2018 年我国互联网网络安全态势综述

国家计算机网络应急技术处理协调中心

2019 年 4 月

目 录

当前，网络安全威胁日益突出，网络安全风险不断向政治、经济、文化、社会、生态、国防等领域传导渗透，各国加强网络安全监管，持续出台网络安全政策法规。2018 年，在中央网络安全和信息化委员会（原“中央网络安全和信息化领导小组”）的统一领导下，我国进一步加强网络安全和信息化管理工作，各行业主管部门协同推进网络安全治理。国家互联网应急中心（以下简称“CNCERT”）持续加强我国互联网网络安全监测，开展我国互联网宏观网络安全态势评估，网络安全事件监测、协调处置和预警通报工作，取得了显著成效。CNCERT 依托我国宏观安全监测数据，结合网络安全威胁治理实践成果，在本报告中重点对 2018 年我国互联网网络安全状况进行了分析和总结，并对 2019 年的网络安全趋势进行预测。

一、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，持续加强公共互联网网络安全监测和治理，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”）等问题也较为严重。

（一）我国网络安全法律法规政策保障体系逐步健全

自我国《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，全国人大常委会发布《十三届全国人大常委会立法规划》，包含个人信息保护、数据安全、密码等方面。党中央、国务院各部门相继发力，网络安全方面法规、规章、司法解释等陆续发布或实施。《网络安全等级保护条例》已向社会公开征求意见，《公安机关互联网安全监督检查规定》、《关于加强跨境金融网络与信息服务管理的通知》、《区块链信息服务管理规定》、《关于加强政府网站域名管理的通知》等加强网络安全执法或强化相关领域网络安全的文件发布。

（二）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 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 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 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 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]。

（三）勒索软件对重要行业关键信息基础设施威胁加剧

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 捕获勒索软件近 14 万个，全年总体呈现增长趋势，特别在下半

[①]CNCERT 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《2018DDoS 攻击态势报告》

年，伴随“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、制造业等是受到勒索软件攻击较严重行业。例如 GlobeImposter、GandCrab 等勒索软件变种攻击了我国多家医疗机构，导致医院信息系统运行受到严重影响。

（四）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也正面临越来

越多的 APT 攻击风险。[④]APT 攻击组织采用的攻击手法主要以鱼叉邮件攻击、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。

（五）云平台成为发生网络攻击的重灾区

根据 CNCERT 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、被篡改网站数量均占比超过 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，攻击者更多的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系统的网络安全防护

[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》。

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。

（六）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%，特别是反射攻击较去年减少了 80%[⑤]。CNCERT 抽样监测发现，2018 年我国境内峰值流量超过 Tbps 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 1.27Tbps。

（七）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

[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《2018DDoS 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》。

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，致其工厂停运。分析发现，Trisis 完整的文件库通过五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 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。

（八）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 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、

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”费用，经济利益受到实质损害。此外，CNCERT 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 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”的方式来传播和诱惑用户下载并安装，可能会造成用户通讯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。

（九）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，我国也发生了包括十几亿条快递公司的用户信息、2.4亿条某连锁酒店入住信息、900 万条某网站用户数据信息、某求职网站用户个人求职简历等数据泄露事件，这些泄露数据包含了大量的个人隐私信息，如姓名、地址、银行卡号、身份证号、联系电话、家庭成员等，给我国网民人身安全、财产安全带来了安全隐患。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》

[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。

（GDPR），掀起了国内外的广泛讨论，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安全尤其是个人隐私数据安全。

二、2019 年网络安全趋势预测

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

（一）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趋势明显，网络攻击事件高发。

（二）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大，针对国家关键信息基础设施的网络攻击将会愈演愈烈。

（三）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，甚至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。

（四）5G、IPv6 等新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、海量的机器通信以及超高可靠低时延的通信，与 IPv6 技术应用共同发展，将真正实现让万物互联，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也将更加突出。同时，区块链技术也受到国内外广泛关注并快速应用，从数字货币到智能合约，并逐步向文化娱乐、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，数字货币被盗、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：2018 年我国互联网网络安全监测数据分析

一、恶意程序

（一）计算机恶意程序捕获情况

2018 年，CNCERT 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 8,132 个。全年计算机恶意程序传播次数[⑦]日均达 500 万余次。按照计算机恶意程序传播来源统计，位于境外的主要是来自美国、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 所示。位于境内的主要是位于陕西省、浙江省和河南省等省份。按照受恶意程序攻击的 IP 统计，我国境内受计算机恶意程序攻击的 IP 地址约 5,946 万个，约占我国 IP 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 年我国受计算机恶意程序攻击的 IP 分布情况如图 2 所示。

