网信动态周报

第 31 期

2022 年

5G 半导体 物联网 安全

8月8日-8月13日

工业控制系统信息安全技术国家工程研究中心　　特约顾问：刘廉如 董伟

1 5G 行业一周要闻

- 英国电信欧洲首家实现 SA 5G 现网 4 载波聚合
- 我国运营商 5G 投资超 4000 亿元
- 英国 Quickline 携手 Mavenir 推出 5G SA Open RAN 网络
- SK 电讯、韩国电信 5G 用户分别达 1170 万和 750 万
- T-Mobile 美国斥资 35 亿美元购买额外 600MHz 频谱牌照
- Kajeet 与三星合作发展 5G 专网，最初瞄准教育领域
- 爱立信发布新一代有源无源天线一体化无线设备实现 5G Massive MIMO 高效部署

■ 英国电信欧洲首家实现 SA 5G 现网 4 载波聚合

据外媒报道，英国电信与诺基亚合作完成了 4 个频谱信道的载波聚合（CA）试验，从而在向商用独立组网（SA）5G 迈进方面取得了进展。英国电信声称，自己是欧洲第一家将 4 个载波单元聚合到 SA 5G 现网中的运营商，并表示该试验分两步进行，首先会在实验室中，然后在不同站点的无线电桅杆上。英国电信指出，到 2021 年底，全球只有大约 20 家移动运营商推出了 SA 5G 网络，但预计 2022 年这一数字将翻一番。

■ 我国运营商 5G 投资超 4000 亿元

从 2022 世界 5G 大会上了解到，我国 5G 网络基站数量达 185.4 万个，终端用户超过 4.5 亿户，均占全球 60% 以上，全国运营商 5G 投资超过 4000 亿元。

■ 英国 Quickline 携手 Mavenir 推出 5G SA Open RAN 网络

据外媒报道，农村宽带服务提供商 Quickline Communications 通过与 Open RAN 软件供应商 Mavenir 合作，在英国北约克郡推出了一张基于云的 5G SA Open RAN 商用网络。Quickline 表示，该公司是英国第一家在共享接入频谱上提供基于云的、采用 5G

SA Open RAN 解决方案的固定无线接入（FWA）商用服务的网络服务运营商。

■ SK 电讯、韩国电信 5G 用户分别达 1170 万和 750 万

韩国两大移动运营商在第二季度获得强劲的 5G 用户增长，并在移动和企业业务推动下实现营收增长。韩国电信（KT）的 5G 用户同比增长 49.2% 至 750 万户，占其近 1400 万总用户基数的 53.6%。SK 电讯（SKT）的 5G 用户同比增长 51.8% 至 1170 万户，占其 3030 万总用户基数的 38.6%。

■ T-Mobile 美国斥资 35 亿美元购买额外 600MHz 频谱牌照

T-Mobile 美国公司同意购买更多 600MHz 频段的频谱牌照，以巩固此前根据租赁协议获得的接入权限，来支持其全国 5G 服务。在提交给美国证券交易委员会（SEC）的文件中，这家德国电信旗下的美国运营商表示，它已同意为牌照向两家特拉华州注册公司 Channel 51 License 和 LB License 总共支付 35 亿美元。这些无线电波覆盖了 20 个市场，许可范围从 10MHz 到 30MHz 不等。T-Mobile 美国指出，它目前通过与卖家的独家租赁协议使用这些牌照。

■ Kajeet 与三星合作发展 5G 专网，最初瞄准教育领域

托管物联网连接提供商 Kajeet 与三星电子美国公司（Samsung Electronics America）合作，部署其私有 5G 平台和 CBRS 设备，以支撑智慧城市、园区、公用电网和工厂连接。作为协议的一部分，Kajeet 现在是三星在美国私有 RAN 产品的授权经销商。Kajeet 计划在专用网络中使用三星的设备，和其基于云的终端、策略和网络管理系统一起。在合作的第一阶段，两家公司瞄准了教育领域，包括向美国多个学区提供专用的 5G 私有网络。Kajeet 还计划与三星一起，通过使用 CBRS 和固定无线接入连接来提高服务不足的社区的宽带覆盖率。

■ 爱立信发布新一代有源无源天线一体化无线设备实现 5G Massive MIMO 高效部署

近期，爱立信面向中国市场重磅推出新一代有源无源天线一体化（A+P）无线设备 AIR3218，具有行业领先的体积和重量，在不增加天面、不需要铁塔改造的情况下，实现 5G Massive MIMO 高效部署。盛夏之际，爱立信携手山西联通正式开启了 AIR3218 的商用部署，现网各项指标表现优异。爱立信 AIR3218 引入了多项技术创新来实现 A+P 产品的“瘦身 + 提效”。首先，AIR3218 采用新一代爱立信硅芯科技（Ericsson Silicon），在提升无线算力的同时显著降低设备耗能，同时结合了 Interleaved AIR 交织天线技术，最大限度减少了产品体积和重量，是目前市场上打造极简 5G Massive MIMO 站点的最优解。除此之外，AIR3218 采用了 Beam Through 技术，创造性地引入 A+P 模块化设计，极大提升了安装的便利性，在充分提高天面利用效率的基础上降低了后期的维护难度。

2 半导体行业一周要闻

- AMD 将于三季度推出 5nm 级处理器
- 韩将向美提出“芯片四方联盟”协商原则——“不刺激中国”
- 高通斥资 42 亿美元购买格芯芯片
- 壁仞发布国内算力最大通用 GPU 芯片
- 快手官宣自研云端 SoC 芯片
- 报告称 2022Q1 智能手机 AP 市场：高通达到 45%，海思接近零
- Gartner：2022 年全球半导体收入增长预计将放缓至 7%
- 移远通信智能模组 SG865W-WF 通过 CE/FCC/IC/KC 多地区权威认证

■ AMD 将于三季度推出 5nm 级处理器

据外媒报道，虽然下半年 PC 市场需求疲弱，但处理器大厂 AMD 对下半年即将推出的 Zen 4 架构处理器仍具信心，认为有助于争取更高市占率。AMD 董事长苏姿丰亦确认，研发代号为 Rapheal 的 5 纳米 Ryzen 7000 处理器会在第三季上市，此外，AMD 还会扩大 5 纳米产品线阵容，台积电独家承接晶圆代工订单。

