含短信和通讯录等用户信息的邮件662498封。

CNCERT/CC分析确认该恶意程序的影响范围后，立即启动针对该恶意程序的处置工作。协调网易公司、新浪公司及中国移动公司对恶意程序所用于接收用户信息的293个恶意邮箱账户进行关停处理，切断了黑客窃取用户信息的途径。

（6）组织开展12次XP补丁验证与分发

微软公司于2014年4月8日正式停止对Windows XP系统的服务支持，且不再提供针对该操作系统的系统安全补丁、升级以及其他相关服务。如果用户继续使用XP系统，新发现的系统漏洞将因安全升级停止而无法被修补，用户受到黑客、木马等威胁和攻击，造成信息泄露、系统瘫痪、财产损失的潜在风险将会显著增加。

在我国，由于目前仍使用XP系统的用户数量较多，XP安全升级停止后，数量众多的XP系统用户计算机可能被黑客控制，用于对有较高价值的目标进行大规模攻击，造成重大信息安全事件和重大经济损失的潜在风险也将会显著增加。

根据CNCERT/CC与微软公司就XP补丁获取方法进行磋商后达成的协定，CNCERT/CC将通过微软公司授权的特定账号，访问微软数据共享中心，下载补丁文件。随后将补丁上传至测试验证平台对其可行性、有效性和安全性进行综合评测，以提高补丁分发和安装的成功率。在获取补丁并进行验证后，CNCERT/CC将XP补丁上传至补丁分发系统进行补丁分发。并将补丁分发系统的IP地址、登录账号和密码提供给需要XP补丁的党政机关和重要信息系统用户。

通过与微软公司商定的补丁获取渠道,2015年1—12月底,CNCERT/CC共获得微软公司提供的112个XP补丁(包括32位中文、英文XP SP3系统补丁和针对32位XP系统的IE8漏洞补丁,以及公开发布的适用于64位Sever 2003系统的补丁)。获取补丁后,CNCERT/CC立即组织对本批补丁进行安装验证,并完成补丁的验证以及中文安装说明的整理。

截至2015年12月,CNCERT/CC已与国省两级政府部门和重要信息系统209家单位建立XP补丁分发联络机制。其中,国家级层面的合作单位23家,省级层面的合作单位共186家。

在当月XP补丁验证通过之后,CNCERT/CC及各分中心会及时通知联络机制内所有单位下载中文和英文系统补丁以及安装说明。

(7) 协调处置我国被植入“Pony”恶意程序的网站

2015年5月5日,CNCERT/CC接到乌克兰CERT-UA的投诉,其称监测发现一台僵尸网络控制服务器,该服务器还感染了一种名为“Pony”的恶意程序,该恶意程序可用来窃取用户的登录密码等。CERT-UA对从服务器中提取的数据进行分析,发现大量境外受恶意程序感染的网站,这其中包括中国、美国、英国、澳大利亚、匈牙利、马来西亚等19个国家的相关网站。经CNCERT/CC验证,对涉及我国的三个被植入恶意程序的网站进行了处置。

(8) 协调处置罗马尼亚机构遭受DDoS攻击事件

2015年4月,CNCERT/CC接到了罗马尼亚CERT-RO投诉我国部分SOHO无线路由器存在安全隐患的问题。CNCERT/CC对事件进行验证分析,发现这些路由器的IP地址和用户凭据信息被攻击者掌握,并被利用发起DDoS攻击等。核实后立即协调相关的基础电信企业进行处置,及时消除安全隐患。

(9) 协调处置加拿大基础设施遭受水坑式攻击事件

2015年3月,CNCERT/CC接到加拿大CCIRC投诉,称加拿大的基础设施遭受水坑式攻击。2014年12月,加拿大的某网站遭到入侵被并发现存在恶意iFrame(HTML标签),2015年2月在用户登录被入侵的网站后,该iFrame会自动使页面跳转到恶意网站,用户在跳转的恶意网站上很可能会感染恶意程序。CNCERT/CC分析了CCIRC



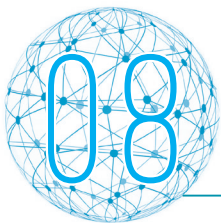
发来的位于中国的恶意程序的IP地址，并协调分中心通知IP所有者进行清理。

（10）协调处置多起涉及俄罗斯政府信息和通信网的网络攻击

2015年，CNCERT/CC接收到多起俄罗斯GOV-CERT.RU投诉的针对俄罗斯联邦政府信息和通信网的网络攻击，攻击类型包括漏洞利用、SSH暴力破解攻击、SQL注入攻击、ICMP FLOOD等。CNCERT/CC验证后，协调分中心通知用户进行清理，提高主机的安全性。

（11）协调处置阿拉伯银行遭受恶意攻击事件

2015年7月，阿拉伯ae-CERT投诉称阿拉伯银行遭受恶意网络攻击，攻击者为恶名昭彰的比特币敲诈团伙DD4BC，该组织对该银行发起严重的DDoS攻击，并勒索该银行提供30比特币才停止攻击。ae-CERT提供了遭受攻击的IP地址和位于我国的参与攻击的IP地址。CNCERT/CC验证后，协调通知用户进行了清理。



网络安全信息通报情况

8.1 互联网网络安全信息通报

2015年，CNCERT/CC继续按照《互联网网络安全信息通报实施办法》要求，作为电信和互联网行业的通报中心，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电信和互联网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。2015年，CNCERT/CC共收到各单位报送的月度信息369份、事件信息和预警信息497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》23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。

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。

2015年发布的重要通报增刊见表8-1。

表8-1 2015年CNCERT/CC发布的重要通报增刊

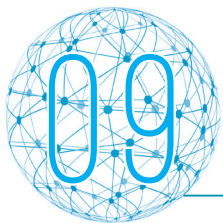
通报期号	通报标题
互联网网络安全信息通报（总第220期）	关于近日网上爆出中国联通所属系统存在高危漏洞情况的通报
互联网网络安全信息通报（总第223期）	关于监控设备存在高危漏洞可被入侵控制并对外发动网络攻击的情况通报
互联网网络安全信息通报（总第224期）	关于微软IIS服务器存在远程代码执行漏洞威胁的情况通报
互联网网络安全信息通报（总第227期）	关于“相册”系列Android恶意程序大面积泄露用户信息的情况通报
互联网网络安全信息通报（总第228期）	关于境外黑客针对我国境内网站发动攻击情况的通报
互联网网络安全信息通报（总第229期）	关于近日支付宝等网络故障的有关情况通报
互联网网络安全信息通报（总第236期）	关于多款APP应用受到Libupnp函数库缓冲区溢出漏洞影响的有骨干情况通报
互联网网络安全信息通报（总第238期）	关于近期Java反序列化漏洞跟踪和威胁风险普查的有关情况通报
互联网网络安全信息通报（总第239期）	关于安卓平台窃取用户短信和通讯录的恶意程序处置情况通报
互联网网络安全信息通报（总第240期）	关于Juniper Networks ScreenOS存在后门漏洞的有关情况通报
互联网网络安全信息通报（总第241期）	关于互联网网络安全威胁治理行动的有关情况通报

8.2 行业外互联网网络安全信息发布情况

2015年，CNCERT/CC通过发布网络安全周报、月报、专报、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254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/CC互联网安全威胁报告》12期、《网络安全月报》12期、《电子银行安全专报》12期、《2014年互联网网络安全态势报告》1份、《2014年中国互联网络网络安全报告》1份；通过期刊杂志发布网络安全数据分析文章36篇。

2015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。代表性的文章包括《2014我国互联网网络安全态势报告多家网站用户数据集体被盗》、《个人信息泄露移动应用成为新“灾区”》、《我国感染移动互联网恶意程序用户超2000万》、《工业互联网和智能设备引关注》、《2015中国网络安全技术对抗赛成功举办》、《互联网网络安全威胁治理行动启动会在京召开》、《互联网网络安全威胁治理行动单月处理投诉超万件》、《DDoS攻击事件半年下降八成》、《我国互联网网络安全威胁治理行动取得阶段性成果》、《我国互联网安全事件半年举报逾十万起互联网业组件联盟应对网安威胁》、《中国互联网络安全威胁治理联盟成立》等。



国内外网络安全监管动态

9.1 2015年国内网络安全监管动态

（1）网络安全法草案全文公布并征求社会意见

2015年6月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。2015年7月6日，网络安全法草案在中国人大网上全文公布，并向社会公开征求意见1个月。

草案规定，因维护国家和社会公共秩序、处置重大突发社会安全事件的需要，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施。草案强调，国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设，鼓励网络技术创新和应用，建立健全网络安全保障体系，提高网络安全保护能力。关于保障网络产品和服务安全，草案规定网络产品和服务提供者不得设置恶意程序，及时向用户告知安全缺陷、漏洞等风险，持续提供安全维护服务等。关于保障网络数据安全，草案要求网络运营者采取数据分类、重要数据备份和加密等措施，防止网络数据被窃取或者篡改。关于监测预警与应急处置，草案规定国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

（2）新国家安全法7月1日起实施，明确建设网络与信息安全保障体系

2015年7月1日，十二届全国人大常委会第十五次会议表决通过了新的国家安全法，国家主席习近平签署的第29号主席令予以公布。法律对政治安全、国土安全、军事安全、文化安全、科技安全等11个领域的国家安全任务进行了明确，自公布之日起施行。

新国家安全法共7章，对维护国家安全的任务与职责，国家安全制度，国家安全保障，公民、组织的义务和权利等方面进行规定。该法明确了国家安全的定义，即国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。法律还明确了国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。在维护国家安全的任务方面，新国家安全法要求，国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，加强知识产权的运用、保护和科技保密能力建设，保障重大技术和工程的安全。国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控。新国家安全法要求，国家安全危机事件发生后，履行国家安全危机管控职责的有关机关应当按照规定，准确、及时报告，并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布。新国家安全法同时明确，公民和组织支持、协助国家安全工作的行为受法律保护。此外，为提升全社会的国家安全意识，新国家安全法将每年4月15日定为全民国家安全教育日，通过多种形式开展国家安全宣传教育活动。

