CAICT 中国信通院　工业互联网产业联盟 Alliance of Industrial Internet

2020 年上半年工业互联网安全态势综述

中国信息通信研究院
工业互联网产业联盟

2020 年 9 月

前　言

在工业和信息化部网络安全管理局的指导下，中国信息通信研究院和工业互联网产业联盟编制形成了《2020 年上半年工业互联网安全态势综述》，通过对工业互联网领域重点行业和相关企业 2020 年上半年的安全威胁监测、分析研判和响应处置等情况进行梳理和分析，总结提出了上半年工业互联网安全态势的十大突出特点，并对下半年工业互联网的安全态势进行了预测。

2020年上半年工业互联网安全态势综述

一、上半年工业互联网安全态势

2020年上半年，我国工业互联网安全态势整体平稳，未发现重大网络安全事件，但恶意网络行为持续活跃，对工业控制系统及设备的攻击持续增多、受攻击的行业范围广，工业互联网安全形势严峻。

（一）我国工业互联网相关恶意网络行为的次数呈现增加趋势，安全隐患突出。2020年1月1日至2020年6月30日，国家工业互联网安全态势感知与风险预警平台持续对全国136个主要工业互联网平台、10万多家工业企业、900多万台联网设备进行安全监测，累计监测发现恶意网络行为1356.3万次，涉及2039家企业。其中，攻击方式以异常流量、非法外联、僵尸网络三类为主，均超过300万次，累计占恶意行为总数的81%，恶意网络行为排名见图1。与此同时，异常流量中包含大量扫描、嗅探行为，表明当前针对工业互联网的网络攻击大部分为实施攻击前的信息搜集，安全隐患不容忽视。

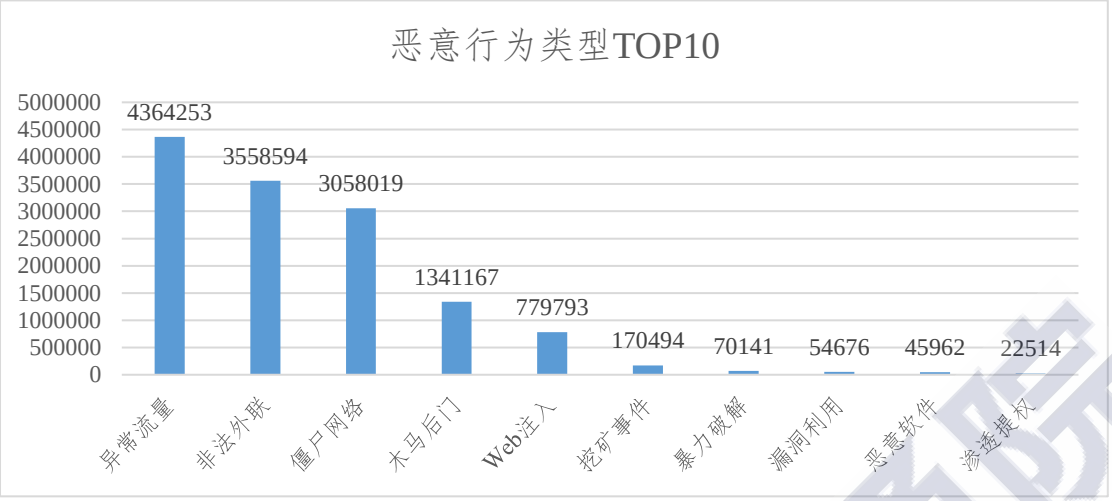

图 1 工业互联网恶意网络行为

（二）工业互联网网络攻击主要集中于基础性行业，疫情期间医疗相关行业成关注重点。当前针对工业互联网的恶意网络行为持续活跃，主要集中于制造业等基础性行业，仅计算机、通信和其他电子设备制造业遭受攻击次数就将近 288 万次。疫情期间，医药制造、医疗器械服务、纺织等疫情相关行业遭受恶意网络行为数量较 2019 年有所上升，但已随疫情好转而持续走低，从 1 月占全部工业企业恶意网络行为的 38.9%降至 6 月占比 10.4%，上半年工业企业及重点行业恶意网络行为态势如图 2 所示。