■ 韩将向美提出“芯片四方联盟”协商原则——“不刺激中国”

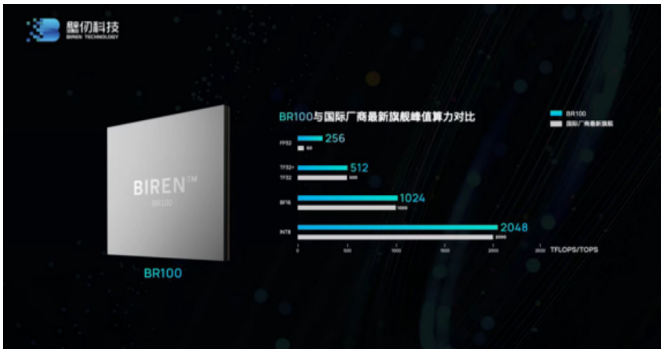
据外媒报道，美国近日向韩方提议，就韩国是否参加“芯片四方联盟”举行预备会晤，韩国政府决定向美国提议要以“两大原则”为基础，讨论今后的半导体合作方向。“两大原则”的具体内容是指“‘芯片四方联盟’参与国应该尊重中国强调的一个中国原则”和“不提及对中国进行出口限制”。韩国政府相关人士称，“‘芯片四方联盟’是为相关国家能在半导体产业发挥协同效应的协议体”，“不是为了在技术上孤立中国的技术安保同盟”。

■ 高通斥资 42 亿美元购买格芯芯片

近日，高通宣布将从美国芯片制造商格芯（Global Foundries）纽约工厂额外购买价值 42 亿美元的半导体芯片，使其到 2028 年的采购总额达到 74 亿美元。格芯方面表示，高通是格芯在 2021 年签署一项长期协议的首批客户之一，协议涵盖多个地理位置和技术。此前，高通与格芯达成了价值 32 亿美元的采购协议，后者为高通生产用于 5G 收发器、Wi-Fi、汽车和物联网连接的芯片。

■ 壁仞发布国内算力最大通用 GPU 芯片

据悉，BR100 系列 2022 年 3 月成功点亮，是国内算力最大的通用 GPU 芯片。主要参数方面，BR100 系列采用 7nm 制程，集成 770 亿晶体管，基于壁仞科技自主原创的芯片架构开发，采用 Chiplet(芯粒)、2.5D CoWoS 等先进的设计、制造与封装技术，可搭配 64GB HBM2E 显存，超 300MB 片上缓存，支持 PCIe 5.0、CXL 互联协议等。

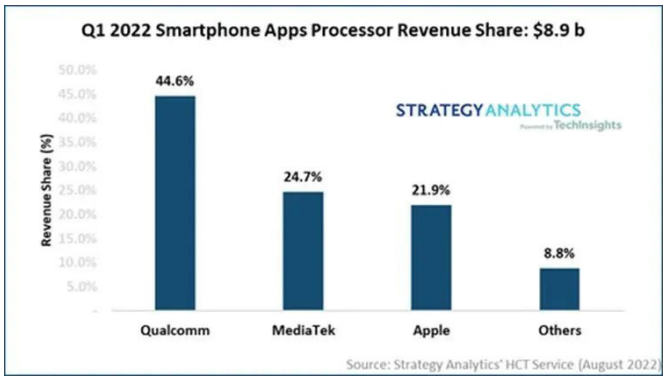


■ 快手官宣自研云端 SoC 芯片

近日，快手公司宣布推出“StreamLake”视频云品牌，用音视频及 AI 能力赋能客户。本次，快手首推以新品牌命名的 StreamLake OS 操作系统，覆盖基础设施、原子能力、产品、客户咨询服务及行业解决方案等多维能力。同时，快手宣布云端智能视频处理 SoC 芯片 SL200 流片成功，面向视频直播点播应用，正在进行线上内测。

■ 报告称 2022Q1 智能手机 AP 市场：高通达到 45%，海思接近零

市场研究公司 Strategy Analytics 发布 2022 年第一季度智能手机 AP（应用处理器）市场份额追踪报告显示，高通持续扩大领先地位，份额高达 45%。联发科以 25% 排名第二，苹果以 22% 份额位居第三。高通市场份额的增长，源于该公司在高端处理器领域保持强势地位。Strategy Analytics 指出，高通 4nm 的旗舰应用处理器骁龙 8 Gen 1 在 2022 年 Q1 获得了强劲的增长势头。高通在中国 5G 手机市场如鱼得水，同时在三星 Galaxy S 手机上的份额的增加推动其智能手机应用处理器的收益创下历史新高。



■ Gartner：2022 年全球半导体收入增长预计将放缓至 7%

根据 Gartner 的最新预测，2022 年全球半导体收入预计将增长 7.4%，相比上一季度预测的 13.6% 有所下降并且远低于 2021 年的 26.3%。Gartner 研究业务副总裁 Richard Gordon 表示：“虽然芯片短缺正在得到缓解，但全球半导体市场正在进入到一个疲软期并将持续到 2023 年末，到那时半导体收入预计将下降 2.5%。半导体终端市场已出现疲软，尤其是那些受到消费者支出影响的市场。通胀、税收和利率的上升加上能源和燃料成本的提高正在给消费者的可支配收入造成压力，影响他们在个人电脑、智能手机等电子产品上的支出。”

表一、2021-2023年全球半导体收入预测（单位：百万美元）

	2021 年	2022 年	2023 年
收入	594,952	639,218	623,087
增长率（%）	26.3	7.4	-2.5

来源：Gartner（2022年7月）

■ 移远通信智能模组 SG865W-WF 通过 CE/FCC/IC/KC 多地区权威认证

移远通信 SG865W-WF 智能模组搭载高通 SoC 芯片 QCS8250，该平台采用 7nm 工艺制程，内部集成八核高性能 KryoTM 585 CPU、AdrenoTM 650 GPU、Adreno 995 DPU、Adreno 665 VPU、HexagonTM DSP 及 SpectraTM 480 ISP 。出色的内部配置为其高达 15TOPS 的综合算力保驾护航。目前，SG865W-WF 的高算力已经覆盖智能摄像头、视频协作、云游戏服务器、智能健身镜、智慧医疗和智慧零售等计算密集型物联网应用，成为诸多智能终端设备算力应用的重要载体。

