2020 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

2021 年 5 月

目 录

一、前言

2020 年，全球突发新冠肺炎疫情，抗击疫情成为各国紧迫任务。不论是在疫情防控相关工作领域，还是在远程办公、教育、医疗及智能化生产等生产生活领域，大量新型互联网产品和服务应运而生，在助力疫情防控的同时也进一步推进社会数字化转型。与此同时，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。

我国持续加强网络安全监测发现和应急处置工作，组织应急演练，并不断加强网络安全法治体系建设。中央网信办发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》；全国人大法工委就《数据安全法(草案)》和《个人信息保护法（草案）》征求意见，进一步强调对数据安全和个人信息的保护；《密码法》正式施行，是我国密码领域的综合性、基础性法律。

本报告以 CNCERT 宏观网络安全监测数据为基础，结合各类安全威胁、事件信息以及网络安全威胁治理实践，对 2020 年我国互联网网络安全状况进行了全面分析和总结，并对 2021 年网络安全关注方向进行预测。

二、2020 年我国互联网网络安全状况

（一）我国网络安全法律法规体系日趋完善，网络安全威胁治理成效显著。

1.我国网络安全法律法规体系建设进一步完善。

2020 年，多项网络安全法律法规面向社会公众发布，我国网络安全法律法规体系日臻完善。国家互联网信息办公室等 12 个部门联合制定和发布《网络安全审查办法》，以确保关键信息基础设施供应链安全，维护国家安全。全国人大法工委就《数据安全法(草案)》和《个人信息保护法（草案）》征求社会公众意见，法律将为切实保护数据安全和用户个人信息安全提供强有力的法治保障。《密码法》正式施行，规定使用密码进行数据加密、身份认证以及开展商用密码应用安全性评估成为系统运营单位的法定义务。《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》正式发布，提出保障国家数据安全，加强个人信息保护，全面加强网络安全保障体系和能力建设，维护水利、电力、供水、油气、交通、通信、网络、金融等重要基础设施安全。中共中央印发《法治社会建设实施纲要(2020－2025 年)》,要求依法治理网络空间，推动社会治理从现实社会向网络空间覆盖，建立健全网络综合治理体系，加强依法管网、依法办网、依法上网，全面推进网络空间法治化，营造清朗的网络空间。同时，国家发改委、工业和信息化部、公安部、交通运输部、国家市场监督管理总局

等多个部门，陆续出台相关配套文件，不断推进我国各领域网络安全工作。

2.网络安全宣传活动丰富、威胁治理成效显著。

党的十八大以来，我国持续加强网络安全顶层设计，每年开展国家网络安全宣传周活动，组织丰富多样的网络安全会议、赛事等活动，不断加大网络安全知识宣传力度。2020 年，CNCERT 协调处置各类网络安全事件约 10.3 万起，同比减少 4.2%。据抽样监测发现，我国被植入后门网站、被篡改网站等数量均有所减少，其中被植入后门的网站数量同比减少 37.3%，境内政府网站被植入后门的数量大幅下降，同比减少 64.3%；被篡改的网站数量同比减少 45.9%。在主管部门指导下，CNCERT 持续开展对被用于进行 DDoS 攻击的网络资源（以下简称“攻击资源”）治理工作，境内可被利用的攻击资源稳定性降低，被利用发起攻击的境内攻击资源数量持续控制在较低水平，有效降低了发起自我国境内的攻击流量，从源头上持续遏制 DDoS 攻击事件。根据外部报告，全年我国境内 DDoS 攻击次数减少 16.16%，攻击总流量下降 19.67%[①]；僵尸网络控制端数量在全球的占比稳步下降至 2.05%[②]。

[①]相关数据来源于中国电信云堤、绿盟科技联合发布的《2020 DDoS 攻击态势报告》
[②]相关数据来源于卡巴斯基公司《DDoS Attacks in Q4 2020》

（二）APT 组织利用社会热点、供应链攻击等方式持续对我国重要行业实施攻击，远程办公需求增长扩大了 APT 攻击面。

1. 利用社会热点信息投递钓鱼邮件的 APT 攻击行动高发。

境外“白象”“海莲花”“毒云藤”等 APT 攻击组织以“新冠肺炎疫情”“基金项目申请”等相关社会热点及工作文件为诱饵，向我国重要单位邮箱账户投递钓鱼邮件，诱导受害人点击仿冒该单位邮件服务提供商或邮件服务系统的虚假页面链接，从而盗取受害人的邮箱账号密码。1 月，“白象”组织利用新冠肺炎疫情相关热点，冒充我国卫生机构对我国 20 余家单位发起定向攻击；2 月，“海莲花”组织以“H5N1 亚型高致病性禽流感疫情”“冠状病毒实时更新”等时事热点为诱饵对我国部分卫生机构发起“鱼叉”攻击。“毒云藤”组织长期利用伪造的邮箱文件共享页面实施攻击，获取了我国百余个单位的数百个邮箱的账户权限。

2. 供应链攻击成为 APT 组织常用攻击手法。

APT 组织多次对攻击目标采用供应链攻击。例如，新冠肺炎疫情防控下的远程办公需求明显增多，虚拟专用网络（VPN）成为远程办公人员接入单位网络的主要技术手段之一。在此背景下，部分 APT 组织通过控制 VPN 服务器，将木马文件伪装成 VPN 客户端升级包，下发给使用这些 VPN 服务器的重要单位。经监测发现，东亚区域 APT 组织以及“海莲花”组织等多个境外 APT 组织通过这一方式对我国党政机关、科研院所等多

个重要行业单位发起攻击，造成较为严重的网络安全风险。2020年底，美国爆发 SolarWinds 供应链攻击事件，包括美国有关政府机构及微软、思科等大型公司在内的大量机构受到影响。