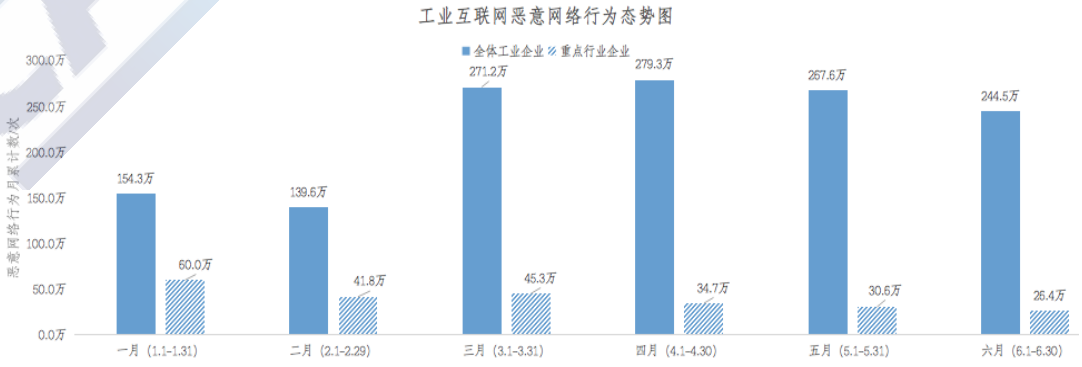

图 2 工业互联网恶意网络行为态势图

（三）来自境外的扫描攻击次数不断攀升，部分物联网设备权限长期被控制。我境内工业互联网遭受境外攻击占比接近 5 成，多个境外 IP 段对我国工业互联网企业进行长期的扫描嗅探、尝试攻击以及外联通信，主要境外攻击来源恶意行为变化趋势如图 3 所示。此外，监测发现僵尸网络行为 305 万起，控制端近 7 成位于境外，其中经研判分析的僵尸网络事件共 121 起，以 Mirai 家族为主，占总量 32.2%。境内部分物联网设备存在持续与境外通信的行为，存在被用于发动 DDoS 攻击的潜在风险。

