2019 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

2020 年 4 月

目 录

前言

2019 年，我国云计算、大数据、物联网、工业互联网、人工智能等新技术新应用大规模发展，网络安全风险融合叠加并快速演变。互联网技术应用不断模糊物理世界和虚拟世界界限，对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战也不断增大，网络空间威胁和风险日益增多。比较突出的问题表现在 DDoS 攻击高发频发且攻击组织性与目的性更加凸显；APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗；事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻；数据安全防护意识依然薄弱，大规模数据泄露事件更加频发；“灰色”应用程序大量出现，针对重要行业安全威胁更加明显；网络黑产活动专业化、自动化程度不断提升，技术对抗更加激烈；工业控制系统产品安全问题依然突出，新技术应用带来新安全隐患更加严峻。

党的十八大以来，习近平总书记就网络安全和信息化工作提出了一系列新理念新思想新战略，系统阐述事关网信事业发展的一系列重大理论和实践问题，形成了关于网络强国的重要思想。2019 年，我国网络安全顶层设计不断完善，《中华人民共和国密码法》、《信息安全技术网络安全等级保护基本要求》（网络安全等级保护 2.0）等多项网络安全相关法律法规、配套制度及有关标准陆续向社会发布。中央网信办、工业和信息化部、公安部等多部门开展了网站安全、App 违法违规收集使用

个人信息、电信和互联网行业提升网络数据安全保护能力、“净网 2019”等专项行动，切实维护了网络空间秩序，网络安全综合治理能力水平不断提升。

本报告以宏观安全监测数据为基础，结合各类安全威胁和事件信息以及网络安全威胁治理实践成果，对 2019 年我国互联网网络安全状况进行了全面分析和总结，并对 2020 年网络安全趋势进行预测。

一、2019 年我国互联网网络安全状况

2019 年，在我国相关部门持续开展的网络安全威胁治理下，DDoS 攻击、APT 攻击、漏洞威胁、数据安全隐患、移动互联网恶意程序、网络黑灰产业、工业控制系统安全威胁总体下降，但呈现出许多新的特点，带来新的风险与挑战。

（一）党政机关、关键信息基础设施等重要单位防护能力显著增强，但 DDoS 攻击呈现高发频发态势，攻击组织性和目的性更加凸显。

1.可被利用实施 DDoS 攻击的境内攻击资源稳定性持续降低，数量逐年递减，攻击资源迁往境外，处置难度提高。

2019 年，国家互联网应急中心（以下简称“CNCERT”）通过《我国 DDoS 攻击资源月度分析报告》[①]定期公布 DDoS 攻击资源（控制端、被控端、反射服务器、伪造流量来源路由器等）并协调各单位处置。与 2018 年相比，境内控制端、反射服务器

[①]2019 年每月的报告可查看链接：https://www.cert.org.cn/publish/main/68/index.html

等资源按月变化速度加快、消亡率明显上升、新增率降低、可被利用的资源活跃时间和数量明显减少——每月可被利用的境内活跃控制端 IP 地址数量同比减少 15.0%、活跃反射服务器同比减少 34.0%。此外，CNCERT 持续跟踪 DDoS 攻击团伙情况，并配合公安部门治理取得了明显的效果。在治理行动的持续高压下，DDoS 攻击资源大量向境外迁移，DDoS 攻击的控制端数量和来自境外的反射攻击流量的占比均超过 90.0%。攻击我国目标的大规模 DDoS 事件中，来自境外的流量占比超过 50.0%。

2.针对党政机关、关键信息基础设施等重要单位发动攻击的组织性、目的性更加明显，同时重要单位的防护能力也显著加强。

2019 年，我国党政机关、关键信息基础设施运营单位的信息系统频繁遭受 DDoS 攻击，大部分单位通过部署防护设备或购买云防护服务等措施加强自身防护能力。CNCERT 跟踪发现的某黑客组织 2019 年对我国 300 余家政府网站发起了 1000 余次 DDoS 攻击，在初期其攻击可导致 80.0%以上的攻击目标网站正常服务受到不同程度影响，但后期其攻击已无法对攻击目标网站带来实质伤害，说明被攻击单位的防护能力已得到大幅提升。

3.DDoS 攻击依然呈现高发频发之势，仍有大量物联网设备被入侵控制后用于发动 DDoS 攻击。

我国发生攻击流量峰值超过 10Gbps 的大流量攻击事件日

均约 220 起，同比增加 40.0%；由于我国加大对 Mirai、Gafgyt 等物联网僵尸网络控制端的治理力度，2019 年物联网僵尸网络控制端消亡速度加快、活跃时间普遍较短，难以形成较大的控制规模，Mirai、Gafgyt 等恶意程序控制端 IP 地址日均活跃数量呈现下降态势，单个 IP 地址活跃时间在 3 日以下的占比超过 60.0%，因此，物联网设备参与 DDoS 攻击活跃度在 2019 年后期也呈下降走势。尽管如此，在监测发现的僵尸网络控制端中，物联网僵尸网络控制端数量占比仍超过 54.0%，其参与发起的 DDoS 攻击的次数占比也超过 50.0%。未来将有更多的物联网设备接入网络，如果其安全性不能提高，必然会给网络安全防御和治理带来更多困难。

（二）APT 攻击监测与应急处置力度加大，钓鱼邮件防范意识继续提升，但 APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗。

1.投递高诱惑性钓鱼邮件是大部分 APT 组织常用技术手段，我国重要行业部门对钓鱼邮件防范意识不断提高。

2019 年，CNCERT 监测到重要党政机关部门遭受钓鱼邮件攻击数量达 50 多万次，月均 4.6 万封，其中携带漏洞利用恶意代码的 Office 文档成为主要载荷，主要利用的漏洞包括 CVE-2017-8570 和 CVE-2017-11882 等。例如“海莲花”组织利用境外代理服务器为跳板，持续对我国党政机关和重要行业发起钓鱼邮件攻击，被攻击单位涉及数十个重要行业、近百个单

位和数百个目标。随着近年来 APT 攻击手段的不断披露和网络安全知识的宣传普及，我国重要行业部门对钓鱼邮件防范意识不断提高。比对钓鱼邮件攻击目标与最终被控目标，大约 90.0%以上的鱼叉钓鱼邮件可以被用户识别发现。

2.攻击领域逐渐由党政机关、科研院所向各重要行业领域渗透。

2019 年，我国持续遭受来自“方程式组织”、“APT28”、“蔓灵花”、“海莲花”、“黑店”、“白金”等 30 余个 APT 组织的网络窃密攻击，国家网络空间安全受到严重威胁。境外 APT 组织不仅攻击我国党政机关、国防军工和科研院所，还进一步向军民融合、“一带一路”、基础行业、物联网和供应链等领域扩展延伸，通信、外交、能源、商务、金融、军工、海洋等领域成为境外 APT 组织重点攻击对象。

3.APT 攻击在我国重大活动和敏感时期更为猖獗频繁。

境外 APT 组织习惯使用当下热点时事或与攻击目标工作相关的内容作为邮件主题，特别是瞄准我国重要攻击目标，持续反复进行渗透和横向扩展攻击，并在我国重大活动和敏感时期异常活跃。“蔓灵花”组织就重点围绕我国 2019 年全国“两会”、新中国成立 70 周年等重大活动，大幅扩充攻击窃密武器库，利用了数十个邮箱发送钓鱼邮件，攻击了近百个目标，向多台重要主机植入了攻击窃密武器，对我国党政机关、能源机构等重要信息系统实施大规模定向攻击。

（三）重大安全漏洞应对能力不断强化，但事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻。

1.我国漏洞信息共享与通报处置工作持续加强，漏洞应急工作开展卓有成效。

2019 年，国家信息安全漏洞共享平台（CNVD）[②]联合国内产品厂商、网络安全企业、科研机构、个人白帽子，共同完成对约 3.2 万起漏洞事件的验证、通报和处置工作，同比上涨 56.0%; 主要完成对微软操作系统远程桌面服务(以下简称“RDP 系统”）远程代码执行漏洞、Weblogic WLS 组件反序列化零日漏洞、ElasticSearch 数据库未授权访问漏洞等 38 起重大风险的应急响应，数量较上年上升 21%。CNVD 联合各支撑单位积极应对上述漏洞威胁，开展技术分析研判、影响范围探测和安全公告发布等应急工作，并第一时间向涉事单位通报漏洞，协调相关方对漏洞及时进行修复和处置。同时，及时公开发布 26 份影响范围广、需终端用户修复的重大安全漏洞通报，使社会公众及时了解漏洞危害，有效化解信息安全漏洞带来的网络安全威胁。

[②]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。

2.漏洞数量和影响范围仍然大幅增加，漏洞消控工作依然任重而道远。

一是披露的通用软硬件漏洞数量持续增长，且影响面大、范围广。2019 年，CNVD 新收录通用软硬件漏洞数量创下历史新高，达 16,193 个，同比增长 14.0%。这些漏洞影响范围从传统互联网到移动互联网，从操作系统、办公自动化系统（OA）等软件到 VPN 设备、家用路由器等网络硬件设备，以及芯片、SIM 卡等底层硬件，广泛影响我国基础软硬件安全及其上的应用安全——以微软 RDP 系统远程代码执行漏洞为例，位于我国境内的 RDP 系统（IP 地址）规模就高达 193.0 万个，其中大约有 34.9 万个系统（IP 地址）受此漏洞影响。此外，移动互联网行业安全漏洞数量持续增长，2019 年，CNVD 共收录移动互联网行业漏洞 1,324 个，较 2018 年同期 1,165 个增加了 13.7%，包括智能终端蓝牙通信协议、智能终端操作系统、App 客户端应用程序、物联网设备等均被曝光存在安全漏洞。

二是 2019 年我国事件型漏洞数量大幅上升。CNVD 接收的事件型漏洞数量约 14.1 万条，首次突破 10 万条，较 2018 年同比大幅增长 227%。这些事件型漏洞涉及的信息系统大部分属于在线联网系统，一旦漏洞被公开或曝光，如未及时修复，易遭不法分子利用进行窃取信息、植入后门、篡改网页等攻击操作，甚至成为地下黑产进行非法交易的“货物”。

三是高危零日漏洞占比增大。近 5 年来，“零日”漏洞[③]收录数量持续走高，年均增长率达 47.5%。2019 年收录的“零日”漏洞数量继续增长，占总收录漏洞数量的 35.2%，同比增长 6.0%。这些漏洞在披露时尚未发布补丁或相应的应急措施，严重威胁我国网络空间安全。