[⑦]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。

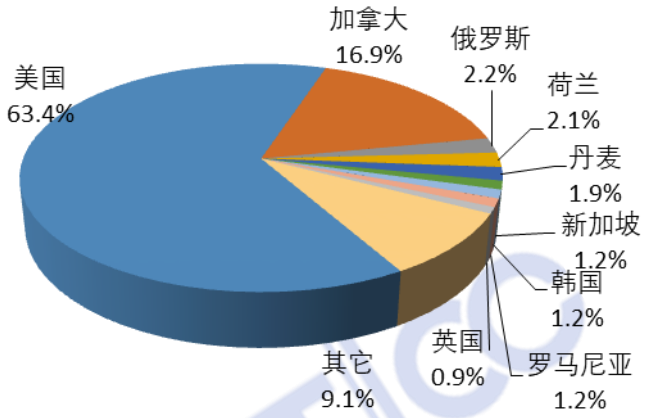

图 1 2018 年计算机恶意代码传播源位于境外分布情况

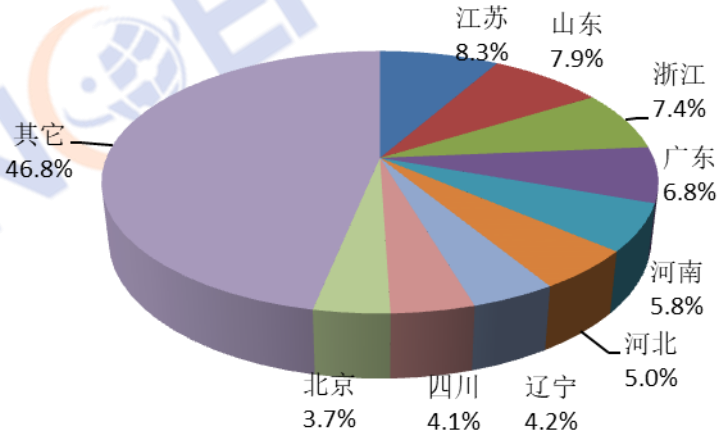

图 2 2018 年我国受计算机恶意代码攻击的 IP 分布情况

（二）计算机恶意程序用户感染情况

据 CNCERT 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 3 所示。位于境外的约 4.9 万个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，分别是约 14,752 个、6,551 个和 2,166 个；就所控制我国境内主机数量来看，位于美国、中国香港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、48 万和

33 万台主机。

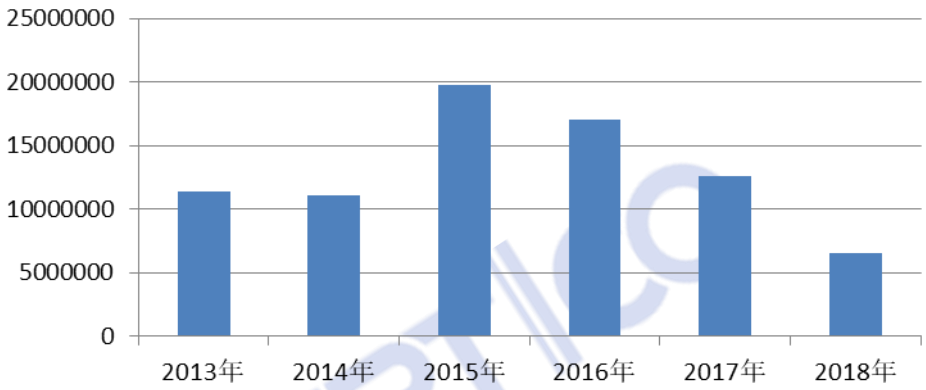

图 3 境内感染计算机恶意程序主机数量变化

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所占本地区活跃 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 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 3,710 个，规模在 10 万台以上的僵尸网络数量达 36 个，如图 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 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[⑧]。