3 工业互联网行业一周要闻

- 腾讯发布四足机器人 Max 二代版本
- 商汤推出专业 AI 下棋机器人
- 工信部将加快实施“机器人 +”应用行动
- 国家矿山安全监察局：“十四五”深入推进非煤矿山机械化、自动化和信息化建设
- 小米首个全尺寸人形仿生机器人“CyberOne”亮相
- 《智能工厂 通用技术要求》将于 10 月 1 日正式实施
- 完成多项工业连接新技术验证，爱立信与中国移动为 5G“无线全连接工厂”注入新动能
- 小米智能工厂二期主体结构封顶，将打造世界级“灯塔工厂”

■ 腾讯发布四足机器人 Max 二代版本

近日，腾讯正式发布由腾讯 Robotics X 实验室自研的多模态四足机器人—Max 二代机器人（以下简称 Max）。据悉，Max 采用原创的腿轮一体的本体设计，能够在梅花桩上完成旋转踏步、单桩跳跃、双轮站立等高难度动作，过桩速度达到“前辈”Jamoca 的 4 倍。依托于机器人视觉定位、地形识别、全向六自由度运动规划、高精度模型预测控制等技术，Max 能够对复杂地形进行精确识别，并且根据地形实时想好步子，避免踩歪、打滑、摔倒等风险。相比一代，Max 在视觉感知、轨迹规划、运动控制等方面实现技术创新，标志着腾讯在机器人灵敏运动研究上取得了新的突破。

■ 商汤推出专业 AI 下棋机器人

据介绍，“元萝卜 SenseRobot” AI 下棋机器人拥有机械臂，可以实际线下陪伴下棋，基于商汤原创的“AI 黑科技”，还可以做到“手眼协同”，实现毫米级的操作精准度，保证在下棋对弈过程中的运行顺畅和落子准确。同时，该机器人可为用户提供专业课程，在家就能完成 16-13 级的官方象棋考级评测，获得专业证书。该机器人标准版售价 1999 元，Pro 版售价 2499 元。

■ 工信部将加快实施“机器人 +”应用行动

近日，工信部装备工业一司副司长汪宏表示，工信部将进一步维护机器人产业链供应链稳定，全面提升产业基础能力，加快实施“机器人 +”应用行动。工信部将深耕行业应用，遴选发布一批应用成效显著的机器人产品

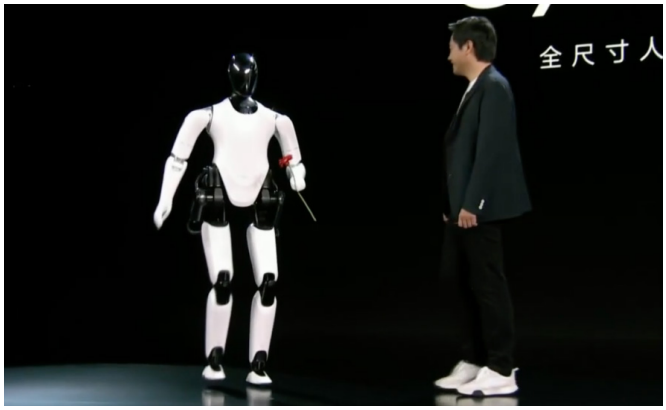
和场景；同时拓展新兴应用，鼓励政产学研协同创新，形成一批先进适用的机器人产品和解决方案，支撑各行业数字化转型和智能化升级。

■ 国家矿山安全监察局：“十四五”深入推进非煤矿山机械化、自动化和信息化建设

应急管理部、国家矿山安全监察局印发《“十四五”矿山安全生产规划》提出，实施矿山智能化发展行动计划，协同推进矿山自动化、智能化建设相关政策配套，分级分类推进矿山智能化建设。因地制宜建设一批效果突出、带动性强的智能化示范工程，总结提炼可复制的智能化建设模式，发挥智能化示范矿山引领作用。推动新建、改扩建矿井及大型煤矿、灾害严重煤矿实现智能化开采。小煤矿深化机械化换人、自动化减人专项行动，逐步向智能化过渡。

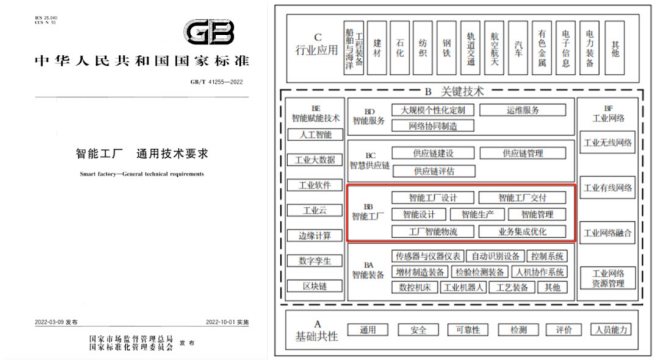
■ 小米首个全尺寸人形仿生机器人“CyberOne”亮相

“CyberOne”中文名“铁大”，整机高为 1.77 米，重量为 52KG，跟正常的成人一般大小。在昨天举行的“雷军年度演讲”现场，“铁大”还和雷军进行了首秀互动。据介绍，“铁大”拥有和人类一样的高智商，它能感知 45 种人类语义情绪，分辨 85 种环境语义。“铁大”采用了小米全自研全身控制算法，协调运动 21 个关节自由度，全身 5 种关节驱动，峰值扭矩可达 300Nm；在视觉方面，通过 Mi Sense 视觉空间系统加持，“铁大”具备三维重建真实世界的能力。



■ 《智能工厂 通用技术要求》将于 10 月 1 日正式实施

上海自仪院牵头制定的 GB/T 41255-2022《智能工厂 通用技术要求》针对智能工厂的智能设计、智能生产、智能管理、智能物流、系统集成等方面提出统一要求，并结合典型行业进行示范应用。该标准的实施将有助于智能工厂达到既定的建设目标，保证智能工厂与各个车间、外协工厂以及集团的协同运行，为智能工厂提供安全可靠的试验验证保障。



■ 完成多项工业连接新技术验证，爱立信与中国移动为 5G“无线全连接工厂”注入新动能

近日，爱立信与中国移动双方在中国移动”载行”5G 工业专网实验室完成了极致高可靠低时延连接等工业专网技术验证，并首次实现端到端时延小于 4ms 的基于无线化可编程逻辑控制器（PLC）的工业运动控制。该合作是“爱立信 - 中国移动无线新技术合作项目 COME2025”的一部分，新技术验证的成功为 5G 时代无“线全连接工厂”注入了新动能。