（四）数据风险监测与预警防护能力提升，但数据安全防护意识依然薄弱，大规模数据泄露事件频发。

1.数据安全保护力度继续加强，及时处置应对大量数据安全事件。

当前，互联网上数据资源已经成为国家重要战略资源和新生产要素，对经济发展、国家治理、社会管理、人民生活都产生重大影响。2019 年，在中央网信办指导下，CNCERT 加强监测发现、协调处置，全年累计发现我国重要数据泄露风险与事件 3000 余起，支撑中央网信办重点对其中 400 余起存储有重要数据或大量公民个人信息数据的事件进行了应急处置。MongoDB、ElasticSearch、SQL Server、MySQL、Redis 等主流数据库的弱口令漏洞、未授权访问漏洞导致数据泄露，成为 2019 年数据泄露风险与事件的突出特点。

2.App 违法违规收集使用个人信息治理持续推进，工作取得积极成效。

针对 App 违法违规收集使用个人信息问题，中央网信

[③] “零日”漏洞是指 CNVD 收录该漏洞时还未公布补丁。

办会同工业和信息化部、公安部、国家市场监督管理总局四部委联合开展 App 违法违规收集使用个人信息专项治理，成立专项治理工作组，制定发布《App 违法违规收集使用个人信息行为认定方法》《App 违法违规收集使用个人信息自评估指南》《互联网个人信息安全保护指南》；建立公众举报受理渠道，截至 2019 年 12 月，共受理网民有效举报信息 1.2 万余条，核验问题 App 2,300 余款；组织四部门推荐的 14 家专家技术评估机构对 1000 余款常用重点 App 进行了深度评估，发现大量强制授权、过度索权、超范围收集个人信息问题，对于问题严重且不及时整改的依法予以公开曝光或下架处理。

3.涉及公民个人信息的数据库数据安全事件频发，违法交易藏入“暗网”。

2019 年针对数据库的密码暴力破解攻击次数日均超过百亿次，数据泄露、非法售卖等事件层出不穷，数据安全与个人隐私面临严重挑战。科技公司、电商平台等信息技术服务类行业，银行、保险等金融行业以及医疗卫生、交通运输、教育求职等重要行业涉及公民个人信息的数据库数据安全事件频发。国内多家企业上亿份用户简历、智能家居公司过亿条涉及用户相关信息等大规模数据泄露事件在网上相继曝光。此外，部分不法分子已将数据非法交易转移至暗网，暗网已成为数据非法交易的重要渠道，涉及银行、证券、网贷等金融行业数据非

法售卖事件最多占比达 34.3%，党政机关、教育、各主流电商平台等行业数据被非法售卖事件也时有发生。目前我国正在积极推进数据安全管理和个人信息保护立法，但我国数据安全防护水平有待加强，公民个人信息防护意识需进一步提升。

（五）恶意程序增量首次下降，但“灰色”应用程序大量出现，针对重要行业安全威胁更加明显。

1.移动互联网恶意程序增量首次出现下降，高危恶意程序的生存空间正在压缩，下架恶意程序数量连续 6 年下降。

2019 年，新增移动互联网恶意程序数量 279 万余个，同比减少 1.4%。根据十四年来的监测统计，移动互联网恶意程序新增数量在经历快速增长期、爆发式增长期后，现已进入缓速增长期，并在 2019 年新增数量首次出现下降趋势，2019 年出现的移动恶意程序主要集中在 Android 平台，根据《移动互联网恶意程序描述格式》（YDT2439-2012）行业标准对恶意程序的行为属性进行统计，具有流氓行为、资费消耗等低危恶意行为的 App 数量占 69.3%，具有远程控制、恶意扣费等高危恶意行为的 App 数量占 10.6%。为从源头治理移动互联网恶意程序，有效切断传播源，CNCERT 着重处理协调国内已备案的 App 传播渠道开展恶意 App 下架工作，2019 年共处理协调 152 个应用商店、86 个广告平台、63 个个人网站、19 个云平台共 320 个传播渠道下架 App 总计 3,057 个，相较 2014 年到 2018 年期间

下架数量 3.9 万个、1.7 万个、0.9 万个、0.8 万个、3,578 个，连续六年呈逐年下降趋势，移动互联网总体安全状况不断好转。

2.以移动互联网仿冒 App 为代表的灰色应用大量出现，主要针对金融、交通、电信等重要行业的用户。

近年来，随着《网络安全法》《移动互联网应用程序信息服务管理规定》等法律、法规、行业与技术标准的相继出台，我国加大了对应用商店、应用程序的安全管理力度。应用商店对上架 App 的开发者进行实名审核，对 App 进行安全检测和内容版权审核等，使得黑产从业人员通过应用商店传播恶意 App 的难度明显增加，但能够逃避监管并实现不良目的的“擦边球”式的灰色应用有所增长。例如：具有钓鱼目的、欺诈行为的仿冒 App 成为黑产从业者重点采用的工具，持续对金融、交通、电信等重要行业的用户形成了较大威胁。2019 年，CNCERT 通过自主监测和投诉举报方式捕获大量新出现的仿冒 App。这些仿冒 App 具有容易复制、版本更新频繁、蹭热点快速传播等特点，主要集中在仿冒公检法、银行、社交软件、支付软件、抢票软件等热门应用上，在仿冒方式上以仿冒名称、图标、页面等内容为主，具有很强的欺骗性。针对银行信用卡优惠、办卡等银行类 App 的仿冒数量最多，其次是仿冒“最高人民法院”、“公安部案件查询系统”、“最高人民检察院”等政务类 App，以及仿冒“微信”、“支付宝”、“银联”等社交软件或支付软件。另外还有部分仿冒 App 在一些特殊时期频繁活跃，例如春运期

间出现了大量仿冒“12306”、“智行火车票”的 App，在“个人所得税”App 推出期间出现了大量仿冒应用。目前，由于开发者在应用商店申请 App 上架前，需提交软件著作权等证明材料，因此仿冒 App 很难在应用商店上架，其流通渠道主要集中在网盘、云盘、广告平台等线上传播渠道。

（六）黑产资源得到有效清理，但恶意注册、网络赌博、勒索病毒、挖矿病毒等依然活跃，高强度技术对抗更加激烈。

1.网络黑产打击取得阶段性成果。

在相关部门指导下，2019 年 CNCERT 依托中国互联网网络安全威胁治理联盟（CCTGA），加强信息共享，支撑有关部门开展网络黑产治理工作，互联网黑产资源得到有效清理。每月活跃“黑卡”总数从约 500 万个逐步下降到约 200 万个，降幅超过 60.0%。2019 年底，用于浏览器主页劫持的恶意程序月新增数量由 65 款降至 16 款，降幅超过 75%；被植入赌博暗链的网站数量从 1 万余个大幅下降到不超过 1 千个，互联网黑产违法犯罪活动得到有力打击。公安机关在“净网 2019”行动中，关掉各类黑产公司 210 余家，捣毁、关停买卖手机短信验证码或帮助网络账号恶意注册的网络接码平台 40 余个，抓获犯罪嫌疑人 1.4 万余名，“黑卡”、“黑号”等黑色产业链条遭到重创，犯罪分子受到极大震慑。

2.网络黑产活动专业化、自动化程度不断提升，技术对抗越发激烈。

2019 年，CNCERT 监测发现各类黑产平台超过 500 个，提供手机号资源的接码平台、提供 IP 地址的秒拨平台、提供支付功能的第四方支付平台和跑分平台、专门进行账号售卖的发卡平台、专门用于赌博网站推广的广告联盟等各类专业黑产平台不断产生。专业化的黑产活动为网络诈骗等网络犯罪活动提供了帮助和支持，加速了网络犯罪的蔓延趋势。例如在“杀猪盘”等网盘诈骗犯罪中，犯罪分子通过个人信息售卖方式获取精准个人信息，从而了解目标人群的爱好特点；通过恶意注册黑产购买社交账号，这些社交账号经过“养号”，具备完整的社交信息，极具迷惑性；通过黑产工具制作团队，快速开发赌博交友网站 App 等诈骗工具。与此同时，黑产自动化工具不断出现，黑产从业门槛逐步降低。网络黑产工具可自动化进行恶意注册、薅羊毛、刷量、改机等攻击，一般人员经简单学习后即可操作使用。各类专业的网络黑产平台通过 API 接口、易语言模块等方式，提供了标准化接口，网络黑产工具通过调用这些接口集成各类资源，用于网络黑产活动。2019 年监测到各类网络黑产攻击日均 70 万次，电商网站、视频直播、棋牌游戏等行业成为网络黑产的主要攻击对象，攻防博弈此消彼长。

3.勒索病毒、挖矿木马在黑色产业刺激下持续活跃。

在互联网黑色产业治理的推进过程中，2019 年，CNCERT

捕获勒索病毒 73.1 万余个，较 2018 年增长超过 4 倍，勒索病毒活跃程度持续居高不下。分析发现，勒索病毒攻击活动越发具有目标性，且以文件服务器、数据库等存有重要数据的服务器为首要目标，通常利用弱口令、高危漏洞、钓鱼邮件等作为攻击入侵的主要途径或方式。勒索攻击表现出越来越强的针对性，攻击者针对一些有价值的特定单位目标进行攻击，利用较长时期的探测、扫描、暴力破解、尝试攻击等方式，进入目标单位服务器，再通过漏洞工具或黑客工具获取内部网络计算机账号密码实现在内部网络横向移动，攻陷并加密更多的服务器。勒索病毒 GandCrab 的“商业成功”[④]引爆互联网地下黑灰产，进一步刺激互联网地下黑灰产组织对勒索病毒的制作、分发和攻击技术的快速迭代更新。GandCrab、Sodinokibi、GlobeImposter、CrySiS、Stop 等勒索病毒成为 2019 年最为活跃的勒索病毒家族，其中 CrySiS 勒索病毒全年出现了上百个变种。随着 2019 年下半年加密货币价格持续走高，挖矿木马更加活跃。“永恒之蓝”下载器木马、WannaMiner、BuleHero 等挖矿团伙频繁推出挖矿木马变种，并利用各类安全漏洞、僵尸网络、网盘等进行快速扩散传播，WannaMine、Xmrig、CoinMiner 等成为 2019 年最为流行的挖矿木马家族。

[④]2019 年 6 月，勒索病毒 GandCrab 运营者称在一年半的时间内获利 20 亿美元，并发表官方声明称该勒索病毒将停止更新。

（七）工业控制系统网络安全在国家层面顶层设计进一步完善,但工业控制系统产品安全问题依然突出，新技术应用带来新安全隐患更加严峻。

1.国家层面工业控制系统网络安全顶层设计不断完善,国家级工业控制系统网络安全监测和态势感知能力不断提升。

网络安全等级保护制度 2.0 版相关的国家标准正式发布，并正式将工业控制系统纳入到网络安全等级保护的范围，并出台了相应的测评要求。工业和信息化部联合教育部、应急管理部、国有资产监督管理委员会等十部委共同印发了《加强工业互联网安全工作的指导意见》，从工业互联网中设备、控制、网络、平台、数据等关键要素出发，提出了 17 项工作任务和 4 项保障措施，有力增强了对于工业互联网安全的政策指导。工业和信息化部于 2018 年、2019 年相继发布工业互联网创新发展工程项目，面向网络安全态势感知、威胁情报、公共服务等方向，建设“国家、地方、企业”三级联动的工业互联网网络安全保障技术平台。CNCERT 在积极参与相关平台建设的同时，着力打造面向互联网侧的工业控制系统威胁监测能力，面向重点行业联网工业控制设备、系统，以及工业云平台等核心网络资产开展全天候的实时监测和态势分析。