[⑧]相关数据来源于卡巴斯基全球 DDoS 攻击趋势报告（2015.Q1-2018.Q4）。

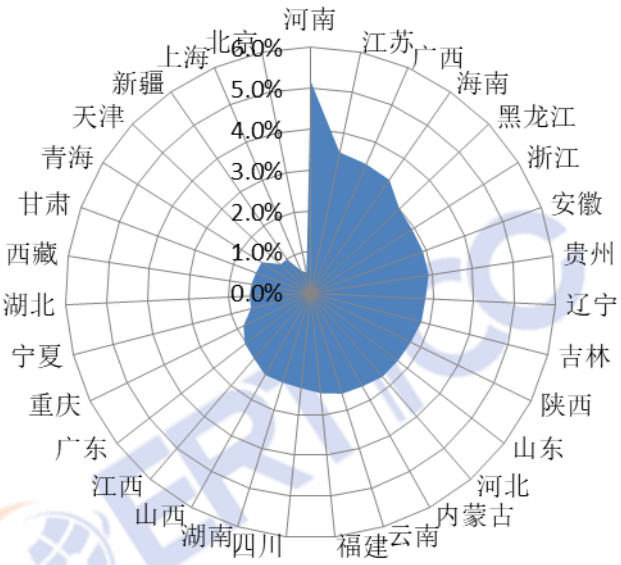

图 4 我国各地区感染计算机恶意程序主机数量占本地区活跃 IP 地址数量比例

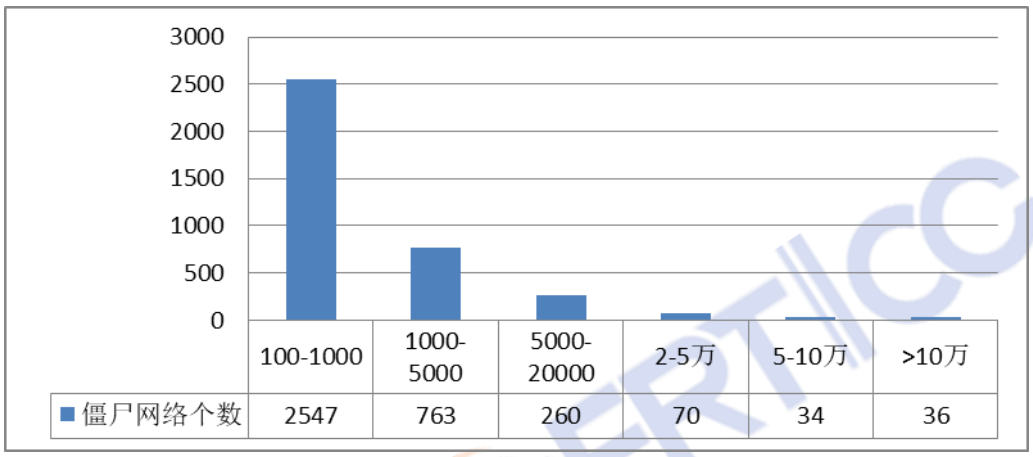

图 5 2018 年僵尸网络的规模分布

（三）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%）[9]，金

[9]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》。

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 通过自主捕获和厂商交换获得移动互联网恶意程序数量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 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[10]，占比分别为 45.8%、24.3%和 14.9%，如图 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 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 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。

[10]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**）

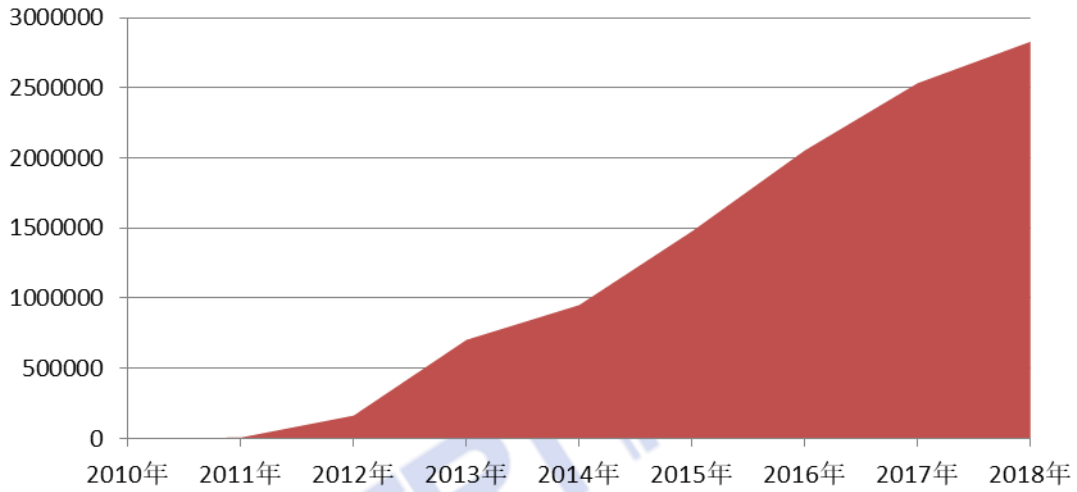

图 6 2010 年至 2018 年移动互联网恶意程序捕获数量走势

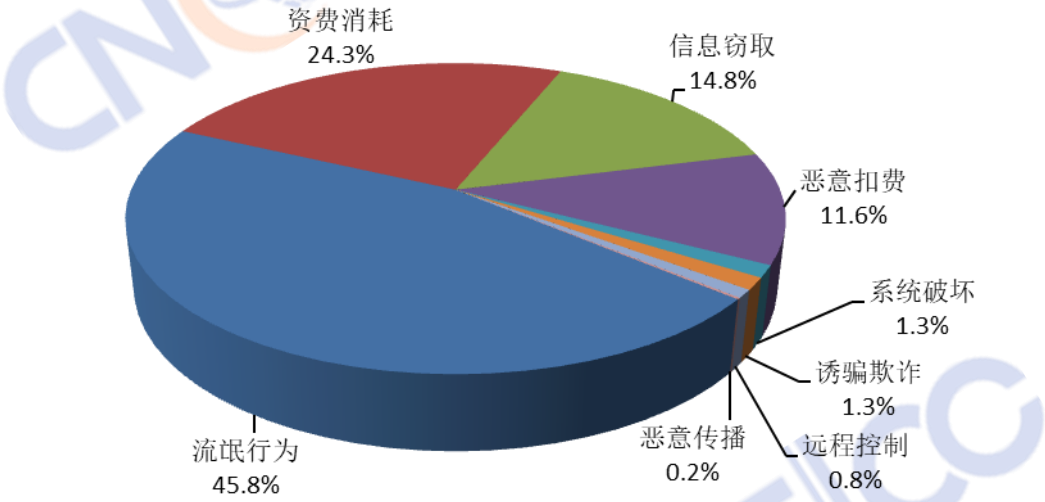

图 7 2018 年移动互联网恶意程序数量按行为属性统计

（四）联网智能设备恶意程序

据 CNCERT 监测发现，目前活跃在智能联网设备上的恶意程序家族主要包括 Ddosf、Dofloo、Gafgyt、MrBlack、Persirai、Sotdas、Tsunami、Triddy、Mirai、Moose、Teaper、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 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、浙江、河南、江苏等地被控联网智能设备 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 1,000 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，如表 1 所示。

