国盟信息安全通报

2020 年 10 月 11 日第 226 期

全国售后服务中心

国盟信息安全通报

（第 226 期）

国际信息安全学习联盟

2020 年 10 月 11 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 369 个，其中高危漏洞 68 个、中危漏洞 239 个、低危漏洞 62 个。漏洞平均分值为 5.21。本周收录的漏洞中，涉及 0day 漏洞 109 个（占 30%），其中互联网上出现“Anchor CMS 存储型跨站脚本漏洞、BigTree CMS 远程执行代码漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2902 个，与上周（2152 个）环比增加 35%。

主要内容

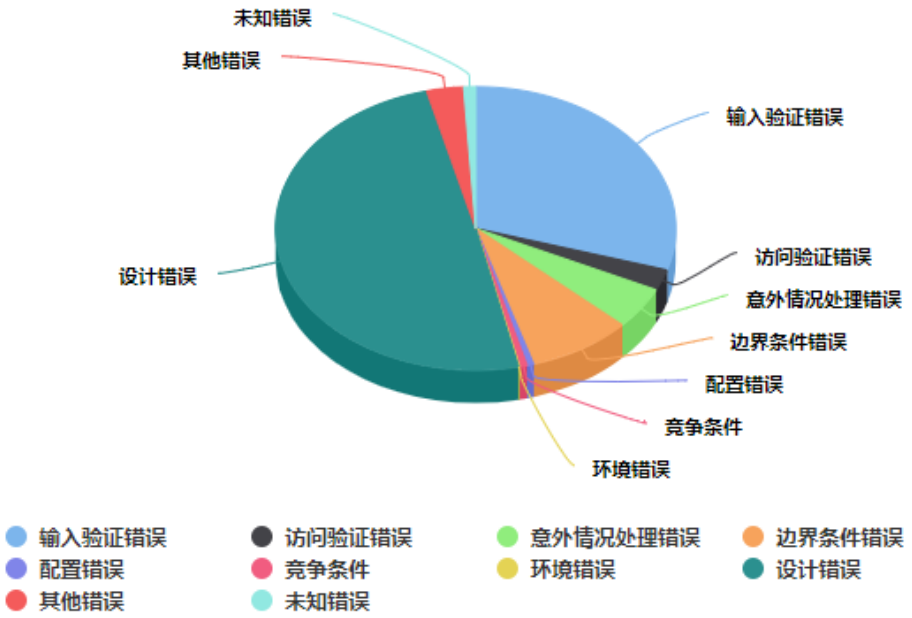
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

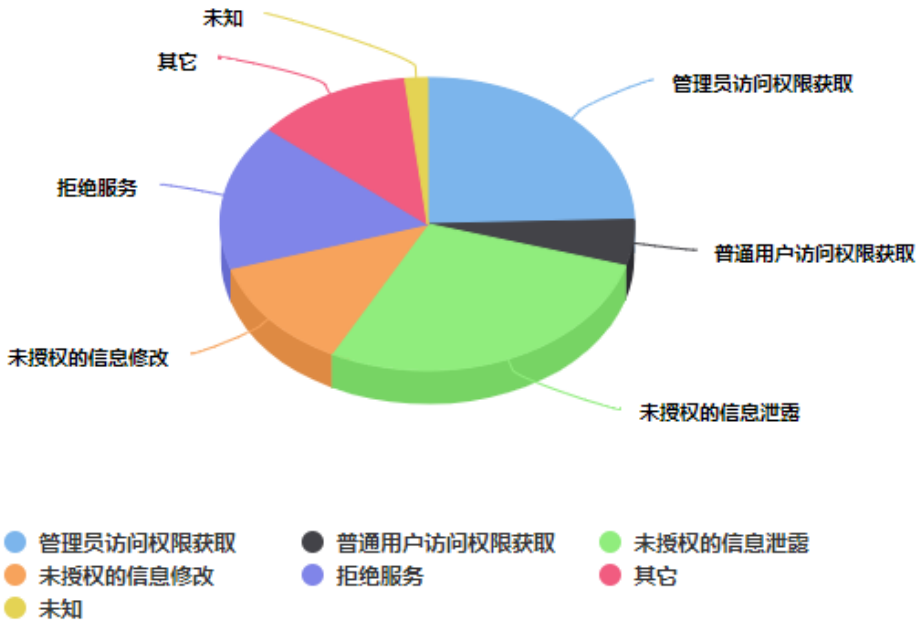
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 369 个，其中高危漏洞 68 个、中危漏洞 239 个、低危漏洞 62 个。漏洞平均分值为 5.21。本周收录的漏洞中，涉及 0day 漏洞 109 个（占 30%），其中互联网上出现“Anchor CMS 存储型跨站脚本漏洞、BigTree CMS 远程执行代码漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2902 个，与上周（2152 个）环比增加 35%。

二、安全漏洞增长数量及种类分布情况

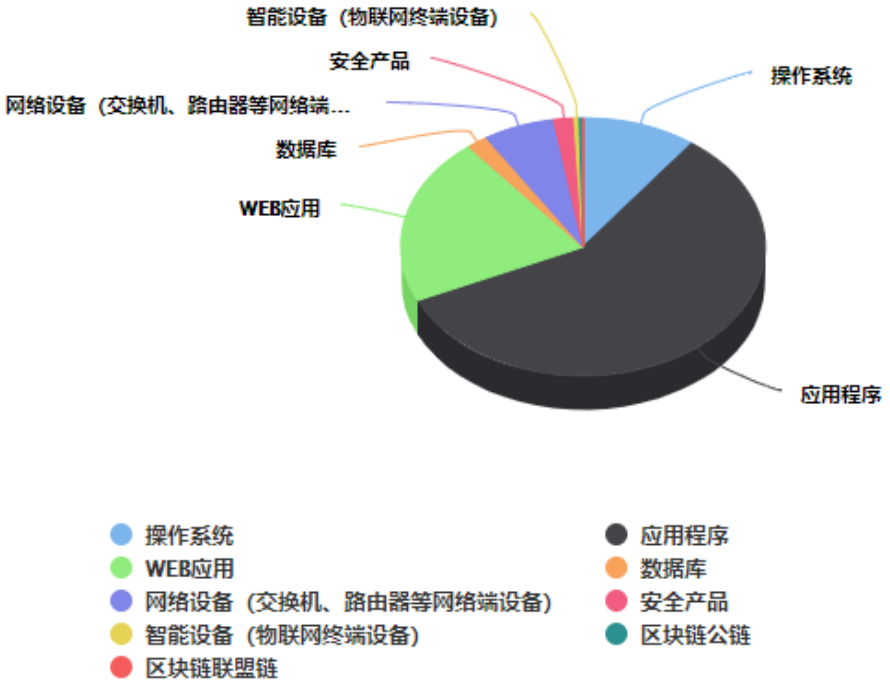
➢ 漏洞产生原因（2020 年 09 月 27 日—2020 年 10 月 11）



➢ 漏洞引发的威胁（2020 年 09 月 27 日—2020 年 10 月 11）



➢ 漏洞影响对象类型（2020 年 09 月 27 日—2020 年 10 月 11）



三、安全产业动态

➢ 制造强国和网络强国建设扎实推进

“十三五”时期是党和国家发展进程中极不平凡的五年。面对错综复杂的国内外形势，以习近平同志为核心的党中央统筹中华民族伟大复兴战略全局和世界百年未有之大变局，审时度势、科学应对，领导全国人民开创了改革开放和社会主义现代化建设新局面。工业和信息化系统坚持以习近平新时代中国特色社会主义思想为指导，坚持稳中求进工作总基调，坚持新发展理念，坚定不移推进供给侧结构性改革，紧扣高质量发展要求，扎实推进制造强国和网络强国建设，促进工业和信息化保持平稳健康发展，为全面建成小康社会提供了坚实支撑。

工业和信息化改革发展成就斐然

综合实力迈上新台阶。2016—2019 年，我国全部工业增加值由 24.54 万亿元增至 31.71 万亿元，年均增长 5.9%，远高于同期世界工业 2.9%的年均增速。2019 年我国制造业增加值占全球比重达 28.1%，连续 10 年保持世界第一制造大国地位。目前，我国是全世界唯一拥有联合国产业分类中所列全部工业门类的国家。在抗击新冠肺炎疫情的大战大考中，我国依靠完备的产业体系、强大的动员组织和产业转换能力，有效保障了应急防控医疗物资生产短时间内十几倍甚至数十倍的增长，不仅满足了国内抗疫需求，而且为全球抗疫提供了有力支

持。我国建成全球规模最大的光纤网络和 4G 网络，光纤用户和 4G 用户占比分别达 93.4%和 80%，均远高于世界平均水平。5G 商用正式启动，建成 5G 基站超过 50 万个，5G 终端连接数超过 1 亿。互联网普及率“十三五”预期目标提前完成，电子商务和移动支付交易额均居世界首位。

重点领域创新取得新突破。移动通信领域，5G 国际标准必要专利占比全球领先，基于蜂窝移动网络的车联网无线通信技术成为国际标准并加速产业化。航空航天领域，载人航天和探月工程取得系列重要成果，“天问一号”火星探测器成功发射，北斗三号全球卫星导航系统正式开通，C919 大型客机加快研制试飞。船舶及海洋工程装备领域，首艘自主建造的极地破冰科考船雪龙 2 号成功交付，“蓝鲸 1 号”首次成功开采可燃冰，首艘国产航母顺利下水。轨道交通领域，“复兴号”动车在世界上首次实现时速 350 公里自动驾驶功能。新能源汽车领域，乘用车量产车型续驶里程达 500 公里以上，动力电池单体能量密度达 270 瓦时/公斤，处于世界领先水平。高端机床装备领域，8 万吨模锻压力机、12 米级卧式双五轴镜像铣机床、1.5 万吨航天构件充液拉深装备等成功研制，配套体系初步形成。新材料领域，C919 用材、8.5 代基板玻璃等实现突破。2019 年，我国规模以上工业企业研发投入强度达 1.32%，比 2015 年提高 0.42 个百分点。