■ 小米智能工厂二期主体结构封顶，将打造世界级“灯塔工厂”

8 月 10 日，位于昌平区史各庄街道的小米智能工厂二期项目实现主体结构封顶。该项目建设用地面积约 5.83 公顷，规划总建筑面积 14.11 万平方米，共分为两个地块，东侧为智能手机工厂、西侧为高科技实验室。未来，该工厂将打造成为京津冀地区智能制造示范工厂和世界级“灯塔工厂”。“为了实现高品质建设，我们在安全管理、

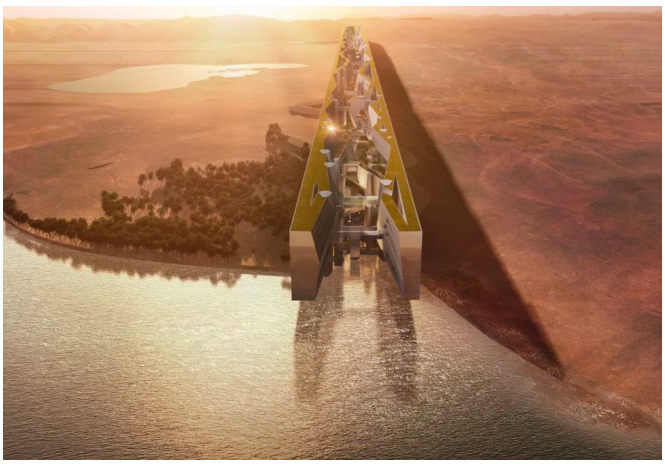
质量把控、技术创新、工序穿插、施工组织等方面做了大量工作。接下来，项目将转入二次结构、装饰装修、洁净工程及机电设备安装阶段，预计 2023 年年底全面交付投入使用。”

4 物联网行业一周要闻

- 沙特计划投 6.8 万亿元造现代版“万里长城”
- 华为办公宝 IdeaHub S2 系列发布
- 全国首个“交通全场景友好型”分布式光储项目投运
- 中国电信天翼物联加入开源鸿蒙社区
- 四部门联合推动家居行业发展
- 亚马逊掌纹支付功能即将推广
- 英国或将要求移民罪犯佩戴智能手表
- 中国联通物联网业务上半年实现收入 43 亿元，同比增 44.1%
- 中兴推出 5G 智能安全帽
- OPPO 首款智能猫砂盆官宣

■ 沙特计划投 6.8 万亿元造现代版“万里长城”

日前，沙特阿拉伯太子穆罕默德·本·萨勒曼宣布了“沙特长城”的设计方案。该计划名为“线之城（THE LINE）”，是萨勒曼在 2021 年年初提出的新型城市构想。在最初想法里，萨勒曼要在一片沙漠里建造一个 170 公里长的线性城市。在这个高度 AI 智能化的城市里，居民步行 5 分钟就能搞定日常所需，且这个城市只用清洁能源运行，不需要汽车和公路，全靠超高速交通和自动驾驶解决通勤。在最新的宣传片里，线之城主体结构是两个细长形的平行城墙，表面铺满了镜子，预计容纳居民数可达 900 万人。



■ 华为办公宝 IdeaHub S2 系列发布

近日，华为与央视联合召开 2022 华为智能协作新品发布会，正式发布首款搭载鸿蒙系统的华为新一代办公宝——IdeaHub S2 系列，其搭载新一代青云平台，CPU 性能提升 123%、GPU 性能提升 475%、NPU 性能提升 4T+2T FLOPS。同时还搭载 4K 视频会议专用摄像机，可实现低带宽、低时延、智能导播、发言人 C 位跟踪、Auto-Framing 智能取景等功能。

■ 全国首个“交通全场景友好型”分布式光储项目投运

据介绍，“交通全场景友好型”分布式光储项目是指利用高速公路项目红线范围内各类闲置交通资产，例如道路边坡、建筑屋顶、弃土场、隧道隔离带、服务区、收费站、沿线电子设备等全场景，建设分布式光储，集成光伏发电、电能储存、车辆充电、风光储氢多源协同的“冷热电”多能供应，实现资源的高效利用。此次在攀大高速全线启动的分布式光储项目装机容量为 2 兆瓦。

■ 中国电信天翼物联加入开源鸿蒙社区

近日，中国电信天翼物联正式加入 OpenHarmony 社区，并主导成立智慧城市蜂窝终端管理 SIG ，填补了中国电信在开源物联网终端操作系统生态领域的空白，中国电信也成为首个加入 OpenHarmony 开源社区的运营商。加入开源鸿蒙后，中国电信天翼物联将全面贡献其自主研发的智慧城市蜂窝终端代码等技术资源与创新经验，加快电信物联网生态与鸿蒙生态的融通互促、协作共享，携手共同繁荣开源生态，赋能产业数字化和数字产业化。

■ 四部门联合推动家居行业发展

据工信部网站 8 月 8 日披露，工信部等四部门近日印发推进家居产业高质量发展行动方案的通知。方案提出，到 2025 年，在家居产业培育 50 个左右知名品牌、10 个家居生态品牌，推广一批优秀产品，建立 500 家智能家居体验中心，培育 15 个高水平特色产业集群。

■ 亚马逊掌纹支付功能即将推广

亚马逊的“掌纹支付”技术，作为 Amazon One 支付服务的一部分，正在扩展至加利福尼亚州的 65 个 Whole Foods 门店。具体使用流程是先提供支付卡和电话号码，同意亚马逊服务条款，然后分享自己的掌纹。设置完成后，便可轻松地将物品带到收银台，而无需掏出钱包、甚至手机，只需将首张悬停在支付认证上方，即可便捷完成支付并离开。

■ 英国或将要求移民罪犯佩戴智能手表

据《卫报》报道，英国政府可能最早可能在 2022 年秋季就会开始使用智能手表来监控被定罪的移民。罪犯们每天最多需要进行五次人脸识别。根据《卫报》获得的文件，受这些条件限制的人需要全天为自己拍照，并全天候跟踪他们的位置。这些照片将与存档的照片进行比较，如果系统无法验证此人的身份，则需要进行人工检查。