3. 部分 APT 组织网络攻击工具长期潜伏在我国重要机构设备中。

为长期控制重要目标从而窃取信息，部分 APT 组织利用网络攻击工具，在入侵我国重要机构后长期潜伏，这些工具功能强大、结构复杂、隐蔽性高。3 月至 7 月，“响尾蛇”组织隐蔽控制我国某重点高校主机，持续窃取了多份文件；9 月，在我某研究机构服务器上发现“方程式”组织使用的高度隐蔽网络窃密工具，结合前期该机构主机被控情况，可以推断，最早可追溯至 2013 年，“方程式”组织就已开始对该研究机构实施长期潜伏攻击。

（三）App 违法违规收集个人信息治理取得积极成效，但个人信息非法售卖情况仍较为严重，联网数据库和微信小程序数据泄露风险较为突出。

1. App 违法违规收集个人信息治理取得积极成效。

App 违法违规收集使用个人信息乱象的治理持续推进，取得积极成效。截至 2020 年底，国内主流应用商店可下载的在架活跃 App 达到 267 万款，安卓、苹果 App 分别为 105 万款、162 万款。为落实《网络安全法》，进一步规范 App 个人信息收集行为，保障个人信息安全，国家互联网信息办公室会同工业和信

息化部、公安部、市场监管总局持续开展 App 违法违规收集使用个人信息治理工作，对存在未经同意收集、超范围收集、强制授权、过度索权等违法违规问题的 App 依法予以公开曝光或下架处理；研究起草了《常见类型移动互联网应用程序（App）必要个人信息范围规定（征求意见稿）》并面向社会公开征求意见，规定了地图导航、网络约车、即时通信等常见类型 App 的必要个人信息范围。

2.公民个人信息未脱敏展示与非法售卖情况较为严重。

监测发现涉及身份证号码、手机号码、家庭住址、学历、工作信息等敏感个人信息暴露在互联网上，全年仅CNCERT就累计监测发现政务公开、招考公示等平台未脱敏展示公民个人信息事件107起，涉及未脱敏个人信息近10万条。此外，全年累计监测发现个人信息非法售卖事件203起，其中，银行、证券、保险相关行业用户个人信息遭非法售卖的事件占比较高，约占数据非法交易事件总数的40%；电子商务、社交平台等用户数据和高校、培训机构、考试机构等教育行业通讯录数据分别占数据非法交易事件总数的20%和12%。

3.联网数据库和微信小程序数据泄露风险问题突出。

CNCERT 持续推进数据安全事件监测发现和协调处置工作，全年累计监测并通报联网信息系统数据库存在安全漏洞、遭受入侵控制，以及个人信息遭盗取和非法售卖等重要数据安全事件 3000 余起，涉及电子商务、互联网企业、医疗卫生、校外培

训等众多行业机构。分析发现，使用 MySQL、SQLServer、Redis、PostgreSQL 等主流数据库的信息系统遭攻击较为频繁。其中，数据库密码爆破攻击事件最为普遍，占比高达 48%，数据库遭删库、拖库、植入恶意代码、植入后门等事件时有发生，数据库存在漏洞等风险情况较为突出。

近年来，微信小程序（以下简称“小程序”）发展迅速，但也暴露出较为突出的安全隐患，特别是用户个人信息泄露风险较为严峻。CNCERT从程序代码安全、服务交互安全、本地数据安全、网络传输安全、安全漏洞等五个维度，对国内50家银行发布的小程序进行了安全性检测，结果显示，平均一个小程序存在8项安全风险，在程序源代码暴露关键信息和输入敏感信息时未采取防护措施的小程序数量占比超过90%；未提供个人信息收集协议的超过80%；个人信息在本地储存和网络传输过程中未进行加密处理的超过60%；少数小程序则存在较严重的越权风险。

（四）漏洞信息共享与应急工作稳步深化，但历史重大漏洞利用风险仍然较大，网络安全产品自身漏洞问题引起关注。

1.漏洞信息共享与应急工作稳步推进。

国家信息安全漏洞共享平台（以下简称“CNVD”）全年新增收录通用软硬件漏洞数量创历史新高，达 20,704 个，同比增长 27.9%，近五年来新增收录漏洞数量呈显著增长态势，年均增长率为 17.6%。全年开展重大突发漏洞事件应急响应工作 36

次，涉及办公自动化系统（OA）、内容管理系统（CMS）、防火墙系统等；开展了对约 3.1 万起漏洞事件的验证和处置工作；及时向社会公开发布影响范围广、需终端用户尽快修复的重大安全漏洞公告 26 份，有效化解重大安全漏洞可能引发的安全风险。

2.历史重大漏洞利用风险依然较为严重，漏洞修复工作尤为重要和紧迫。

经抽样监测发现，利用安全漏洞针对境内主机进行扫描探测、代码执行等的远程攻击行为日均超过 2176.4 万次。根据攻击来源 IP 地址进行统计，攻击主要来自境外，占比超过 75%。攻击者所利用的漏洞类型主要覆盖网站侧、主机侧、移动终端侧，其中攻击网站所利用的典型漏洞为 Apache Struts2 远程代码执行、Weblogic 反序列化等漏洞；攻击主机所利用的典型漏洞为“永恒之蓝”、OpenSSL“心脏滴血”等漏洞；攻击移动终端所利用的典型漏洞为 Webview 远程代码执行等漏洞。上述典型漏洞均为历史上曾造成严重威胁的重大漏洞，虽然已曝光较长时间，但目前仍然受到攻击者重点关注，安全隐患依然严重，针对此类漏洞的修复工作尤为重要和紧迫。

3.网络安全产品自身漏洞风险上升。

CNVD 收录的通用型漏洞中，网络安全产品类漏洞数量达 424 个，同比增长 110.9%，网络安全产品自身存在的安全漏洞需获得更多关注。终端安全响应系统（EDR）、堡垒机、防火墙、

入侵防御系统、威胁发现系统等网络安全防护产品多次被披露存在安全漏洞，由于网络安全防护产品在网络安全防护体系中发挥着重要作用，且这些产品在国内使用范围较广，相关漏洞一旦被不法分子利用，可能构成严重的网络安全威胁。