产业结构优化迈出新步伐。传统产业改造提升加快，钢铁去产能提前两年完成“十三五”目标，产能利用率和企业经营效益明显提高。战略性新兴产业和先进制造业加速壮大，智能制造深入推进，工业互联网发展进入快车道，一批数字化车间和智能工厂初步建成。截至 2020 年 6 月，制造业重点领域企业关键工序数控化率和数字化研发设计工具普及率分别达到 51.1%和 71.5%。云计算、大数据、物联网、人工智能、区块链等新技术新业态蓬勃兴起，数字经济发展势头良好，对国民经济增长的贡献率不断提高。绿色制造工程持续推进，2016—2019 年全国规模以上工业企业单位工业增加值能耗累计下降超过 15%，万元工业增加值用水量累计下降 27.5%。“增品种、提品质、创品牌”战略深入实施，标准体系持续完善。区域布局不断优化，一批先进制造业集群加快发展壮大。

优质企业发展壮大展示新气象。企业综合实力、竞争能力显著增强，一批骨干龙头企业脱颖而出。2020 年我国有 133 家企业进入《财富》世界 500 强榜单，比 2016 年增加 23 家，跃居世界首位。《福布斯》发布的 2019 全球数字经济百强企业榜单中，我国有 14 家企业上榜，中国移动、阿里巴巴跻身前十。中小企业茁壮成长，培育“专精特新”企业 2 万多家，遴选“小巨人”企业 248 家、单项冠军企业 417 家，一些科技型独角兽企业形成了自己的核心技术和重要影响力。大中小企业融通发展成效凸显，打造形成融通型和专业资本集聚型特

色载体的开发区101个，制造业重点行业骨干企业“双创”平台普及率超过80%，推动形成“龙头企业+孵化”共生共赢生态。创业创新服务体系进一步完善，培育国家小型微型企业创业创新示范基地329家，大众创业、万众创新蔚然成风。

行业发展动力活力得到新提升。“放管服”改革持续深化，工业和信息化领域行政审批事项压减一半以上，非行政许可审批事项全部取消，工业生产许可证种类减少近60%。减税降费成效初显，制造业增值税税率由17%降至13%，企业社保缴费费率从20%降至16%。今年抗击疫情期间，系列惠企政策密集出台，预计为企业新增减负超过2.5万亿元。开放合作层次显著提升，一般制造业有序放开，电信领域开放持续扩大，一批重大外资项目批复落地。与“一带一路”沿线30多个国家签署产能合作协议，高铁、核电、卫星等成体系走出国门，中国制造在全球产业链供应链中的地位和影响力持续攀升。

取得的宝贵经验和启示

我国工业和信息化改革发展成就是在国内外经济形势严峻复杂、不稳定性不确定性明显增强、风险挑战持续加大的背景下取得的，是以习近平同志为核心的党中央坚强领导的结果，是习近平新时代中国特色社会主义思想科学指引的结果，是各地区各部门协同努力、全系统团结奋斗的结果。成绩来之不易，经验弥足珍贵。

坚持和加强党的全面领导，始终把握改革发展正确方向。党的十八大以来，习近平总书记高度重视发展壮大实体经济，围绕加快推进新型工业化、促进信息化、振兴制造业提出一系列新思想、新论断、新要求，为各项工作指明了前进方向、提供了根本遵循。我们坚持以习近平新时代中国特色社会主义思想为指导，坚决贯彻落实党中央、国务院决策部署，谋划了一批重大举措，解决了一批突出问题，行业发展取得历史性成就。实践证明，必须毫不动摇坚持和加强党的全面领导，把践行“两个维护”体现到行业管理工作的各方面各环节，始终把握改革发展正确方向。

坚持以人民为中心的发展思想，不断增强人民群众的获得感、幸福感、安全感。习近平总书记强调，不断提高人民生活质量和水平，是我们一切工作的出发点和落脚点。我们着力提高供给体系质量，推进重点领域创新发展，提升信息通信服务质量和水平，抓好脱贫攻坚等三大攻坚战相关任务落实，有效满足人民群众日益增长的个性化、多层次产品和服务需求。疫情防控中，我们坚决贯彻落实习近平总书记关于“坚持把人民群众生命安全和身体健康放在第一位”的重要指示精神，全力以赴保障医疗物资供给，为疫情防控阻击战取得重大战略成果提供了有力支撑。面对我国社会主要矛盾变化的新特征新要求，必须始终践行以人民为中心的发展思想，加快调整优化现有供给结构，推动改革发展成果更多更公平惠及全体人民。

坚持新发展理念，加快推动高质量发展。我们牢固树立创新、协调、绿色、开放、共享的新发展理念，持续深化供给侧结构性改革，坚持质量第一、效益优先，把注意力集中到解决各种发展不平衡不充分的问题上来，一手抓传统产业改造提升，一手抓新兴产业培育壮大，实施制造业创新中心、工业强基等重大工程，纵深推进信息化和工业化深度融合，加强信息网络基础设施建设，实施工业互联网创新发展战略，加快制造业数字化、网络化、智能化转型，推动行业质量变革、效率变革、动力变革。新形势下，必须坚持以新发展理念引领高质量发展，坚持稳中求进工作总基调，既要坚持稳字当头，做好“六稳”工作、落实“六保”任务，保持工业通信业运行在合理区间；又要积极进取，在“巩固、增强、提升、畅通”上下功夫，提升工业基础能力和产业链现代化水平，实现量的合理增长和质的稳步提升。

坚持正确处理政府和市场的关系，增强行业发展动力与活力。习近平总书记强调，经济体制改革仍然是全面深化改革的重点，经济体制改革的核心问题仍然是处理好政府和市场关系。我们在全面深化改革上狠下功夫，加快转变政府职能，深化落实“放管服”和重点领域改革，推进产业政策向普惠化、功能性转型，提高行业治理能力，稳步推进对外开放，为制造强国和网络强国建设注入强劲动力。面对国内外发展环境的深刻变化，必须坚定不移深化改革、扩大开放，以更大的勇气、更多的举措破除深层次体制机制障碍，全面提高对外开放水平，打造市场化、法治化、国际化营商环境，使市场在资源配置中起决定性作用，更好发挥政府作用，让行业发展动力与活力竞相迸发。

坚持底线思维，坚决防范化解重大风险。习近平总书记强调，坚持底线思维，增强忧患意识，提高防控能力，着力防范化解重大风险，保持经济持续健康发展和社会大局稳定。我们加强关键核心技术攻关，打好产业基础高级化、产业链现代化攻坚战，推进城镇人口密集区危险化学品生产企业搬迁改造，加强网络与信息安全保障，促进了工业和信息化平稳健康发展。当前，世界进入动荡变革期，不稳定性不确定性明显增强，必须统筹发展和安全，牢固树立底线思维，增强忧患意识，有效应对一系列新的风险挑战，切实维护国家安全，维护社会稳定大局。

我国即将全面建成小康社会，进而乘势而上开启全面建设社会主义现代化国家新征程。制造业是国家经济命脉，信息化是经济社会发展重大趋势。我们要深刻认识肩负的责任与使命，胸怀“两个大局”，对国之大者心中有数，更加紧密地团结在以习近平同志为核心的党中央周围，坚持以习近平新时代中国特色社会主义思想为指导，坚持稳中求进工作总基调，践行新发展理念，坚持高质量发展要求，紧紧围绕构建新发展格局，以供给侧结构性改革为主线，着力深化改革开放，着力增强创新能力，着力推进融合发展，加快提高产业链供应链

稳定性和竞争力，扎实推进制造强国和网络强国建设，更好支撑我国经济行稳致远、社会安定和谐，为实现“两个一百年”奋斗目标、实现中华民族伟大复兴的中国梦作出新的更大贡献。（来源：人民日报）

➢ CNNIC 发布第 46 次《中国互联网络发展状况统计报告》

2020 年 9 月 29 日，中国互联网络信息中心（CNNIC）在京发布第 46 次《中国互联网络发展状况统计报告》（以下简称《报告》）。《报告》围绕互联网基础建设、网民规模及结构、互联网应用发展、互联网政务发展和互联网安全等五个方面，力求通过多角度、全方位的数据展现，综合反映 2020 年上半年我国互联网发展状况。

互联网激发磅礴力量，助力抗疫斗争取得重大胜利

《报告》显示，截至 2020 年 6 月，我国网民规模达 9.40 亿，较 2020 年 3 月增长 3625 万，互联网普及率达 67.0%，较 2020 年 3 月提升 2.5 个百分点。CNNIC 党委书记、副主任吴铁男指出，在此次疫情期间，我国互联网产业展现出巨大的发展活力和韧性，不仅为精准有效防控疫情发挥了关键作用，还在数字基建、数字经济、数字惠民和数字治理等方面取得了显著进展，成为我国应对新挑战、建设新经济的重要力量。

CNNIC 副主任张晓对报告进行了解读，从八个方面总结了 2020 年上半年中国互联网发展亮点：

一是“网”汇力量，“新业态”助抗疫稳大局。上半年，在线教育、在线医疗、远程办

公等应用服务在维持社会经济正常运转、稳住民生基本所需方面发挥了巨大作用。截至 2020 年 6 月，在线教育用户规模达 3.81 亿，占网民整体的 40.5%；在线医疗用户规模达 2.76 亿，占网民整体的 29.4%；远程办公用户规模达 1.99 亿，占网民整体的 21.2%。

二是“网”罗科技，“新基建”注活力扩增量。上半年，中央密集部署加快“新基建”进度，多个重要领域取得积极进展：截至 2020 年 6 月底，5G 终端连接数已超过 6600 万，三家基础电信企业已开通 5G 基站超 40 万个。工业互联网领域已培育形成超过 500 个特色鲜明、能力多样的工业互联网平台。截至 2020 年 7 月，我国已分配 IPv6 地址用户数达 14.42 亿，IPv6 活跃用户数达 3.62 亿，排名前 100 位的商用网站及应用已经全部支持 IPv6 访问。