■ 中国联通物联网业务上半年实现收入 43 亿元，同比增 44.1%

中国联通近日正式发布半年财报。数据显示，中国联通物联网业务上半年实现收入达到 43 亿元，同比增长 44.1% 。在物联网业务方面，中国联通加速推进人机物泛在互联，坚持 5G 引领的网业协同策略，自主定制增强雁飞芯模能力，推动行业部件融入场景、实现突破。截至 2022 年 6 月，中国联通物联网连接数达到 33,553 万户，车联网前装市场份额占比达到 70%。

■ 中兴推出 5G 智能安全帽

近日，中兴通讯在 2022 世界 5G 大会上推出了 5G 智能安全帽 MT5000，利用 5G 大带宽、低时延的特性，集成了 5 大类 20 项功能，包括语音控制、视频控制、定位、气体检测、报警等，实现智能感知识别人员分析。

■ OPPO 首款智能猫砂盆官宣

据悉，当前有关自动猫砂盆的安全问题层出不穷，甚至有夹伤甚至夹死猫的事情发生。而 OPPO 新款智能猫砂盆采用一体化结构防夹设计，支持六重安全防护，不用担心小猫被夹。该猫砂盆还适用多种猫砂，支持一键清理、抚平、换猫砂，智能识别记录不同爱猫的如厕次数和时长。

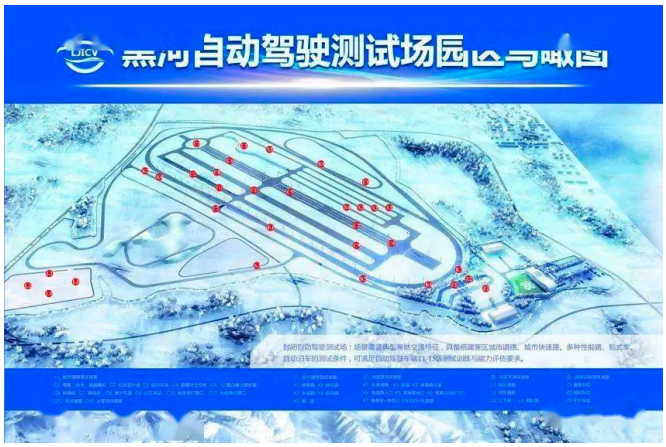
5 车联网行业一周要闻

- 黑河自动驾驶测试场已完成 5G 专网基站建设
- 交通运输部：鼓励在条件相对可控的场景使用自动驾驶汽车从事出租汽车客运经营活动
- 集度 2023 年底进军国内 46 城 2024 年交付第二款量产车
- 中国全无人自动驾驶首次收费运营：起步价 16 元
- 富士康获得首份自动驾驶电动拖拉机订单
- 小米汽车自动驾驶首期投入 33 亿元 2024 年进入行业第一阵营
- 车载 CIS 加速渗透 算力正向平台聚拢

■ 黑河自动驾驶测试场已完成 5G 专网基站建设

从黑河移动公司获悉， 黑河自动驾驶测试场已完成 5G 专网基站建设，预计 10 月末完成后期平台建设。这也是 5G 技术在全国首次应用于高寒地区自动驾驶测试领域。

该项目将为黑河自动驾驶测试场提供 5G 专网、5G 专网运营平台、WLAN 和专线等网络与技术支撑。其中 5G 专网为专享模式，可实现测试场和办公楼 5G 覆盖，为客户提供一体化专网基础设施和 5G 专网自助服务管理平台，依托 5G 专网实现专网状态的可视化查看，提供网络资源监控、智能运维、告警提醒等功能。



■ 交通运输部：鼓励在条件相对可控的场景使用自动驾驶汽车从事出租汽车客运经营活动

近日，交通运输部就《自动驾驶汽车运输安全服务指南（试行）》（征求意见稿）公开征求意见。在保障运输安全的前提下，鼓励在封闭式快速公交系统等场景使用自动驾驶汽车从事城市公共汽（电）车客运经营活动，在交通状况简单、条件相对可控的场景使用自动驾驶汽车从事出租汽车客运经营活动，在点对点干线公路运输、具有相对封闭道路等场景使用自动驾驶汽车从事道路普通货物运输经营活动。

■ 集度 2023 年底进军国内 46 城 2024 年交付第二款量产车

集度 CEO 夏一平介绍，2023 年集度门店将进军 46 城，2028 年将具备全年交付 80 万台的能力。“2023 年，集度量产交付的首款汽车机器人产品将拥有同时期业界体验最好的‘门到门、启到停’高阶自动驾驶能力”。夏一平进一步透露，集度即将发布首款汽车机器人量产车型的限定版，并将同步开启预订，预计于 2023 年下半年正式交付；其第二款车型的外观设计将在 2022 年底的广州车展亮相，预计于 2024 年开始交付。

■ 中国全无人自动驾驶首次收费运营：起步价 16 元

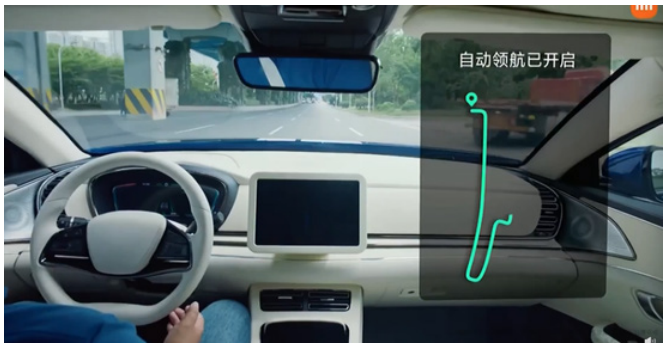
近日，重庆、武汉两地政府部门率先发布自动驾驶全无人商业化试点政策。百度拿到全国首批无人化示范运营资格，被允许车内无安全员的自动驾驶车辆在社会道路上开展商业化服务。目前，百度“萝卜快跑”已经在重庆市永川区、武汉经开区推出自动驾驶付费出行服务，投放的车型为第五代车 Apollo Moon 极狐版。定价遵循专车标准，以里程和时长作为计费单位，起步价 16 元，里程单价 2.8 元 / 公里，另外试运行期间折扣低至 1 折，运营时间为 9:00-17:00。