（五）恶意程序治理成效明显，但勒索病毒技术手段不断升级，恶意程序传播与治理对抗性加剧。

1.计算机恶意程序感染数量持续减少，移动互联网恶意程序治理成效显现。

我国持续开展计算机恶意程序常态化打击工作，2020 年成功关闭 386 个控制规模较大的僵尸网络，近五年来我国感染计算机恶意程序的主机数量持续下降，并保持在较低感染水平，年均减少率为 25.1%。为从源头上治理移动互联网恶意程序，有效切断传播源，CNCERT 重点协调国内已备案的 App 传播渠道开展恶意 App 下架工作，2014 年到 2020 年期间下架数量分别为 3.9 万个、1.7 万个、8,910 个、8,364 个、3,578 个、3,057 个、2,333 个，恶意 App 下架数量持续保持逐年下降趋势。

2.勒索病毒的勒索方式和技术手段不断升级。

勒索病毒持续活跃，全年捕获勒索病毒软件78.1万余个，较2019年同比增长6.8%。近年来，勒索病毒逐渐从“广撒网”转向定向攻击，表现出更强的针对性，攻击目标主要是大型高价值机构。同时，勒索病毒的技术手段不断升级，利用漏洞入侵过程以及随后的内网横向移动过程的自动化、集成化、模块化、组织化

特点愈发明显，攻击技术呈现快速升级趋势。勒索方式也持续升级，勒索团伙将被加密文件窃取回传，在网站或暗网数据泄露站点上公布部分或全部文件，以威胁受害者缴纳赎金，例如我国某互联网公司就曾遭受来自勒索团伙Maze实施的此类攻击。

3. 采用 P2P 传播方式的联网智能设备恶意程序异常活跃。

P2P传播方式是恶意程序的传统传播手段之一，具有传播速度快、感染规模大、追溯源头难的特点，Mozi、Pinkbot等联网智能设备恶意程序家族在利用该传播方式后活动异常活跃。据抽样监测发现，我国境内以P2P传播方式控制的联网智能设备数量非常庞大，达2299.7万个。全年联网智能设备僵尸网络控制规模增大，部分大型僵尸网络通过P2P传播与集中控制相结合的方式对受控端进行控制。为净化网络安全环境，CNCERT组织对集中式控制端进行打击，但若未清理恶意程序，受感染设备之间仍可继续通过P2P通信保持联系，并感染其他设备。随着更多物联网设备不断投入使用，采用P2P传播的恶意程序可能对网络空间产生更大威胁。

4. 仿冒 App 综合运用定向投递、多次跳转、泛域名解析等多种手段规避检测。

随着恶意App治理工作持续推进，正规平台上恶意App数量逐年呈下降趋势，仿冒App已难以通过正规平台上架和传播，转而采用一些新的传播方式。一些不法分子制作仿冒App并通过分发平台生成二维码或下载链接，采取“定向投递”等方式，通过短

信、社交工具等向目标人群发送二维码或下载链接，诱骗受害人下载安装。同时，还综合运用下载链接多次跳转、域名随机变化、泛域名解析等多种技术手段，规避检测，当某个仿冒App下载链接被处置后，立即生成新的传播链接，以达到规避检测的目的，增加了治理难度。

（六）网页仿冒治理工作力度持续加大，但因社会热点容易被黑产利用开展网页仿冒诈骗，以社会热点为标题的仿冒页面骤增。

1.通过加强行业合作持续开展网页仿冒治理工作。

为有效防范网页仿冒引发的危害，CNCERT 围绕针对金融、电信等行业的仿冒页面进行重点处置，全年共协调国内外域名注册机构关闭仿冒页面 1.7 万余个；对于其他仿冒页面，通过中国互联网网络安全威胁治理联盟（CCTGA）联合国内 10 家浏览器厂商通过协同防御试点方式，在用户访问钓鱼网站时进行提示拦截，全年提示拦截次数达 3.9 亿次。

2.仿冒 ETC 页面井喷式增长。

2019 年以来，电子不停车收费系统（ETC）在全国大力推广，ETC 页面直接涉及个人银行卡信息。不法分子通过仿冒 ETC 相关页面，骗取个人银行卡信息。2020 年 5 月以来，以“ETC 在线认证”为标题的仿冒页面数量呈井喷式增长，并在 8 月达到峰值 5.6 万余条，占针对我国境内网站仿冒页面总量的 91%。此类仿冒页面承载 IP 地址多位于境外，不法分子通过“ETC 信

息认证”“ETC 在线办理认证”“ETC 在线认证中心”等不同页面内容诱骗用户提交姓名、银行账号、身份证号、手机号、密码等个人隐私信息，致使大量用户遭受经济损失。

3.针对网上行政审批的仿冒页面数量大幅上涨。

受新冠肺炎疫情影响，大量行政审批转向线上。2020 年底，出现大量以“统一企业执照信息管理系统”为标题的仿冒页面，仅 11 月至 12 月即监测发现此类仿冒页面 5.3 万余条。不法分子通过该类页面诱骗用户在仿冒页面上提交真实姓名、银行卡号、卡内余额、身份证号、银行预留手机号等信息。此外，监测还发现大量以“核酸检测”“新冠疫苗预约”等为标题的仿冒页面，其目的在于非法获取用户姓名、住址、身份证号、手机号等个人隐私信息。

（七）工业领域网络安全工作不断强化，但工业控制系统互联网侧安全风险仍较为严峻。

1.监管要求、行业扶持和产业带动成为网络安全在工业领域不断落地和深化的三大动力。

随着等保 2.0 标准正式实施，公安部制定出台《贯彻落实网络安全等级保护制度和关键信息基础设施保护制度的指导意见》，建立并实施关键信息基础设施安全保护制度。为满足监管要求和行业网络安全保障需求，国家相关主管部门加大对重点行业网络安全政策和资金扶持力度，工控安全行业蓬勃发展。为行业量身定做的、具有实际效果的安全解决方案得到更多认