2.工业控制系统产品漏洞数量居高不下。

工业控制产品广泛应用于能源、电力、交通等关键信息基础设施领域，其安全性关乎经济社会的稳定运行。根据国内外

主流漏洞平台的最新统计，2019 年收录的工业控制产品漏洞数量依然居高不下且多为高中危漏洞，说明工业控制产品的网络安全状况依然严峻。随着国家监管部门和关键信息基础设施运营单位对网络安全重视程度的不断提高，以及相关配套法规和安全检测工作的开展，工业领域的网络安全意识有所增强，工业控制产品由于软件代码缺陷所导致的安全漏洞在被大量曝光的同时也在逐步得到修复、呈向好趋势。由于有些产品需要考虑现行标准和原有产品的兼容性，在一定程度上制约了厂商在安全设计上的缺失，如有的产品设计缺少身份鉴别、访问控制等最基本的安全元素，导致安全缺陷与漏洞数量居高不下，此类问题需引起有关部门的高度关注。

3.互联网侧暴露面持续扩大，新技术的应用给工业控制系统带来了新的安全隐患。

随着工业互联网产业的不断发展，工业企业上云、工业产业链上下游协同显著增强，越来越多的工业行业的设备、系统暴露在互联网上。例如，2019 年监测发现的暴露在互联网上的可编程逻辑控制器（以下简称“PLC”）高达 2,583 台，同比增加 8.7%。标识解析、5G、工业物联网等新技术的应用为智能工业赋能，但也将带来信息爆炸、数据泄露等安全隐患，以及海量智能设备的接入和认证管理等安全问题。在标识解析技术应用上，工业和信息化部发布《工业互联网发展行动计划（2018-2020 年）》提出“标识解析体系构建行动”的发展目标，

表示标识解析系统作为一个重要的网络基础设施，将在架构、协议、数据、运营等多个层面均存在网络安全风险，直接关乎工业互联网的安全运行。在 5G 技术应用上，工业和信息化部印发《“5G+工业互联网”512 工程推进方案》，提出将促进 5G 技术与 PLC、分布式控制系统（DCS）等工业控制系统的融合创新，培育“5G+工业互联网”特色产业。5G 技术方案的高速率、大容量、低延时的特性所带来的大流量数据对于传统网络安全监测分析技术将带来巨大的挑战。在工业物联网应用上，大量物联网设备应用在工业领域，涉及智能网关、摄像头、门禁、打印机等多种设备类型，由于物联网设备接入方式灵活、分布位置广泛，其应用打破了工业控制系统的封闭性，带来了新的安全隐患。

二、2020 年网络安全关注方向预测

预计 2020 年，我国更多网络安全政策法规与治理措施将陆续出台实施，网络安全治理力度将进一步加大，但网络空间也将面临一些新问题与新挑战。2020 年值得关注的网络安全方向如下:

（一）规模性、破坏性急剧上升成为有组织网络攻击新特点

随着国际局势渐趋复杂，有组织的网络攻击出于政治目的发起的网络攻击行动持续高发。近年来，针对我国发起的 APT 攻击事件持续曝光，攻击规模和烈度逐年递增，攻击目标涉及

国计民生的重要部门和行业。此外，常在敏感时间节点发起有针对性的攻击渗透以最大程度博取政治利益。在当前全球贸易疲弱、经济下行压力持续背景下，国际间摩擦将从经贸领域逐渐扩散至更多领域，网络攻击作为以小博大的非常规手段将受到各方面势力的高度关注，有组织网络攻击的规模性、破坏性恐将急剧上升。面对愈加严峻的有组织有目的网络攻击形势，各单位难以独立应对，应加强数据情报互通、监测手段互补等方面的能力建设，构建网络安全一体化防护机制，共同应对新的高级网络攻击威胁。

（二）体系化协同防护将成关键信息基础设施网络安全保障新趋势

政府机关、能源、金融、交通、通信等重要行业领域关键信息基础设施的网络安全状况日趋严峻。2019 年，境外陆续发生多起电力系统遭漏洞攻击或加密勒索攻击的恶性事件，引发城市大范围停电，严重影响了当地经济社会正常运转。在 5G 网络加快覆盖的大背景下，关键信息基础设施暴露在互联网上的情况持续增多。由于承载服务、信息的高价值性，预计在 2020 年，针对关键信息基础设施的网络窃密、远程破坏攻击、勒索攻击会持续增加。除利用安全漏洞、弱口令等常见方式实施攻击外，通过软硬件供应链、承载服务的云平台作为攻击途径的事件或呈上升趋势，关键信息基础设施的安全问题将受到强烈关注。随着《关键信息基础设施安全保护条例》的加快出台，

关键信息基础设施的认定以及各行业、部门、机构的职责愈加清晰。通过各方的共同应对和协同防护，我国关键信息基础设施网络安全评估、监测、防护体系将逐步建立。

（三）政策法规与执法监管多管齐下为数据安全和个人信息保护提供新指引

数据安全立法进程正加快推进，数据安全保护法律体系正在逐步建立，公民数据安全保护意识日渐增强。2019 年，国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》，出台了《儿童个人信息网络保护规定》，全国人大常委会正在制定《个人信息保护法》。中央网信办、工业和信息化部、公安部等监管部门日益提高执法监管力度，加大对违规采集和使用个人信息、泄露或售卖用户数据、侵害用户隐私权益的企业查处力度。但重要数据和个人信息泄露或滥用问题仍较为严重，存在个人信息滥用及不合理披露的情况，对公民个人生活造成影响。2020 年，在国家相关政策法规以及执法监管下，相关企业将落实主体责任，依托业务数据安全、安全运行维护等数据安全治理手段，逐步建立起制度化、体系化、规范化的数据安全管理机制，加快落实数据安全的合规性要求。

（四）精准网络勒索集中转向中小型企事业单位成为网络黑产新动向

自 2017 年 WannaCry 蠕虫病毒在全球范围爆发以来，勒索

软件进入了大众的视野。勒索攻击利用比特币等数字货币的匿名性，使得攻击者更容易隐藏其踪迹，追踪溯源难度较大，成为网络黑产的高发类型。近年来，勒索攻击的目标逐渐转向网络安全防护较为薄弱的中小型企事业单位。一些专业化的黑客组织出于非法牟取经济利益的目的，通过实施攻击渗透并植入勒索软件等方式，将单位内网中的重要网络资产和数据进行加密，使其日常业务工作无法开展，从而勒索大量赎金。从攻击手法来看，勒索软件逐渐呈现出专业性高、针对性强的特点，有向“泛 APT 攻击”发展的趋势。面对精准勒索攻击这一网络安全威胁，各单位应增强安全防护技术手段，提高员工防范意识和操作规范，加强对重要数据的加密和备份等工作。

（五）远程协同热度突增引发新兴业态网络安全风险新思考

2020 年初，全球突发新型冠状病毒感染的肺炎疫情，在其影响下，远程办公、医疗、教育等远程协同类的业态模式热度突增，大量传统行业也正加快转向通过互联网开展远程业务协作，随之而来的数据泄露、网络钓鱼、勒索病毒、网络诈骗等网络安全风险和威胁日益凸显。目前，我国已经发生多起通过办公电子邮件传播恶意软件，以及对在线教育平台发起 DDoS 攻击的事件。由于远程办公、医疗、教育涉及节点众多，应用环境复杂，包括网络接入环境、终端设备、数据存储、云平台、可信认证、密码强度等，若存在薄弱环节，可能引发网络远程

协同业态中的系统运行安全、网络边界安全、数据安全等方面的风险。预计 2020 年，针对远程协同类相关业态的网络安全风险和威胁将逐渐出现，引发更多对安全风险的关注。为应对新业态带来的潜在网络安全风险，各方需加强对远程协作加速应用过程中的安全监测和动态评估，及时、有效地应对可能出现的漏洞隐患、网络攻击，保障新业态的蓬勃稳定发展。

（六）5G 等新技术新应用大量涌现或面临网络安全新挑战

2019 年，5G 商用牌照正式发放、IPv6 网络流量快速增长、区块链技术助力金融发展等，这些新技术带来了新活力，新业务蓬勃发展。5G 技术与 IPv6 的特点决定两者必将产生深度融合，引发智能制造、车联网、智慧能源、远程协作、个人 AI 辅助等新技术、新应用、新业态不断涌现，然而对于给网络带来怎样的新威胁和风险，产生怎样的新攻击类型，采用怎样的防御应对手段等都亟待研究。在区块链技术方面，近年来区块链相关系统安全问题频繁暴露，“技术+金融”等新型攻击手段涌现，引起的安全事故损失高达上百亿美元，又由于区块链技术的匿名性和节点全球分布的特征，使用区块链数字资产做资金转移隐蔽性高，难以追溯和识别身份，为犯罪分子利用勒索病毒收取勒索资金等犯罪行为提供了便利。亟需深入研究区块链的安全风险，健全区块链系统级安全防护技术和安全评估手段，建立适应区块链分布式技术机制的安全保障体系。

三、对策建议

面对网络安全新形势、新挑战，我们应继续坚持以习近平新时代中国特色社会主义思想，特别是习近平总书记关于网络强国的重要思想为指导，坚持总体国家安全观、树立正确的网络安全观，加快网络安全技术创新、产业发展、人才培养、协同合作等全面发展，有效提高我国网络空间安全保障能力。

（一）强化关键信息基础设施保护

针对关键信息基础设施的有组织、有目的、高强度网络攻击愈加明显的趋势，建议我国加快出台关键信息基础设施安全保护相关法律法规，落实运营单位主体责任和保护部门的监管责任，统筹开展网络安全检查，强化网络安全态势感知，监测预警和应急处置能力建设，提升抵御网络攻击威胁的能力，构建我国网络空间安全一体化防护体系。工业控制系统作为我国关键信息基础设施的重要做成部分，广泛用于电力、石化、轨交、制造等诸多领域，随着物联网、5G、云计算、大数据等技术发展和广泛应用，工业控制系统正从专用、封闭状态逐步向通用、开放方向发展，建议进一步加强工业控制系统网络安全研究投入，构建面向新应用形态的高仿真工控系统实验环境，能够满足互联网新技术的融合并持续迭代升级，实现跨行业、跨领域的仿真环境互联互通与共建共用。