（3）中国刑法修正案（九）草案维护信息网络安全

2015年8月29日，备受关注的刑法修正案（九）由十二届全国人大常委会第十六次会议审议通过。刑法修正案（九）特别重视打击网络犯罪，将网络视为打击犯罪活动的重要“战场”。一是，为进一步加强公民个人信息的保护，修改出售、非法提供因履行职责或者提供服务而获得的公民个人信息犯罪的规定，扩大犯罪主体的范围；同时，增加规定出售或者非法提供公民个人信息的犯罪。二是，针对一些网络服务提供者不履行网络安全管理义务造成严重后果的情况，增加规定：网络服务提供者不履行网络安全管理义务，经监管部门通知采取改正措施而拒绝执行，致使违法信息大量传播导致用户信息泄露，造成严重后果，或者致使刑事犯罪证据毁灭或遗失，严重妨害司法机关追究犯罪，将对网络提供者追究刑事责任。三是，对为实施诈骗、销售违禁品、管制物品等违法犯罪活动而设立网站、通信群组、发布信息的行为，进一步明



确规定如何追究刑事责任；针对在网络空间传授犯罪方法，帮助他人犯罪的情况，增加规定：明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通信传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的追究刑事责任。四是，针对开设“伪基站”等严重扰乱无线电秩序，侵犯公民权益的情况，修改扰乱无线电通信管理秩序罪，降低构成犯罪门槛，增强可操作性。五是，针对在信息网络或者其他媒体上恶意编造、传播虚假信息，严重扰乱社会秩序的情况，增加编造、传播虚假信息的犯罪规定。此外，还对单位实施侵入、破坏计算机信息系统犯罪规定了刑事责任。

（4）国务院印发《关于积极推进“互联网+”行动的指导意见》

2015年7月，国务院印发《关于积极推进“互联网+”行动的指导意见》（以下简称《指导意见》），这是推动互联网由消费领域向生产领域拓展，加速提升产业发展水平，增强各行各业创新能力，构筑经济社会发展新优势和新动能的重要举措。

《指导意见》围绕转型升级任务迫切、融合创新特点明显、人民群众最关心的领域，提出了11个具体行动：一是“互联网+”创业创新，充分发挥互联网对创业创新的支撑作用，推动各类要素资源集聚、开放和共享，形成大众创业、万众创新的浓厚氛围。二是“互联网+”协同制造，积极发展智能制造和大规模个性化定制，提升网络化协同制造水平，加速制造业服务化转型。三是“互联网+”现代农业，构建依托互联网的新型农业生产经营体系，发展精准化生产方式，培育多样化、网络化服务模式。四是“互联网+”智慧能源，推进能源生产和消费智能化，建设分布式能源网络，发展基于电网的通信设施和新型业务。五是“互联网+”普惠金融，探索推进互联网金融云服务平台建设，鼓励金融机构利用互联网拓宽服务覆盖面，拓展互联网金融服务创新的深度和广度。六是“互联网+”益民服务，创新政府网络化管理和服务，大力发展线上线下新兴消费和基于互联网的医疗、健康、养老、教育、旅游、社会保障等新兴服务。七是“互联网+”高效物流，构建物流信息共享互通体系，建设智能仓储系统，完善智能物流配送调配体系。八是“互联网+”电子商务，大力发展农村电商、行业电商和跨境电商，推动电子商务应用创新。九是“互联网+”便捷交通，提升交通基础设施、运输工具、运行信息的互联网化水平，创新便捷化交通运输服务。十是“互联网+”绿色生态，推动互联网与生态文明建设深度融合，加强资源

环境动态监测，实现生态环境数据互联互通和开放共享。十一是“互联网+”人工智能，加快人工智能核心技术突破，培育发展人工智能新兴产业，推进智能产品创新，提升终端产品智能化水平。

（5）工业和信息化部调整部分机构职能强化网络安全管理

2015年7月10日，《中央编办关于工业和信息化部有关职责和机构调整的通知》正式对外公布，工业和信息化部官方网站各司局的名称相应调整。本次调整的相关职责和机构主要涉及网络、通信领域。

通知显示，调整后工业和信息化部负责网络强国建设相关工作，推动实施宽带发展等。具体的机构调整方案是，将电信管理局更名为信息通信管理局，主要职责包括依法对电信和互联网等信息通信服务实行监管，承担互联网行业管理，拟订市场准入、监管政策、标准并组织实施等。与此前电信管理局的职责相比，信息通信管理局的职责主要是增加了对互联网行业的管理，包括承担移动互联网及智能终端的管理，拟订网络有关数据采集、传输、存储、使用管理政策，规范信息通信服务市场；拟订网络架构与运行管理、互联互通与结算政策并监督执行等。将通信保障局更名为网络安全管理局，与原来的通信保障局相比，网络安全管理局的职责更多。新增职责主要涉及互联网安全，包括制定互联网安全的规划、政策和标准；建立电信网、互联网新技术、新业务安全评估制度并组织实施；指导督促电信企业和互联网企业落实网络与信息安全管理责任，组织开展网络环境和信息治理，配合处理网上有害信息，配合打击网络犯罪和防范网络失窃泄密等。将通信发展司更名为信息通信发展司，与此前通信发展司主要负责协调公用通信网、互联网、专用通信网的建设，监督管理通信建设市场和拟订电信业务资费政策和标准并监督实施等相比，更名后的信息通信发展司增加了承担信息通信企业“走出去”和国际信息通道建设相关工作。

（6）工业和信息化部组织开展电信行业网络安全试点示范工作

2015年8月，工业和信息化部发出通知，组织开展电信行业网络安全试点示范工作（以下简称试点示范）。通知指出，2015年试点示范项目的申请主体为基础电信企业集团公司或省级公司，试点示范项目为已建或在建（含已立项）的网络安全管理系统或技术平台。试点示范项目遴选以“示范效果好、实用价值高、推广潜力大”为标



准，重点考察试点示范项目是否具备实践基础、较强的技术或管理创新性和良好的应用效果；是否具有普遍适用性、可复制性和推广价值；能否坚持持续改进，发挥综合效益。工业和信息化部对于入选的试点示范项目，在其申请国家专项资金、科技评奖等方面，将按照有关政策予以支持。2015年电信行业网络安全试点示范重点引导方向包括企业内部集中化安全管理、网络和信息资产安全管理、数据安全保护、抗拒服务攻击、云平台安全防护、域名系统安全及其他创新性显著、安全防护效果突出、示范价值较高的项目等。

（7）工业和信息化部推进基础电信企业网络与信息安全责任考核工作

为促进信息通信业健康有序发展，维护国家网络与信息安全，推动基础电信企业进一步健全网络与信息安全管理长效机制，深入落实网络与信息安全责任，2012年，工业和信息化部 and 国资委联合下发了《关于开展基础电信企业网络与信息安全责任考核有关工作的指导意见》，将三家基础电信企业各省（区、市）公司网络与信息安全责任落实情况纳入集团公司内部考核体系，并于2013年正式启动省级基础电信企业网络与信息安全考核工作，将组织保障、制度建设、技术手段建设、监管配合等重点工作纳入考核。2015年是开展考核工作的第三年，为进一步优化完善考核机制、巩固深化考核工作成效，工业和信息化部网络安全管理局开展了大量工作，一是抓好上年度考核评分与整改落实工作。为确保高效、准确、客观地反映一年来各省公司的工作成果，研究建立了考核申诉与复核通报机制、加强评分结果的分析和核验，从制度上确保考核评分公开公正，减少分歧和偏差。同时，要求企业按期将问题及时整改到位。二是突出重点，优化精简考核指标。结合工作实际，加大对专职机构设置、网络信息安全技术手段建设、新技术新业务安全评估、电话用户实名登记等重点工作的考核力度，进一步细化完善考核指标，增加考核要求的针对性和可操作性。三是强化考核工作宣贯部署和监督检查，加大工作指导和督促力度，确保各个环节工作力度不松懈，考核要求不走样。

（8）《中国互联网协会漏洞信息披露和处置自律公约》在京签署

为进一步规范网络安全漏洞的信息披露和处置工作，在工业和信息化部的指导下，中国互联网协会网络与信息安全工作委员会（秘书处设在国家互联网应急中心）

组织有关单位起草了《中国互联网协会漏洞信息披露和处置自律公约》（以下简称公约），并于6月19日组织乌云、补天、漏洞盒子等民间漏洞平台、重要行业部门、基础电信企业、软硬件厂商、网络安全企业与国家互联网应急中心等32家单位举行了签约仪式。

公约签订是首次以行业自律的方式规范漏洞信息的接收、处置和发布工作。公约规定了国家互联网应急中心、漏洞报告平台以及软硬件生产厂商、信息系统管理方在漏洞披露和处置方面的责任和自律条款，提出漏洞信息披露的“客观、适时、适度”三原则，并要求各方加强协同配合，积极做好漏洞的验证、评估、修复和用户的主动响应工作。公约强调要遵守国家政策法规和政府主管部门规定，重点做好涉及政府和重要信息系统部门的漏洞披露和处置工作，同时也要积极保障用户的漏洞知情权和安全利益。

9.2 2015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

- 美国网络安全相关法令政策

（1）美众议院通过网络安全法案保障企业与政府分享信息

2015年4月22日，美国众议院通过一项法案，要求企业向联邦调查人员提供访问其计算机网络、查阅数据记录的权限。该法案将为向政府部门共享网络威胁信息的公司提供保障，免除其法律责任，同时增加了隐私保护条款。如果一家公司向美国政府分享信息，那么只有其数据经过了两轮清理，筛除其中的个人信息，才能受到法律保护，免于承担责任。第一轮筛选工作由该公司在将信息提交给政府之前完成，第二轮筛选工作由接收信息的政府机构负责。

（2）美参议院通过《美国自由法案》限制政府监听

2015年6月1日，美国参议院通过了《美国自由法案》。该法案将取代即将过期的《爱国者法案》的部分条款，同时加大对政府间谍活动的监管。《美国自由法案》旨



在遏制政府对美国本土的监控，还将采取措施使美国国家安全局的活动更加透明和负责。《美国自由法案》通过为法院指定的公共倡导者设立新职位，以参与FISC诉讼程序。该法案建立了一系列全新改进的程序获取美国民众的通话记录，但这些获取需求必须集中在一个明确的“选择项”上，目的是禁止大量收集客户数据。