可，如电网等较早开展工控安全的行业，已逐步从合规性需求向效果性需求转变。除外围安全监测与防护，核心软硬件的本体安全和供应链安全日益得到重视。

2.工业控制系统互联网侧安全风险仍较为严峻。

监测发现，我国境内直接暴露在互联网上的工控设备和系统存在高危漏洞隐患占比仍然较高。在对能源、轨道交通等关键信息基础设施在线安全巡检中发现，20%的生产管理系统存在高危安全漏洞。与此同时，工业控制系统已成为黑客攻击利用的重要对象，境外黑客组织对我国工控视频监控设备进行了针对性攻击。2月，针对存在某特定漏洞工控设备的恶意代码攻击持续半个月之久，攻击次数达6,700万次，攻击对象包含数十万个IP地址。为有效降低工业控制系统互联网侧的安全风险，各相关行业需加大资金投入力度，提升工控设备漏洞安全监测能力，加强处置力度，从而及时消除互联网侧安全风险暴露点。

三、2021年网络安全关注方向预测

（一）与社会热点相关联的APT攻击活动仍将持续。

2020年，全球范围内多个APT组织都发起以新冠疫情主题为诱饵的APT攻击。攻击者通过“鱼叉”钓鱼邮件等方式对分布在全球的攻击目标实施窃密和控制。2021年，在新冠肺炎疫情持续扩散、各国规模化开展疫苗采购和接种工作的背景下，这类攻击方式仍将流行，以窃取新冠肺炎疫苗相关信息为目标的APT攻击活动将持续，政府机构、关键信息基础设施运营者、

疫苗生产厂商、卫生组织、医疗机构等将成为重点攻击目标。

（二）App 违法违规收集使用个人信息情况将进一步改善。

在移动互联网时代，个人信息已成为高价值的数据资源，加强 App 个人信息保护势在必行。近年来，国家互联网信息办公室、工业和信息化部、公安部、国家市场监管总局四部门启动了 App 违法违规收集使用个人信息治理工作，对用户规模大、问题突出的 App 采取公开曝光、约谈、下架等处罚措施，App 违法违规收集使用个人信息问题有所改善。然而，我国 App 数量庞大，更新频繁，且新应用层出不穷，仍存在 App 过度超范围收集个人信息、个人信息滥用等情况，公民合法权益受到侵犯。2021 年，随着《个人信息保护法》的即将出台，以及国家监管部门监督和治理力度不断加大，相关运营企业将更加重视个人信息保护工作，规范收集使用个人信息行为。

（三）网络产品和服务的供应链安全问题面临挑战。

近年来，因停止提供基础产品组件或服务，或遭受网络攻击等方式而发生的网络产品和服务供应链安全问题时有发生。任何产品和服务的供应链只要在某个环节出现问题，都可能影响整个供应链的安全运行，破坏性巨大。面对愈加严峻的供应链安全形势，预计各行业领域政策标准将陆续出台，区块链等新技术也将为保障供应链安全提供可能的解决方案。

（四）加强关键信息基础设施安全保护成为社会共识。

2020 年 4 月 13 日，国家互联网信息办公室等 12 个部门联

合发布《网络安全审查办法》，明确关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照办法进行网络安全审查。近年来，针对关键信息基础设施的信息窃取、攻击破坏等恶意活动持续增加，相关安全问题也受到社会关注。例如，新冠肺炎疫情发生以来，涉及医疗卫生的关键信息基础设施成为攻击者的重点攻击对象。预计 2021 年，关键信息基础设施安全保护的顶层设计、体系建设等将持续完善。

（五）远程协作安全风险问题或将更受重视。

2020 年，全球出现多起涉及远程会议软件、VPN 设备等的网络安全事件，远程协作中的网络安全问题得到高度重视，2020 年 3 月全国信息安全标准化技术委员会出台《网络安全标准实践指南-远程办公安全防护》。2021 年，攻击者或将针对远程协作环境下的薄弱环节，重点针对使用的工具、协议以及所依赖的信息基础设施开展攻击，远程协作安全风险问题将受到更多关注和重视，需要更体系化的安全解决方案。

（六）全社会数字化转型加快背景下将着力提升数据安全防护能力。

随着云计算、大数据、物联网、工业互联网、人工智能等新技术新应用的大规模发展，互联网上承载的数据和信息越来越丰富，这些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。随着全社会数字化进程的加快，数据的价值将更为凸显。

近年来针对数据的网络攻击以及数据滥用问题日趋严重，数据安全风险将更加突出。2021 年，随着《数据安全法》的即将出台，数据安全管理将会进一步加强，数据安全治理水平也将得到有效提升。

附件：2020 年我国互联网网络安全监测数据分析

（一）恶意程序

1.恶意程序捕获情况

全年捕获恶意程序样本数量超过 4,200 万个，日均传播次数达 482 万余次，涉及恶意程序家族近 34.8 万个。按照传播来源统计，境外来源主要是来自美国、印度等，具体分布如图 1 所示；境内来源主要来自河南省、广东省和浙江省等。按照攻击目标 IP 地址统计，我国境内受恶意程序攻击的 IP 地址约 5,541 万个，约占我国 IP 地址总数的 14.2%，这些受攻击的 IP 地址主要集中在山东省、江苏省、广东省、浙江省等地区。2020 年我国受恶意程序攻击的 IP 地址分布情况如图 2 所示。