（二）提升数据安全管理和个人信息保护力度

建议加快个人信息保护、数据安全管理、个人信息出境安

全、儿童个人信息网络保护等数据安全和个人信息保护相关法律法规制定进程，完善国家数据安全和个人信息保护的法制体系，进一步提高全社会加强数据安全管理和个人信息保护意识。推动收集重要数据和个人信息的备案制度尽快落地，明确监管范围，建立通报体系，细化处罚措施，配备激励机制。同时，建立个人信息和重要数据安全监管技术体系，鼓励备案政企进行数据安全风险自评估，个人信息和重要数据出境安全评估，常态化开展数据安全检查评估，督促落实网络运营者主体责任。

（三）加快网络安全核心技术创新突破

建议加强网络安全核心技术攻关，建立健全我国网络空间安全一体化防护能力。强化威胁预测，开展网络安全未知威胁检测技术研究，利用机器学习、人工智能等新技术，提升海量流量中高级威胁线索发现水平，实现网络攻击事件的快速发现与场景还原。强化威胁感知，增强态势感知预测技术，基于大数据分析与宏观微观态势研判，实现对重大网络攻击事件的提前预警，及时做好防范与有效应对。强化威胁防御，构建网络攻击实时防御技术，实现监测体系与处置体系的实时联动，确保受到网络攻击时能第一时间高效处置。

（四）壮大网络安全技术产业规模和网络安全人才队伍

当前我国网络安全技术产业尚有较大发展空间，网络安全人才供给侧短缺。建议进一步优化网络安全技术产业的规划和整体布局，完善支持网络安全技术产业发展的政策措施，加快

推进我国网络安全产业高质量发展，培育一批具有国际竞争力的网络安全企业。同时，我国还需持之以恒抓好网络安全人才培养。加强网络空间安全学科专业建设，实施好一流网络安全学院建设示范项目，加快建设国家网络安全人才与创新基地，形成人才培养、技术创新、产业发展的良好生态。

（五）扩大国内外网络安全合作

当前，维护网络安全成为国际社会的共同责任。构建网络空间命运共同体，既是顺应信息时代发展潮流的必然选择，也是应对网络空间风险挑战的迫切需要。建议我国在巩固深化网络安全国内合作的同时，进一步扩大并深化网络安全国际合作。充分发挥政府、企业、科研院所、行业组织等各方作用，建立国家级、省级国内网络安全应急协作体系，面向行业建立网络安全漏洞、网络病毒、网络攻击活动等威胁情报共享与威胁治理技术平台和工作机制，形成国家、省（市、区）、行业有机联合的纵深防御体系，为提供有价值的威胁情报和畅通的治理通道。强化在网络安全技术、经验、标准等方面国际合作，推动构建开放合作的网络安全应急国际合作模式，加快推进与“一带一路”沿线等国家在网络安全领域交流合作。

结语

2019 年，我国网络安全防护水平得到全面提升，APT 攻击发现能力加强、漏洞修复进度加快、网站攻击应对能力提升、重要数据和个人信息保护全面得到重视，有力保障了新中国成

立 70 周年、第二届“一带一路”国际合作峰会等多项重要活动的顺利举办。与此同时，我们也注意到，区块链、人工智能、5G、IPv6 等新技术快速发展，基于这些新技术的互联网应用也将越来越普及。我们不仅要持续应对恶意程序、安全漏洞、DDoS 攻击等传统安全威胁，也需要积极研究新技术领域带来的网络安全新问题。

我们相信，在全社会的共同努力下，我国网络安全保障体系必将不断健全，网络安全能力水平必将不断提升，我们一定将会迎来更加清朗、安全的网络空间。

附件：2019 年我国互联网网络安全监测数据分析

为全面分析 2019 年我国互联网在恶意程序传播、漏洞风险、DDoS 攻击、网站安全等方面的具体情况，CNCERT 对全年监测数据进行了全面、系统分析，对攻击来源、攻击对象、攻击规模等进行了梳理，以更直观的方式展现我国网络安全现状。

（一）恶意程序

1.计算机恶意程序捕获情况

2019 年，全年捕获计算机恶意程序样本数量超过 6,200 万个，日均传播次数达 824 万余次，涉及计算机恶意程序家族 66 万余个。按照传播来源统计，位于境外的主要是来自美国、俄罗斯和加拿大等国家或地区，来自境外的具体分布如图 1 所示；位于境内的主要是浙江省、广东省和江苏省等省份。按照目标 IP 统计，我国境内受计算机恶意程序攻击的 IP 地址约 6,762 万个，约占我国 IP 总数的 18.3%，这些受攻击的 IP 地址主要集中在山东省、江苏省、浙江省、广东省等地区，2019 年我国受计算机恶意程序攻击的 IP 分布情况如图 2 所示。

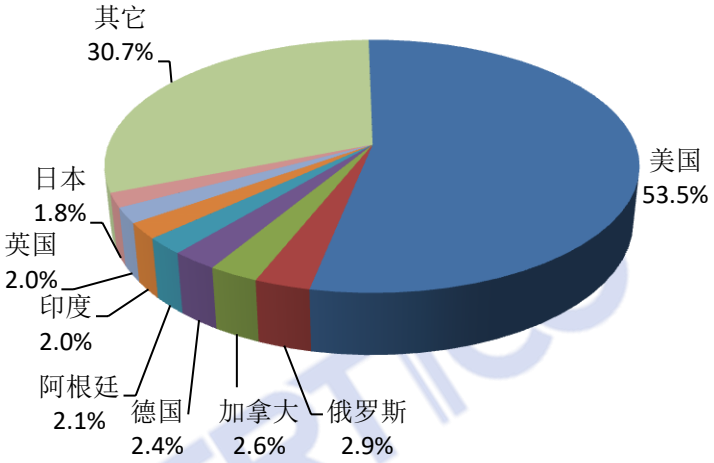

图 1 2019 年计算机恶意代码传播源位于境外分布情况

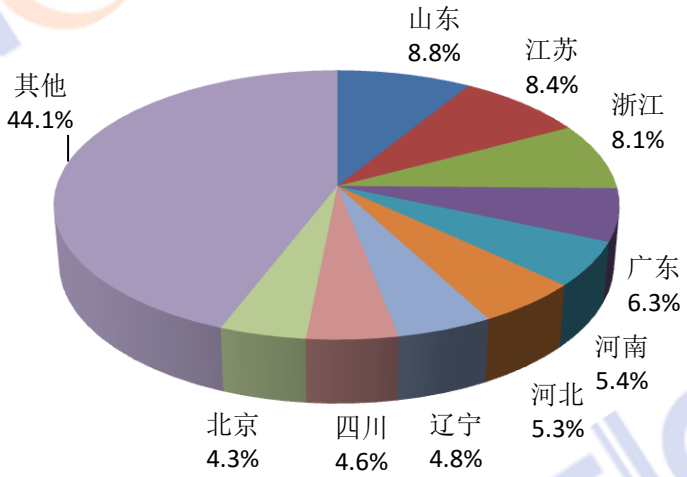

图 2 2019 年我国受计算机恶意代码攻击的 IP 分布情况

2.计算机恶意程序用户感染情况

2019 年，我国境内感染计算机恶意程序的主机数量约 582 万台，同比下降 11.3%，如图 3 所示。位于境外的约 5.6 万个计算机恶意程序控制服务器控制了我国境内约 552 万台主机，就控制服务器所属国家来看，位于美国、日本和中国香港的控制服务器数量分列前三位，分别是约 1.8 万个、5,883 个和 2,783

个，具体分布如图 4 所示；就所控制我国境内主机数量来看，位于美国、荷兰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 429 万、149 万和 95 万台主机，如图 5 所示。此外，根据 CNCERT 抽样监测数据，针对 IPv6 网络的攻击情况也开始出现，2019 年境外约 3,000 个 IPv6 地址的计算机恶意程序控制服务器控制了我国境内约 4.0 万台 IPv6 地址主机。