三是“网”促发展，“新经济”扩内需助转型。截至 2020 年 6 月，我国电商直播、短视频及网络购物用户规模较 3 月增长均超过 5%，电商直播用户规模达 3.09 亿，较 2020 年 3 月增长 4430 万，规模增速达 16.7%，成为上半年增长最快的个人互联网应用，为促进传统产业转型、带动农产品上行提供了积极助力。网络零售用户规模达 7.49 亿，占网民整体的 79.7%，市场连续七年保持全球第一，为形成新发展格局提供了重要支撑。

四是“网”有温度，“新惠民”利普惠助脱贫。截至 2020 年 6 月，我国网民规模已经达到 9.40 亿，相当于全球网民的五分之一。互联网普及率为 67.0%，约高于全球平均水平 5 个百分点。城乡数字鸿沟显著缩小，城乡地区互联网普及率差异为 24.1%，2017 年以来首次缩小到 30%以内，网络扶贫作为扶贫攻坚的重要手段，已越来越多地被网民所了解和参与。

五是“网”来文化，“新传播”讲故事树新风。截至 2020 年 6 月，我国网络视频（含短视频）用户规模达 8.88 亿，占网民整体的 94.5%，其中短视频已成为新闻报道新选择、电商平台新标配。网络新闻用户规模为 7.25 亿，占网民整体的 77.1%，网络新闻借助社交、短视频等平台，通过可视化的方式提升传播效能，助力抗疫宣传报道。

六是“网”知天下，“新工具”零距离看世界。截至 2020 年 6 月，我国网络支付用户规模达 8.05 亿，较 2020 年 3 月增长 4.8%，占网民整体的 85.7%，移动支付市场规模连续三年全球第一，在疫情期间发挥了重要惠民作用，拓展了更多“+支付”的应用场景；即时通信成为疫情期间发展最快的应用之一，用户规模达 9.31 亿，较 2020 年 3 月增长 3466 万。

七是“网”填需求，“新服务”保运力补供给。受疫情影响，线上化渠道为服务业提供了新的发展窗口。网上外卖、在线教育、网约车、在线医疗等数字服务蓬勃发展，用户规模分别达 4.09 亿、3.81 亿、3.40 亿和 2.76 亿，占网民整体的比例分别为 43.5%、40.5%、36.2%和 29.4%，在满足网民需求的同时也为服务业的数字化发展提供了助力。

八是“网”谈治理，“新治理”推立法谋创新。截至 2020 年 6 月，我国在线政务服务用户规模达 7.73 亿，占网民整体的 82.2%。上半年政府治理体系不断完善、治理能力不断提升。《中华人民共和国民法典》《中华人民共和国数据安全法（草案）》逐步推动数字治理有法可依；围绕政府、平台、社会的多元协同治理体系正在加速形成；在线政务服务日趋成熟，国家政务服务平台建设成效凸显。

推进“互联网+政务服务”，疫情防控、复工复产两不误

中共中央党校（国家行政学院）电子政务研究中心主任、国家电子政务专家委员会副主任王益民认为，《报告》数据充分体现了上半年在疫情的淬炼下，我国互联网+政务服务水平不断提升，数字治理体系不断完善。一是国家政务服务平台建设成效凸显。截至 2020 年 6 月，国家政务服务平台注册用户达 1.26 亿人，总计访问人数 10.02 亿人，总浏览量 58.91 亿次。“横到边、纵到底”的“覆盖城乡、上下联动、层级清晰”五级网上服务体系初步形成。二是网格化治理推陈出新，多个省市的城乡社区都通过社区微信群、小程序等数字化工具积极开展防疫工作，成为基层治理的一大创新。三是“互联网+政务服务”有力助推疫情后复工复产，国家政务服务平台陆续推出“小微企业和个体工商户服务专栏”和疫情防控、复工复产、就业服务等 15 个服务专题，同时建设“防疫健康信息码”，汇聚并支撑各地共享“健康码”数据 6.23 亿条，累计服务 6 亿人次，成为此次大数据支撑疫情防控的重要创新。

我国网民安全体验持续提升，网络安全环境进一步改善

中国互联网协会副理事长黄澄清表示，2020 年上半年在国家互联网信息办公室、工业

和信息化部等相关部门针对各类网络安全问题进行持续打击下，我国网络安全环境呈现出不断向好的发展态势。一是在政策制定层面，《中华人民共和国民法典》《中华人民共和国数据安全法（草案）》等相关法律法规的陆续出台，推动我国网络安全法律体系持续完善。二是在基础设施方面，我国大力推进国家顶级域名解析节点部署，先后引入 F、I、L、J、K 根镜像服务器，推动网络基础设施安全保障更加完备。三是在用户安全方面，《报告》数据显示网民遭遇网络安全问题日趋改善，未遭遇任何网络安全问题的网民占比连续五年保持提升。四是在产业发展方面，我国网络安全产业发展进入“快车道”，现有网络安全产品和服务已经从基础网络安全领域延伸到云服务、大数据、物联网、工业控制、5G 等不同应用场景，实现了对于基础设备、基础技术、安全系统、安全服务等多个维度的全面覆盖。

“新基建”背景下，数字经济新业态助力提升中国经济“韧性”

国家创新与发展战略研究会副理事长，中国科学院大学网络经济和知识管理研究中心主任吕本富认为，在上半年新冠肺炎疫情的冲击下，中国经济被迫拉伸了“韧带”，在供应链、企业管理和商业活动等方面都面临着全新的挑战。而数字经济的新业态、新模式以及数字技术的迅猛发展，为提升中国经济“韧带”的韧性，推动形成新的经济增长点提供了重要的支撑。一是 5G、工业互联网等数字技术为数字经济提供了底层基础。借助数字技术，大规模匹配算法和高速网络传输到云端，信息的传输更快、能量的耗散更少，推动数字经济成为“低熵经济”。二是网络购物等数字消费为推动经济内循环提供了新动力。上半年，网络零售的规模已经超过社会消费品零售总额的四分之一，对消费的支撑作用进一步增强。此次《报告》数据显示，生鲜电商、农产品电商、跨境电商、二手电商等电商新模式也保持较快发展，用户规模分别达到 2.57 亿、2.48 亿、1.38 亿和 6143 万，在推动农产品上行、带动消费回流和促进闲置经济发展方面发挥了积极作用。三是以远程办公等为代表的数字服务正在形成新的服务业态。从《报告》中可以发现，在线教育、在线医疗、远程办公的用户规模分别达 3.81 亿、2.76 亿和 1.99 亿，成为极具发展潜力的互联网应用，在推动服务业创新的同时不断增强经济的韧性。

网络扶贫成效显著，要对标乡村振兴建立长效机制

原中国社会科学院信息化研究中心主任汪向东认为，此次《报告》用多个维度数据记录了我国在网络扶贫方面取得的显著成效，非常难得。一是农村实现网络覆盖，城乡差异显著缩小。《报告》数据显示，上半年农村地区互联网普及率为 52.3%，较 2020 年 3 月提升 6.1 个百分点，城乡地区互联网普及率差异缩小 6.3 个百分点。二是农村和城市“同网同速”的时代正在到来。全国贫困村通光纤比例从 2017 年的不足 70%提升至 98%，深度贫困地区贫

困村通宽带比例从 25%提升至 98%。三是网络扶贫成效得到广大网民认可。截至 2020 年 6 月，认可互联网在“为贫困群众提供帮助”“通过电商助力农产品销售”“为贫困群众提供更多工作和医疗教育机会”的网民比例较 2020 年 3 月均有所提升。汪向东还表示，网络扶贫要在巩固和扩大脱贫攻坚成果的基础上对标乡村振兴，建立长效机制，需要通过网络消费扶贫实现从助力限期脱贫到助力稳定脱贫，从扶助绝对贫困到扶助相对贫困，从“输血”到“造血”，从助力扶贫到振兴产业的转变。（来源：网信中国）

- **第 46 次《中国互联网络发展状况统计报告》全文**
- http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202009/P020200929546215182514.pdf

➢ 健全数据分级分类规则，完善网络数据安全立法

随着信息技术和人类生产生活交汇融合，通过网络收集、存储、传输、处理和产生的各种电子数据迅猛增长、海量聚集并成为重要的市场经济要素，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。2016 年 11 月颁布的《网络安全法》建立了网络数据安全相关制度，2019 年 5 月《数据安全管理办法》草案公开征求意见，2020 年 7 月《数据安全法》草案公开征求意见，数据安全已经成为网络安全乃至国家安全法制体系中的核心内容之一。在即将构建形成的数据安全和个人信息保护体系下，应当更加具体地回应网络数据利用和保护的正当需求，通过配套条例和规章健全数据分级分类规则，完善网络数据安全立法。

一、确立网络数据安全分级分类的基本思路

传统网络数据安全侧重于静态保护，主要是防止网络数据泄露、窃取、篡改、毁损，维护网络数据的完整性、保密性和可用性。新一代网络数据安全处于数字经济繁荣发展和全面数字化转型的新时代，需要适应动态保护的需求，确保数据在各类场景下收集、利用、流转、开放、共享等不同行为时的安全与自由。场景差异会形成不同的正当价值和安全风险，分级分类保护应当成为网络数据安全立法的基本思路。

数据分级分类最初是网络运营者对数据资产进行一致性、标准化管理的方法，随后成为网络数据安全风险管理的技术方案。根据《网络安全法》第21条的规定，网络运营者应当采取数据分类、重要数据备份和加密等措施。《数据安全法（征求意见稿）》第19条提出：国家对数据实行分级分类保护。由此可见，数据分级分类的主体由“网络运营者”转变为“国家”，国家对数据进行分级分类的方法不仅包括制定重要数据目录，更需要结合典型的数据应用场景制定配套的网络数据安全法规。只有在数据安全配套法规中确立基本的数据分级分类规则，才能为制定数据分级分类目录、技术标准和企业数据安全管理实践提供更加明确的统一指引。