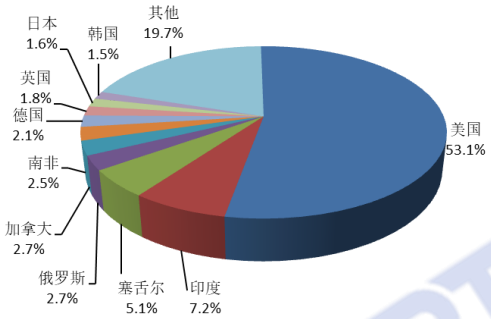

图 1 2020 年恶意程序传播源位于境外分布情况

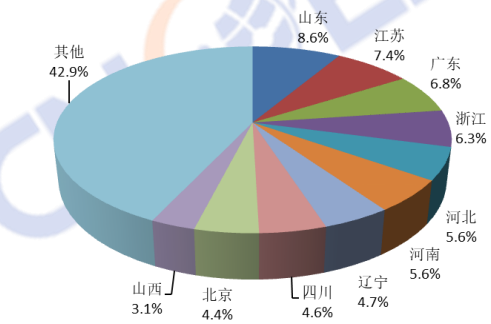

图 2 2020 年我国受恶意程序攻击的 IP 地址分布情况

2.计算机恶意程序用户感染情况

全年，我国境内感染计算机恶意程序的主机数量约 534 万台，同比下降 8.3%，如图 3 所示。位于境外的约 5.2 万个计算机恶意程序控制服务器控制了我国境内约 531 万台主机。就控制服务器所属地区来看，位于美国、中国香港和荷兰的控制服务器数量分列前三位，分别是约 1.9 万个、2,854 个和 2,083 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、荷兰和德国的控制服务器控制规模分列前三位，分别控制我国境内约 446 万、215 万和 194 万台主机，如图 5 所示。此外，根据 CNCERT 针对 IPv6 网络攻击的抽样监测数据显示，2020 年境外约 3,500 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 3.3 万台 IPv6 地址主机。

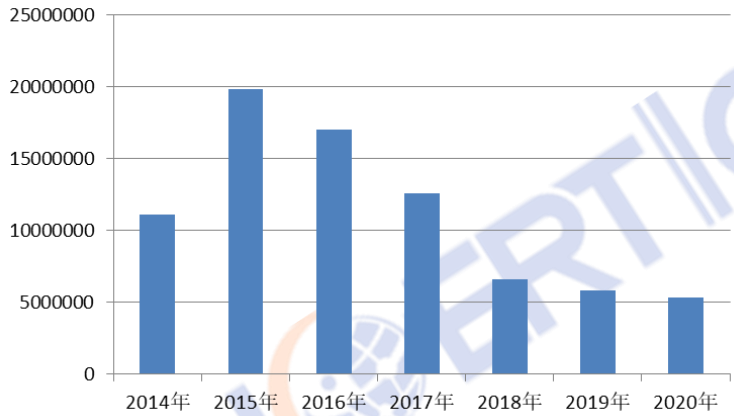

图 3 境内感染计算机恶意程序主机数量统计

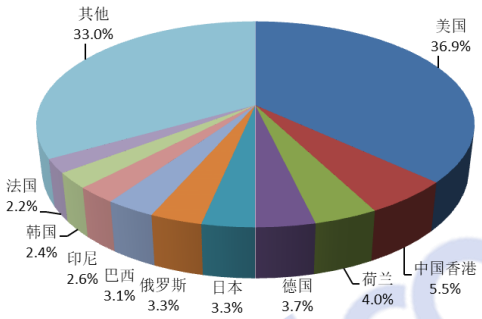

图 4 2020 年控制我国境内主机的境外计算机恶意程序控制服务器数量分布

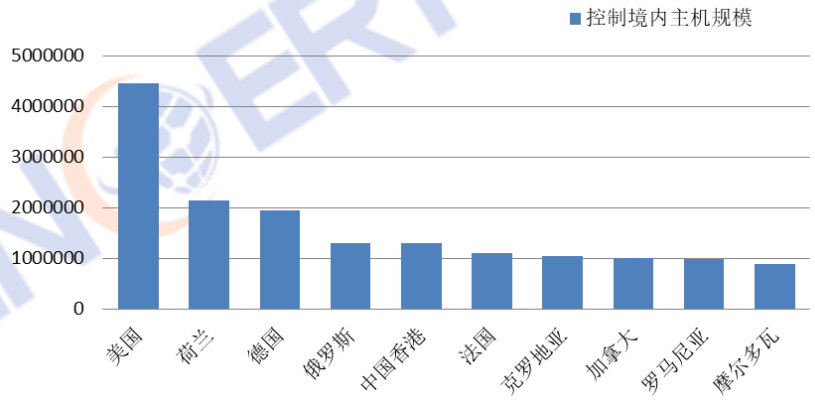

图 5 2020 年控制我国境内主机数量 TOP10 的国家或地区

从我国境内感染计算机恶意程序主机所属地区看，感染主机主要分布在江苏省（占我国境内感染数量的 12.1%）、浙江省（占 11.5%）、广东省（占 11.4%）等地区，如图 6 所示。在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 8,423 个，同比增长 50.1%，规模在 10 万台以上的僵尸网络数量达 39 个，如图 7 所示。CNCERT 协调相关机构成功关闭 386 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。

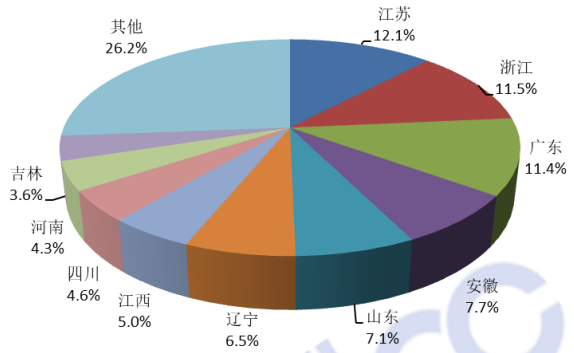

图 6 2020 年我国境内感染计算机恶意程序主机数量按地区分布

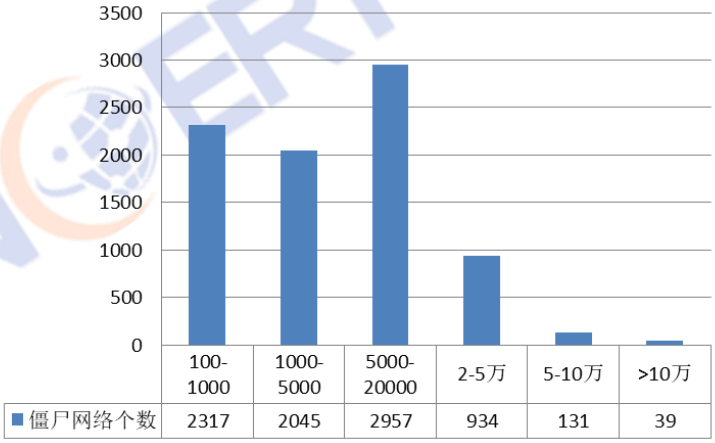

图 7 2020 年僵尸网络的规模分布

3.移动互联网恶意程序

全年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约 303 万个，同比增长 8.5%，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 48.4%、21.1%和 12.7%，如图 9 所示。CNCERT 连续八年联合应用商店、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，2020 年累计协调国内 569 家提供移动应用程序下载服务的平台下架 2,333 个移动互联网恶意程序，有效控制了移动互联网恶意程序传播途径，防范移动互联网恶意程序危害。