表 1 2018 年联网智能设备僵尸网络控制规模统计情况

僵尸网络控制规模	僵尸网络个数（按控制端 IP 地址统计）	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 万至 5 万	19	位于我国境内 1 个、境外 18 个
5 千至 1 万	42	位于我国境内 1 个、境外 41 个
1 千至 5 千	294	位于我国境内 2 个、境外 292 个

二、安全漏洞

（一）安全漏洞收录情况

2014 年以来，国家信息安全漏洞共享平台（CNVD）[11]收录安全漏洞数量年平均增长率为 15.0%，其中，2018 年收录

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

安全漏洞数量同比减少了 11.0%，共计 14,201 个，高危漏洞收录数量为 4,898 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 5,381 个，同比增长 39.6%，如图 8 所示。安全漏洞主要涵盖 Google、Microsoft、IBM、Oracle、Cisco、Foxit、Apple、Adobe 等厂商产品，如表 2 所示。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 9 所示。

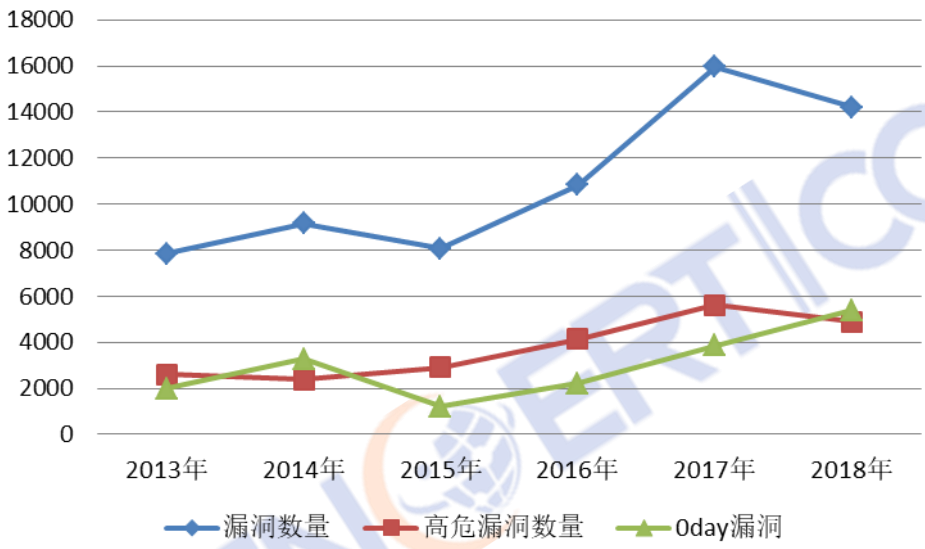

图 8 2013 年至 2018 年 CNVD 收录安全漏洞数量对比

[12] “零日”漏洞是指 CNVD 收录该漏洞时还未公布补丁。

表 2 2018 年 CNVD 收录漏洞涉及厂商情况统计

漏洞涉及厂商	漏洞数量（单位：个）	占全年收录数量百分比	环比
Google	693	4.9%	-38.8%
Microsoft	667	4.7%	-1.0%
IBM	564	4.0%	-1.7%
Oracle	481	3.4%	-37.9%
Cisco	422	3.0%	-12.6%
Foxit	369	2.6%	/
Apple	367	2.6%	-15.2%
Adobe	352	2.5%	0.6%
WordPress	261	1.8%	-27.5%
Linux	193	1.4%	-15.4%
其他	9,832	69.2%	-5.5%

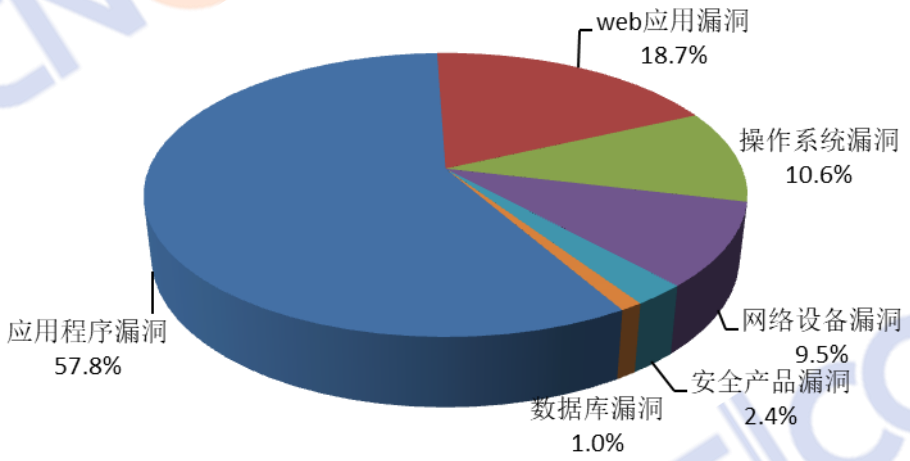

图 9 2018 年 CNVD 收录漏洞按影响对象类型分类统计

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数量 1,150 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 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%。