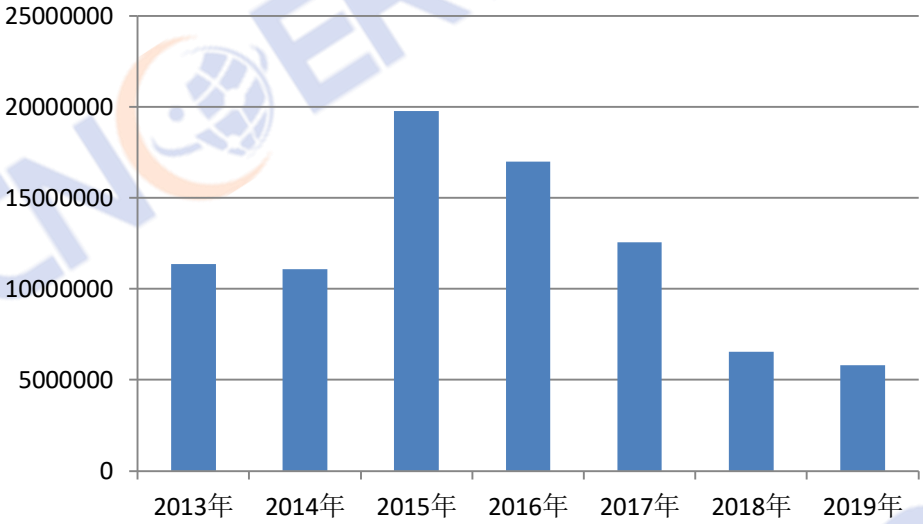

图 3 境内感染计算机恶意程序主机数量变化

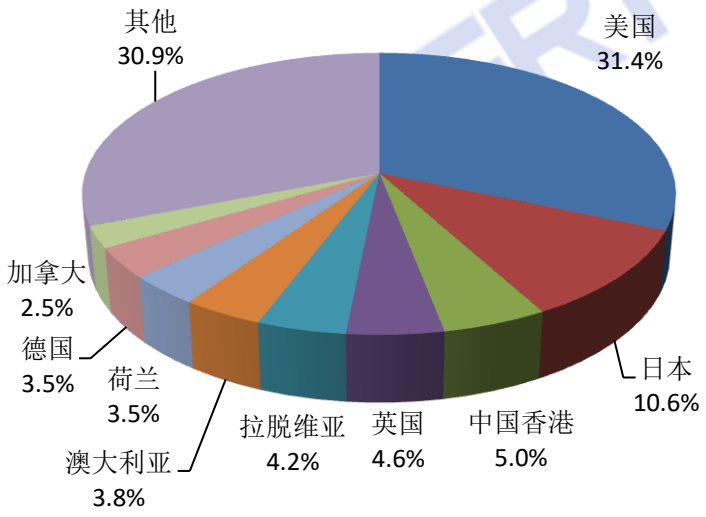

图 4 2019 年控制我国境内主机的境外木马和僵尸网络控制端分布

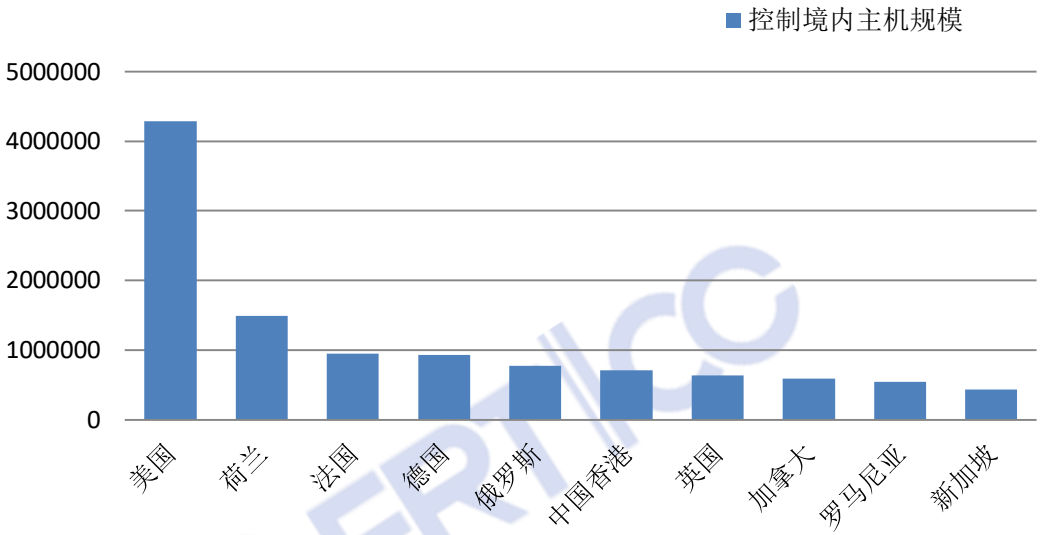

图 5 2019 年控制我国境内主机数量 TOP10 的国家或地区

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 11.3%）、江苏省（占 10.9%）、浙江省（占 10.7%）等省份，具体分布如图 6 所示。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 5,612 个，规模在 10 万台以上的僵尸网络数量达 39 个，如图 7 所示。2019 年，CNCERT 协调相关机构成功关闭 1,548 个控制规模较大的僵尸网络，有效控制计算机恶意程序感染主机引发的危害。

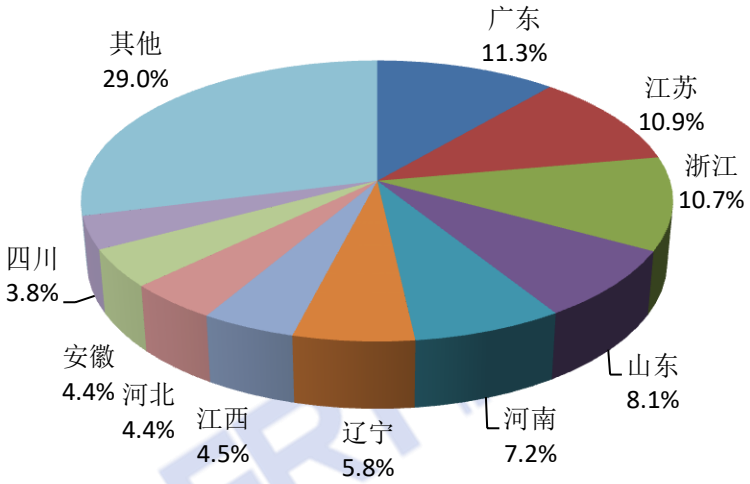

图 6 2019 年我国境内感染木马或僵尸程序的主机数量按地区分布

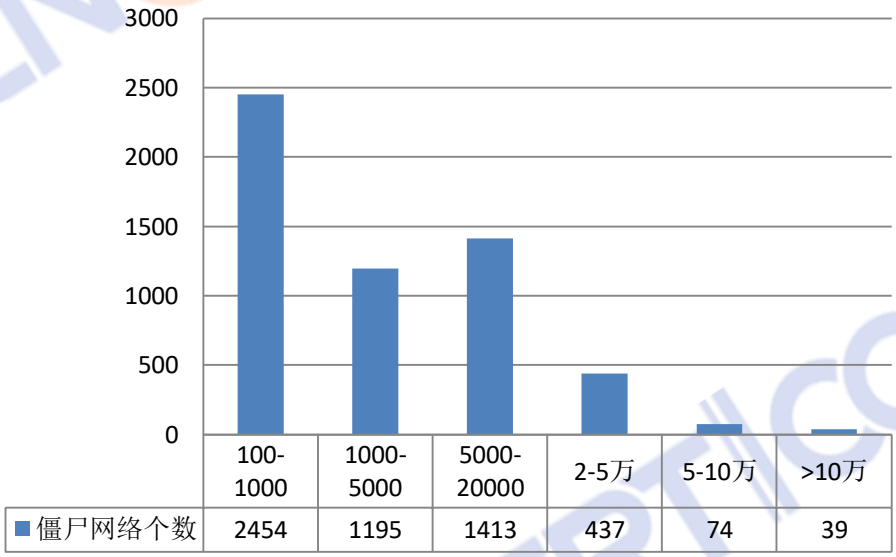

图 7 2019 年僵尸网络的规模分布

3.移动互联网恶意程序

2019 年，CNCERT 通过自主捕获和厂商交换新增获得移动互联网恶意程序数量 279 万余个，同比减少 1.4%，近五年来增速持续保持放缓，并首次出现增量下降，如图 8 所示。通过对恶意程序的恶意行为统计发现，排名前三的仍然是流氓行为类、资费消耗类和信息窃取类，占比分别为 36.1%、33.2%和 11.6%，

如图 9 所示。其中，流氓行为类、信息窃取类所占比例同比均有所减少。CNCERT 连续七年联合应用商店、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，2019 年累计协调国内 319 家提供移动应用程序下载服务的平台，下架 3,057 个移动互联网恶意程序，在有效防范移动互联网恶意程序危害、严格控制移动互联网恶意程序传播途径做出较大贡献。

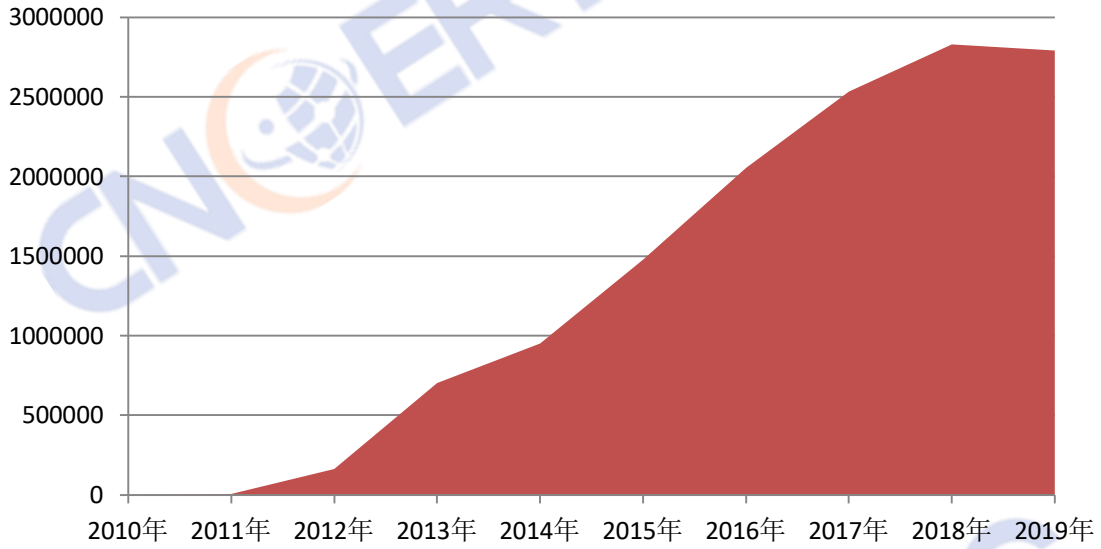

图 8 2010 年至 2019 年移动互联网恶意程序捕获数量走势

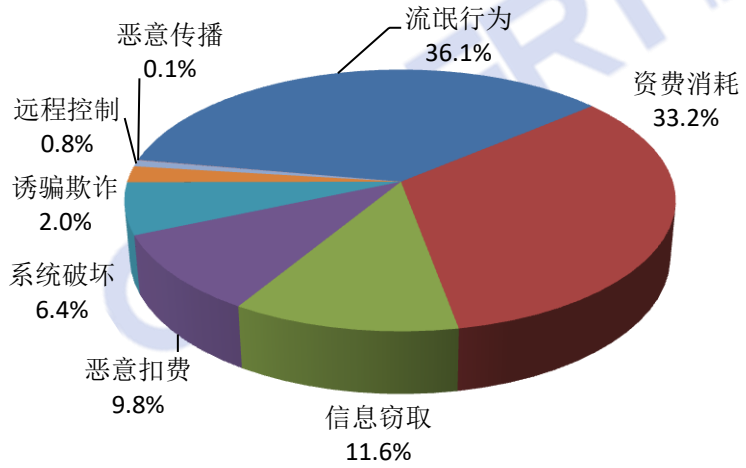

图 9 2019 年移动互联网恶意程序数量按行为属性统计

4.联网智能设备恶意程序

目前活跃在智能设备上的恶意程序家族超过 15 种，包括 Mirai、Gafgyt、Dofloo、Tsunami、Hajime、MrBlack 等。这些恶意程序一般通过漏洞、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，主要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。2019 年，CNCERT 捕获智能设备恶意程序样本约 324.1 万个，其中大部分属于 Mirai 家族和 Gafgyt 家族（占比 86.1%）。服务端传播源 IP 地址约 2.78 万个，其中绝大部分传播源 IP 位于境外（占比 79.9%），我国境内疑似受感染智能设备 IP 地址数量约 203.8 万个（同比上升 31.8%），主要位于浙江、江苏、山东、辽宁、河南等地，被控联网智能设备日均向 1,528 个目标发起 DDoS 攻击。

（二）安全漏洞

2019 年，国家信息安全漏洞共享平台（CNVD）收录安全漏洞数量创下历史新高，收录安全漏洞数量同比增长了 14.0%，共计 16,193 个，2013 年以来每年平均增长率为 12.7%。其中，高危漏洞收录数量为 4,877 个（占 30.1%），同比减少 0.4%，但“零日”漏洞收录数量持续走高，2019 年收录的安全漏洞数量中，“零日”漏洞收录数量占比 35.2%，达 5,706 个，同比增长 6.0%，如图 10 所示。安全漏洞主要涵盖的厂商或平台为谷歌