从联系的角度而言，数据分级分类也可以称之为数据分类保护，这是因为数据分级也是对数据进行分类的一种表现形式。从区分的角度而言，数据分级是对数据分类之后采取的安全等级规则。国家在数据安全立法中，应当根据数据对国家安全、公共利益或者公民、组织的不同意义和可能的损害后果，对不同类别的数据分别采取严格保护、内容监管、鼓励流动、强制公开等不同管理方法的数据利用规则，并对不同级别的数据分别采取不同授权和责任模式的数据处理规则。

数据分类是对数据应用过程中涉及的数据进行分类，按照来源可以区分为公共数据、组织数据和个人数据，按照数据的公开程度可以区分为网络公开数据、有限公开数据和秘密保护数据，它们在法律中应当具有不同的安全与发展规则。结合不同的应用场景，还可以对这些数据做进一步分类。例如，我国《宪法》第40条建立了严格的私人通信保护制度，主要规范对象是电信运营商和国家机关，但是现代的互联网通信工具和交流平台形成了通信内容容易被转发，私人通信联络和公共信息传播界限不清的问题，不利于建立与数据类型相适应的安全保护秩序。所以，有必要在互联网通信场景下区分私人通信和公共信息，便于网络运营者和用户明确其所处网络社交场景的私人属性或者公共属性，从而按照分类管理的思路建立私人通信严格保密、公共信息有序管理的网络数据安全规范。

数据分级处理规则主要适用于个人数据，包括不同类型的个人数据存在安全等级差异，以及同一类个人数据在不同场景下的安全等级差异。根据《个人信息安全规范》，个人数据

可以划分为一般数据、敏感数据和高度敏感数据三类。其中，收集一般个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。此外，个人生物识别信息属于高度敏感数据，收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。对于这些推荐性国家标准中的管理性规范，需要通过立法程序转化为相应的法律规则。

二、引导公共属性数据相互共享和对外开放

公共属性的数据也被称之为公共利益数据，是由政府部门或者网络运营企业收集、存储，但属于社会中各类人力资源、财产资源共同参与创造的数据，可以在政府和企业之间相互共享，也可以基于公共利益目的对外开放。公共属性数据的共享与开放包括企业对政务数据的使用（G2B）、政府机构对企业数据的使用(B2G)、政府不同部门之间的数据共享（G2G）。

G2B 数据在国内外已经形成普遍共识的政务数据开放趋势。例如，国家地理信息数据可以为旅游或者交通产品开发提供基础，司法机关的裁判数据可以为企业合规和法律研究提供帮助。G2G 数据的共享主要是政府内部数据平台建设和数据融合能力的建设问题，它可以提高政府内部管理的一体化水平，同时也可以为单一市场中运营的企业减轻重复报送数据的成本。B2G 方向的数据开放与共享属于一个近年来才意识到重要性问题，由于涉及到网络运营企业商业秘密、企业数据私有财产保护、个人信息安全保护义务等价值冲突，是需要数据安全法规进行协调的重要领域。

数字经济的发展使得网络运营企业积累了大量的数据，充分利用其中具有公共属性的数据，有助于完善城乡规划、道路交通、民生保障、生态环境、社会安全、自然灾害、公共健康等社会管理和公共事务，帮助政府建立基于实证数据的公共决策方向。例如，道路交通导航地图运营商的数据可以为早晚高峰的交通拥堵治理提供支撑，医院治疗疾病的数据可以为公共健康防治提供决策依据，汇总的、匿名的社交媒体数据可以为传染病防控措施及其效果提供信息参考。

严格保护个人数据安全的欧洲，也在长期推进企业与政府部门之间的数据共享。2018 年 4 月，欧洲委员会通信网络内容与技术执行署就发布了《欧洲数据经济中的私营部门数据共享指南》，提出了 B2G 数据共享的模型和基本原则。欧盟委员会在 2020 年 2 月发布的《欧洲数据战略》明确了 B2G 数据共享的重要性，欧盟 B2G 数据共享高级别专家组也在同一时

间发布了《迈向基于公共利益的企业对政府数据共享的欧洲战略》（Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest），不仅总结了 B2G 数据共享存在的现实问题，还从法律、技术、管理等多个维度提出了可能的解决方案。

我国数字经济的发展也形成了大量掌握在企业手中的公共属性数据，在制定数据安全法规过程中，需要按照数据场景化管理的思路，区分政府调取企业数据、企业向政府共享数据两种类型。对于政府调取企业数据，需要在内容上划定政府调取网络运营企业数据的范围，在程序上确定政府调取数据的方法，在责任上明确政府的安全保障责任，在外部监督上建立备案审查和权利救济机制。对于企业向政府共享数据，主要是按照平等协商的机制实现，注重提高数据共享技术的安全性和数据利用的有效性，同时要避免损害他人合法权益。企业与政府之间无论是调取还是共享数据，政府都应当考虑企业数据的质量和处理成本，为企业提供公共属性数据作出必要的经济补偿，或者向企业提供数据反馈等其他合理的对价。

企业掌握的公共利益数据可以为个人和组织提供信息获取服务，同时可以为各类研究人员、公共机构、中小企业、初创企业参与科技创新和数字经济发展提供便利。对于与公共利益有关的数据，政府应当按照法定的程序向社会或者特定申请人公开其获得的企业数据。但是，政府从企业获取的数据一般不得超出法定使用目的范围，特别是要避免行政权力对数据自由竞争市场的不正当干预。

三、推动企业数据安全有序的利用与流转

企业数据是企业通过合法形式取得的具有完全权属、有限权属、无权属的各类数据。企业对于无权属的他人数据只能按照约定目的和方式进行管理和使用，对于处理大量他人数据的网络运营者应当依法建立数据安全体系，为他人提供数据收集、存储、加工、分析、传输等服务的企业，应当通过向主管部门备案、建立相互隔离的数据安全环境等措施。对于完全权属和有限权属的数据，企业可以在权利范围内进行交易、共享和开放。

企业可以通过买卖、互换、许可使用等方式交易其合法取得且有相应处置权利的数据。随着数据价值的上升，数据被国家列为与土地、劳动力、资本、技术等相并列的生产要素，在国内外市场中诞生了行纪、中介和代理等多种类型的数据交易中间商。《数据安全（征求意见稿）》第 30 条规定：从事数据交易中介服务的机构在提供交易中介服务时，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。然而，何种数据可以进行交易，数据可以如何进行交易，数据交易中如何保障安全，需要相关配套规定进一步细化规则。在《民法典》确认数据财产权的基础上，尚需要进一步明确数据财产权的分配规则，特别是明确物联网等共同创建数据的权利归属和权利行使规则，并对数据交易合同的相

关法律适用规则予以规范。此外，需要明确数据交易参与方的职责和监管制度，促进形成一批专业能力强、运营规范、抗风险能力强的数据交易中间服务机构。

企业数据共享是以无偿形式为他人利用自身数据提供便利的一种方式，企业除了向政府共享数据外，还可以向其他企业共享其数据，包括在同一生态内的不同企业、不同生态内的不同企业之间进行数据共享，甚至是同一企业的不同部门。在不同企业之间进行数据共享有利于提升数据平台的服务能力、减少数据重复收集的成本，特别是大量汇聚第三方应用、第三方商店的平台存在大量数据共享行为，但是接受数据共享的处理者可能引发不确定性数据泄露或者滥用的风险。一方面，我们应当鼓励数据安全管理能力强的平台企业向他人共享数据，不仅可以缩小数据鸿沟，还可以避免中小企业数据安全管理能力不足引发的风险。另一方面，不同主体之间开展数据共享需要明确各自的安全管理职责，并按照过错原则承担相应的法律责任。

互联网的本质是数据流动，打破数据垄断和避免数据孤岛是企业数据开放的主要目标。企业数据开放的对象包括企业自主拥有的、具有数据基础设施地位的数据，也包括在企业平台上展示的网络公开数据。对于具有数据基础设施地位的数据或者数据设施，应当要求企业按照透明、公平、合理、非歧视原则提供必要的开放利用条件。对于网络公开数据，企业应当建立公平、自由的访问规则，避免采取不合理的访问限制措施。与此同时，数据爬虫技术改变了网络公开数据获取的传统规则，一方面要支持符合行业惯例的数据获取行为，从而为数据产业的发展提供必要的法律环境；另一方面，应当为企业采取“Robot 协议”等措施保障其系统正常运行提供必要的强制性保障。

四、确保新技术对个人数据利用的安全

信息技术的创新发展优化了个人数据的利用效率和方式，出现了用户画像、个性化推荐、自动化决策、深度伪造、人脸识别等提升个人数据利用风险的新技术，也出现了差分隐私、多方计算等减少个人数据利用风险的新技术。在数据安全配套法规中，应当引导网络运营者

采取有利于个人数据安全利用的新技术，通过技术手段实现安全和发展的双重目标，有效避免个人数据利用过程中出现的安全风险。对于各类挖掘个人数据潜在价值的新技术，应当进行数据安全风险评估，并在相关法规中建立场景化的数据利用规则。

人脸识别是国内外舆论广泛关注的个人数据使用技术，对于何种场景可以利用，人脸生物信息如何存储，如何保障此类高度敏感数据的安全，需要建立配套的法律规则。缺乏人脸等个人生物识别信息的安全规则容易引发舆论的恐慌，安全可控的法律规则不仅可以增强消费者对新技术的信心，还可以为新技术的部署提供稳定的指引和预期。

用户画像、个性化推荐都是基于用户的个人信息和网络使用行为所形成的数据融合和算法应用，其可能提高信息的获取效率，但是也可能导致个人被标签化或者隐私泄露，故而应当为这类行为提供“选择-退出”的功能，避免对个人强迫提供技术服务。

自动化决策和深度伪造对于个人的权益往往会产生直接的影响，甚至在某些情况下会严重影响社会公共秩序。对于自动化决策，应当提高此类算法的透明度和可解释性，避免算法黑箱风险。对于深度伪造等信息聚合技术，应当通过标记等规则避免数据滥用行为。