（3）美国最严网络中立规则《网络开放指令》生效

2015年6月12日，美国最严网络中立规则《网络开放指令》所有条款如期生效。根据新的监管规则，互联网属于一种电信服务，互联网将按照类似电话之类的公用设施进行监管，其中宽带网络运营商被重新分类为Title II基础电信运营商。

（4）美国通过网络安全法案鼓励分享计算机攻击信息

2015年10月27日，参议院通过了《网络安全信息共享法案》。该法案将允许私营企业将其用户信息与国土安全部共享，而国土安全部有义务将其数据分享至所有相关政府机构，包括联邦调查局和国家安全局。该法案的支持者认为，《网络安全信息共享法案》将鼓励企业与政府部门共享信息，从而有助于阻止网络攻击，但多名隐私维权人士对此表示质疑，认为它不能保护用户隐私，且对防止网络攻击帮助甚微。苹果、谷歌和推特等美国硅谷的大型科技公司也纷纷表明立场，反对该法案。

（5）美国新网络安全战略攻击性升级

2015年4月23日，美国五角大楼发布新版网络安全战略，首次公开表示美军在与敌人发生冲突时，将把网络战作为选项之一，这是五角大楼发布的第二份网络安全战略报告。美国国防部于2011年7月首次发布网络安全战略报告，很少提及五角大楼的网络攻击能力。而该项战略中称，美国政府和企业受到的网络攻击比先前更严重、更复杂，美国国防部“应当有能力通过实施网络战，干扰敌人的指挥，控制网络以及与军事有关的关键基础设施和武器设施”。

● 美国其他网络安全相关举措

（1）美国拟设立新机构协调网络安全工作

美国政府拟设立一个名为“网络威胁情报整合中心”的新机构，负责协调美国现有各个网络安全部门的工作，提高美国应对网络威胁的能力。这个新设机构将在国家情报总监

的指导下工作，其功能类似“9·11”事件后美国设立的全国反恐中心。该机构将整合国土安全部、联邦调查局等各个部门搜集的网络威胁信息，为政策制定者等提供分析报告。

（2）美国将制裁对美实施恶意网络攻击的个人和实体

2015年4月1日，美国总统奥巴马签署一份行政命令，宣布美国将采取措施制裁那些对美国实施恶意网络攻击的个人和实体。根据白宫发布的声明，奥巴马授权美国财长在与国务卿、司法部长协商的基础上，对实施恶意网络活动、对美国国家安全、外交政策、经济安全和金融稳定构成“显著”威胁的个人和实体实施制裁，涉事个人或实体的资产将被冻结，禁止入境美国，禁止与美国公民或公司进行商业往来。这些恶意网络活动须满足以下至少一项条件：显著破坏美国关键基础设施；出于商业竞争优势、个人经济利益考虑，窃取美国经济资源、商业秘密、个人身份信息或金融信息；接收或使用通过网络活动手段获得的商业秘密，并从中获益；破坏美国计算机网络或为上述活动提供物质支持。

（3）美国发布指南以确保政府数据安全

2015年6月20日，美国国家标准与技术研究院发布了《受控非密信息保护指南》，旨在帮助联邦机构确保由承包商存储的敏感政府数据的机密性。该指南长达76页，提供了特定情况下如何保护受控非密信息机密性的建议和要求，这些特定情况包括：当这些信息存储在非联邦信息系统和非联邦机构内部时；当存储这类信息的系统并非由联邦机构的承包商或是代表联邦机构的相关组织使用和运营时；当授权的法律、法规或政策没有对相关受控非密信息的机密性安全防护提出特定要求时。指南中提出的要求适用于处理、存储或传输这类信息的非联邦信息系统和机构的所有部门。

（4）美国国防部发布云安全指南

2015年9月，美国国防信息系统局（DISA）发布了新版云安全指南，旨在辅助国防部（DoD）保护本国网络免遭黑客攻击。新指南由三部分构成，包括两份新版需求文件和一份新版作战概念手册。同以往相比，该指南对云安全的概念、实现云安全的步骤均做了更加全面的诠释。此外，新指南还规定组织机构及管理者在利用商业云产品时应承担的责任。该指南的发布印证了国防部增加采用商业云产品的事实。指南还指出：“由于DoD力求达到部门负责人最大限度地利用云计算的目标，因而必须一直



保护DoDIN边界不受外部连接网络的威胁。CAP能积极主动地阻断黑客攻击DoDIN基础设施,尤其能提高云服务环境中任务应用的通畅度,因而植入多重信息保障功能以检测和防范不同类型的外部攻击。”

(5) 美国海军新建网络安全部门

美国海军在海军作战部长办公室下设立一个新的网络安全部门,负责监督海军的网络安全工作,以应对日益增长的网络威胁。该网络安全部门由约40名人员组成,其职责包括同步网络安全策略、标准和要求,并对投资进行评估和评级。

9.2.1.2 美洲其他国家网络安全监管动态

(1) 加拿大警方设黑客部门调查网络犯罪

由于近年来网络犯罪案件呈现不断上升的趋势,加拿大皇家骑警(RCMP)宣布了一项5年网络犯罪战略计划,将至少招募40个IT专业人士成立全新打击网络犯罪的部门,以保护当地的居民。加拿大政府已向警方拨款3000万加元,此项计划将一直持续到2020年年底,直至加拿大各地建立完善的网络犯罪执法体系。据悉,在2011-2013年,加拿大网络犯罪案件增长了近40%,2013年网络犯罪案件已增至4400多起。

(2) 厄瓜多尔政府采取措施加强网络安全防范

自2010年以来,厄瓜多尔政府和企业网站已经遭受100次以上的黑客袭击,其中不乏厄瓜多尔国会、财政部、环保部、交通和公共工程部等重要部门,因资料泄露、系统维护所造成的损失较大。为了改变这种局面,厄瓜多尔政府开始重视网络安全,特别划拨800万美元预算,计划在军方成立网络指挥部,建立反网络攻击系统,并开始对人员进行技术培训。同时厄瓜多尔政府将加强国家情报系统的人员设施配置,希望通过增强抵御性措施,保护政府网站系统的健康运行。

9.2.2 欧洲地区网络安全监管动态

(1) 俄罗斯新法规定公民数据只能存储于境内服务器

2015年9月1日,俄罗斯《个人数据保护法》生效。该法规定,俄罗斯公民的个人信息数据只能存储于俄罗斯境内的服务器中,以实现数据本地化;任何收集俄罗斯公

民个人信息的本国或者外国公司在处理与个人信息相关的数据，包括采集、积累和存储时，必须使用俄罗斯境内的服务器；个人信息不只包括姓名、住址、出生日期等，而是与公民身份相关的任何信息。并规定，在一些特殊情况下可以在俄罗斯境外的服务器上处理个人信息数据：执法、行使国家机关和地方政府的权力，以及以达成国际协议为目的的行为。俄罗斯联邦通信、信息技术和大众传媒监督局将履行监督职责，违法的公司将会被起诉，除此之外还将被处以最高达30万卢布的罚款。

（2）欧盟新安全计划剑指网络恐怖犯罪

2015年4月28日，欧盟委员会披露了最新推出的2015-2020年安全计划。根据这一计划，欧盟在未来5年内将强化对网络恐怖犯罪的监控，阻止极端主义思想在网络上传播，防止恐怖分子通过网络获取资金，并打击武器在网络上非法买卖。

（3）欧洲废除欧美数据安全港协议

欧盟与美国15年前签订的《安全港协议》允许网络运营商忽略欧盟各国法定差异，在美国与欧盟之间合法传输网络数据。一直以来，包括谷歌、脸书等4000多家美国科技公司的欧洲运营模式都受到该协议的保护。2015年10月6日，欧洲法院作出判决，认定欧美2000年签署的关于自动交换数据的《安全港协议》无效。今后，美国网络科技公司把收集到的欧洲公民数据送往美国将受到法律限制，这一裁定对脸书、谷歌、亚马逊等美国互联网巨头影响重大。

（4）欧盟达成首个网络安全法协议

2015年12月8日，欧盟议会与成员国在经过长达5个小时的协商后，就欧盟首个网络安全法达成协议，以应对日益增加的网络安全风险。即将出台的《网络与信息安全法》要求关键领域，如交通、能源、医疗和金融领域的企业向欧盟汇报涉及网络安全的活动。相比于网络公司，航空和石油管道运营商将要面临更加严格的监管。新法同时规定，包括谷歌、亚马逊、易趣、思科在内的互联网运营商需要向有关当局及时反映网络安全事故，违反这一规定的公司将会受到相应的制裁。

（5）英国政府公布网络安全学徒计划

2015年4月1日，英国政府公布了国家网络安全计划。英国政府将与多方组织合作提



供一定数量的学徒培训机会，从而增加公务员队伍中网络专家的数量，同时还将在继续教育和高等教育中设置网络安全培训课程。英国政府在公务员快速通道学徒项目中增加了网络安全培训，并且在科技雇主合作平台的支持下创建了网络安全培训框架。

9.2.3 亚洲地区网络安全监管动态

（1）日本政府出台新网络安全战略扩大监管范围

2015年5月25日，日本政府在首相官邸举行由阁员组成的“网络安全战略本部”会议，制定了新的《网络安全战略》，提出要以此确保网络空间的自由和安全。这是日本政府自2013年以来首次更新网络安全战略。2015年9月4日，日本政府在内阁会议上正式通过了旨在确保网络空间安全的新指针“网络安全战略”。新的网络安全战略将强化应对向每个日本国民发放一个号码的“个人号码制度”。为减少黑客入侵的途径，新战略提出把处理重要信息的政府机构信息系统与网络隔断开来。

（2）日本大学加大网络安全人才培养力度

2014年6月，日本九州大学与美国马里兰大学巴尔的摩分校签订协议，引进了网络安全对策教育项目与人才培养方面的经验技术，并于2014年12月设立了推进网络安全技术研究及专家培养等工作的研究机构“网络安全中心”。2013年7月，会津大学开设了面向社会人士的专业讲座，假想黑客非法入侵银行系统提取顾客存款，介绍相关手段和对策。