（Google）、WordPress、甲骨文（Oracle）等，如表 1 所示。按影响对象分类统计，排名前三的是应用程序漏洞（占 56.2%）、Web 应用漏洞（占 23.3%）、操作系统漏洞（占 10.3%），如图 11 所示。

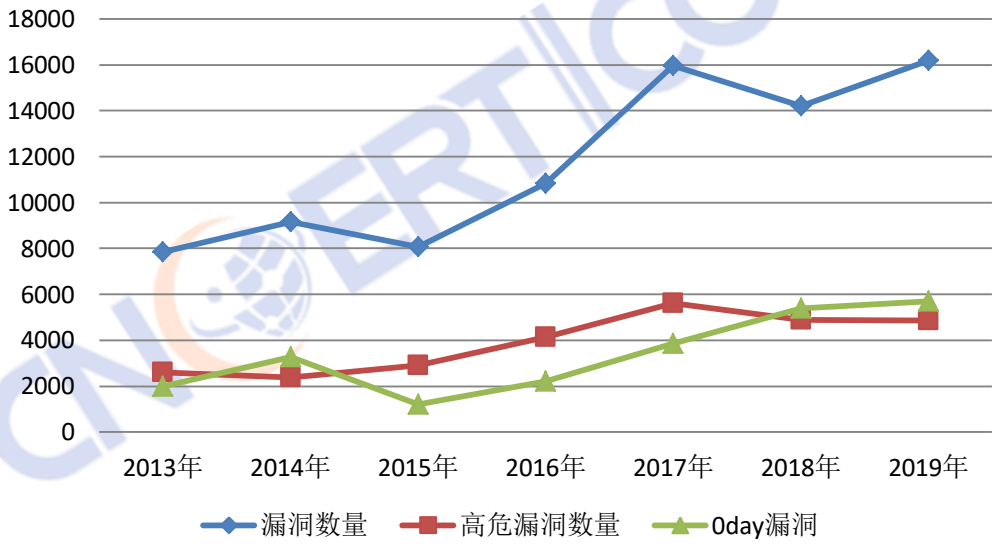

图 10 2013 年至 2019 年 CNVD 收录安全漏洞数量对比

表 1 2019 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	951	5.9%	37.2%
WordPress	888	5.5%	240.2%
Oracle	841	5.2%	74.8%
Adobe	618	3.8%	75.6%
Microsoft	616	3.8%	-7.6%
IBM	451	2.8%	-20.0%
Cisco	388	2.4%	-8.1%
CloudBees	307	1.9%	/
cPanel	271	1.7%	/
Linux	270	1.7%	39.9%
其他	10,592	65.4%	7.7%

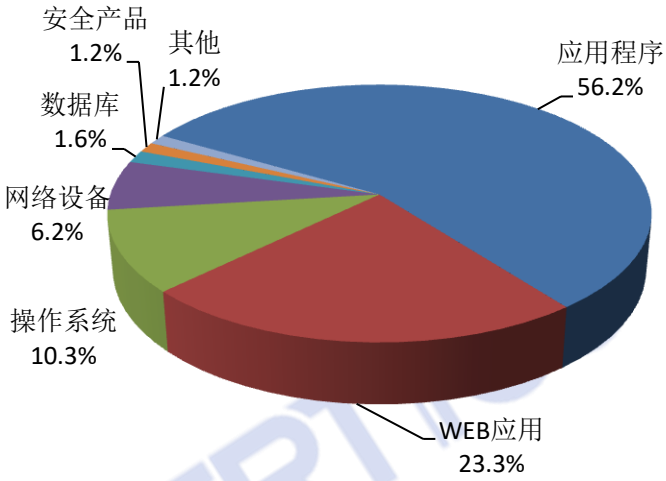

图 11 2019 年 CNVD 收录安全漏洞按影响对象分类统计

2019 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 1,214 个（占全年收录数量的 7.5%）、638 个（占 3.9%）、443 个（占 2.7%）和 131 个（占 0.8%），如图 12 所示。其中移动互联网子漏洞库收录数量持续增长，较 2018 年增长了 5.6%。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 2.9 万起，同比大幅增长 42.1%。

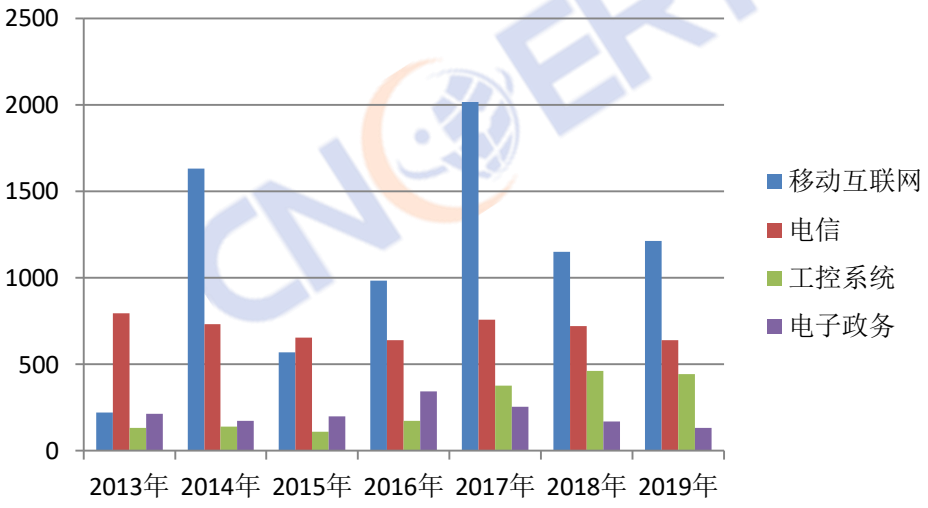

图 12 2013 年至 2019 年 CNVD 子漏洞库收录情况对比

（三）拒绝服务攻击

DDoS 攻击是难以防范的最常见网络攻击手段之一，2019 年仍然呈现高发频发之势，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）事件数量平均每日 220 起，同比增加 40%。

1.攻击资源活跃情况

2019 年，CNCERT 每月对用于发起 DDoS 攻击的攻击资源进行了持续分析，并联合基础电信企业和云服务提供商持续开展攻击资源治理工作，可被利用的资源稳定性降低，每月可利用的活跃资源数量控制在较低的水平。每月用于发起 DDoS 攻击的活跃 C&C 控制服务器数量平均 370 台，活跃的非法受控主机有 33 万台，反射攻击服务器约 203 万台，遭受大流量攻击的目标 IP 地址数量约 6,000 个。

2.来自境外攻击情况

2019 年，CNCERT 持续监测分析来自境外的 DDoS 攻击流量发现，境外攻击流量超过 10Gbps 的大流量攻击事件日均 120 余起；境外攻击的主要攻击方式是 UDP Flood、TCP SYN Flood、Memcached Amplification、NTP Amplification 和 DNS Amplification，这五种攻击占比达到 89%，为躲避溯源，黑客倾向于使用这些便于隐藏攻击源的攻击方式；98%境外攻击的攻击时长小于 30 分钟，DDoS 即服务模式兴起，攻击者越来越精细化的调度利用攻击资源，以对外提供更多服务；攻击目标

主要位于浙江、广东、江苏、山东、北京等经济较为发达的省市。

3.攻击团伙监测及打击情况

2019 年，CNCERT 持续监测和跟踪我国境内的大规模攻击团伙 16 个，并进行了对攻击资源的长效治理。特别是 2019 年 3 月份以来，支撑中央网信办、公安部开展了重要团伙的打击工作，在“净网 2019”专项行动中抓获违法犯罪嫌疑人 379 名，清理位于北京市的被控主机 7,268 台。据统计，专项打击期间，境内 DDoS 攻击控制端环比下降 30%，参与攻击信息系统环比下降 41%，境内 DDoS 攻击犯罪态势得到明显遏制[⑤]。

（四）网站安全

2019 年 5 月至 2019 年 12 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合开展了全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。为支撑做好相关工作，CNCERT 进一步扩大了我国网站监测范围，加强了网页仿冒、网站后门、网页篡改等网络攻击的监测能力。

1.网页仿冒

2019 年，监测发现约 8.5 万个针对我国境内网站的仿冒页面，页面数量较 2018 年增长了 59.7%。从承载仿冒页面 IP 地

[⑤]相关数据来自光明网 2019 年 12 月 16 日新闻报道《北京市公安局专项打击 DDoS 攻击类违法犯罪》。

址归属情况来看，绝大多数位于境外，主要分布在中国香港和美国，如图 13 所示。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 2.3 万余个。

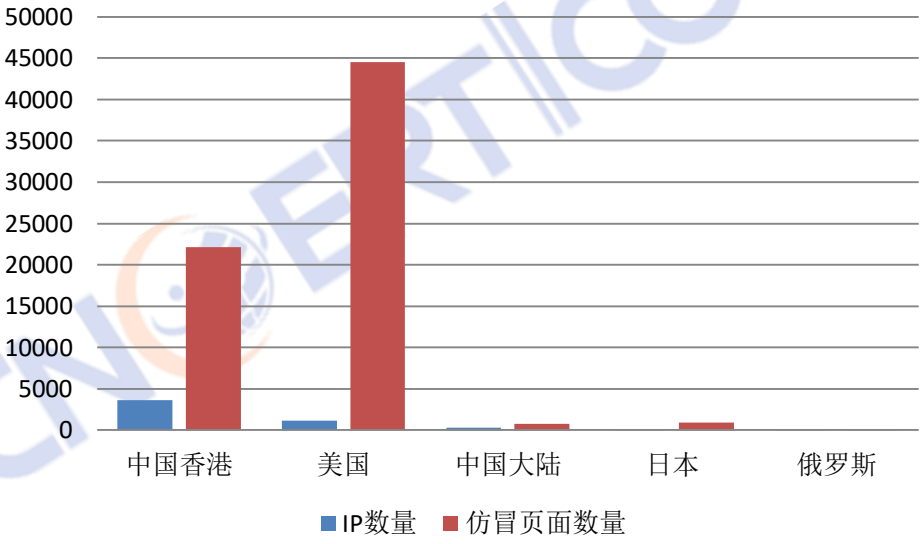

图 13 2019 年承载仿冒页面 IP 地址和仿冒页面数量分布

2.网站后门

2019 年，CNCERT 进一步提升了网站后门监测能力，监测到境内外约 4.5 万个 IP 地址对我国境内约 8.5 万个网站植入后门，我国境内被植入后门的网站数量较 2018 年增长超过 2.59 倍。其中，约有 4 万个境外 IP 地址（占全部 IP 地址总数的 90.9%）对境内约 8 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 33.5%，其次是位于英国和中国香港的 IP 地址，如图 14 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，有约 2.3 万个，其次是位于菲律宾和美国的 IP 地址，分别控制了我国境内约 2 万个和 1.8