目前，《欧洲数据战略》已经明确提出了一系列数据安全与利用的配套立法计划，美国联邦和各地方也在出台一系列数据利用的补充法律制度。我国在《网络安全法》已经颁布施行，《数据安全法》和《个人信息保护法》处于起草中的背景之下，还需要同时启动网络数据安全相关配套法规的立法储备工作，构建法律、行政法规和规章衔接配套的网络安全、数据安全和个人信息保护的法律协调体系。在行政法规层面进行网络数据安全管理制度的立法储备工作中，应当着力细化《网络安全法》《数据安全法》和《个人信息保护法》中的相关规则，吸收《数据安全管理办法（征求意见稿）》和国内外数据安全法治最新进展的经验，按照数据分级分类管理的思路，科学划分数据的应用场景，通过一般规则和场景规则相结合的模式建立具有可操作性的配套法律制度。（来源：清华大学法学院助理研究员 刘云）

➢ 个人信息保护法草案本月将正式亮相

2020 年 10 月 4 日，一直备受关注的个人信息保护法草案即将揭开神秘面纱于本月正式亮相。消息显示，十三届全国人大常委会第七十二次委员长会议决定于 10 月 13 日至 17 日在京举行十三届全国人大常委会第二十二次会议。根据委员长会议建议，本次常委会将审议全国人大常委会委员长会议关于提请审议个人信息保护法草案的议案。

就在不久前，一则“清华大学教授拒绝人脸识别门禁”的消息引发了热议。此前，江苏常州部分社区强制居民“刷脸进社区”也曾引发争议。近年来，随着大数据、人工智能等新技术的发展，个人信息的收集、应用更加广泛，加强个人信息保护的任务也更加艰巨。个人信息泄露事件频现，引发了广泛的公众关注。尤其是新冠疫情期间，个人信息泄露问题不时见诸媒体，包括人脸识别在内的人体生物信息采集技术的愈发广泛的应用，更是引发了个人信息保护的担忧。在技术不断发展的今天，如何处理好个人信息利用和保护已经成为突出问题。

从 2018 年开始抓紧开展研究起草工作

个人信息保护事关广大人民群众的切身利益，事关国家信息安全，事关数字经济发展。一直以来，个人信息安全问题是社会各界关注的焦点，有关个人信息保护的立法呼声也很高。

近年来，按照党中央的决策部署，全国人大及其常委会在制定、修改网络安全法、刑法、电子商务法等法律中，对个人信息权益、个人信息处理规则、个人信息安全保护措施等都作出了相关的规定，不断完善个人信息保护相关法律制度，但是都不是集中的全面的规定，针对个人信息保护的专门性立法迟迟未出台。据了解，按照全国人大常委会立法规划和立法工作计划安排，从 2018 年开始，法工委就会同中央网络安全和信息化委员会办公室在认真总结网络安全法等法律实施经验、深入研究个人信息利用和保护中的突出问题、借鉴有关国家和地区法律制度的基础上，抓紧开展个人信息保护法的研究起草工作。

民法典为专门立法提供基本依据

值得一提的是，今年 5 月，十三届全国人民代表大会第三次会议审议通过了我国首部民法典。民法典将于 2021 年 1 月 1 日施行。此次民法典的最大亮点之一就是人格权编单独成编，对个人信息受法律保护的权利内容及其行使等作了原则规定。

“应当说，民法典为个人信息保护法的制定提供了基本依据。” 谈及民法典与个人信息保护法之间的关系，清华大学法学院教授程啸指出，民法典作为市民社会和市场经济的基本法，其对个人信息保护的规定侧重于确立大的原则方向、规定最重大、最基本的问题，如个人信息的界定、私密信息保护的法律适用、个人信息权益的内容以及个人信息的合理使用制度等。而个人信息保护法在很大程度上就个人信息和隐私权保护领域中与民法典相关联、相配套的法律。

“个人信息保护法本身并非单纯的民事特别法，而是一部运用民事、行政、刑事等综合性手段对于个人信息加以保护，对于自然人个人信息权益、信息自由、公共利益等多重利益关系加以协调的法律。”程啸说。

出台个人信息保护法必要且重要

在当前网络信息科技高速发展，尤其是世界各国都非常重视对于个人信息和数据保护的大背景下，对于个人信息保护进行专门的立法即制定个人信息保护法十分必要且重要。

“可以说，个人信息保护法是个人信息保护领域中最为全面最为集中的法律规范，有了这样一部法律，我国就真正形成了以民法典、个人信息保护法为核心的，相关领域特别法为辅助的科学合理的个人信息保护法律规范体系。”程啸说。

他同时强调指出，制定个人信息保护法的基本出发点就是落实宪法的规定，实现党的十九大提出的保护人民人身权、财产权和人格权的要求，充分保障自然人的人格尊严和自由，同时也能够更好地适应互联网和大数据时代发展的需要，推进国家治理体系和治理能力的现代化。特别是在当前复杂的国际斗争形势下，制定一部我国的个人信息保护立法也有利于全面提升我国的信息安全，更好地保护我国公民、法人和非法人组织的合法权益。

五大立法内容值得重点关注

那么，此次个人信息保护法中都有哪些内容需要重点关注呢？程啸认为，五方面内容值得期待：

首先，如何通过确立科学合理的个人信息处理规则来协调自然人的个人信息权益保护与信息自由流动、合理使用之间的关系。其中，告知和同意规则是个人信息处理的基本规则。一方面对于敏感的个人信息必须确立严格的告知和同意规则，即非经告知并取得同意不得处理，除非法律、行政法规基于公共利益或者维护信息主体自身合法权益而作出特别的规定。

另一方面，非敏感的个人信息、公开的个人信息等在必须且合理的前提下还是应当尽量允许使用，同时要符合比例原则的要求。

其次，对于个人信息权益的内容和行使要进行更具体的规范。目前对于是否需要规定被遗忘权、个人数据可携带权等仍然存在很大的争论。此外，对于自然人就其个人信息的查询权、复制权、更正权、删除权等如何行使，也需要作出更具体、更明确的规定。

再次，对于国家机关和承担行政职能的法定机构处理个人信息的专门规定。政府部门处理个人信息不同于私人企业，它们是因为要履行法定的职责，是为了公共利益，具有强制性。也就是说，对于国家机关而言必须处理相应的个人信息，对于自然人而言，则必须提供相应的个人信息。同时，国家机关因为没有履行个人信息安全保护义务等违法行为而产生的赔偿责任，属于国家赔偿责任。

第四，对于个人信息的跨境转移加以科学规范。这涉及到国家安全、公共安全以及公共利益的保护的问题，因此要详细规范个人信息的境内存储和安全评估以及何种情形下可以进行跨境转移。

第五，个人信息安全问题，即如何通过综合的措施（自律和他律）来保护个人信息的安全，防止出现个人信息泄露、非法买卖、非法利用等，以及个人信息被泄露或被非法利用后的民事责任、行政责任以及刑事责任等。具体而言，在侵害个人信息的民事责任中需要明确归责原则究竟是过错责任、过错推定责任还是无过错责任，同时，明确赔偿的范围和计算方法等。

此外，由于目前我国个人信息保护领域存在“九龙治水”的局面，相关部门对于各自领域的个人信息都负有保护和管理职责，如网络、金融、医疗卫生、教育、工信、消费者保护、不动产登记等都涉及到对相应的个人信息进行管理和保护的职责，是否有必要设立一个独立的个人信息保护机构来专门负责个人信息的保护与执法工作，对于个人信息保护机构作出专门的规定，也是值得关注的问题。（来源：法制日报）

四、政府之声

➢ 中国人民银行印发《金融数据安全数据安全分级指南》

2020 年 9 月 23 日，中国人民银行正式发布《金融数据安全数据安全分级指南》（JR/T 0197—2020）金融行业标准。标准给出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程，并给出了金融业机构典型数据定级规则供实践参考，适用于金融业机构开展数据安全分级工作，以及第三方评估机构等参考开展数据安全检查与评估工作。

《指南》列出的影响对象包括国家安全、公众权益、个人隐私、企业合法权益等;影响程度从高到低划分为非常严重、严重、中等和轻微;附录中给出了金融行业典型数据类型及建议划分的最低安全级别。值得注意的是，《指南》特别强调金融业机构应高度重视个人金融信息相关数据，在数据安全定级过程中从高考虑。其中，个人金融信息中的 C3 类信息(主要为用户鉴别信息，如各类账户密码)属于 4 级数据;C2 类信息(主要包括支付账号、动态口令等)为 3 级数据;C1 类信息(主要包括账户开立时间、开立机构等)为 2 级数据。（来源：中国人民银行）

- **《金融数据安全数据安全分级指南》**
- **全文：**https://www.cfstc.org/bzgk/gk/view/bzxq.jsp?i_id=1873

➢ CNCERT:《2020 年上半年我国互联网网络安全监测数据分析报告》 发布

2020 年 9 月 26 日， CNCERT 对上半年监测数据进行了梳理，形成《2020 年上半年我国互联网网络安全监测数据分析报告》。

“外交部发言人办公室”消息，在 9 月 29 日外交部例行记者会上，有记者问：据报道，中国国家互联网应急中心日前发布的 2020 年上半年中国互联网网络安全监测数据分析报告显示，中国遭受来自境外的网络攻击持续增加，美国是针对中国网络攻击的最大来源国。中方对此有何评论？汪文斌：我们注意到这份报告。报告内容反映了中国在网络安全领域面临的一些突出挑战。报告内容反映了中国在网络安全领域面临的一些突出挑战。首先，中国仍是网络攻击的主要受害者之一，在疫情期间遭受的网络攻击有增无减。其次，美国是针对中国网络攻击的最大来源国。从境外计算机恶意程序捕获次数、境外恶意程序控制服务器数量、境外拒绝服务攻击（DDoS）次数、向中国境内网站植入后门等多项指标看，美国都高居首位。第三，针对中国关键信息基础设施的网络侦察值得关注。报告显示，中国工业控制系统的网络资产持续遭受来自境外的扫描嗅探，日均超过 2 万次，目标涉及境内能源、制造、通信等重点行业的联网工业控制设备和系统。与其他类型网络攻击相比，上述网络侦察行动更可能具有较强的政府背景。在此情况下，中方更有理由对此前美国媒体关于美大力推行网络空间“持续交手”战略、降低授权门槛肆意对他国关键信息基础设施发动攻击的报道表示担忧。我想强调的是，网络攻击是各国面临的共同挑战，中国一贯主张各国在相互尊重、平等互利的基础上加强对话合作，共同应对这一挑战。我们也呼吁各国在网络空间采取负责任的行为。