（3）日本政府拟高薪从民间招募网络高手对抗黑客攻击

2015年6月15日，日本政府宣布，为了应对日渐增加的网络攻击，特别是为2020年的东京夏季奥运会做准备，日本政府决定提供优厚的待遇，从民间招募所谓的“反黑客组织”，利用其具备的信息系统防护专业知识，对抗黑客的攻击。日本政府除了希望这支由民间招募的“反黑客组织”能够对网络攻击进行监测、分析与应对之外，也希望他们能够研拟出防骇的预备措施。

（4）韩国称将增加网络安全工作人员投入对抗网络攻击

韩国核监管部门计划加强打击网络攻击的能力，并增加网络安全工作的人员投

入，以此应对黑客攻击引发的对核安全的关注。在提交总统的年度简报中，韩国核安全安保委员会（NSSC）称，将建立一支队伍对抗网络攻击，将从事网络安全工作的人员从原来的3人增加到30人。报告中称，委员会将建立一支抵御核灾难的训练系统，强化应急准备工作，建立一支队伍来对抗针对核反应堆的网络攻击。委员会还将建立法律框架，涵盖核反应堆从设计到关停的全部程序，以及未来老化反应堆关停的预备流程。

（5）韩国总统府将新设网络安保秘书室

2015年3月31日，韩国总统朴槿惠在总统府青瓦台主持召开国务会议，会上通过了在青瓦台国家安保室旗下新设网络安保秘书室的相关议案。韩联社报道说，在韩国水电与核电公司等遭到疑为来自朝鲜的网络攻击事件频频发生的情况下，韩国政府此举旨在构筑系统性的应对体系。韩国网络安保秘书室成立后，将任命网络安保秘书，这一职位将由在该领域长期工作、具有组织领导力的专家担任。现隶属于国家安保室危机管理中心的网络危机应对小组将并入新成立的网络安保秘书室，未来创造科学部、国家情报院、行政自治部等政府机构将向网络安保秘书室派遣工作人员。

（6）新加坡政府将成立网络安全局

为了应对日益严重的全球网络安全问题，重点研究国家网络安全策略，新加坡政府于2015年4月1日成立新加坡网络安全局（CSA），新加坡通信和新闻部部长雅国（Yaacob Ibrahim）担任该机构负责人。除监督新加坡网络安全政策外，该机构还负责监管全国日益发展的网络安全产业。

（7）印度尼西亚将设置国家级网络安全机构

印度尼西亚信息与通信部部长鲁迪安塔拉表示，为了切实加强网络安全管理，印度尼西亚正在积极筹备，将新组建一个专门负责网络安全的政府机构。届时，该机构将协调国防、商务、教育等各个政府部门的网络安全工作。



安全组织发展情况

10.1 网络安全信息通报成员发展情况

2015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2015年12月，全国共有764家信息通报工作成员单位（2014年是586家），形成较稳定的信息通报工作体系。与2014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178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。2015年，CNCERT/CC网络安全协作平台二期全面投入使用，进一步促进电信和互联网行业内信息共享。

全国764家^[21]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公司、中国联合网络通信集团有限公司及各省分公司、中国移动通信集团公司及各省分公司

[21] 统计通报成员单位数量时，除基础电信企业外，均将企业子公司或分公司与总公司或总部统计为一家通报成员单位。

(续表)

域名注册管理和 服务机构 (22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、阿里巴巴通信技术(北京)有限公司 ^[22] 、厦门东南融通在线科技有限公司、厦门易名网络科技有限公司、厦门三五互联科技股份有限公司、厦门市纳网科技有限公司、厦门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、郑州紫田网络科技有限公司、上海美橙科技信息发展公司
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 (82家)	北京安信华科技有限公司、北京安氏领信科技发展有限公司、北京互联互通网络科技有限公司华南分公司、北京启明星辰信息安全技术有限公司、北京瑞星信息技术有限公司、北京神州绿盟科技有限公司、北京天融信科技有限公司、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、东软系统集成工程有限公司、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、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 ^[23] 、浪潮集团有限公司、北京网御星云信息技术有限公司、奇虎360软件(北京)有限公司、恒安嘉新(北京)科技有限公司、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、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、南京钦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、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、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、杭州安恒信息技术有限公司、江苏国瑞信安科技有限公司、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、湖南中科博华科技有限公司、广东腾安网络技术有限公司、安徽中新软件有限公司、杭州华三通信技术有限公司(贵阳办事处)、

[22] 原北京万网志成科技有限公司。

[23] 原金山网络科技有限公司。



(续表)

安全企业 (82家)	北京微智信业科技有限公司、西安四叶草信息技术有限公司、甘肃海丰信息科技有限公司、北京安赛创想科技有限公司、壹进制信息技术有限公司、新疆志冠信息技术有限公司、新疆熙菱信息技术有限公司、山西同昌信息技术实业有限公司、上海斗象信息科技有限公司、东巽科技(南京)有限公司、江苏金盾检测技术有限公司、无声信息技术有限公司 ^[24]
增值电信业务 经营企业(493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、北京世纪互联宽带数据中心有限公司、长城宽带网络服务有限公司、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、黑龙江农垦通信有限公司、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技术有限公司、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、南昌领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、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、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、大江网、江西人才网、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、

[24] 原成都天融信网络安全技术有限公司。

(续表)

增值电信业务 经营企业 (493家)	江西省国荣医疗信息股份有限公司、江西新华发行集团有限公司、江西省凯恩科技信息有限公司、江西朗博文通信有限公司、江西省天域星空文化传播有限公司、江西洪城信息自动化有限公司、江西大集供应链管理有限公司、江西中投科信科技有限公司、江西省鸿联九五信息产业有限公司、江西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、福建省英捷电子科技有限公司、厦门联点网络科技有限公司、厦门优势互动网络科技有限公司、福州易桥网络科技有限公司、福州中旭网络技术有限公司、厦门聪讯达网络科技有限公司、厦门富事达网络科技有限公司、厦门国域网络科技有限公司、厦门鑫点击网络科技股份有限公司、金桥网络通信有限公司、厦门聚夏网络科技有限公司、厦门中科瑞信息技术有限公司、厦门诚域网络科技有限公司、厦门易商网络科技有限公司、厦门云缔网络服务有限公司、福州诚立信网络技术有限公司、福州乐成网络科技有限公司、福建乐天移动信息技术有限公司、福州兴奕盛网络科技有限公司、厦门中搜科技有限公司、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、南昌帆远科技有限公司、
-------------------------------	--



(续表)

增值电信业务
经营企业 (493家)

江西电信信息产业有限公司、卓望数码技术(深圳)有限公司、南昌安服信息产业有限公司、江西省多奇实业有限公司、江西纵横天亿通信有限公司、南昌易动力网络科技有限公司、江西信达信息传媒有限公司、南昌天速网络通讯有限责任公司、南昌博明科技有限公司、南昌信捷信息传媒有限公司、南昌市优凯信息技术有限公司、江西安通科技有限公司、国栗科技、新余国栗科技有限公司、江西文星科技有限公司、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、湖北长江时代通信有限公司、武汉商启网络信息有限公司、武汉迈异信息科技有限公司、鹏博士电信传媒集团武汉数据中心、武汉华安华盖网络科技有限公司、湖北盛天网络技术股份有限公司、湖北嘟嘟网络技术有限公司、武汉三江航天网络通信有限公司、湖北省楚天广播电视信息网络有限责任公司、武汉新艾普网络有限公司、湖北电信实业有限责任公司、武汉迅驰时代信息科技有限公司、湖北楚天传媒网络科技有限公司、百纳(武汉)信息技术有限公司、武汉汉网网络传媒有限公司、湖北连连科技有限公司、武汉亿房信息股份有限公司、武汉拇指通科技有限公司、武汉电信实业责任有限公司、湖北省音信数据通信技术有限公司、武汉飞游科技有限公司、武汉天伦网络技术有限公司、湖北景顺兴和信息技术有限公司、湖北七维网络技术有限公司、武汉联合信通科技有限公司、武汉天游网络科技有限公司、武汉家事易农业科技有限公司、湖北东慧通信网络投资有限公司、武汉极天网络服务有限公司、湖北音信数据通信技术有限公司、武汉亿媒百分网络科技有限公司、湖北新领域文化传媒有限公司、湖北楚唐科技有限公司、武汉虹翼信息有限公司、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、四川环游网络科技有限公司、四川梦网网络科技有限公司、四川星锐互动网络科技有限公司、广州市圣辉信息技术有限公司、深圳市奥软网络科技有限公司、广州神马移动信息科技有限公司、广东太平洋互联网信息服务有限公司、北京网康科技有限公司、乌鲁木齐新太博软件信息技术有限公司、上海安硕信息技术股份有限公司、太原市网联天地信息技术有限公司、山西网脉信息技术有限公司、山西奥科宏联信息技术有限公司、山西安科瑞忆信息技术有限公司、山西三叶虫信息技术开发有限公司、山西新誉东科信息技术有限公司、山西捷正气象信息技术有限公司、山西通达信息技术有限公司、山西海硕信息技术服务有限公司、山西安德信息技术有限公司、太原易扬众和信息技术有限公司、山西世泽信息技术有限公司、山西汇智鑫达信息技术有限公司、山西天宇智翔信息技术有限公司、阳泉东云信息技术服务有限公司、运城海数信息技术有限公司、山西并和利马信息技术有限公司、上海有孚计算机网络有限公司、上海安畅网络科技股份有限公司、上海信息产业(集团)有限公司、南京钛迅信息技术股份有限公司、上海理想信息产业(集团)有限公司、上海贝锐信息科技有限公司、上海恩度网络科技有限公司、上海创旗天下科技有限公司、上海悠扬新媒信息技术有限公司、上海地面通信信息网络有限公司、上海数讯信息技术有限公司、上海热线信息网络有限公司、小沃科技有限公司、上海臣翊网络科技有限公司、上海欧网网络科技有限公司、