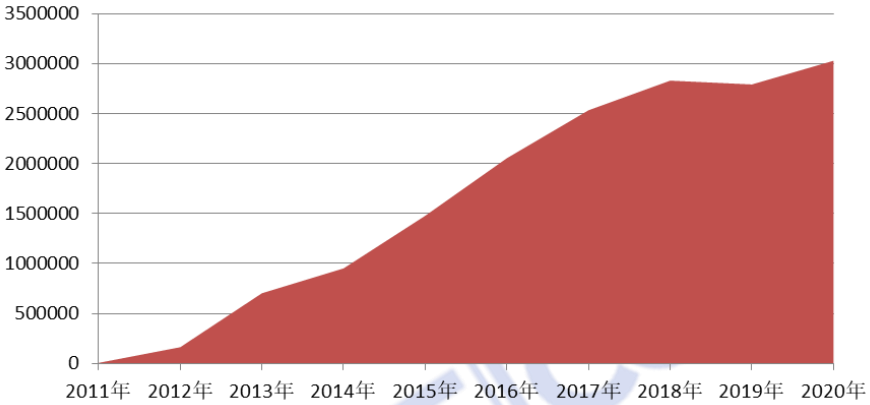

图 8 2011 年至 2020 年移动互联网恶意程序捕获数量走势

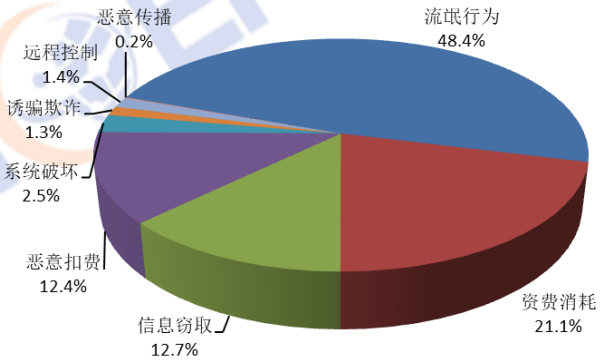

图 9 2020 年移动互联网恶意程序数量按行为属性统计

4.联网智能设备恶意程序

全年捕获联网智能设备恶意程序样本数量约 341 万个，同比上升 5.2%。其中，排名前两位的恶意程序样本家族及变种为 Mirai、Gafgyt，占比分别为 77.5%和 13.9%，其他数量较多的家族还有 Tsunami、Mozi、Dark Nexus 等。全年监测发现联网智能设备恶意程序传播源 IP 地址约 51.99 万个，其中，境外传播源 IP 地址主要分布在印度、俄罗斯、韩国、巴西、美国等国家或地区。

根据抽样监测，发现境内联网智能设备被控端 2929.73 万个，感染的恶意程序家族主要为 Pinkbot、Tsunami、Gafgyt、

Mirai 等，通过控制联网智能设备发起的 DDoS 攻击日均 3000 余起。其中，以 P2P 传播模式控制的感染端 2299.7 万个，主要位于山东省、浙江省、河南省、江苏省等地区。目前，采用 P2P 传播方式的联网智能设备恶意程序非常活跃，给联网智能设备控制端集中打击清理工作带来新挑战。通过对联网智能设备被控所形成的僵尸网络进行分析，发现累计控制规模大于 10 万的僵尸网络共 53 个，控制规模为 1 万至 10 万的僵尸网络共 471 个，控制规模较大的控制端主要分布在美国、荷兰、俄罗斯、法国、德国等，控制规模较大的恶意程序家族包括 Tsunami、Gafgyt、Moobot、Cayosin、Fbot、Mirai 等。

（二）安全漏洞

国家信息安全漏洞共享平台（CNVD）收录安全漏洞数量共计 20,704 个，继续呈上升趋势，同比增长 27.9%，2016 年以来年均增长率为 17.6%。其中，高危漏洞数量为 7,420 个（占 35.8%），同比增长 52.1%；“零日”漏洞数量为 8,902 个（占 43.0%），同比增长 56.0%，如图 10 所示。按影响对象分类统计，排名前三的是应用程序漏洞（占 47.9%）、Web 应用漏洞（占 29.5%）、操作系统漏洞（占 10.0%），如图 11 所示。