中国将采取必要措施，增进自身网络安全，特别是保护关键信息基础设施免受威胁和破坏。（来源：国家互联网应急中心、外交部）

- **《2020 年上半年我国互联网网络安全监测数据分析报告》**
- **全文：**https://www.cert.org.cn/publish/main/upload/File/2020Report(2).pdf

➢ 《北京市促进数字经济创新发展行动纲要(2020-2022 年)》通知发布

2020 年 9 月 22 日，由北京市经济和信息化局组织编制的《北京市促进数字经济创新发展行动纲要(2020-2022 年)》(以下简称《行动纲要》)，经报市政府批准，日前正式发布。《行动纲要》提出，将北京市打造成为我国数字经济发展的先导区和示范区；建设成为国际数字化大都市、全球数字经济标杆城市。

《行动纲要》提出，以全面推动北京市数字经济高质量发展为方向，围绕基础设施建设、数字产业化、产业数字化、数字化治理、数据价值化和数字贸易发展等任务，开展九项重点工程。按照《行动纲要》，到 2022 年，北京市数字经济增加值占地区 GDP 比重达到 55%；基础设施建设及数字产业化能力不断夯实提升，建设完善的数字化产业链和数字化生态；一二三产业数字化转型持续深化，中小企业数字化赋能稳步推进，产业数字化水平显著提升；基本形成数据资源汇聚共享、数据流动安全有序、数据价值市场化配置的数据要素良性发展格局；突破制约数字经济发展的体制机制约束和政策瓶颈，建立数字贸易试验区，开展数据跨境流动安全管理试点，构建适应开放环境的数字经济和数字贸易政策体系。（来源：北京市经济和信息化局）

- **《北京市促进数字经济创新发展行动纲要(2020-2022 年)》全文：**

- http://www.beijing.gov.cn/zhengce/zhengcefagui/202009/W020200924388973594427.pdf

➢ 《贵州省政府数据共享开放条例》发布

2020 年 9 月 23 日-25 日，贵州省第十三届人民代表大会常务委员会第十九次会议在贵阳举行，会议表决通过了《贵州省政府数据共享开放条例》(以下简称《条例》)，《条例》自 2020 年 12 月 1 日起施行。

《条例》共七章 45 条，从政府数据管理、政府数据共享、政府数据开放、监督管理等明确贵州省政府数据共享开放事项。官方表示，《条例》旨在推动政府数据共享开放，加快政府数据汇聚、融通、应用，培育发展数据要素市场，提升政府社会治理能力和公共服务水平，促进经济社会发展。《条例》规定：“政府数据共享开放应当具有合法目的和用途，遵循正当、必要、适度的原则，依法维护国家安全、公共安全、经济安全、社会稳定，保守国家秘密，保护商业秘密、隐私和个人信息。”

《条例》明确，政府数据共享开放应当在全省统一的政府数据共享平台、开放平台上进行。省人民政府大数据主管部门负责全省统一的政府数据共享平台、开放平台的建设和运行维护。鼓励各市、州人民政府通过全省统一的政府数据共享平台建设本行政区域的基础数据、主题数据。此外，《条例》还规定，任何单位或者个人对获取到的有条件共享开放的政府数据，不得擅自转让、改变用途或者使用范围，不得利用政府数据从事违法犯罪活动。擅自转让获取的有条件开放的政府数据、改变用途或者使用范围的，由县级以上人民政府大数据主管部门责令改正，有违法所得的，没收违法所得，并可处以违法所得 1 倍以上 10 倍以下罚款；没有违法所得的，处以 1 万元以上 5 万元以下罚款。（来源：贵州日报）

五、本期重要漏洞实例

➢ Microsoft Windows ActiveX Installer Service 权限提升漏洞

发布日期：2020-09-21
更新日期：2020-09-21
受影响系统：
Microsoft Windows Server 2008 R2 SP1
Microsoft Windows 7 SP1
Microsoft Windows Windows Server 2012
Microsoft Windows 8.1
Microsoft Windows RT 8.1 SP0
Microsoft Windows Server 2012 R2
Microsoft Windows 10
Microsoft Windows 10 1607
Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Microsoft Windows Server 1903
Microsoft Windows 10 1709
Microsoft Windows 10 1803
Microsoft Windows 10 1809
Microsoft Windows 10 1903
Microsoft Microsoft Windows Server 1909
Microsoft Windows 10 1909
Microsoft Windows Server 2004
Microsoft Windows 10 2004
描述：

CVE(CAN) ID: CVE-2020-1402
Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。
Microsoft Windows ActiveX Installer Service 存在权限提升漏洞，该漏洞源于 Windows ActiveX 安装程序服务未能正确处理内存，攻击者可通过运行特制应用程序利用该漏洞提升权限。
建议：

厂商补丁：
Microsoft
厂商已发布了漏洞修复程序，请及时关注更新：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1402

➢ Google Chrome 数据验证不足漏洞

发布日期：2020-09-23
更新日期：2020-09-23
受影响系统：
Google Chrome <85.0.4183.121
描述：

CVE(CAN) ID: CVE-2020-15964
Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具，其特点是简洁、快速。
Google Chrome 85.0.4183.121 之前版本中的媒体存在数据验证不足漏洞。远程攻击者可通过特制 HTML 页面利用该漏洞导致堆损坏。
建议：

厂商补丁：

Google
厂商已发布了漏洞修复程序，请及时关注更新：
https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html

➢ McAfee VirusScan Enterprise 权限许可和访问控制问题漏洞

发布日期：2020-09-22
更新日期：2020-09-22
受影响系统：
Mcafee VirusScan Enterprise <8.8 Patch 14
描述：

CVE(CAN) ID: CVE-2019-3585
McAfee VirusScan Enterprise（VSE）是美国迈克菲（McAfee）公司的一套杀毒软件。该软件提供全方位的安全防护、扫描内存以查找恶意代码和为远程系统优化更新等功能。
McAfee VSE 8.8 Patch 14 之前版本中的 Microsoft Windows client (McTray.exe)存在权限许可和访问控制问题漏洞。本地攻击者可通过运行 McAfee Tray 利用该漏洞以较高的权限与 On-Access Scan Messages - Threat Alert 窗口进行交互。
建议：

厂商补丁：
McAfee
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://kc.mcafee.com/corporate/index?page=content&id=SB10302

➢ Cisco Aironet Access Points UDP Flooding 拒绝服务漏洞

发布日期：2020-09-24
更新日期：2020-10-09
受影响系统：
Cisco Business 200 Series APs
Cisco Integrated Access Point on 1100 Integrated Service
Cisco Aironet 1540 Series APs
Cisco Aironet 1560 Series APs
Cisco Aironet 1800 Series APs
Cisco Aironet 2800 Series APs
Cisco Aironet 3800 Series APs
Cisco Aironet 4800 APs
Cisco Business 100 Series APs and Mesh Extenders
Cisco Catalyst 9100 APs
Cisco Catalyst IW 6300 APs
Cisco ESW6300 Series APs
描述：

CVE(CAN) ID: CVE-2020-3560
Cisco Aironet Access Points（aps）是美国思科（Cisco）公司的一款网络接入点设备。
Cisco Aironet Access Points (APs) 存在拒绝服务漏洞。该漏洞源于程序在处理特定数据包时出现资源管理不当。未经身份认证的远程攻击者可通过发送特制的 UDP 数据包利用该漏洞破坏 AP 和无线 LAN 控制器之间的连接导致受影响的设备无法处理客户端通信或导致设备重新加载，从而造成拒绝服务。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironet-dos-VHr2zG9y
建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-aironet-dos-VHr2zG9y）以及相应补丁：
cisco-sa-aironet-dos-VHr2zG9y：Cisco Aironet Access Points UDP Flooding Denial of Service Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironet-dos-VHr2zG9y

六、本期网络安全事件

➢ 新加坡加密货币交易所网站遭攻击：至少致 1.5 亿美元损失

2020 年 9 月 28 日，据外媒报道，新加坡加密货币交易所 KuCoin 今日披露了一次大规模黑客攻击。该公司在其网站上发布的一份声明中证实，一名黑客侵入了其系统并清空了其热钱包(hot wallets)中的所有资金。热钱包是连接到互联网的加密货币管理应用。冷钱包(cold wallets)为离线存储。