(续表)

增值电信业务 经营企业 (493家)	上海福虎信息科技有限公司、上海天奕达电子科技有限公司、成都思维世纪科技有限责任公司、安徽中新软件有限公司、安徽易速网络科技有限公司、安徽炎黄网络科技有限公司、安徽希望网络科技有限公司、安徽网新科技有限公司、安徽八度网络科技有限公司、烟台海港信息通信有限公司、泰安市诺盾网络有限公司、济南雷欧网络科技有限公司、青岛万拓网络技术有限公司、新汶矿业集团有限责任公司、烟台开发区金桥奈特通信工程有限公司、枣庄矿业(集团)有限责任公司、青岛世迈网络科技有限公司、莱芜无上网络有限公司、山东东岳能源有限责任公司、济南天地网联科技有限公司、青岛中鲁通网络通信有限公司、济南息宽数据服务有限公司、济南创易信通科技有限公司、济南广电嘉和数字电视有限责任公司、济南网宿科技有限公司、济南普恒网络科技有限公司、青岛数码港通信服务有限公司、济南迅网互联网络科技有限公司、济南企联信息技术有限公司、青岛聚贤科贸有限公司、枣庄畅捷网络科技有限公司、青岛市鼎点网络技术有限公司、青岛有线电视网络有限公司、青岛嘉华网络股份有限公司、潍坊威龙电子商务科技有限公司、山东开创集团有限公司、青岛网信通信工程有限公司、青岛网信信息科技有限公司、济宁睿智网络通信工程有限公司、青岛先达电脑资讯有限公司、聊城市钢联网络科技有限公司、济南辰启网络科技有限公司、兖矿集团有限公司、淄博齐鲁石化资产经营管理有限公司、山东千翔网络科技有限公司、山东网星传媒有限公司、胜利油田胜利影视制作中心、东营华联网络科技有限公司、山东齐鲁八达网络通信技术有限公司、山东华云网络技术有限公司、青州双翼网络服务有限公司、山东竞星信息科技有限公司、菏泽互动传媒有限责任公司、曲阜市速达网络有限公司、山东日照港股份有限公司、临沂嘉联网络技术有限公司、山东康网网络科技有限公司、山东远洋网络科技有限公司、潍坊极锐网络科技有限公司、青岛友邻客信息科技有限公司、山东达通网络信息有限公司、济南网阳科技有限公司、山东中邦网络有限公司、山东长城宽带信息服务有限公司、青岛祥通网络技术有限公司、山东云立方信息技术有限公司、山东艾维通信有限公司、德州畅想软件开发有限公司、淄博宽正数码网络科技有限公司、山东北方网络通信有限责任公司、山东振华通信工程有限公司、山东维平信息安全测评技术有限公司、山东舜网传媒股份有限公司、东营天宇智能科技有限公司、青岛丽点网络传媒有限公司、临沂在线信息技术有限公司、山东银通通讯网络科技有限公司、山东银澎百盛云计算技术有限公司、高密市翼天网络技术有限公司、潍坊绿网网络信息服务有限公司、临沂沂滨科技网络有限公司、济南瀚森网络技术有限公司、山东福迈网络科技有限公司、青岛东瑞达信息技术有限公司、山东天津网络科技有限公司、东营长江通信有限公司、沈阳华兴通信工程有限责任公司、辽宁同人电子商务有限公司、沈阳敏捷世纪科技有限公司、沈阳市朗格科技发展有限公司、辽宁益通机械汽车信息有限公司、辽宁天禹星科技股份有限公司、大连经典网络发展有限公司、大连龙图信息技术股份有限公司、辽宁荣诺易居科技有限公司、大连汇海网络科技有限公司、辽宁聚品佳电子商务有限公司、大连恒基电子技术有限公司、沈阳市众诚志联网络技术有限公司、沈阳泰衡科技有限公司、沈阳加尔科技贸易有限公司、沈阳旭宏升通信信息有限公司、大连聚盟科技发展有限公司、大连集龙科技有限公司、辽宁麒润传媒广告有限公司、沈阳泰立康通信有限公司、沈阳泰合通讯有限公司、沈阳升荣信息技术有限公司、鞍山市千华网络传媒有限公司、大连新欣网络技术有限公司、葫芦岛市宏大电子商务有限责任公司、大连锐赢科技有限公司、沈阳瑞道科技有限公司、
-------------------------------	---



(续表)

增值电信业务 经营企业 (493家)	大连凡宇新世界商贸有限公司、辽阳大千电信有限公司、沈阳信影网络科技有限公司、辽宁神州云信息技术有限公司、沈阳新广电媒介网络信息有限公司、沈阳金丝网电子商务有限公司、沈阳华迅网络技术有限公司、沈阳讯网网络科技有限公司、沈阳分分钟科技有限公司、沈阳五爱电子商务信息有限公司、沈阳赤联科技有限公司、辽宁三技科技有限公司、沈阳海风网络科技有限公司、沈阳众智网络科技有限公司、沈阳统智科技有限公司、亿达信息技术有限公司、大连西盈信息技术有限公司、辽宁桑地系统集成开发有限公司、哈尔滨华风科技有限公司、哈尔滨宏鼎信息技术有限公司、哈尔滨恒天通信维护有限公司、哈尔滨英纳特科技有限公司、哈尔滨安信与诚科技开发有限公司、黑龙江亚泰通讯设备有限公司、哈尔滨郎新世纪科技贸易有限公司、黑龙江龙云气象科技有限公司、哈尔滨娱科迪迅科技发展有限公司、黑龙江恒泰信息科技有限公司、大庆市天昊伟业科技有限公司、黑龙江创立信息技术有限公司、哈尔滨巨众惠泽信息技术有限公司、黑龙江佳通信息技术有限公司、大庆中级石油通信建设有限公司、哈尔滨凌之迅网络技术有限公司、黑龙江博瑞商业发展有限公司、黑龙江乾方传媒科技有限公司、黑龙江森宇科技发展有限公司、大庆神州导航通信有限公司、吉林省颐翔通信有限公司、吉林省承信网络信息技术有限责任有限公司、吉林省启众传媒有限公司、吉林省伟豪信息产业有限公司、长春锐安信息技术有限公司、长春市电信规划设计院有限公司、吉林省威光信息技术有限公司、吉林乐冠网络科技有限公司、延吉神奇网络科技有限公司、吉林省盛诺科技有限公司、吉林省福昌科贸有限公司、吉林省隆腾科技有限公司、吉林省节约网络科技有限公司、吉林省经纬通信有限公司、吉林省一点通通信科技有限公司、吉林省联驰网络科技有限公司、珲春高兴经贸有限公司、吉林省永和超城科技有限公司、长春慧康科技信息有限责任公司、长春市元兴通信发展有限公司、吉林省鑫应信息科技开发有限公司、松原市有展科技发展有限公司、吉林省万兴通信科技有限公司、长春市蓝调电子科技有限公司、长春市众邦创通电信工程有限公司、辽源市广源网络传媒有限公司、吉林省人人科技有限公司、吉林省没想到信息科技有限公司
其他 (7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

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。

2015年CNVD全年新增信息安全漏洞8080个，其中高危漏洞2909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5828余次漏洞分析和验证工作。2015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。截至2015年年底，CNVD网站共发展2100余个白帽子注册用户以及170个行业单位用户，全年协调处置23000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。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做出积极回应。

截至2015年12月底，CNVD平台体系的成员单位情况见表10-2。

表10-2 CNVD平台体系的成员单位情况（排名不分先后）

CNVD技术合作组（16家）	国家互联网应急中心（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 北京安信天行科技有限公司 看雪安全网站 上海交通大学网络信息中心 北京安赛创想科技有限公司
CNVD用户支持组（30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



(续表)

CNVD用户支持组 (30家)	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 中兴通讯股份有限公司 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 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 盈世信息科技（北京）有限公司 电子政务组： 北京拓尔思信息技术股份有限公司 陕西时光软件有限公司 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 联动优势科技有限公司
-----------------	--

(续表)

CNVD合作伙伴(3家)	WOORYUN漏洞报告平台 补天漏洞报告平台 漏洞盒子漏洞报告平台
--------------	---

10.3 ANVA成员发展情况

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

2015年5月,在CNCERT/CC主办的“2015中国计算机网络安全大会”上,ANVA组织召开“反网络病毒最佳实践”英文国际技术沙龙,邀请了来自澳大利亚CERT、罗马尼亚CERT、斯里兰卡CERT、柬埔寨CERT、APNIC、TEAM CYMRU、微软等国家级CERT、国际网络安全组织及企业的技术专家,以及来自东软、腾讯、安天等国内网络安全企业的技术专家共同分享在反网络病毒方面的工作成果。沙龙上国内外专家进行充分的技术交流,取得了良好的效果。

2015年,ANVA持续开展黑信息共享和白名单检测认证等工作。在黑名单信息共享方面,2015年,ANVA对外发布移动恶意程序黑名单2.9万条,移动恶意程序传播源黑名单1790条,恶意地址黑名单12万条。在发布“黑名单”的同时,ANVA积极推动移动应用程序“白名单”认证工作。“白名单”认证工作启动于2013年,旨在积极倡导ANVA联盟成员建立移动互联网的健康生态,对移动互联网生态环境中APP开发者、应用商店和安全软件这三个关键环节进行约束,实现APP开发者提交安全可靠“白应用”、应用商店传播“白应用”、终端安全软件维护“白应用”的良性循环。2015年中国移动、炫彩互动网络科技有限公司、广州酷狗计算机科技有限公司三家移动互联网企业的4款数字证书和4款APP通过了白名单认证,成为2015年度首批“移动互联网应用自律白名单”成员,其中包括“中国移动MM”、“中国电信爱游戏”、