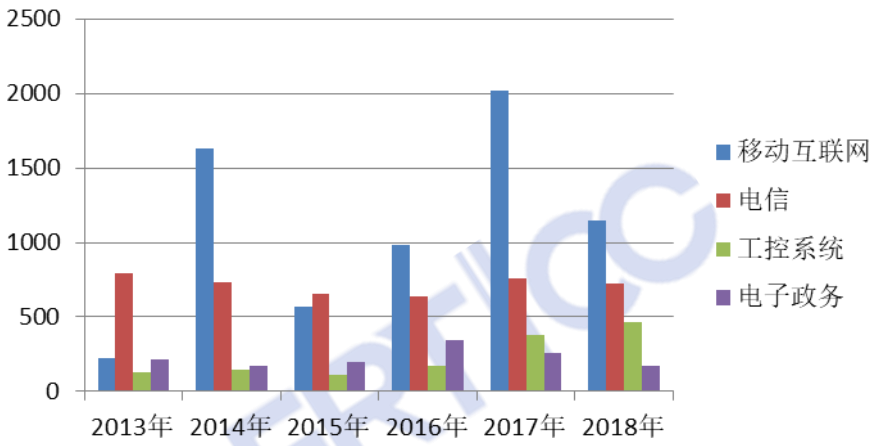

图 10 2013 年至 2018 年 CNVD 子漏洞库收录情况对比

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也相继爆出存在严重安全漏洞。

（二）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安全漏洞有 2,244 个，同比增长 8.0%。这些安全漏洞涉及的类

[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措程序来获取敏感信息。

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。

三、拒绝服务攻击

2018年，CNCERT抽样监测发现我国境内峰值超过10Gbps的大流量分布式拒绝服务攻击（DDoS攻击）事件数量平均每月超过4,000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。

（一）攻击资源情况

2018年，CNCERT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C&C控制服务器[15]数量共2,108台，总肉鸡[16]数量约144万台，反射攻击服务器约197万台，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产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。

（二）攻击团伙情况[17]

2018年，CNCERT共监测发现利用僵尸网络进行攻击的DDoS攻击团伙50个。从全年来看，与DDoS攻击事件数量、

[15]C&C控制服务器：全称为Command and Control Server，即“命令及控制服务器”，目标机器可以接收来自服务器的命令，从而达到服务器控制目标机器的目的。
[16]肉鸡：接收来自C&C控制服务器指令，对外发出大量流量的被控互联网设备。
[17]CNCERT发布的《2018年活跃DDoS攻击团伙分析报告》

C&C 控制服务器数量一样，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 C&C 控制服务器有 358 个，攻击目标有 2.8 万个，如表 3 所示。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 3 2018 年活跃攻击团伙基本信息表

团伙编号	最早活跃时间（年月日）	最近活跃时间（年月日）	活跃月份（年月）	C&C 数量（单位：个）	肉鸡数量（单位：个）	攻击目标数目（单位：个）
G1	20180101	20181231	201812	283	571,016	21,324
G2	20180502	20181230	201808	9	384	57
G3	20180308	20181104	201802	2	462	2
G4	20180101	20180731	201805	4	1,779	185
G5	20180721	20181222	201803	2	509	20
G6	20180606	20180925	201802	2	543	74
G7	20180531	20180801	201804	8	1,426	369
G8	20180723	20180911	201803	2	654	476
G9	20180511	20180712	201803	9	13,035	642
G10	20180708	20180905	201803	2	699	87
G11	20180303	20180515	201803	12	2,921	47
G12	20180707	20180902	201803	2	3,243	380
G13	20180614	20180827	201803	5	13,290	5,440
G14	20180109	20180225	201802	2	639	142
G15	20180907	20181027	201802	8	8,358	4,023
G16	20180802	20180816	201801	74	10,936	747

四、网站安全

2018 年，CNCERT 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[18]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 发现这些攻击多带有黑帽 SEO[19]、网页篡改等典型黑产利益意图，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 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。

（一）网页仿冒

2018 年，CNCERT 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 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，

[18]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。

[19]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，获利主要的特点是短平快，为了短期内的非法利益而采用的方法。

主要分布在美国和中国香港，如图 11 所示。

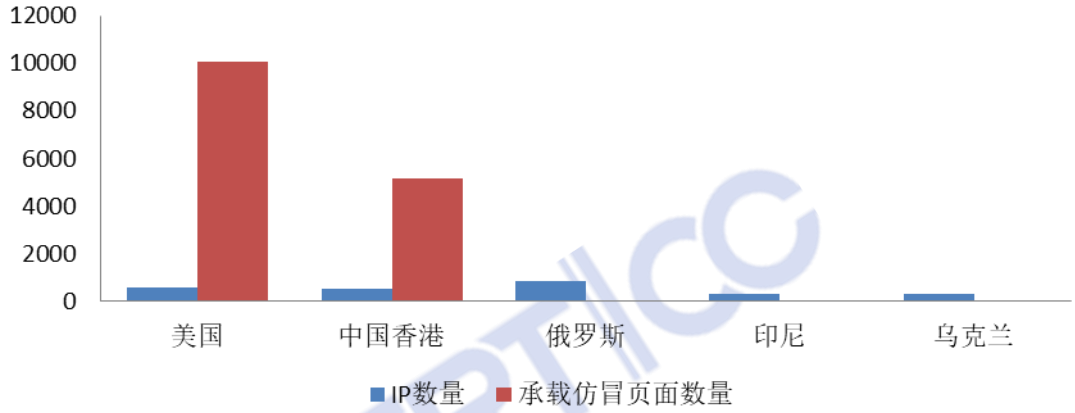

图 11 2018 年承载仿冒页面 IP 地址和仿冒页面数量分布

（二）网站后门

1. 我国境内被植入后门情况

2018 年，CNCERT 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%，其次是位于中国香港和俄罗斯的 IP 地址，如图 12 所示。从控制我国境内网站总数来看，位于中国香港的 IP 地址控制我国境内网站数量最多，有 3,994 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 3,607 个和 2,011 个网站。