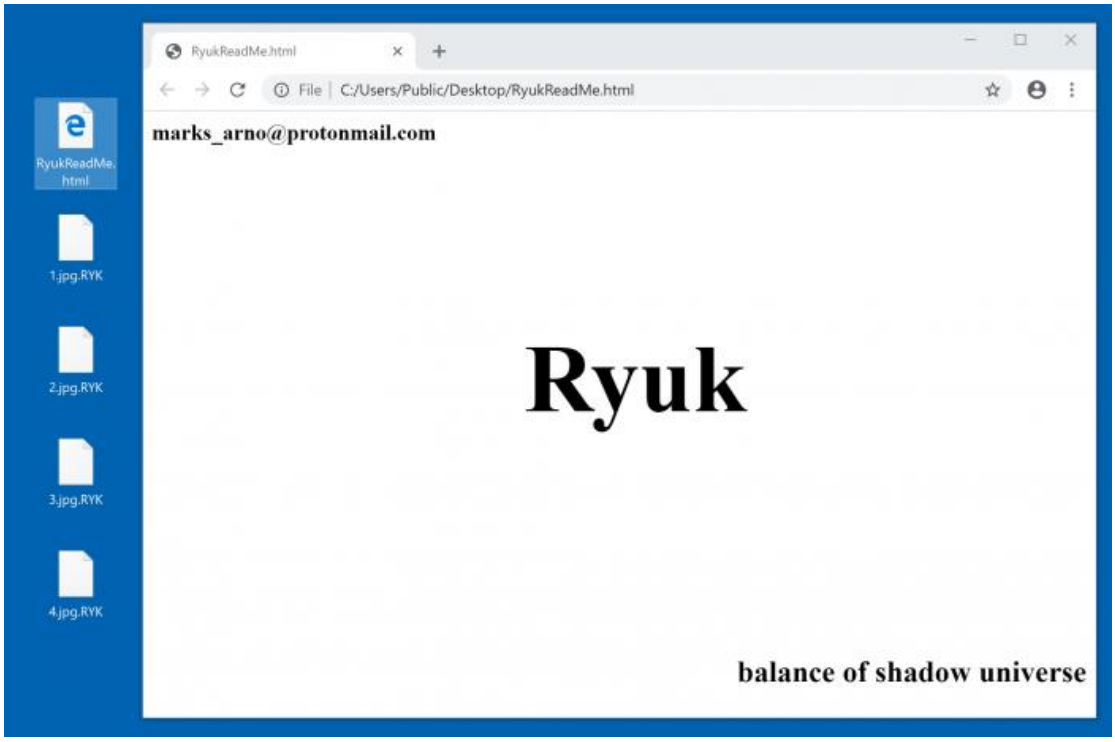
像 KuCoin 这样的加密货币交易所会使用热钱包作为他们的临时存储系统来存储目前在平台上交换的资产，它们被用来推动转换操作和资金转移。

KuCoin 表示，9 月 26 日，他们发现黑客从热钱包中大量取款。该公司表示，其已启动了安全审计并发现了资金的丢失。KuCoin 表示，黑客成功盗取了比特币资产、ERC-20 代币以及其他类型的代币。根据用户追踪被盗资金的 Etherium 地址，目前估计损失最小为 1.5 亿美元。虽然 KuCoin 没有回复记者的进一步置评请求。但该公司 CEO Johnny Lyu 计划在 2020 年 9 月 26 日 12:30 (UTC+8)通过直播的方式提供更多关于安全漏洞的细节。

另外，KuCoin 还承诺补偿那些在黑客攻击中使用其冷钱包而失去资金的用户。在该公司的安全团队调查这一事件期间，存款和取款服务都已经被暂停。（来源：新浪）

➢ 美国大型连锁医院 UHS 遭遇勒索软件攻击系统全部瘫痪

2020 年 9 月 28 日报道，美国最大的医疗服务机构之一 Universal Health Services 遭到了勒索软件的攻击。据两名知情人士透露，周日凌晨，UHS 系统遭到攻击，全国各地包括加州和佛罗里达州的多家 UHS 机构的电脑和电话系统被锁定。其中一人说，电脑屏幕上的文字发生了变化，其中提到了 "影子宇宙"，与 Ryuk 勒索软件的典型症状一致。"每个人都被告知关闭所有的电脑，不要再打开它们，"该人士说我们被告知，要过几天电脑才能再次启动。"



目前还不知道勒索软件攻击对患者护理产生了什么影响。

目前，UHS 还没有做出更多的回应，比如病人是否转到了其他医院。对于这起事故，UHS 没有提供更具体的细节，但有人自称为员工在 Reddit 论坛上发帖称，该连锁医院的网络在周日晚间遭到勒索软件攻击。这些帖子应证了来自华盛顿特区 UHS 机构的一位临床医生的警告。

美国医院协会(American Hospital Association)高级网络安全顾问约翰·里吉(John Riggi)称：这是一次“疑似勒索软件攻击”，黑客用恶意代码感染网络，使数据混乱，然后要求支付恢复服务的费用。他还说，在新型冠状病毒流行期间，越来越多的犯罪分子把目标瞄准了医疗机构的网络。

越来越多的勒索软件供应商在加密目标服务器之前，从他们渗透的网络中下载数据，用于敲诈。本月早些时候，已知的首起勒索软件事件发生在德国杜塞尔多夫。此前，黑客攻击

导致 IT 系统瘫痪，一名需要紧急入院的重病患者只能被带到另一个城市治疗，最终不幸死亡。

网络安全公司 Emsisoft 汇编的数据显示：仅在美国，去年就有 764 家医疗服务提供商受到勒索软件的侵害。该公司估计，美国每年在恢复失去生产力方面的损失将达 90 亿美元(约合 614.1 亿人民币)。对于那些不愿支付赎金的人来说，唯一有效的恢复方法就是每天进行系统数据备份。（来源：互联网综合整理）

➢ 全球航运业一周内遭遇第二次网络攻击 引发供应链中断担忧

2020 年 10 月 2 日，据报道，全球航运业在一周内遭受了第二次网络攻击，这引发了人们对供应链中断的担忧。目前，这些供应链已经十分紧张，可能无法在消费者需求的传统旺季及时运送商品。国际海事组织（International Maritime Organization）周四发表声明说，该组织的 IT 系统遭受了一次复杂的网络攻击。

国际海事组织是联合国旗下的一个海事行业监管机构，组织表示，目前一些网络服务无法使用，网络入侵正在影响他们的公共网站和内部系统。

本周早些时候，全球运力第四大集装箱班轮公司达飞海运（CMA CGM SA）披露，其信息系统受到了攻击。达飞海运星期四表示，公司各办事处“正在逐步重新连接到网络，以提高了预订和文件处理的时间。”

达飞海运在一份电子邮件声明中表示：“我们怀疑这是一次数据泄露，我们正在尽一切可能评估其潜在规模和性质。”据 Alphaliner 的数据，达飞海运是全球五大集装箱班轮之一，其运力占全球的 65%。

近年来，一系列网络事件困扰着航运业，其中最大的一起是 2017 年的网络入侵，导致总部位于哥本哈根的马士基公司损失了约 3 亿美元。

网络安全公司 Pen Test Partners 的安全专家肯·芒罗（Ken Munro）表示："马士基事件显然引起了骗子和网络罪犯的注意，他们意识到航运业受到了严重冲击。如果岸上的系统无法预订集装箱，船只就无法装载货物，也就无法产生收入。因此，针对航运公司的网络攻击对勒索软件运营商来说是有利可图的。"

虽然暂时并不能肯定，最近的网络攻击会对全球贸易造成短暂的刺激，还是会引发更大范围的破坏。但物流专家李·克拉斯科夫（Lee Klaskow）表示："网络威胁短期内肯定会带来不利影响，让人头疼。"

对于那些仍在等待季节性周期恢复正常的航运公司来说，最近网络攻击行动发生的时机尤其糟糕。由于消费者被迫在家工作、在网上购买必需品，从纸巾、口罩到蹦床和电脑显示器等各种物品的供应链都很紧张。此外，由于电子商务采购依然强劲，企业也在补充库存，货主对供应链的需求并未减少，但运力却在下降。因此，自今年年初以来，跨越太平洋运输集装箱的基准成本增加了两倍。（来源：新浪科技）

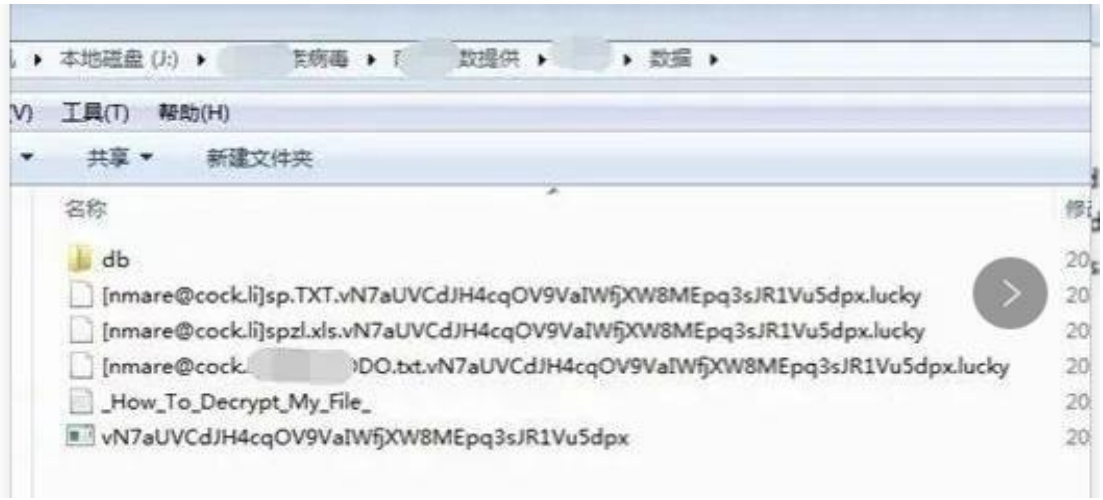
➢ 国内首个比特币勒索病毒制作者落网：曾迫使一上市公司停工 3 天

2020 年 10 月 8 日，当前，勒索病毒不断蔓延，各类新型病毒层出不穷，一些企业、金融机构甚至政府网站遭到攻击，犯罪嫌疑人索要赎金只认比特币，以逃避警方追查。在"净网 2020"专项行动中，南通、启东两级公安机关联手，成功侦破一起由公安部督办的特大制作、使用勒索病毒破坏计算机信息系统从而实施网络敲诈勒索的案件，抓获巨某、谢某、谭某等 3 名犯罪嫌疑人，其中巨某系多个比特币勒索病毒的制作者。这是全国公安机关抓获的首名比特币勒索病毒的制作者。截至案发，巨某已成功作案百余起，非法获利的比特币折合人民币 500 余万元。