“酷狗音乐”等应用程序。

为建设安全的移动互联网生态环境，营造安全的移动APP下载环境，遏制手机病毒的传播蔓延趋势，引导网民下载使用可信的APP，保障网民的手机安全，减少感染手机病毒的风险，在中国互联网协会网络与信息安全工作委员会的指导下，在中国互联网协会移动互联网工作委员会的支持下，ANVA组织国内主流应用商店开展了“3·15白名单专项工作”，推出“3·15白名单APP专题”，为网民铺设可信移动APP下载入口。在“3·15白名单专项工作”期间，网民可通过小米手机、华为手机、OPPO手机、一加手机、HTC手机、朵唯手机、酷派手机等手机自带的应用商店客户端进入“3·15白名单APP专题”页面，也可通过中国移动MM、小米应用商店、木蚂蚁、优亿市场、华为应用市场、OPPO软件商店、PP助手、应用汇、91助手、安卓市场、百度手机助手、360手机助手、中国电信天翼空间、腾讯应用宝等14家国内知名应用商店Web网站和Android手机客户端进入“3·15白名单APP专题”页面，下载并使用“白名单APP”。此外，360手机卫士、瑞星手机安全软件、安全管家、趋势科技移动安全防护、网秦安全等手机安全软件客户端也会帮助网民对“白名单APP”进行标识，并引导网民更多地使用“白名单APP”。

在联盟成员发展方面，2015年ANVA积极吸纳中国信息通信研究院、深圳宇龙通信公司、珠海魅族科技有限公司、微软中国等网络安全领域企业与机构加入联盟，总计新增4家企业，截至2015年12月，ANVA联盟成员单位数量已达44家，成员单位具体情况见表10-3。

表10-3 ANVA联盟成员单位列表（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
 南京翰海源信息技术有限公司
 北京智游网安科技有限公司
 北京数字认证股份有限公司
 中国信息通信研究院
 深圳宇龙通信公司
 珠海魅族科技有限公司
 微软中国

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。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，强化我国公共互联网网络安全技术体系建设，促进我国互联网网络安全预警发现和应急响应的能力，为维护我国互联网网络安全做出积极贡献，在国家重大活动期间为保障网络安全发挥重要的技术支撑作用。

2015年3-5月底，结合互联网网络安全应急工作及国内网络安全服务行业的发展需要，CNCERT/CC组织开展第六届CNCERT/CC网络安全应急服务支撑单位选拔工作。本次选拔工作得到通信行业和网络安全服务行业相关单位的大力支持和积极响应，参选企业数量较往届有较大比例的增长，竞争更加激烈，选拔难度进一步加大。经过两轮细致评估和审查，最终评选出8个国家级和42个省级网络安全应急服务支撑单位。

第六届CNCERT/CC网络安全应急服务支撑单位见表10-4（有效时限为2015年5月25日-2017年5月25日）。

表10-4 第六届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
北京天融信网络安全技术有限公司	国家级	CNCERT/CC-2015-170525GJ001
哈尔滨安天科技股份有限公司	国家级	CNCERT/CC-2015-170525GJ002
北京奇虎科技有限公司	国家级	CNCERT/CC-2015-170525GJ003
北京启明星辰信息安全技术有限公司	国家级	CNCERT/CC-2015-170525GJ004
恒安嘉新（北京）科技有限公司	国家级	CNCERT/CC-2015-170525GJ005
中国电信集团系统集成有限责任公司	国家级	CNCERT/CC-2015-170525GJ006
杭州安恒信息技术有限公司	国家级	CNCERT/CC-2015-170525GJ007
沈阳东软系统集成工程有限公司	国家级	CNCERT/CC-2015-170525GJ008
深圳市深信服电子科技有限公司	省级	CNCERT/CC-2015-170525SJ001

(续表)

安徽中新软件有限公司	省级	CNCERT/CC-2015-170525SJ002
成都卫士通信息产业股份有限公司	省级	CNCERT/CC-2015-170525SJ003
成都思维世纪科技有限责任公司	省级	CNCERT/CC-2015-170525SJ004
北京知道创宇信息技术有限公司	省级	CNCERT/CC-2015-170525SJ005
重庆远衡科技发展有限公司	省级	CNCERT/CC-2015-170525SJ006
北京傲盾软件有限责任公司	省级	CNCERT/CC-2015-170525SJ007
中金金融认证中心有限公司	省级	CNCERT/CC-2015-170525SJ008
北京网康科技有限公司	省级	CNCERT/CC-2015-170525SJ009
江西安服信息产业有限公司 ^[25]	省级	CNCERT/CC-2015-170525SJ010
重庆贝特计算机系统工程有限公司	省级	CNCERT/CC-2015-170525SJ011
任子行网络技术股份有限公司	省级	CNCERT/CC-2015-170525SJ012
上海谐润网络信息技术有限公司	省级	CNCERT/CC-2015-170525SJ013
上海银基信息安全技术股份有限公司	省级	CNCERT/CC-2015-170525SJ014
上海中科网威信息技术有限公司	省级	CNCERT/CC-2015-170525SJ015
成都宇扬科技信息技术有限责任公司	省级	CNCERT/CC-2015-170525SJ016
甘肃海丰信息科技有限公司	省级	CNCERT/CC-2015-170525SJ017
上海斗象信息科技有限公司	省级	CNCERT/CC-2015-170525SJ018
四川无声信息技术有限公司	省级	CNCERT/CC-2015-170525SJ019
北京神州绿盟科技有限公司西安分公司	省级	CNCERT/CC-2015-170525SJ020
北京金创鑫诚科技有限责任公司	省级	CNCERT/CC-2015-170525SJ021
贵州亨达集团科技股份有限公司	省级	CNCERT/CC-2015-170525SJ022
南京钛迅信息技术股份有限公司	省级	CNCERT/CC-2015-170525SJ023
江苏天创科技有限公司	省级	CNCERT/CC-2015-170525SJ024
江苏君立华域信息安全技术有限公司	省级	CNCERT/CC-2015-170525SJ025
福建富士通信软件有限公司	省级	CNCERT/CC-2015-170525SJ026
江苏国瑞信安科技有限公司	省级	CNCERT/CC-2015-170525SJ027
山西同昌信息技术实业有限公司	省级	CNCERT/CC-2015-170525SJ028
杭州智御网络科技有限公司	省级	CNCERT/CC-2015-170525SJ029
郑州市景安网络科技股份有限公司	省级	CNCERT/CC-2015-170525SJ030
中国信息安全测评中心华中测评中心	省级	CNCERT/CC-2015-170525SJ031
网神信息技术(北京)股份有限公司	省级	CNCERT/CC-2015-170525SJ032
杭州思福迪信息技术有限公司	省级	CNCERT/CC-2015-170525SJ033

[25] 原名为“南昌安服信息产业有限公司”，2016年1月4日名称变更为“江西安服信息产业有限公司”，特此说明。



(续表)

中国电子科技集团公司第三十三研究所	省级	CNCERT/CC-2015-170525SJ034
新疆天山智汇信息科技有限公司	省级	CNCERT/CC-2015-170525SJ035
山东安云信息技术有限公司	省级	CNCERT/CC-2015-170525SJ036
蓝盾信息安全技术有限公司	省级	CNCERT/CC-2015-170525SJ037
北京互联互通网络科技有限公司	省级	CNCERT/CC-2015-170525SJ038
山东新潮信息技术有限公司	省级	CNCERT/CC-2015-170525SJ039
天讯瑞达通信技术有限公司	省级	CNCERT/CC-2015-170525SJ040
汕头市易动通信科技有限公司	省级	CNCERT/CC-2015-170525SJ041
中国移动通信集团辽宁有限公司	省级	CNCERT/CC-2015-170525SJ042



国内外网络安全重要活动

11.1 国内重要网络安全会议和活动

（1）CNCERT/CC发布《2014年我国互联网网络安全态势报告》

2015年4月30日，国家互联网应急中心（CNCERT/CC）在京举办“2014年我国互联网网络安全态势报告”（简称“2014年态势报告”）发布会，对2014年我国互联网网络安全的总体形势和主要特点进行发布和说明。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 and 安全厂商等30余家单位的专家和代表出席了发布会。

2014年态势报告是CNCERT/CC在工业和信息化部指导下，从网络安全行业角度出发，根据日常工作积累的数据和信息总结编撰而成。在网络安全形势部分，分别从网络基础设施和公共互联网网络环境两个方面，分析基础网络、域名系统、工业互联网面临的威胁，总结木马僵尸网络、拒绝服务攻击、安全漏洞、网络数据泄露、移动互联网恶意程序、网页仿冒、网站攻击等方面的形势特点，最后展望2015年值得关注的热点问题。

（2）2015中国网络安全技术对抗赛在武汉举行

2015年5月26日，在工业和信息化部的指导下，国家互联网应急中心（CNCERT/CC）在湖北省武汉市举办2015年中国网络安全技术对抗赛。这是继2014年在广州市汕头市首次举办此类赛事后，2015年再次举办。大赛以宣传普及网络安全知识，提高网络安全防护意识，推动网络安全技术的发展与应用为目标，邀请多名网络安全专家担当裁判，确保比赛公平公正进行。

本届大赛吸引了来自全国各地的36支队伍共106名队员参加，采用对抗赛和攻坚赛的混合竞赛模式，全面考验参赛队伍的渗透测试、漏洞分析、挖掘利用、漏洞修复、



安全防护等网络攻防实战能力。经过一天的激烈对决，6支优秀的队伍脱颖而出，获得丰富奖金。

（3）2015年中国计算机网络安全大会在湖北武汉召开

2015年5月27-28日，以“智能网络·安全护航”为主题的2015年中国计算机网络安全大会（第12届）在湖北省武汉市召开，来自政府和重要信息系统、企业、行业协会、科研院所等单位以及来自CNCERT/CC国际合作伙伴的代表共700余人参加本次大会。

大会由工业和信息化部指导，国家计算机网络应急技术处理协调中心主办，中国电子学会、中国互联网协会网络与信息安全工作委员会和中国通信学会通信安全技术委员会协办。大会历经12年发展，为政府、业界及公众之间搭建起坚实的沟通桥梁，有效促进了网络安全保障成果和经验的分享，深化推动网络安全技术的交流与合作。

（4）第二届国家网络安全宣传周启动

2015年6月1日，第二届国家网络安全宣传周在京启动。本届宣传周由中央网信办、中央编办、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、共青团中央、中国科协共10个部门共同主办，沿用首届“共建网络安全，共享网络文明”主题，于2015年6月1-7日在全国各地同步开展。