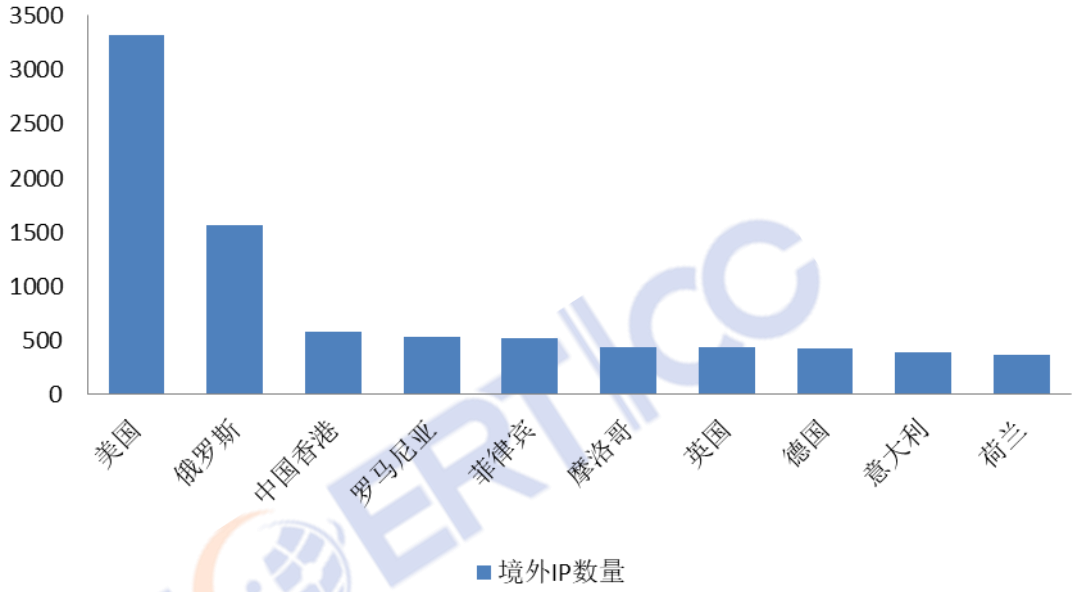

图 12 2018 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

2. 网站后门“攻击团伙”情况[20]

2018 年，CNCERT 监测发现，攻击活跃在 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，如图 13 所示。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。

[20]CNCERT 发布的《2018 年网站攻击态势及“攻击团伙”挖掘分析报告》

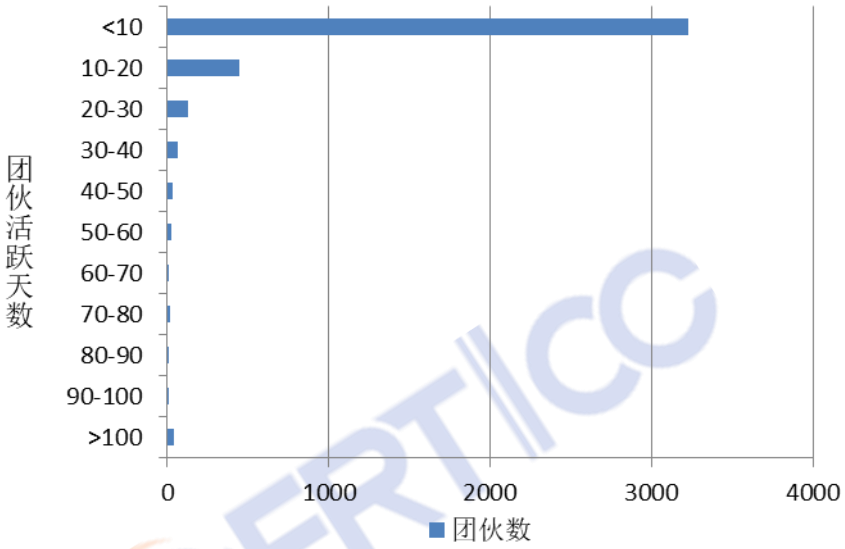

图 13 不同活跃天数的“攻击团伙”数量统计

（三）网页篡改

2018 年，CNCERT 监测发现我国境内遭篡改的网站有 7,049 个，较 2017 年的约 2 万个有大幅的下降，下降了 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 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比例为 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。