收银系统被黑，超市遭网络勒索

今年 4 月，启东某大型超市的收银系统遭到攻击，被黑客植入勒索病毒，造成系统瘫痪无法正常运转。接到报案后，南通市公安局成立由启东、网安、法制等组成的专案组，开展破案攻坚。"通过数据勘验，我们找到一个如何解密文件的全英文留言，要求受害人必须支付 1 比特币作为破解费用。"网络攻防专家、南通市公安局网安支队三大队副大队长许平楠

说，经对该超市的服务器进行数据勘验，发现黑客锁定的服务器中所有文件均被加密，文件的后缀名都变成了“lucky”，文件和程序均无法正常运行，而在 C 盘根目录下有个自动生成的文本文档，留有黑客的比特币收款地址和邮箱联系方式。



“这是一起典型的使用勒索病毒破坏计算机信息系统从而实施网络敲诈勒索的案件。”许平楠说，近年来，比特币勒索病毒攻击在全国乃至全球范围内整体呈上升趋势，令人深恶痛绝，但发起每次攻击的始作俑者身份始终成谜。对这起案件，尽管专案组做了大量工作，但始终没有丝毫进展，侦查陷入僵局。

警方顺藤摸瓜，病毒制作者落网

案件侦查过程中，受害超市负责人反映，由于被锁服务器中有重要工作数据，格式化将带来巨大损失，其联系了外地一家数据恢复公司，以更低的价格委托解锁加密文件，后对方成功对服务器数据进行了解密。

“一般来说，没有病毒制作者的解密工具，其他人是无法完成解密的。”专案组成员、启东市公安局网安支队民警黄潇艇说，勒索病毒入侵电脑，对文件或系统进行加密，每一个解密器都是根据加密电脑的特征新生成的，只有按要求支付比特币才能解开。

获悉这一情况，专案组判断，其中定有隐情。经过走访调查，这家数据恢复公司的负责人吐露实情，原来他们通过邮箱直接与黑客取得联系，最终花了 0.5 比特币的代价得到解锁工具，从而顺利完成任务，赚取差价。专案组通过相关记录，深度研判分析，不仅排除了数据恢复公司的作案嫌疑，还成功锁定犯罪嫌疑人的真实身份为巨某，案件侦破工作取得重大进展。5 月 7 日，专案组在山东威海将巨某抓获归案，并在其居住地查获作案用的电脑。民警在其电脑中还找到相关邮件记录、比特币交易记录以及相关勒索病毒工具的源代码。

自认完美犯罪，赎金只认比特币

经查，巨某今年 36 岁，内蒙古赤峰人，自幼喜好并自学钻研计算机知识，精通编程、

网站攻防等技术，后成立工作室，利用自己开发的软件炒股，起初赚了不少钱，后亏损 300 多万元。2017 年下半年的某天，债台高筑的巨某偶然间得知有黑客用勒索病毒将他人电脑文件加密锁定后敲诈钱财，于是灵机一动，尝试开发病毒程序，通过研究“永恒之蓝”工具以及“撒旦”等勒索病毒，巨某编写了“satan_pro”病毒程序，用于作案。

“被植入病毒的服务器中，所有的数据库文件、文档都会被加密，只有通过邮箱联系我，支付比特币，我才会把解锁工具发给对方。”巨某交代称，自己开发了一款网站漏洞扫描软件，在获得相关控制权限后，就有针对性地在一些服务器植入勒索病毒。为避免破解和逃避公安机关的追查，巨某又陆续升级开发了“nmare”“evopro”“svmst”“5ss5c”等 4 款勒索病毒，除了索要难以追查的比特币作为赎金，他还通过境外的网盘和邮箱将解密软件发送给受害人，并经常更换，到手的比特币也都是通过境外网站交易。尽管巨某机关算尽，自认为犯罪行为天衣无缝，最终还是没能逃出办案民警的法眼。

社会危害严重，行业乱象不容忽视

经大量工作，专案组查明，巨某先后向 400 多家网站和计算机系统植入敲诈勒索病毒，受害单位涉及企业、医疗、金融等行业，启东这家超市收银系统即是被植入了“nmare”病毒。案件中，苏州某上市科技公司的系统被巨某植入病毒，导致停产停工三天，损失巨大。

期间，数家数据恢复公司主动联系巨某寻求合作，最终，巨某与谢某、谭某经营的一家数据恢复公司谈妥，由巨某编程，病毒中的联系方式和比特币账户为该公司所有，再由公司寻找目标植入病毒，到手后按比例分成。6 月 4 日，谢某、谭某在广州落网。

“犯罪手法隐蔽，社会危害大，同时也暴露出数据解密行业的乱象。”南通市公安局网安支队支队长张建说，近年来，勒索病毒攻击破坏案件时有发生，侵害目标多为党政机关和企事业单位的重要信息系统，严重危害正常办公秩序和经济运行秩序，甚至有数据恢复公司主动与黑客取得联系，共同开展攻击破坏和敲诈勒索，同时借机抢占勒索病毒解密市场，成为勒索病毒蔓延扩散的帮凶。目前，3 名涉案犯罪嫌疑人均因涉嫌敲诈勒索罪被执行逮捕。

警方提醒：广大企业和群众平时应养成良好的安全文明上网习惯，注重信息安全等级保护，及时更新系统和软件，安装正规的杀毒软件和防护墙，修补漏洞，同时定期对重要数据进行备份。此外，一旦使用的计算机感染了病毒，还需尽快修改支付密码，以免造成其他财产损失。（来源：南通公安）

➢ 日本东京证券交易所因系统故障取消全天交易

2020 年 10 月 1 日早间 7:40，日本东京证券交易所因系统问题暂停交易，东京证券交易所交易网络系统（TOSTNET） 也暂停交易。东京证券交易所在官网的声明中称，不知道什么时候会恢复，此时也不接受订单。交易所没有详细说明问题的本质，只是说它与市场信息的分布有关。

据东京证券交易所母公司日本交易所集团（JPX）1 日在其官网发布的公告说，东京证券交易所因交易系统故障取消当天交易。据《日本经济新闻》网站报道，这是该交易所首次因

系统故障取消全天交易。

当地时间 1 日上午 9 时前后，日本交易所集团连发 3 条公告宣布，因交易信息传输系统故障，停止东京证券交易所所有股票交易。当天已发出的行情信息无效，何时恢复交易暂不确定。由于系统修复无望，上午 11 时 30 分之后，日本交易所集团发出第四条公告，宣布取消 1 日全天交易。目前，2 日是否重开交易仍不确定。


マーケットニュース

2020/10/01

障害に伴う売買の停止について

シェア ツイート

平素は、当取引所証券市場の運営につきまして、格別のご高配を賜り、厚く御礼申し上げます。

本日、相場情報の配信に障害が発生しており、東京証券取引所における全銘柄の売買を停止いたしますのでお知らせします。併せて、その時点より注文受付につきましても不可となります。復旧については現在のところ未定ですが、今後の予定については改めてご連絡いたします。

※ 大阪取引所の売買は、通常どおり行われております。

截至记者发稿时，东京证券交易所和交易系统开发方富士通公司仍在调查故障发生原因。这是东京证券交易所继 2005 年 11 月因系统故障全面停止交易以来再次发生此类事故。上次系统故障发生后，早盘交易全面停止，故障排除后午盘交易得以重开。

据日本共同社称，日本交易所集团(JPX)旗下的东京证券交易所 10 月 1 日因系统故障停止了所有股票交易，订单受理也已暂停。据悉，从上午 9 点开盘前起，股市信息发布出现问题。目前正在加紧修复。札幌、名古屋和福冈证券交易所也停止了所有股票交易。

在与东京证券交易所使用不同系统的日本交易所集团旗下的大阪交易所，股指等的期货交易早盘正常进行，日本交易所集团旗下东京商品交易所也实施了原油期货等的日间交易。

报道称，机构投资者等使用的东证场外交易也已停止。由于发生系统故障，东京股市主要股指的日经指数和东证指数(TOPIX)处于无法正常计算的状态。

据第一财经，1 日原定有广岛银行股份改制的“广银控股”等 3 家企业挂牌上市，但目前无法交易。据 JPX 介绍，东证上市企业总市值规模为仅次于美国 2 家交易所的全球第三。目前约有 3700 家上市企业，9 月 30 日估算成交量 14.42 亿股、成交额 2.9 万亿日元（约合人民币 1867 亿元）。（来源：新华社）

➢ 黑客入侵乌干达移动支付系统 涉及多家银行、运营商

2020 年 10 月 8 日，据央视新闻援引乌干达当地媒体报道，日前黑客入侵了乌干达

MTN、Airtel 通讯公司使用的第三方移动支付系统，消息人士说黑客卷走两家公司数十亿先令的资金（注：1 乌干达先令=0.001840 人民币）。据了解，被黑客入侵的两家公司占据乌干达移动支付 90%的份额。

受损失的通讯公司发表联合声明称：此次事件影响到了银行到移动货币的交易，相关服务目前已经暂停，他们将尽快修复。至于相关损失，通讯公司表示暂不透露。

“从周四晚上开始，黑客一直到周六才被发现。到目前为止，黑客已经给自己发送了将近 13 亿乌干达先令，已经设法从 Airtel 的资金中取出了 9 亿乌干达先令。我们估计 MTN 也损失了差不多两倍的钱，因为他们是移动货币的领导者。当欺诈被发现时，所有通过 Pegasus 进行的交易都被暂停。”消息来源称。

Pegasus 成立于 2007 年，每年处理高达 1.7 万亿乌干达先令的金融交易。这包括移动钱包聚合、移动支付和汇款、贷款和储蓄，以及短信、通话时间和数据加载等增值服务。该公司的旗舰产品 PegPay 支付平台目前正被银行、电信、公用事业公司(如零售商、付费电视提供商和学校)等多家机构用于汇总和管理用于内部和外部目的的金融交易。（来源：安全学习那些事）

信息安全意识产品服务

021-33663299