■ 富士康获得首份自动驾驶电动拖拉机订单

全球最大电子产品代工制造商富士康近日宣布，将从 2023 年初开始在俄亥俄州的工厂为加州 Monarch Tractor 公司生产自动驾驶电动 MK-V 系列拖拉机。据悉，这是自去年收购电动汽车初创公司 Lordstown Motors 的俄亥俄州工厂以来，富士康签订的首份制造合同。该工厂曾是通用汽车公司的组装厂。Monarch Tractor 没有透露拖拉机的成本，但表示自动驾驶软件将单独销售，农民必须每月支付费用才能获得服务。

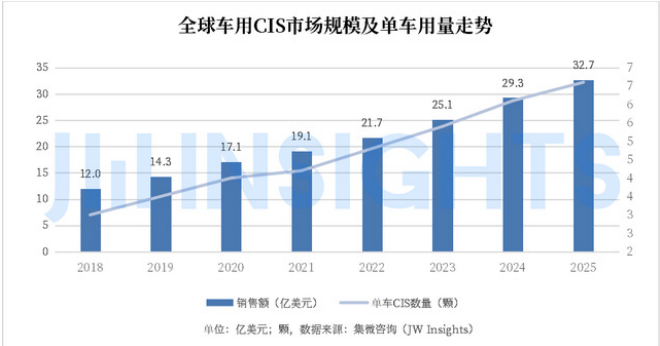
■ 小米汽车自动驾驶首期投入 33 亿元 2024 年进入行业第一阵营

在小米秋季新品发布会在京举行，小米公布了自动驾驶技术路面测试的实拍视频，展示其自动驾驶技术算法及全场景覆盖的能力。在小米披露的自动驾驶路面测试的实拍视频中，测试车辆在无保护自动掉头，自动环岛绕行及自动下连续坡道等多个场景，都实现了智能自动辅助驾驶体验。小米自动驾驶团队宣布将创新推出一体化的泊车智能解决方案，涵盖“预定车位”、“自主代客泊车”、“机械臂自动充电”等多项功能，未来还将打通其他停车场服务，在遵守国家相关法规前提下，实现智能化与服务化的体验融合。



■ 车载 CIS 加速渗透 算力正向平台聚拢

在智能网联汽车和自动驾驶的强力助推下，全球车载 CIS 的市场需求不断攀升。根据集微咨询（JW Insights）发布的数据，2021 年全球汽车电子行业的 CIS 市场规模约为 19.1 亿美元，到 2025 年将增长至 32.7 亿美元，年复合增速达 14.3%。



6 科技行业一周要闻

- 跨国全息传送首次实现：将人从美国“传送”到加拿大
- 我国 IPv6 网络活跃用户达 6.93 亿
- 科大讯飞推出古风高保真数字孪生虚拟人
- Counterpoint：2022 年折叠屏智能手机出货量将达到 1600 万部，同比增长 73%
- 印度拟将中国大陆手机制造商逐出低端市场

■ 跨国全息传送首次实现：将人从美国“传送”到加拿大

近日，加拿大科学家首次实现了国际间的全息传送 - 将一个人以全息图像的形式从美国阿拉巴马州传输到加拿大安大略省，团队其他人的全息图被传输到阿拉巴马州亨茨维尔市。据悉，全息传送的是全息图和远距离传输的组合体，可以将人或者物体的全息图传送到另一个位置，有点类似我们在电影中看到的全身投影。具体来说就是首先要创建一个人或物体的全息影像，接收端的用户要带上全息透镜就能看到传过来的全息影像，如果两人都带上全息透镜并将自己的全息影像发送过去，两人就可以在虚拟现实中互动，比如最基础的握手。

■ 我国 IPv6 网络活跃用户达 6.93 亿

近年来，工业和信息化部持续开展“IPv6 网络就绪”、“IPv6 端到端贯通”、“IPv6 流量提升”等系列专项工作，推动我国 IPv6 规模部署实现跨越式发展。截至目前，我国的 IPv6“高速公路”全面建成，信息基础设施 IPv6 服务能力已基本具备。IPv6 是用于替代 IPv4 的下一代 IP 协议，其地址数量号称可以为全世界的每一粒沙子编上一个地址。目前，我国 IPv6 互联网活跃用户数达 6.93 亿，移动网络 IPv6 流量占比突破 40%。

■ 印度拟将中国大陆手机制造商逐出低端市场

8 月 8 日，据台媒《经济日报》援引彭博社的报道称，印度打算限制中国大陆智能手机生产商出售价格在 12000 卢比（150 美元）以下的设备，以推动印度国内苦苦挣扎的手机产业发展。据知情人士透露，由于愈来愈担心 realme 和传音等品牌挤压印度本土制造商的生存空间，印度当局此举旨在将中国大陆手机巨头挤出该国较为低端的市场。报道认为，此举应不至于影响苹果或三星电子，因为这两大厂商的手机价格较高。但若离开印度入门级手机市场，小米等中国大陆品牌势必将会受到冲击。

■ 科大讯飞推出古风高保真数字孪生虚拟人

据悉，此次虚拟人整体打造，也是讯飞苏研院首次将 AI 技术与影视技术打通，塑造出的高保真孪生形象，对比常见的虚拟人，团队的着眼点从“更美”转换到“更真”，为未来元宇宙中人的形象，拓宽了想象空间。为真人打造其孪生形象，首先需要原型人物进入由百余台高清单反组成的相机阵列中，阵列系统在 0.1 秒内完成人体信息采集后，再通过 AI 算法进行自动化建模，根据不同的精度要求，建模时长可相应调整。初步生成白模后，确认人体的主要特征信息齐全，此时一个完整的 3D 人体模型便打造完成。

■ Counterpoint：2022 年折叠屏智能手机出货量将达到 1600 万部，同比增长 73%

近日，Counterpoint Research 发布报告称，折叠屏手机仍然是 2022 年增长最快的智能手机产品类别，预计 2022 年折叠屏同比增长 73% 至 1600 万台。其中，三星继续领先，今年上半年三星在折叠屏手机市场的份额为 62%。随着新 Galaxy Fold 4 和 Flip 4 机型的推出，报告预计下半年这一比例将跃升至 80%。Counterpoint Research 预测数据显示，今年全球折叠屏智能手机市场将从去年的 900 万部增长 73%，至 1600 万部；预计明年也将继续出现强劲增长，预计到 2023 年折叠屏手机将增长到 2600 万台。2022 年 6 月，三星在 2022 年上半年占据了折叠屏智能手机的主要市场份额，占总市场份额的 62%；华为和 OPPO 分列第二和第三。