万个网站。此外，随着我国 IPv6 规模部署工作加速推进，支持 IPv6 的网站范围不断扩大。2019 年，根据 CNCERT 监测数据显示，攻击源、攻击目标为 IPv6 地址的网站后门事件有 2,262 起，共涉及攻击源 IPv6 地址 131 个、被攻击的 IPv6 地址解析网站域名 66 个。

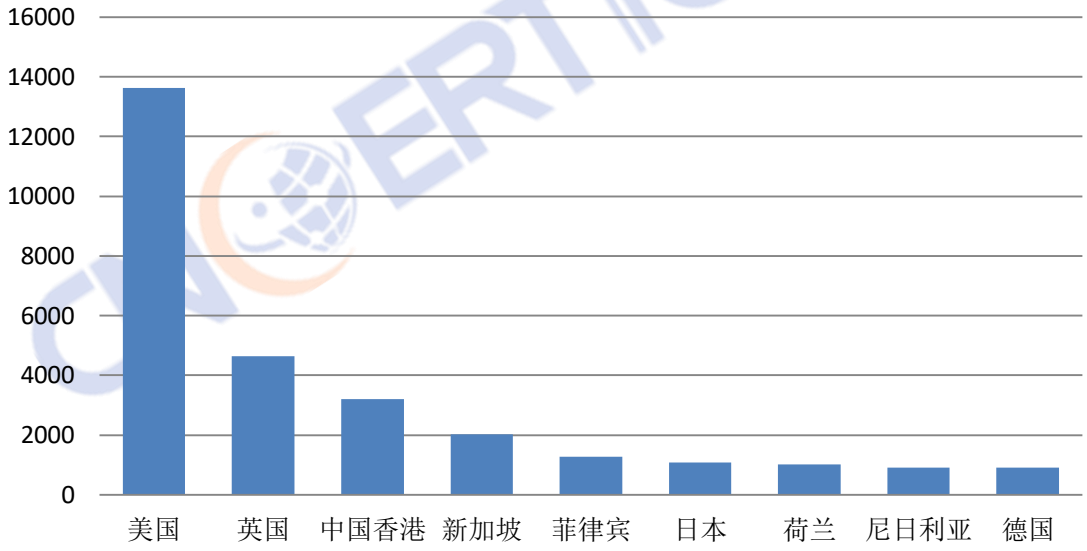

图 14 2019 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

3.网页篡改

2019 年，我国境内遭篡改的网站有约 18.6 万个，其中被篡改的政府网站有 515 个。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大幅下降，占比较小。从境内被篡改网页的顶级域名分布来看，“.com”、“.net”和“.org”占比分列前三位，分别占总数的 75.2%、4.7%和 1.2%，占比分布情况与 2018 年无明显变化，如图 15 所示。

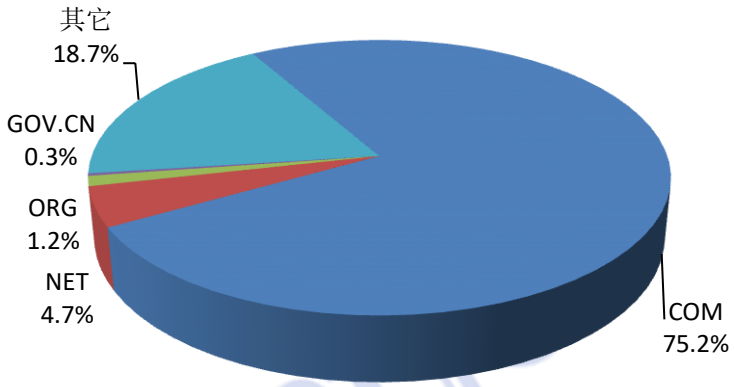

图 15 2019 年境内被篡改网站按顶级域名分布

（五）云平台安全

2019 年，发生在我国云平台上的网络安全事件或威胁情况相比 2018 年进一步加剧。首先，我国主流云平台上发生的各类网络安全事件数量占比仍然较高，遭受 DDoS 攻击次数占境内目标被攻击次数的 74.0%、被植入后门链接数量占境内全部被植入后门链接数量的 86.3%、被篡改网页数量占境内被篡改网页数量的 87.9%。其次，攻击者经常利用我国云平台发起网络攻击。云平台作为控制端发起 DDoS 攻击次数占境内控制发起 DDoS 攻击次数的 86.0%、作为木马和僵尸网络恶意程序控制的被控端 IP 地址数量占境内全部被控端 IP 地址数量的 89.3%、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 81.0%。

（六）工业控制系统安全

1.工业控制系统互联网侧暴露情况

2019 年，暴露在互联网上的工业设备 7,325 台，相比 2018 年增加 21.7%，如下图 16 所示，涉及西门子、韦益可自控、罗克韦尔等 39 家国内外知名厂商的 PLC 设备、智能楼宇、数据采集等 50 种设备类型，且存在高危漏洞隐患的设备占比约 35%。电力、石油天然气、医疗健康、煤炭、城市轨道交通等重点行业暴露的联网监控管理系统 2,249 套，相比 2018 年增加了 21.9%，其中医疗健康行业 709 套、电力 653 套、石油天然气 584 套、煤炭 203 套、城市轨道交通 100 套，涉及的类型包括政府监管、企业经营管理类、企业生产管理、工业云平台等，详见图 17、图 18，其中存在信息泄露、配置不当、跨站请求伪造等高危漏洞隐患的系统占比约 46.1%。暴露面的持续扩大，使工业控制系统的安全运营面临更大的风险隐患。

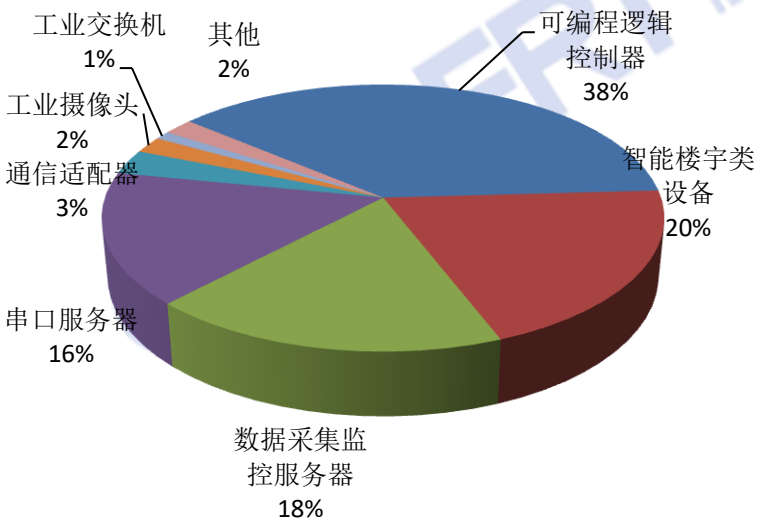

图 16 2019 年监测发现的联网工业设备的类型统计

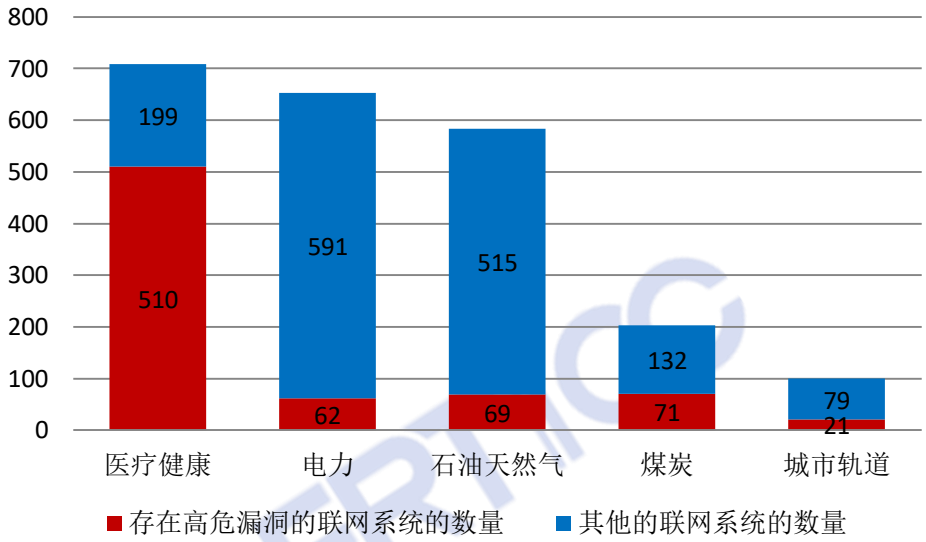

图 17 2019 年监测发现的重点行业联网监控管理系统的漏洞威胁统计

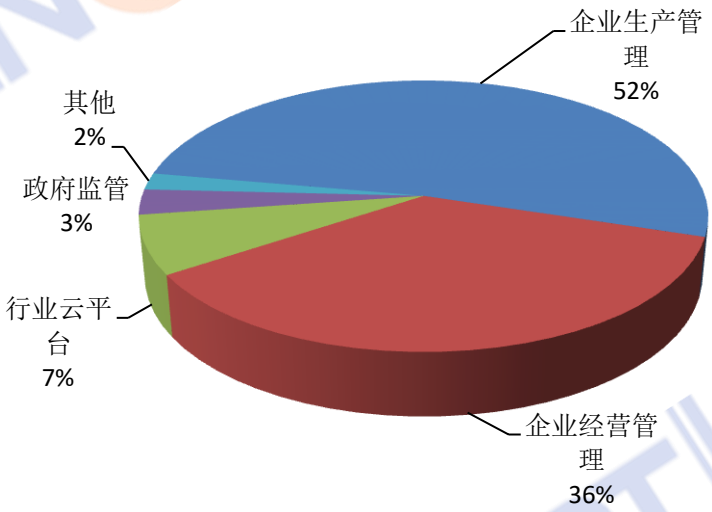

图 18 2019 年监测发现的重点行业联网监控管理系统的类型统计

2.工业控制系统互联网侧威胁监测情况

2019 年，面向国内工业控制系统的网络资产嗅探事件约 14,900 万起，较上年 4,451 万起有显著增长。经分析，嗅探行为源自于美国、瑞士、法国等境外 130 个国家，目标涉及国内能源、制造、通信等重点行业的联网工业控制设备和系统。大量关键信息基础设施及其联网控制系统的网络资产信息被境外