宣传周设立了启动日、金融日、电信日、政务日、科技日、法治日、青少年日共7个主题日，并开展公众体验展、青少年网络安全知识竞赛、全国网络安全宣传作品大赛、“讲述身边的网络安全故事”文章和微视频征集展映、打击网络违法犯罪专题讲座等活动。

（5）中国互联网协会——2015中国网络安全论坛成功召开

2015年7月23日，2015中国网络安全论坛成功举办。论坛以“共建网络安全 为互联网+护航”为主题，来自中央网信办、工业和信息化部、国家互联网应急中心、中国现代国际关系研究院、中国互联网络信息中心等政府和专业机构的领导及来自腾讯、微软亚太研发集团、中国移动、知道创宇、安全、360企业、杭州安存等多位互联网业内知名专家出席了论坛。

（6）互联网网络安全威胁治理行动启动会在京召开

2015年7月31日，国内24家单位在京举办互联网网络安全威胁治理行动启动会（以下简称“行动”），并在会上共同签署《互联网网络安全威胁治理行动承诺书》。CNCERT/CC和中国互联网协会网络与信息安全工作委员会主持召开启动会，并牵头组织开展此次行动。

本次行动重点打击DDoS攻击和网页植入暗链等黑客活动，以行业自律的方式，动员行业内相关单位，从加强监测入手，通过密切配合、积极处置、曝光攻击者黑名单等措施，有效防范和治理威胁互联网网络安全的行为。同时，在行动开展期间，CNCERT/CC和中国互联网协会网络与信息安全工作委员会接收来自广大网民的互联网网络安全威胁举报，并积极开展核实处置工作，治理效果显著。

11.2 国际重要网络安全会议和活动

（1）中国-东盟双方支持建立中国-东盟国家计算机应急响应组织合作机制

2015年1月22-23日，第九次中国-东盟电信部长会议在泰国曼谷召开，工业和信息化部尚冰副部长共同主持会议并做主题发言。工业和信息化部相关司局领导和CNCERT/CC黄澄清主任等陪同参加。会议支持中方提出的关于建立中国-东盟国家计算机应急响应组织合作机制的倡议，一致认为该机制是加强双方网络安全合作的重要平台。

此次CNCERT/CC提出的建立中国-东盟国家计算机应急响应组织合作机制，旨在为加强中国与东盟国家在网络安全领域的合作提供优先的信息共享和事件处理通道，有效提升全局网络安全威胁的分析预警能力，提高跨境网络安全事件处置速度，完善双方网络安全应急响应体系。具体内容包括建立联系机制、优化事件响应、加强信息和数据共享、开展能力建设、推动项目合作等。

（2）CNCERT/CC圆满完成2015年APCERT应急演练

2015年3月18日，CNCERT/CC参加亚太计算机应急响应组织（APCERT）发起举办的2015年亚太地区网络安全应急演练，圆满完成各项演练任务。



2015年APCERT演习的主题是“超越传统来源的网络攻击”。本次演练旨在检验亚太地区的CERT协作应对网络攻击的能力，共有来自19个经济体（澳大利亚、孟加拉、文莱、中国大陆、中国台湾、中国香港、印度、印度尼西亚、日本、韩国、老挝、中国澳门、马来西亚、蒙古、缅甸、新加坡、斯里兰卡、泰国和越南）的25个CERT团队参加此次演习。此次演练第4次邀请伊斯兰计算机应急响应合作组织（OIC-CERT）成员（埃及、摩洛哥和突尼斯）的三个CERT团队参加。本次演练的事件响应由多个组织协作完成，反映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。CNCERT/CC积极参与演练全过程，并圆满完成演练任务。

（3）2015网络空间国际会议聚焦网络安全

2015年4月16日，为期两天的2015网络空间国际会议在荷兰海牙启幕，中国、欧盟及主办方荷兰等都将焦点集中在网络安全，期望各方共筑网络安全防线、共建网络空间秩序。来自100多个国家和地区的1800多名国际组织、政府、企业、学术界、社会及媒体代表参加了会议。

中国代表团团长、中国驻荷兰大使陈旭指出，中国倡导构建和平、安全、开放、合作的网络空间，主张联合国在涉网络领域继续发挥国际和平与安全方面的主导作用。他强调，中国主张各国网络空间活动应遵守国家主权、和平利用、不干涉内政、和平解决争端等原则，推动加强合作打击网络恐怖主义。此外，中国还呼吁加强网络能力建设和互联网治理改革，以弥合“数字鸿沟”。

（4）中俄签署国际信息安全合作协定

2015年5月8日，习近平主席访问俄罗斯期间，中俄外长在两国元首见证下签署了《中华人民共和国政府和俄罗斯联邦政府关于在保障国际信息安全领域合作协定》。

协定强调信息通信技术应用于促进社会和经济发展和人类福祉，促进国际和平、安全与稳定，国家主权原则适用于信息空间。指出中俄将致力于构建和平、安全、开放、合作的国际信息环境，建设多边、民主、透明的国际互联网治理体系，保障各国参与国际互联网治理的平等权利。

协定将利用信息通信技术侵犯他国主权和安全，破坏信息基础设施，恐怖和违法犯罪活动，干涉他国内政，煽动民族、种族、教派间仇恨等列为国际信息安全领域的

主要威胁。协定规划了中俄开展合作的主要方向，包括建立共同应对国际信息安全威胁的交流和沟通渠道，在打击恐怖主义和犯罪活动、人才培养与科研、计算机应急响应等领域开展合作，并加强在联合国、国际电联、上海合作组织、金砖国家、东盟地区论坛等框架下的合作。

协定的签署体现了中俄在国际信息安全领域的高水平互信与合作，是中俄全面战略协作伙伴关系的重要方面，为两国在国际信息安全领域深化合作提供法律和机制保障。

（5）第三届中日韩互联网应急年会在日本召开

2015年8月24—25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日本东京，召开了第三届中日韩互联网应急年会。

本次会议是根据三方于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，是继2013年上海年会及2014年首尔年会后的第三次年会。本次会议总结回顾了涉及三方重大跨境安全事件上的联合处置和预防工作。三方均派技术人员参与了本次会议，并在会议上交流了网络安全威胁的最新信息。本次会议的核心成果是利用评估指标实现网络安全事件联合应急处置的规范化，从而保证安全事件得到及时、有效的处理。

最后，三方重申，将通过以下三个方面继续加强现有的合作：通过共享感染指标（Indicators of Compromise, IOC）、网络安全风险评估和降低网络威胁的措施，三方继续努力合作，如参与恶意程序的清理，促进互联网的健康发展。进一步探索各方网络安全事件的处置能力及方法，开展更多的面对面及在线形式的会议和培训。本次会议圆满成功，并暂定下次年会将由CNCERT/CC于2016年夏季主办。

（6）与东盟建立网络安全事件共同响应机制

2015年9月13日，中国—东盟信息港论坛在广西南宁开幕。论坛以“互联网+海上丝绸之路——合作·互利·共赢”为主题。国家发改委林念修副主任表示，国家发改委将会同有关部门，制定东盟信息港的远景规划，研究时间表、路线图。

林念修在发言中表示，建设中国—东盟信息港是构建中国—东盟命运共同体的标志性工程。国家发改委将会同国家有关部门和广西壮族自治区，抓紧制定信息港的远景



规划,研究时间表、路线图,确定年度目标和重点工作,务实推动信息港建设。

林念修建议从多方面重点开展合作。首先是建设完善区域通信、互联网、卫星导航等重要信息基础设施,构筑中国-东盟区域“信息高速公路”,构建连接中国-东盟各国的跨境网络陆海通道。加快推进卫星导航、移动通信等技术在东盟区域内的系统应用推广,推动云计算、大数据等信息服务发展应用,夯实信息化基础。

他提出,与东盟在跨境电子商务信用、通关和检验检疫等领域建立信息共享和互信互认机制,加强物流通关、检验检疫、金融支付、旅游、会展等方面的合作,打造合作共赢的电子商务生态圈。运用大数据等信息技术,联合分析、共同应对金融风险、经贸风险,推动区域经济合作向纵深发展。

林念修表示,要建设中国-东盟信息港产业园,搭建信息共享和经验交流平台,汇聚中国-东盟投资、贸易、应急、公共管理等方面信息,开展商贸服务、应急联动等方面的信息共享和交流合作。健全应急联动、网络安全事件共同响应等机制,共同应对疫情、突发事件和自然灾害等各类挑战,加强网络安全协作。

(7) 中国互联网安全领袖峰会举行,中美网络安全公开对话

2015年9月29日,2015中国互联网安全大会(ISC 2015)暨中国互联网安全领袖峰会在北京国家会议中心召开,这是继5天前刚刚在西雅图举行的中美互联网论坛之后,中美在网络安全领域的首次高层公开对话和交流。作为ISC 2015的开幕峰会,中国互联网安全领袖峰会专注于网络安全,多名中美相关高层领导出席会议并发表演讲。与之前“中美网络安全二轨对话”等高层闭门会谈不同,此次是中美国务院网络空间安全智库和专家首次在公开会议上就中美网络安全进行公开对话。来自全球的顶级安全智库、全球19所知名大学与国内10大研究机构的研究学者、全球30多家安全企业 and 安全团队的专家一起,在中国互联网安全领袖峰会、全球互联网安全精英峰会和13个分论坛上,围绕超过110个演讲议题进行深入有效的探讨。

(8) 中英签订首个网络安全协议

2015年10月21日,英国首相卡梅伦在同中国国家主席习近平在唐宁街10号首相官邸进行会晤后表示,英中两国已经就打击网络犯罪问题签署了一项“高级别安全对话”协议,旨在防止以盗窃知识产权或瘫痪系统为目的的对两国企业的网络攻击。双