资料来源：Counterpoint Research 可折叠智能手机预测，2022 年 8 月。

■ 印度拟将中国大陆手机制造商逐出低端市场

8 月 8 日，据台媒《经济日报》援引彭博社的报道称，印度打算限制中国大陆智能手机生产商出售价格在 12000 卢比（150 美元）以下的设备，以推动印度国内苦苦挣扎的手机产业发展。据知情人士透露，由于愈来愈担心 realme 和传音等品牌挤压印度本土制造商的生存空间，印度当局此举旨在将中国大陆手机巨头挤出该国较为低端的市场。报道认为，此举应不至于影响苹果或三星电子，因为这两大厂商的手机价格较高。但若离开印度入门级手机市场，小米等中国大陆品牌势必将会受到冲击。

7 安全一周要闻

- IDC：2026 年中国网络安全市场规模将超 318 亿美元，全球占比约 11.1%
- 黑客公布马斯克“星链”攻击工具
- 阿卡迈阻止了欧洲最大型 DDoS 攻击
- 《云计算安全责任共担模型》行业标准正式发布
- 德国工商总会被网络攻击打爆了
- 导弹制造商 MBDA 否认被黑客入侵，承认数据丢失
- 大华 IP 摄像机漏洞可能让攻击者完全控制设备
- BlackCat 勒索软件声称对欧洲天然气管道进行攻击
- 黑客组织公开 2TB 电子邮件，揭露南美洲多家矿业公司黑幕
- 美国众议院通过了《勒索软件法案》主要应对俄罗斯、朝鲜、伊朗在内的多国勒索软件攻击
- Magecart 对餐厅订餐系统进行攻击
- 欧洲能源网安警报！卢森堡电力和天然气管道公司遭 BlackCat 勒索攻击恐遭大规模数据泄露
- 中欧天然气管道公司疑遭勒索软件攻击，150GB 数据失窃
- 航天工业五个重大网络安全事件
- 奇安信集团董事长齐向东： 以“零事故”为目标护航 5G 融入千行百业
- 海莲花组织（APT32）针对我国关基单位攻击活动分析

■ IDC：2026 年中国网络安全市场规模将超 318 亿美元，全球占比约 11.1%

近日，IDC 发布报告称，2021 年全球网络安全 IT 总投资规模为 1687.7 亿美元（约 1.14 万亿元人民币），并有望在 2026 年增至 2875.7 亿美元（约 1.94 万亿元人民币），五年复合增长率（CAGR）为 11.3%。从中国市场来看，IDC 预计 2026 年中国网络安全 IT 支出规模将达到 318.6 亿美元（约 2144.18 亿元人民币），全球占比约为 11.1%，五年 CAGR 约为 21.2%。

■ 黑客公布马斯克“星链”攻击工具

在拉斯维加斯举行的 Black Hat 安全会议上，比利时鲁汶大学 (KU Leuven) 的安全研究员 Lennert Wouters 将首次披露 Starlink 用户终端（即位于住宅和建筑物上的星链卫星天线）的安全漏洞。Wouters 将详细介绍攻击者如何利用一系列硬件漏洞访问 Starlink 系统并在设备上运行自定义代码。为了访问星链卫星天线的软件，Wouters 改造了他购买的一个星链天线，并制作了一个可以连接到星链天线的定制黑客工具。该工具使用一种被称为 modchip 的定制电路板，零件成本仅约 25 美元。连接到星链天线后，该自制工具就能够发起故障注入攻击，暂时使系统短路以绕过星链的安全保护。这个“故障”使 Wouters 能够进入被锁定的星链系统。

■ 阿卡迈阻止了欧洲最大型 DDoS 攻击

Akamai Technologies（阿卡迈技术公司，下称阿卡迈）平息了欧洲史上最大型分布式拒绝服务（DDoS）攻击，将一家东欧公司从 30 多天的持续重创中解救出来。作为网络安全和云服务供应商，阿卡迈表示，攻击高潮出现在 7 月 21 日，14 个小时内达到峰值每秒 6.596 亿数据包（Mpps）和每秒 853.7 千兆比特每秒（Gbps）。

■ 《云计算安全责任共担模型》行业标准正式发布

为建立更加精细可落地、普遍适用于云计算行业的安全责任共担模型，提升云服务客户责任共担意识与承担水平，2019 年起，由中国信息通信研究院（以下简称“中国信通院”）牵头，联合数十家云服务商开展了云计算安全责任共担的相关研究，制定 YD/T 4060—2022《云计算安全责任共担模型》行业标准，该标准已于 2022 年 7 月正式发布施行。

■ 德国工商总会被网络攻击打爆了

据 Bleeping Computer 消息，网络攻击组织盯上了德国工商总会 (DIHK)，对其发起了大规模的网络攻击。DIHK 无力面对如此强力的网络攻击，直接躺平：被迫关闭了所有的 IT 系统，关闭所有的数字服务、电话和电子邮件服务器。根据德国有关法律规定，所有德国境内企业（除手工业者、自由职业者及农业加工业外）均必须加入德国工商会。目前，尚未了解 DIHK 被攻击的原因，也没有黑客组织声称对此次攻击负责。在被攻击之后，DIHK 在网站上发布了一份简短的通知，并表示关闭系统和数字服务是预防网络攻击造成更大损失的一种措施，也让 IT 团队有更多的时间摸清此次网络攻击的情况，并针对性的给出解决方案，提高系统的防护能力。 DIHK 总经理迈克尔伯格曼通过 LinkedIn 发布消息称，网络攻击发生在 8 月 3 日，并指出是一次大规模的攻击事件。DIHK 暂时也无法确定修复时间许多多久，这也就意味着无法确定服务恢复的时间。有安全专家指出，此次网

络攻击有可能是勒索组织所为，DIHK 被迫关闭所有系统和数字服务，其目的是防止恶意软件快速传播，但这种猜测尚未得到官方的证实。截至目前也没有哪个勒索软件在其官网上宣布成功入侵 DIHK 的消息。
https://www.freebuf.com/news/341115.html