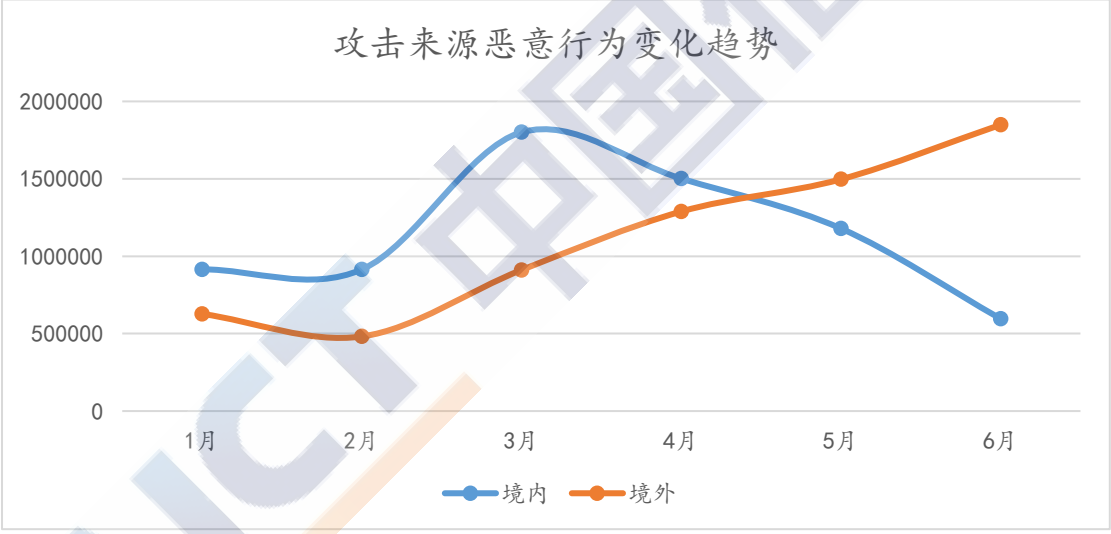

图 3 攻击来源恶意行为变化趋势

（四）工业互联网安全威胁信息通报处置机制初步建立，疫情期间发挥重要作用。建立安全威胁信息监测预警、通报处置闭环机制，对相关威胁信息开展监测、研判和处置，为疫情防控提供坚实网络安全保障。截至 2020 年 6 月 30 日，累计研判威胁信息 424 例，其中包括 152 家疫情物资生产、医药制造相关企业感染僵尸网络或木马后门，69 家医疗机构

存在远程代码执行、任意文件写入等高危漏洞。与此同时，按照公共互联网网络安全应急处置机制完成通报处置 119 例，其中包括疫情重点医院、医疗器械制造企业等相关单位 55 例。

（五）联网工业设备漏洞数量多、级别高，潜在威胁不容忽视。截至 2020 年 6 月 30 日，累计监测发现联网工控设备漏洞隐患 946 个，其中高危漏洞 385 个，中危漏洞 472 个，中、高危漏洞占漏洞总数的 90.6%。漏洞隐患类型将近 20 种，主要为缓冲区堆溢出、设计缺陷、非法授权和跨站脚本等，占漏洞隐患总量的 63.2%，漏洞危害等级和漏洞类型分布如图 4 所示。部分漏洞存在公开利用代码，被攻击者获取后可轻易取得设备控制权限，存在较大安全风险。

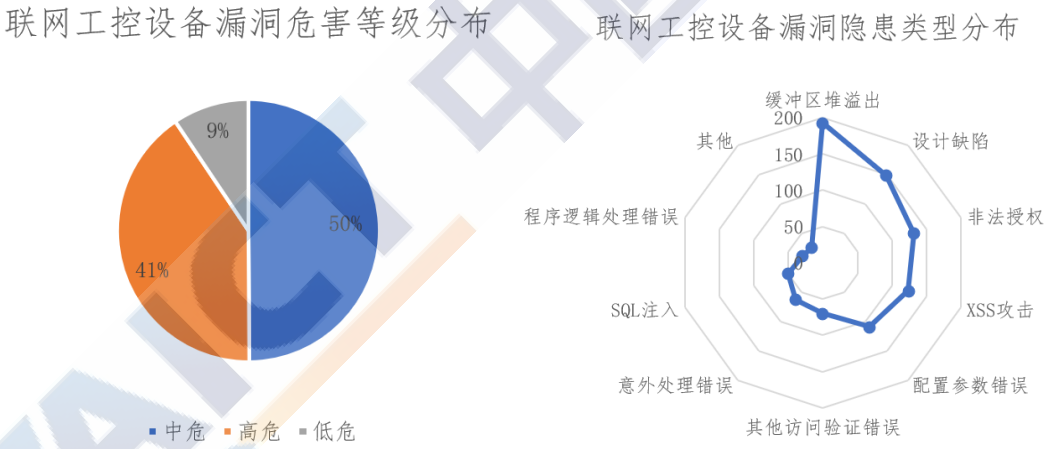

图 4 联网工控设备漏洞隐患危害等级分布和漏洞隐患类型图

（六）联网工业设备及系统“带病运行”情况普遍存在，被攻击门槛低。上半年发现的 946 个漏洞共涉及 212 个工业设备及控制系统，包括人机交互接口（HMI）、企业资源计划系统（ERP）和可编程逻辑控制器（PLC）等，占总数的 92%。这些漏洞主要在 2011 年-2013 年间对外发布，表明当前存在

大量老旧工业控制系统或设备，未及时升级或更新补丁，存在较大安全风险，更容易遭受黑客的攻击，会影响电力、制造等行业，对基础设施安全形成较大威胁。

（七）多个 0DAY 漏洞被爆出，给我国工业互联网造成严重安全隐患。工业互联网设备和控制系统越来越多地被挖掘存在 0DAY 漏洞，如某工控厂商 PLC 设备存在一系列未公开的 0DAY 漏洞，近万台正在产线上使用的工控设备受此漏洞威胁。恶意用户无需任何权限即可访问这些管理接口，黑客可通过删除安全访问限制后直接控制 PLC，远程修改其中的各种配置信息，导致系统故障、停产，甚至引发安全生产事故，安全隐患突出。