方将同意既不会监视双方企业的知识产权及机密信息，又不会容忍这一行为。该协议是英国和中国首次在网络安全领域许诺共同合作。

卡梅伦称是中国和英国迈向未来更广泛的安全合作的第一步。

（9）CNCERT/CC参加东盟地区2015年度应急演练

2015年10月28日，CNCERT/CC参加了2015年度东盟地区网络安全应急演练，圆满完成了各项演练任务。

本次演练共有来自13个国家（东盟十国以及中国、澳大利亚和日本）的15个CERT参加。此次演练围绕应急处置协作和入侵分析等设计了6个模拟场景。各CERT按照自身事件处置流程，对接收的投诉事件进行调查分析和应急处置，完成恶意程序和攻击源分析，以及事件的应急处置，并提交详细的恶意程序分析报告和总结。演练有效检验和提升各国CERT的网络安全事件处置和协同配合能力。

（10）中韩信息通信主管部门网络安全会议在京召开

为落实工业和信息化部与韩国未来创造科学部签署的网络安全合作谅解备忘录，2015年10月30日，工业和信息化部与韩国未来创造科学部在北京共同召开中韩信息通信主管部门网络安全会议。本次会议是2014年两部签署谅解备忘录以来的第一次会议。会议通报中韩两国信息通信领域网络安全管理工作最新进展情况，回顾双方合作成果，重点围绕网络安全管理政策、网络基础设施保护、网络安全应急响应、网络数据与用户信息保护、网络安全技术和产业发展等议题进行深入交流。双方一致认为，中韩两部门在网络安全管理和技术方面的经验值得相互借鉴，进一步加强中韩信息通信领域网络安全交流合作，有利于双方共同提升网络安全管理水平。中韩双方基础电信企业、CERT、研究机构、行业协会以及阿里巴巴公司、奇虎360公司等互联网企业代表参加会议。

（11）第七届中国-东盟网络安全研讨会在北京召开

2015年11月3-5日，由工业和信息化部国际合作司主办，CNCERT/CC承办的第七届中国-东盟网络安全研讨会在中国北京召开。来自柬埔寨、印度尼西亚、老挝、马来西亚、新加坡、缅甸、菲律宾、泰国、越南9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。各方在会议上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，并就进一步如何扩展和深化合作，增强信任关系



和互助进行探讨。

会议期间，CNCERT/CC向东盟代表介绍其近年来在网络安全应急领域的发展情况和技术管理措施和做法，并为东盟代表开展网络安全应急能力建设的培训，帮助其提高对本国网络安全事件的预警和响应能力。

此外，CNCERT/CC还组织安全企业面向东盟参会代表开展有关网络安全事件分析和移动互联网安全的培训。

（12）中美举行首次打击网络犯罪及相关事项高级别联合对话

2015年12月1日，首次中美打击网络犯罪及相关事项高级别联合对话在华盛顿举行。对话由中国国务委员郭声琨与美国司法部部长林奇、国土安全部部长约翰逊共同主持。中美双方在此次对话中达成《打击网络犯罪及相关事项指导原则》，决定建立热线机制，就网络安全个案、网络反恐合作、执法培训等达成广泛共识，取得积极成果，在落实两国元首达成的共识方面取得重要进展。此外双方决定于2016年6月在北京举行第二次对话。

（13）第二届世界互联网大会召开，习近平就共同构建网络空间命运共同体提出5点主张

2015年12月16日，以“互联互通、共享共治——构建网络空间命运共同体”为主题的第二届世界互联网大会在浙江乌镇开幕，中共中央总书记、中国国家主席习近平出席大会开幕式并就共同构建网络空间命运共同体提出5点主张。

习近平指出，网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体。对此，习近平提出5点主张。

第一，加快全球网络基础设施建设，促进互联互通。网络的本质在于互联，信息的价值在于互通。只有加强信息基础设施建设，铺就信息畅通之路，不断缩小不同国家、地区、人群间的信息鸿沟，才能让信息资源充分涌流。中国正在实施“宽带中国”战略，预计到2020年，中国宽带网络将基本覆盖所有农村，打通网络基础设施“最后一公里”，让更多人用上互联网。中国愿同各方一道，加大资金投入，加强技术支持，共同推动全球网络基础设施建设，让更多发展中国家和人民共享互联网带来

的发展机遇。

第二，打造网上文化交流共享平台，促进交流互鉴。文化因交流而多彩，文明因互鉴而丰富。互联网是传播人类优秀文化、弘扬正能量的重要载体。中国愿通过互联网架设国际交流桥梁，推动世界优秀文化交流互鉴，推动各国人民情感交流、心灵沟通。我们愿同各国一道，发挥互联网传播平台优势，让各国人民了解中华优秀传统文化，让中国人民了解各国优秀文化，共同推动网络文化繁荣发展，丰富人们精神世界，促进人类文明进步。

第三，推动网络经济创新发展，促进共同繁荣。当前，世界经济复苏艰难曲折，中国经济也面临着一定下行压力。解决这些问题，关键在于坚持创新驱动发展，开拓发展新境界。中国正在实施“互联网+”行动计划，推进“数字中国”建设，发展分享经济，支持基于互联网的各类创新，提高发展质量和效益。中国互联网蓬勃发展，为各国企业和创业者提供广阔市场空间。中国开放的大门永远不会关上，利用外资的政策不会变，对外商投资企业合法权益的保障不会变，为各国企业在华投资兴业提供更好服务的方向不会变。只要遵守中国法律，我们热情欢迎各国企业和创业者在华投资兴业。我们愿意同各国加强合作，通过发展跨境电子商务、建设信息经济示范区等，促进世界范围内投资和贸易发展，推动全球数字经济发展。

第四，保障网络安全，促进有序发展。安全和发展是一体之两翼、驱动之双轮。安全是发展的保障，发展是安全的目的。网络安全是全球性挑战，没有哪个国家能够置身事外、独善其身，维护网络安全是国际社会的共同责任。各国应该携手努力，共同遏制信息技术滥用，反对网络监听和网络攻击，反对网络空间军备竞赛。中国愿同各国一道，加强对话交流，有效管控分歧，推动制定各方普遍接受的网络空间国际规则，制定网络空间国际反恐公约，健全打击网络犯罪司法协助机制，共同维护网络空间和平安全。

第五，构建互联网治理体系，促进公平正义。国际网络空间治理，应该坚持多边参与，由大家商量着办，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各个主体作用，不搞单边主义，不搞一方主导或由几方凑在一起说了算。各国应该加强沟通交流，完善网络空间对话协商机制，研究制定全球互联网治理规则，使全球互联网治理体系更加公正合理，更加平衡地反映大多数国家意愿和利益。举办世界互联网大会，就是希望搭建全球互联网共享共治的平台，共同推动互联网健康发展。



2016年值得关注的热点问题

根据对2015年我国互联网网络安全形势特点的分析，CNCERT/CC预测2016年值得关注的热点问题主要如下。

（1）将有更多APT攻击事件被曝光

近年来，针对我国的网络窃密、监听等攻击事件频发，网络空间的网络安全攻防对抗日趋激烈。行业报告显示，2015年对我国发起APT攻击的黑客组织近30个，主要针对我国境内科研教育、政府机构等。随着行业对APT攻击事件的了解加深，“仍有众多APT攻击事件尚未被识别”这一观点已是业内共识。同时，我国安全行业在技术、人才等多方面加大了投入，对APT攻击发现能力提高。因此，预计在2016年有更多的APT攻击组织、事件和手段将被曝光。

（2）云平台和大数据的安全防护能力将是关注重点

随着云计算、大数据等新技术、新业务的应用与发展，更多政府和企业将系统部署到云平台，大量涉及国计民生、企业运营的数据和用户个人信息存储在云上，吸引了攻击者的目光。攻击者不断挖掘云平台自身可能存在的安全漏洞，一旦发现漏洞并加以利用，可能导致严重的大规模信息泄露事件发生。此外，攻击者也可以利用云平台实施网络攻击，例如在云平台上部署网络攻击控制端、仿冒站点或发动DDoS攻击等。因此，云平台和大数据的安全防护将成为行业重点关注的问题。

（3）行业合作和国际合作需求继续加强

威胁互联网网络安全的黑客行为涉及多个环节，例如，黑客需要连接互联网、注册域名、托管用于攻击的服务器、发布推广攻击工具和服务，涉及基础电信企业、非经营性互联单位、域名注册服务机构、互联网和安全企业、数据中心、应用商店等。

为有效应对网络威胁、改善公共互联网网络安全环境，需在共享威胁信息、完善合作机制、成立产业联盟等方面加强行业合作。此外，随着我国境内互联网网络安全环境治理的持续深入推进，来自境外的网络攻击事件数量上涨趋势明显，预计2016年关于跨境网络安全事件处置的合作需求将继续上升。

（4）物联网智能设备将面临更多网络安全威胁

随着物联网技术的发展，智能穿戴设备、智能家电、智能交通等产品逐渐普及。然而，智能设备安全防护能力普遍较弱，弱口令、安全配置不当、升级维护机制不健全等问题导致智能设备普遍存在安全隐患且难以修复。2016年，随着我国“互联网+”行动计划、“中国制造2025”计划、智慧城市建设等的不断推进，大量的物联网智能设备不断涌现，在还未建立完善的网络安全保障措施情况下，物联网智能设备的安全问题将更为突出，可能面临更多的网络安全威胁。

（5）精准网络诈骗和敲诈勒索行为将更加猖獗

2015年已发生多起精准网络诈骗和敲诈勒索事件，预计2016年，此类事件将会越来越多。黑客将大量制作伪装成正常应用的恶意程序，通过钓鱼短信、小型网站、社交平台等渠道散播，欺骗用户安装并窃取用户个人信息，进而实施精准网络诈骗。此外，低成本高收益的勒索软件将大量出现，且针对移动智能终端的敲诈勒索行为将更为盛行。



网络安全术语解释

- 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

- 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

- 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。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^[26]、网银木马^[27]、窃密木马^[28]、远程控制木马^[29]、流量劫持木马^[30]、下载者木马^[31]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。

[26] 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。

[27] 网银木马是用于窃取用户网银、证券等账号的木马。

[28] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。

[29] 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。

[30] 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。

[31] 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。

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

僵尸网络是指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

拒绝服务攻击是指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，以期使目标系统停止提供服务。

- 网页篡改

网页篡改是指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

网页仿冒是指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）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。

感谢您阅读CNCERT/CC《2015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