嗅探，给我国网络空间安全带来隐患。

2019 年，我国根云、航天云网、OneNET、COSMOPlat、奥普云、机智云等大型工业互联网云平台，其服务行业如表 2 所示，持续遭受来自境外的网络攻击，平均攻击次数达 90 次/日，较上一年提升了 43%，攻击类型如图 19 所示，涉及远程代码执行、拒绝服务、Web 漏洞利用等，工业云平台承载着大量接入设备、业务系统，以及企业、个人信息和重要数据，使其成为网络攻击的重点目标。

表 2 我国大型工业云平台

平台名称	平台企业	服务行业
RootCloud	三一重工	机械制造、金融、售后服务
OneNET	中国移动	可穿戴设备、移动健康、智能创客、车联网
COSMOPlat	海尔	大数据增值、协同制造、知识共享、检测与认证
INDICS	航天科工	机械设备、能源、智能家居
OceanConnect	华为	公共事业、能源、车联网、智慧家庭
阿里云	阿里	智慧城市、智能制造、智能医疗
iSESOL	智能云科	智能制造、金融
M81	浪潮	机械制造、供应链、质量控制
BEACON	富士康	网络通讯、电子消费、零部件制造
ProudThink	奥普	工业物联网、智能制造、工业大数据
Gizwits	机智云	电子信息、能源、制药

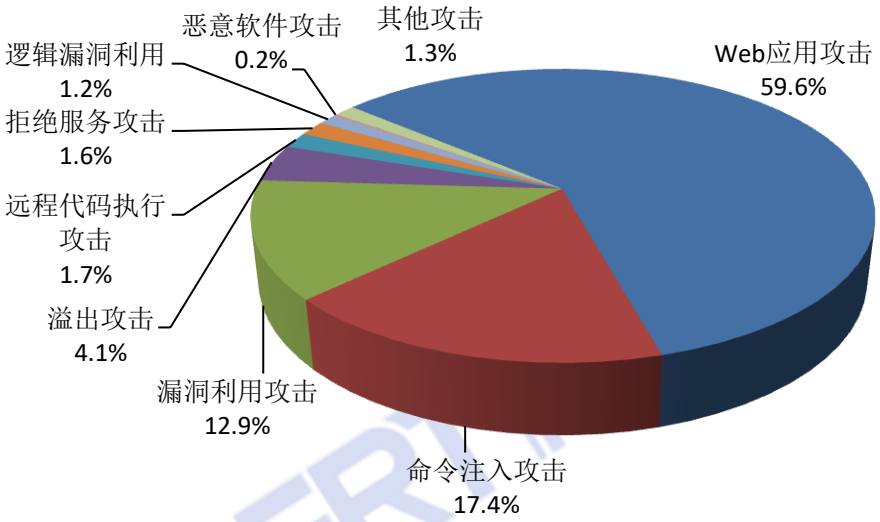

图 19 工业云平台攻击事件的类型分布

工业控制系统中的智能传感器、网关、摄像头、门禁、打印机等物联网设备给工业控制系统带来的安全风险值得关注。2019 年 CNCERT 通过互联网监测和定位后发现，关键信息基础设施行业有 1,773 台打印机连接在互联网上，其中工业领域相关的打印机有 78 台，涉及石油、电力、煤炭、制造等行业，分布如图 20 所示。针对上述重点行业的 78 台打印机进行为其一周的监测分析，发现攻击事件 130 次，主要攻击类型包括恶意代码、获取权限、密码窃取、WEB 应用攻击四大类，分布如图 21 所示。打印机等物联网设备部署于在生产和办公的网络环境中，一旦受控，将使工业控制系统面临“一点突破、全网皆失”的风险。

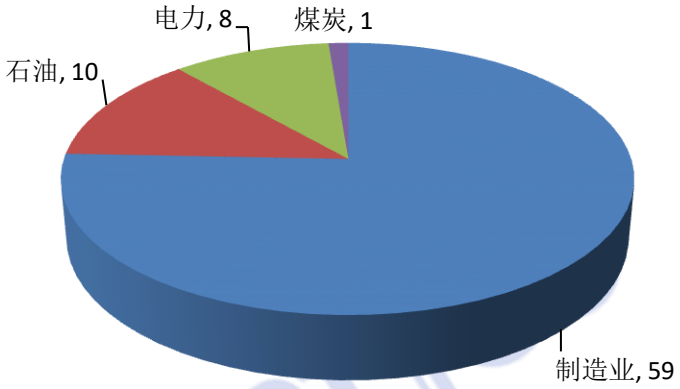

图 20 工业行业暴露的联网打印机统计图

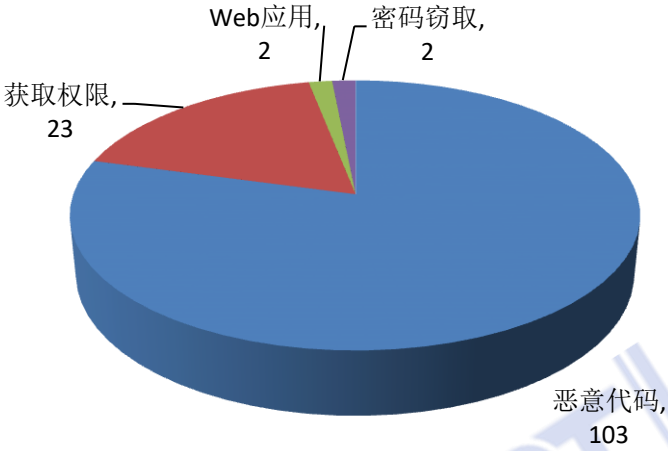

图 21 打印机网络攻击类型统计

3.工业控制产品安全漏洞情况

2019 年，CNVD、Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）及国家信息安全漏洞库（CNNVD）四大漏洞平台新增收录工业控制系统产品漏洞共计 690 个，其中高中危漏洞占比达 92.8%。如图 22 和图 23 所示，漏洞影响的产品广泛应用于制造业、能源、水务、商

业设施、石化、医疗、交通、农业、信息技术、航空等关键信息基础设施行业，漏洞涉及的产品供应商主要包括西门子（Siemens）、施耐德（Schneider）、研华（Advantech）、摩莎（Moxa）、趋势科技（TRENDnet）、三菱（Mitsubishi）、欧姆龙（Omron）、和友讯（D-Link）等。

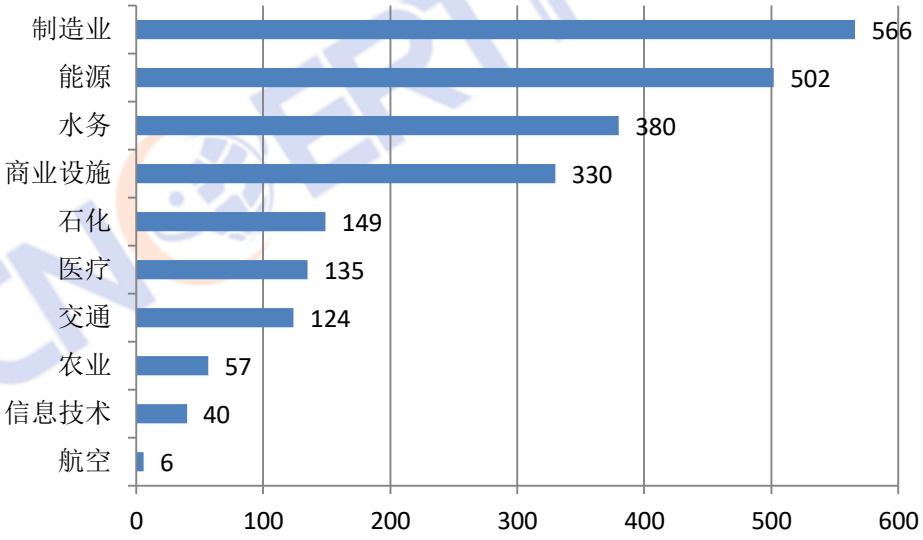

图 22 2019 年新增工业控制产品漏洞的行业分布 TOP10

（注：受漏洞影响的产品可应用于多个行业）

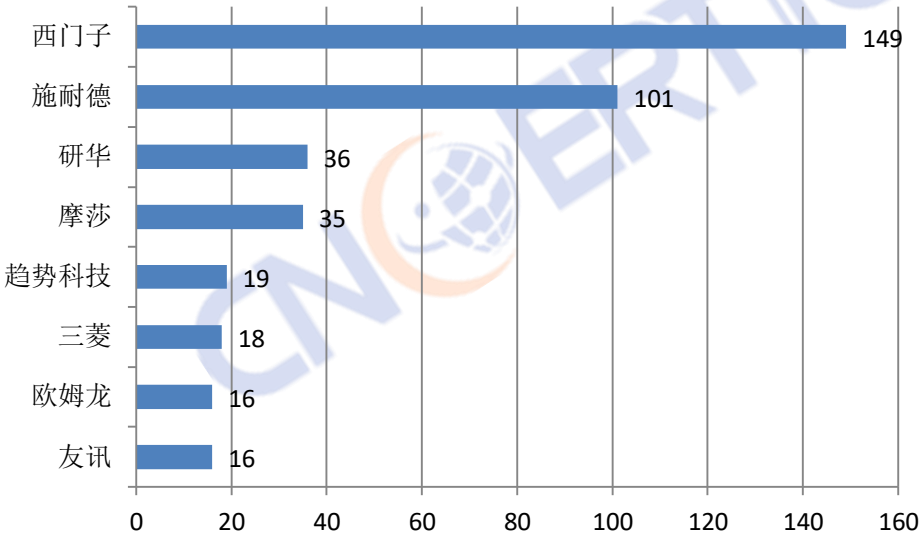

图 23 2019 年新增工业控制产品漏洞的供应商分布 TOP8

为缓解工业控制产品漏洞影响，在相关部门指导下，CNCERT 长期开展针对工业控制产品等网络关键设备的安全检测工作。2019 年，CNCERT 重点对西门子、罗克韦尔、施耐德等厂商的 13 款最新固件版本的 PLC 测试后发现，虽然因代码缺陷导致的安全漏洞较之前已明显减少，但在 PLC 产品安全设计方面，如身份鉴别、访问控制粒度等，仍有较大改进空间，尤其个别厂商仍在沿用“FTP+硬编码口令”方式进行固件升级。对现行标准和原有产品的兼容性考虑，是阻碍厂商在安全设计上做大幅改进的主要原因之一。此外，CNCERT 协助某电网集团对国内主流产品供应商的电力系统二次设备进行了入网安全测试，在 28 个厂商、70 个装置型号（包含保护装置、测控装置、智能远动、站控软件、PMU 等）的产品中均发现了高中危漏洞，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。在测试中发现的漏洞，在某电网集团的督导下，均在积极修复中。