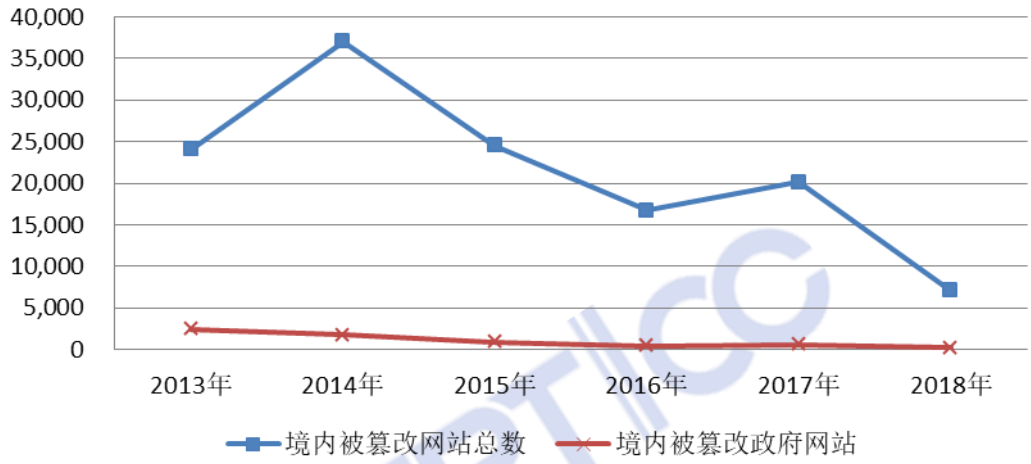

图 14 2013 年至 2018 年我国境内被篡改网站数量情况

五、工业互联网安全

（一）工业网络产品安全检测情况

为贯彻《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 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[21]。2018 年，CNCERT 使用该平台，对主流工控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 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 15 所示。利用这些漏洞，攻击者可使工控设备宕机，甚至获取设备控制权限，可能对其他工业

[21] ISASecure 是国际权威的工控安全认证体系，以标准覆盖面广、认证难度大而著称。目前全球仅有五款检测工具通过了其 CRT 工具认证，其它四款均为国外产品。

网络设备发起攻击。CNCERT 还分析发现，在电力设备测试中发现部分漏洞呈现同源性特征，经分析因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。

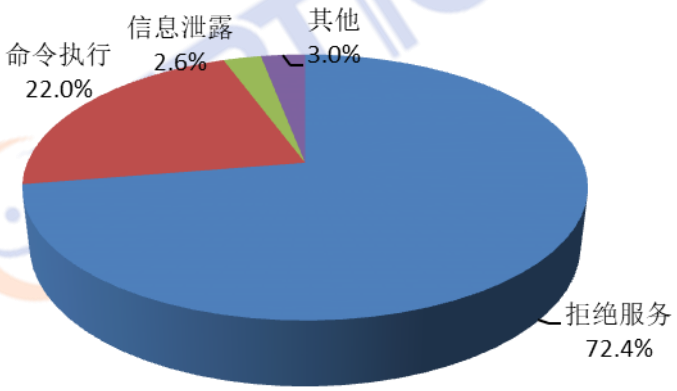

图 15 2018 年工业网络产品安全检测中发现的高危漏洞类型分布

（二）联网工业设备和工业云平台暴露情况

2018 年，CNCERT 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 4,451 万起，较 2017 年数量暴增约 17 倍；发现我国境内暴露的联网工业设备数量共计 6,020 个，涉及西门子、韦益可自控、罗克韦尔等 37 家国内外知名厂商产品，如图 16 所示，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 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，并监测发现根云、航天云网、COSMOPlat、OneNET、OceanConnect 等大型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。

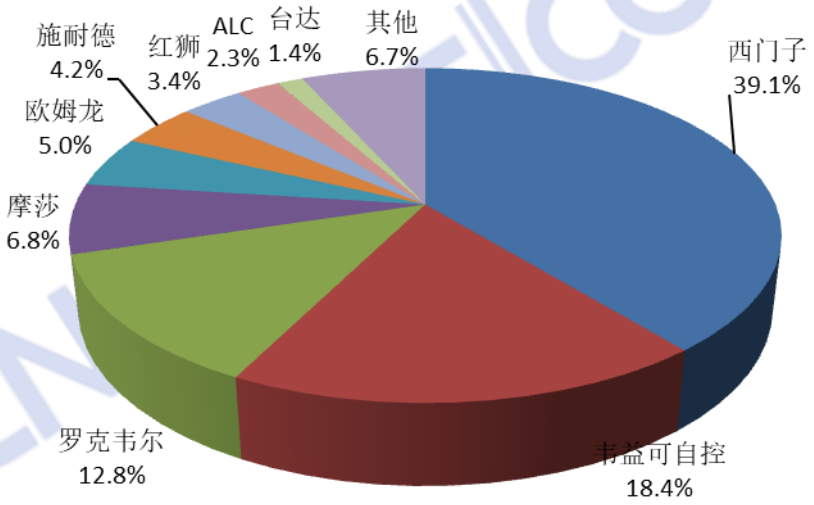

图 16 2018 年发现的联网工业设备厂商分布情况

(三) 重点行业远程巡检情况

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。为评估重要行业联网工业监控管理系统的网络安全风险情况，2018 年 CNCERT 对电力、城市公用工程、石油天然气三个行业开展了远程安全巡检工作，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 1,015 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 17 所示。同时，CNCERT 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境外恶意嗅探、网络攻击的情况。