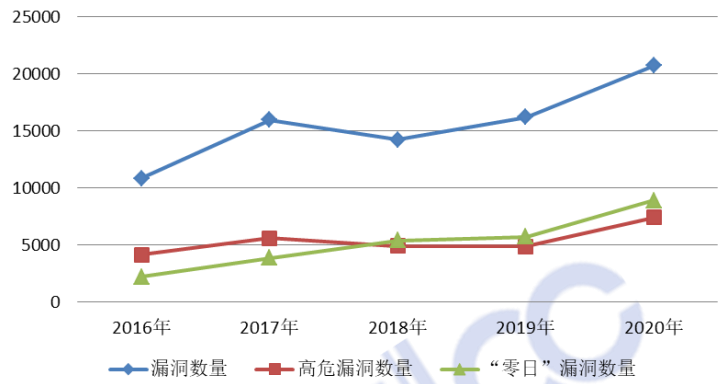

图 10 2016 年至 2020 年 CNVD 收录安全漏洞数量对比

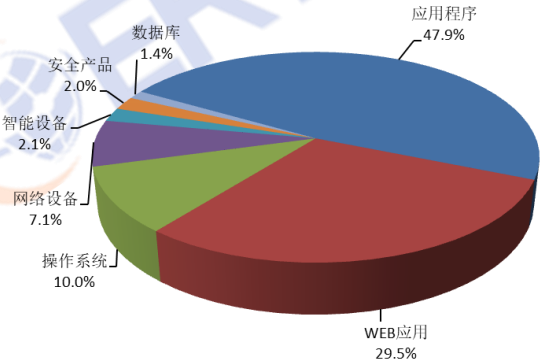

图 11 2020 年 CNVD 收录安全漏洞按影响对象分类统计

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四类子漏洞库的建设工作，分别新增收录安全漏洞数量 1,665 个（占全年收录数量的 8.0%）、1,039 个（占 5.0%）、706 个（占 3.4%）和 209 个（占 1.0%），如图 12 所示。同 2019 年相比，四类子漏洞库收录数量均有不同程度的增长，同比增长分别为 37.1%、62.9%、59.4%和 59.5%。

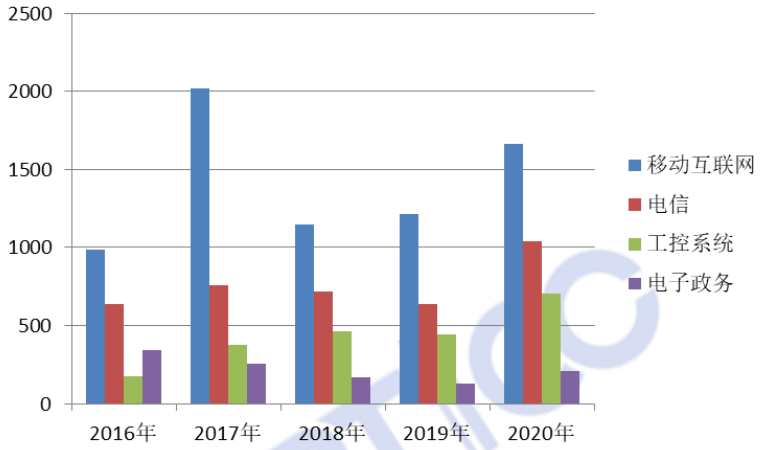

图 12 2016 年至 2020 年 CNVD 子漏洞库收录情况对比

（三）拒绝服务攻击

因为攻击成本低、效果明显，DDoS 攻击仍是目前互联网用户面临的较常见、影响较严重的网络安全威胁之一。为降低 DDoS 攻击对我国基础网络和关键信息基础设施的威胁，CNCERT 持续加强对境内目标遭大流量攻击情况的监测跟踪分析，针对所发现的被用于进行 DDoS 攻击的网络资源重点开展治理。

1.境内目标遭大流量 DDoS 攻击情况

在监测发现的境内目标遭峰值流量超过 1Gbps 的大流量攻击事件中，攻击方式为 TCP SYN Flood、UDP Flood、NTP Amplification、DNS Amplification 和 SSDP Amplification 这五种攻击的占比达到 91.6%；攻击目标主要位于浙江省、山东省、江苏省、广东省、北京市、上海市、福建省等 7 个地区的事件占比达到 81.8%；12 月份是全年攻击最高峰，攻击异常活跃。经对每起攻击事件的攻击时长分析，发现攻击时长不超过 30 分

钟的攻击占比高达 94.4%，表明当前攻击者倾向于最优化使用攻击资源，利用大流量攻击瞬时打瘫攻击目标，以对外提供更多服务并非法获利。

2.被用于进行 DDoS 攻击的网络资源活跃情况

通过开展对境内目标遭大流量 DDoS 攻击事件的持续分析溯源，发布《我国 DDoS 攻击资源季度分析报告》，定期公布控制端、被控端、反射服务器、伪造流量来源路由器等被用于进行 DDoS 攻击的网络资源（以下简称“攻击资源”）情况，进一步协调各单位处置，境内可被利用的攻击资源稳定性降低，被利用的活跃境内攻击资源数量控制在较低水平。与 2019 年相比，境内各类攻击资源数量持续减少，境内活跃控制端数量同比减少 47.6%、受控端数量同比减少 39.9%、活跃反射服务器同比减少 20.4%、跨域伪造路由器同比减少 59.1%；而与此同时，境外各类攻击资源数量不断增加，境外活跃控制端数量同比增加 27.6%、受控端数量同比增加 37.0%、活跃反射服务器同比增加 0.3%，攻击资源向境外迁移趋势明显。

（四）网站安全

1.网页仿冒

近年来，不法分子通过网页仿冒诈骗获利的方式层出不穷，其仿冒对象已不仅仅局限于银行类、支付类网站网页，利用社会热点事件开展的网页仿冒诈骗呈爆炸式增长。全年监测发现约 20 万个针对我国境内网站的仿冒页面，同比增长约 1.4 倍。

其中，大部分为关于“ETC 在线认证”网站、网上行政审批等利用社会热点的仿冒页面。为有效防范网页仿冒引发的危害，CNCERT 围绕针对金融、电信等行业的仿冒页面进行重点处置，全年共协调关闭仿冒页面 1.7 万余个；对于其他仿冒页面，通过中国互联网网络安全威胁治理联盟（CCTGA）联合国内 10 家浏览器厂商通过协同防御试点方式，对用户访问钓鱼网站进行提示拦截，全年提示拦截次数达 3.9 亿次。

2.网站后门

监测发现境内外约 2.6 万个 IP 地址对我国境内约 5.3 万个网站植入后门，我国境内被植入后门的网站数量同比下降 37.3%。其中，境外 IP 地址约有 2.57 万个（占全部 IP 地址总数的 97.7%），对境内约 5.25 万个网站植入后门。从境外 IP 地址分布来看，位于菲律宾的 IP 地址最多，占境外 IP 地址总数的 18.9%，且所属地址段非常集中，超过半数集中于 14 个 C 段地址；其次是位于美国和中国香港的 IP 地址，如图 13 所示。从控制我国境内网站总数来看，位于菲律宾的 IP 地址控制我国境内网站数量最多，约 1.9 万个，其次是位于中国香港和美国的 IP 地址，分别控制我国境内约 1.1 万个和 0.8 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。2020 年，攻击源、攻击目标为 IPv6 地址的网站后门事件有 382 起，共涉及攻击源 IPv6 地址 101 个。