（八）勒索软件对工业互联网威胁加剧，安全事件频繁曝出。勒索病毒通过互通的工业网络在站与站之间、供应链上游与下游之间造成大面积传播，在汽车、能源、制造业等重要领域均爆出相关安全事件，后果影响严重。某国际知名汽车公司遭勒索软件重创，引起其计算机服务器和相关网络毁损以及电子邮件无法使用，对部分产线和业务运作造成影响。美国某芯片制造商遭 Maze 勒索软件攻击，造成 10.3GB 的会计和财务信息泄漏。欧洲某能源系统商遭到 SNAKE 勒索软件攻击，导致其内部 IT 网络中断。

（九）车联网领域成为网络攻击新趋向，大量用户数据和个人隐私面临泄露风险。随着车联网智能化和网联化的不

断推进，该领域安全威胁事件日益剧增。2020 年 5 月，英国谢菲尔德市爆发大规模道路通行记录数据泄露事件，约 860 万条记录道路通行数据被泄露；同月，匿名黑客从交警登记处获取超过 1.29 亿俄罗斯车主的数据，并将其暴露在“暗网”上以获取加密货币。英国某媒体调查报告披露，汽车行业两大巨头公司的两款畅销车存在严重安全漏洞，黑客可利用该漏洞发动攻击，窃取车主的个人隐私信息甚至操控车辆。

（十）安全投资融资活跃，推动工业互联网安全产业快速发展。随着工业互联网政策的持续利好，网络安全关注度持续上升，工业互联网安全市场投融资高涨，奇安信、启明星辰、六方云等安全企业积极推进工业互联网安全技术研发突破，红杉资本、盈动资本等专业投资机构等相继发力布局。根据网上公开信息统计，2020 年上半年国内累计投融资事件 26 起，投融资规模达 15 亿元。其中工业互联网安全、数据安全、云安全等领域成为 2020 年上半年市场投融资热点，上半年国内网络安全投融资领域分布情况图 5 所示。