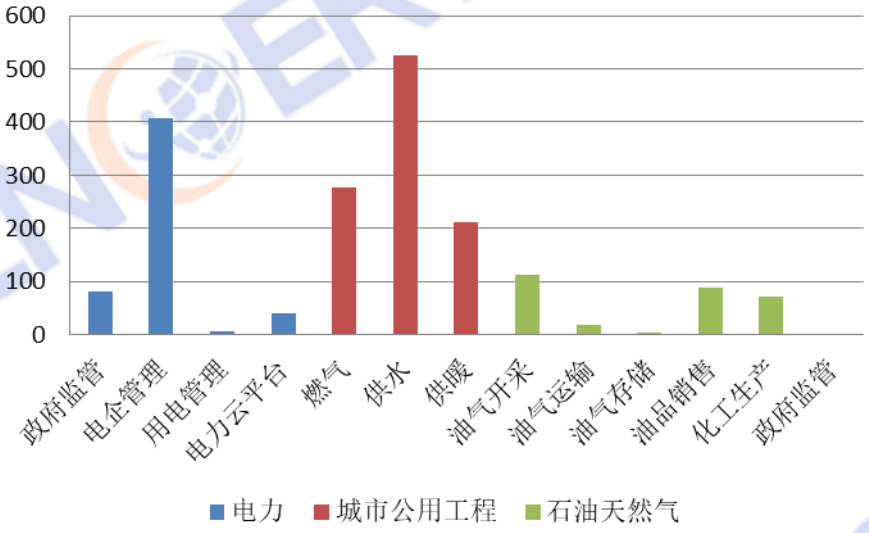

图 17 2018 年发现的重点行业联网监控管理系统分类

六、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 发挥技术优势，建设了国家互联网金融风险分析技术平台网络安全监测功能，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 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。

（一）互联网金融网站安全情况

2018 年，CNCERT 发现互联网金融网站的高危漏洞 1,700 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%）和远程代码执行漏洞 85 个（占比 5.0%），如图 18 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，互联网金融平台的网络安全防护能力有所加强，特别是规模较大的平台，但仍有部分平台安全防护能力不足，安全隐患较多，CNCERT 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 项。

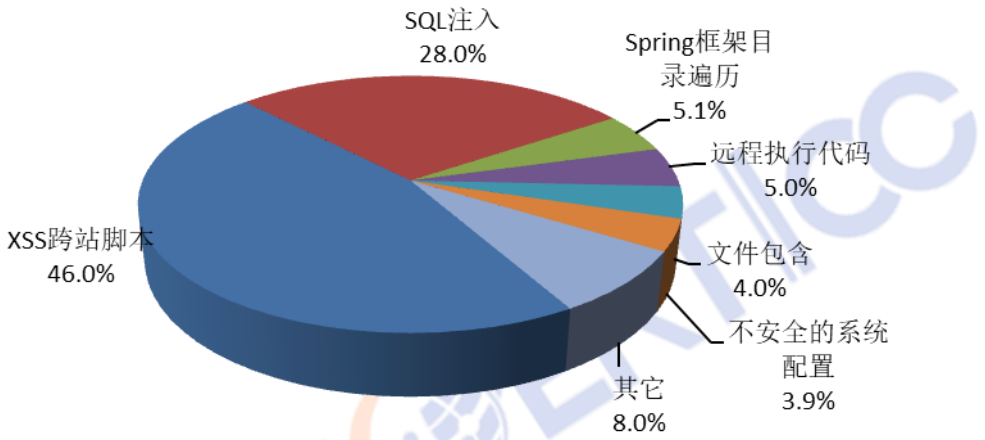

图 18 互联网金融网站高危漏洞分布情况

（二）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 对 430 个互联网金融 APP 进行检测，发现安全漏洞 1,005 个，其中高危漏洞 240 个，明文数据传输漏洞数量最多有 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%)和源代码反编译漏洞有 31 个(占 12.9%)，如图 19 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。

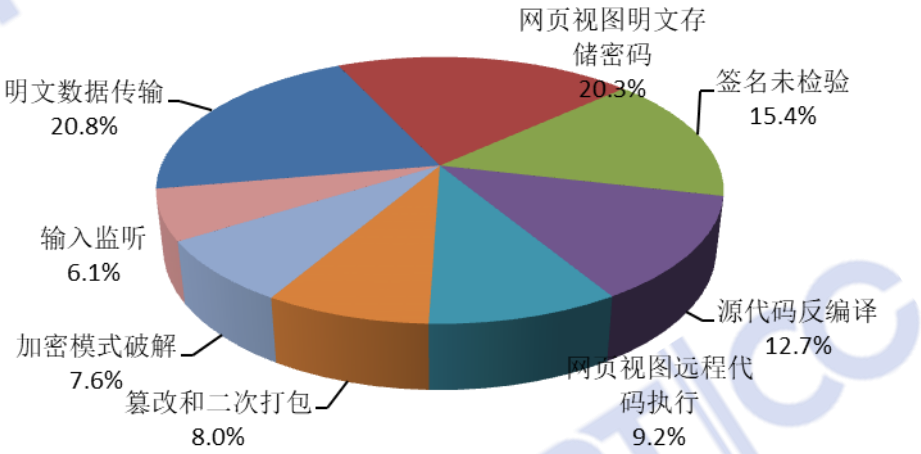

图 19 互联网金融移动 APP 高危漏洞分布情况

（三）区块链系统安全情况

伴随互联网金融的发展，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。首先，区块链系统往往自带金融属性，直接运行数字货币等资产；其次，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，一旦丢失或盗取无法找回；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。