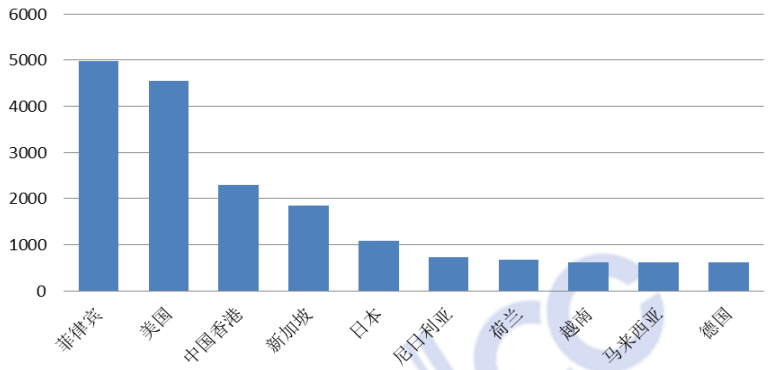

图 13 2020 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

3.网页篡改

我国境内被篡改的网站约 10 万个，同比减少 45.9%，其中被篡改的政府网站有 494 个。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 73.8%、5.2%和 1.7%，占比分布情况与 2019 年无明显变化，如图 14 所示。

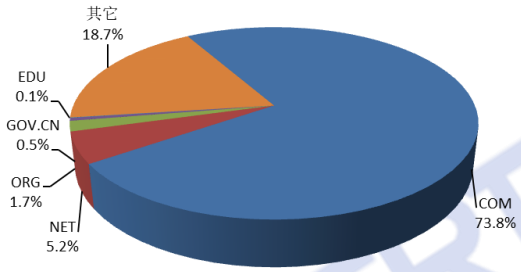

图 14 2020 年境内被篡改网站按顶级域名分布

（五）云平台安全

随着业务不断上云，发生在我国云平台上的网络安全事件或威胁数量居高不下。首先，发生在我国云平台上的各类网络安全事件数量占比仍然较高，其中云平台上遭受大流量 DDoS 攻击的事件数量占境内目标遭受大流量 DDoS 攻击事件数的

74%、被植入后门网站数量占境内全部被植入后门网站数量的88.1%、被篡改网站数量占境内全部被篡改网站数量的88.6%。其次，攻击者经常利用我国云平台发起网络攻击，其中云平台作为控制端发起 DDoS 攻击的事件数量占境内控制发起 DDoS 攻击的事件数量的 81.3%、作为木马和僵尸网络恶意程序控制端控制的 IP 地址数量占境内全部数量的 96.3%、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 83.3%。

（六）工业控制系统安全

CNCERT 持续扩大监测和巡检范围，发现境内大量暴露在互联网的工业控制设备和系统。其中，设备类型包括可编程逻辑控制器、串口服务器等，各类型占比如图 15 所示；系统涉及电力、石油天然气、轨道交通等重点行业，覆盖企业生产管理、企业经营管理、政府监管、工业云平台等几大类型，如图 16、图 17 所示。

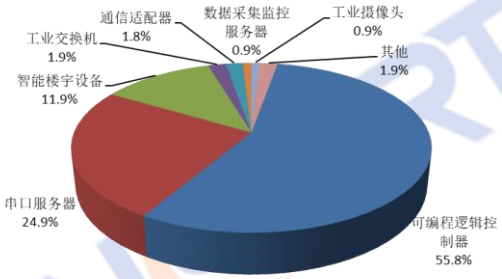

图 15 2020 年监测发现的联网工业设备的类型统计

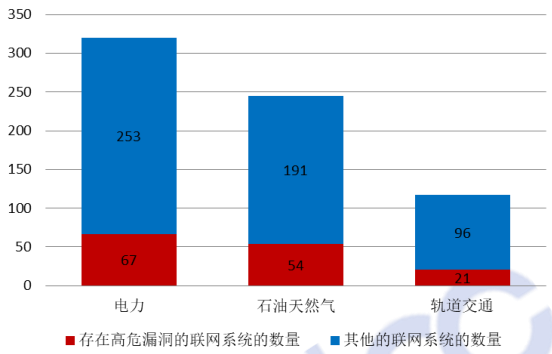

图 16 2020 年监测发现的重点行业联网监控管理系统的漏洞威胁统计

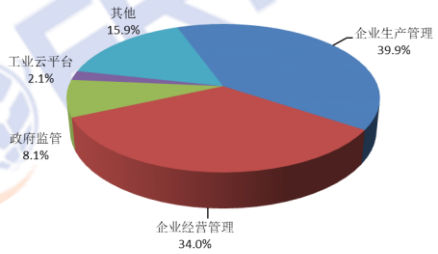

图 17 2020 年监测发现的重点行业联网监控管理系统的类型统计

（七）区块链安全

区块链领域共发生安全事件 555 起，每月均有新增安全事件。其中，9 月份发生安全的事件数量最多，达 69 起，下半年事件数量较上半年增长 32.1%。从发生事件具体领域来看，DeFi[③]、数字钱包、资产交易平台发生安全事件数量排前三名，如图 18 所示。

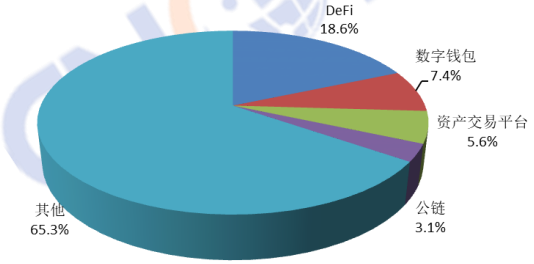

图 18 2020 年区块链相关领域发生安全事件次数统计

[③]Defi 全称是 Decentralized Finance。