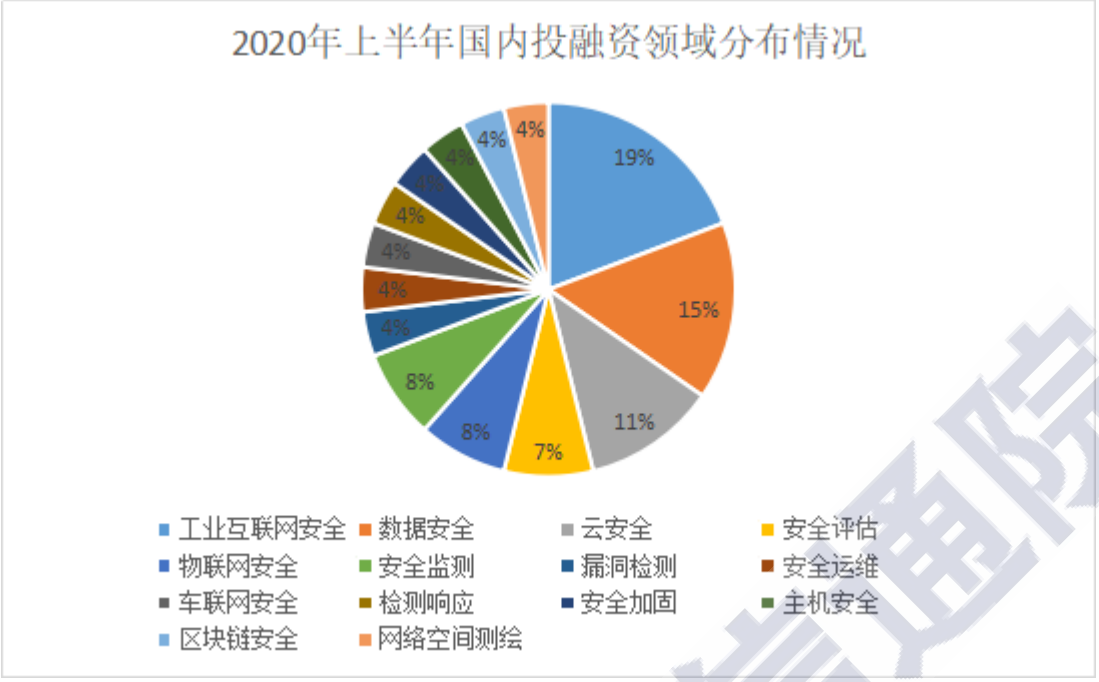

图 5 国内投资领域分布情况

二、下半年工业互联网安全态势预判

（一）“新基建”下的工业互联网面临安全新挑战。随着人工智能、5G 等新一代信息技术和机器人等高端装备与工业互联网融合应用，设备联网、企业上云加速安全风险传导延展，网络攻击面从边界向核心不断扩大，推动工业互联网安全防护工作逐步向动态协同转变，安全风险挑战进一步升级。

（二）恶意网络行为将有增无减。2020 年上半年，源于境外的攻击不断增多，包括持续性嗅探扫描、僵尸网络远控等，预计下半年该趋势将延续。从监测角度看，僵尸网络控制端与境内被控端可能通过加密传输信息，监测难度将大幅增加。来自境外 IP 对我国工业互联网进行长期、持续、广泛

的嗅探扫描，需引起关注。

（三）0DAY 漏洞数量将进一步提高，漏洞影响范围将进一步扩大。2020 上半年 CNVD 新增的工业控制系统漏洞数量达到 315 个，广泛涉及制造业、能源、交通、医疗等行业，仅上半年的数量已达到 2019 年全年新增数量的 76.3%，下半年 0DAY 漏洞数量将会持续增加，行业分布依旧广泛。从工业企业角度看，工控设备中不仅存在老旧且利用门槛低的漏洞，更存在曝出 0DAY 漏洞的风险，企业安全防护面临挑战。

（四）工业互联网数据安全将成为企业亟待应对的关键问题。工业互联网数据种类和保护需求多种多样，设计、生产、操控等各类数据分布在云平台、用户端、生态端等多种设施上，目前单点、离散的数据保护措施难以有效保护工业互联网数据安全。工业互联网承载着事关企业生产、社会经济乃至国家安全的重要工业数据，一旦被窃取、篡改或流动至境外，将对国家安全造成严重威胁。

（五）工业互联网安全融合应用解决方案将不断涌现。安全厂商纷纷积极探索 5G、大数据、人工智能、区块链等新兴技术在工业互联网安全解决方案中的应用。例如，某厂商推出 AI 安全免疫系统，通过流量监测、结合机器学习和人工智能算法，为每个设备和用户建立起各自的健康模型，形成新型威胁感知方案。工业互联网产业联盟将持续编制《工业互联网安全典型解决方案》，不断探索与新兴技术的融合，

为企业部署安全防护措施提供可参考的模式。

（六）跨部门、跨行业、跨平台的威胁信息通报处置机制将协同推进。随着越来越多的设备联网、企业上云，企业很难进行单独的防御，行业及地方主管部门、工业互联网企业、设备提供商、安全服务商等需要建立协同机制，共同应对来自各领域的安全威胁与挑战。工业互联网安全监测预警、重大网络安全事件报告、威胁信息通报、应急处置等系列机制将进一步完善，逐步形成行业协同、政企联动、动态闭环的主动防御模式。

本报告由工业和信息化部网络安全管理局指导，由中国信息通信研究院和工业互联网产业联盟共同完成。国家工业信息安全发展研究中心、中国电子技术产业发展研究院、中国电子技术标准化研究院、中国工业互联网研究院以及六方云、绿盟、启明星辰、东方国信、特变电工、亚鸿世纪、富士康、树根互联、和利时、顶象、徐工信息、恒安嘉新等多家企事业单位对本报告的编写提供了大力支持。