■ 导弹制造商 MBDA 否认被黑客入侵，承认数据丢失

欧洲导弹开发商和制造商表示，黑客试图用从外部硬盘驱动器获得的非敏感信息来勒索该公司。一个自称为 Adrastea（Andrastea）的组织表示，他们从 MBDA 获取了 60 GB 的文件，其中包括有关该公司参与“封闭军事项目”的秘密信息。然而，MBDA 否认 Adrastea 入侵了该公司的内部系统，表示其内部系统未被破坏，但该公司承认威胁行为者从外部硬盘驱动器访问了非敏感数据。“数据的来源已经确定，是从外部硬盘驱动器获取的。已经证实，公司的安全网络没有发生黑客攻击。到目前为止，该公司的内部验证程序表明，网上提供的数据既不是机密数据，也不是敏感数据，“发言人说。MBDA 是欧洲导弹的开发商和制造商，名称中的四个字母代表三家法国、意大利和英国公司合并成为 MBDA，法国公司 Matra，英国 BAe Dynamics 和意大利 Alenia。Adrastea 在一个流行的俄语黑客论坛 XSS 上宣布了有关泄漏的消息，这意味着威胁行为者已经访问了 MBDA 的意大利分支机构，并窃取了与该公司与意大利国防部合作有关的文件。威胁行为者表示，他们已经下载了防空、导弹系统和海岸保护系统的设计文档，演示文稿，与其他国防承包商的通信以及其他敏感信息。
https://cybernews.com/news/missile-maker-mbda-denies-being-hacked-admits-to-data-loss/

■ 大华 IP 摄像机漏洞可能让攻击者完全控制设备

大华开放网络视频接口论坛（ONVIF）标准实施中存在编号为 CVE-2022-30563（CVSS 得分：7.4）的安全漏洞，该漏洞在被利用时可能导致夺取对 IP 摄像机的控制权。“攻击者可能会滥用该漏洞，通过嗅探以前未加密的 ONVIF 交互并在对摄像机的新请求中重播凭据来破坏网络摄像机，”Nozomi Networks 表示。此问题已在 2022 年 6 月 28 日发布的补丁中得到解决。ONVIF 管理开放标准的开发和使用，用于基于 IP 的物理安全产品（如视频监控摄像机和门禁系统）如何以与供应商无关的方式相互通信。Nozomi Networks 识别出的错误存在于中国公司大华开发的某些 IP 摄像机中实施的所谓“WS-UsernameToken”身份验证机制中，允许攻击者通过重放凭据来破坏摄像机。换句话说，成功利用该漏洞可能允许攻击者秘密添加恶意管理员帐户并利用该帐户以不受限制地访问具有最高权限的受影响设备，包括观看实时摄像机源。威胁参与者需要安装此攻击的所有操作都是能够捕获一个使用 WS-UsernameToken 架构进行身份验证的未加密 ONVIF 请求，然后使用该请求发送具有相同身份验证数据的伪造请求，以诱骗设备创建管理员帐户。“威胁行为者，特别是民族国家威胁组织，可能对入侵 IP 摄像机感兴趣，以帮助收集有关目标公司设备或生产过程的情报，”研究人员说。“这些信息可能有助于在发动网络攻击之前进行的侦察。随着对目标环境的更多了解，威胁行为者可以制定自定义攻击，从而物理中断关键基础设施中的生产流程。”https://thehackernews.com/2022/07/dahua-ip-camera-vulnerability-could-let.html

■ BlackCat 勒索软件声称对欧洲天然气管道进行攻击

ALPHV 勒索软件团伙（又名 BlackCat）上周声称对中欧国家的天然气管道和电力网络运营商 Creos Luxembourg S.A. 的网络攻击负责。Creos 的所有者 Encevo 在五个欧盟国家担任能源供应商，他于 7 月 25 日宣布，他们在 7 月 22 日至 23 日遭受了网络攻击，导致 Encevo 和 Creos 的客户门户变得不可用，但所提供的服务没有中断。7 月 28 日，该公司发布了有关网络攻击的最新消息，调查结果显示，网络入侵者已从访问的

系统中泄露了“一定数量的数据”。当时，Encevo 无法估计影响的范围，并恳请客户耐心等待，直到调查结束，届时每个人都会收到个性化通知。目前，建议所有客户重置其在线帐户凭据，他们使用这些凭据与 Encevo 和 Creos 服务进行交互。此外，如果这些密码在其他站点上相同，则客户也应在这些站点上更改其密码。ALPHV / BlackCat 勒索软件组织在 7 月 30 日将 Creos 添加到其勒索网站，威胁要发布 180000 个被盗文件，总计 150 GB，包括合同、协议、护照。账单和电子邮件。ALPHV / BlackCat 最近推出了一个新的勒索平台，他们使访问者可以搜索被盗数据，目的是增加受害者的压力，让他们支付赎金。

https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

■ 黑客组织公开 2TB 电子邮件，揭露南美洲多家矿业公司黑幕

该组织希望揭露该地区的环境破坏黑幕，并谴责美国和其他国际政府和公司掠夺该地区资源的行为对环境造成了破坏。8 月 3 日，一个黑客团体发布了来自中美洲和南美洲多家矿业公司的超过 2TB 的被黑电子邮件和文件，揭露该地区的环境破坏黑幕。该组织自称 Guacamaya（一种鸟类的名称），发布了来自五家公共和私营矿业公司以及两个负责环境监督的公共机构的文件，一个在哥伦比亚，另一个在危地马拉。这些材料被发布到一个名为 Enlace Hacktivista 的网站上，该网站用于记录黑客历史、共享教育资源，并为“黑客发布他们的攻击、泄密和公报”提供空间。在与这些材料一起发布的一份西班牙语声明中，该组织谴责美国和其他国际政府和公司掠夺该地区资源的行为对环境造成了破坏。Guacamaya 在 3 月发布了来自一家瑞士投资集团的采矿子公司的 4.2 TB 的材料，其中详细说明了这些公司在危地马拉的明显污染。这些文件成为涉及全球 65 名记者的大规模报道项目的一部分，该项目不仅暴露了污染证据，还暴露了操纵地方政府和监视记者的努力。在那次黑客攻击之后，该组织发布了一段视频，详细说明了他们如何访问系统并窃取文件和电子邮件。“黑客的角色是在任何有尊严的愤怒和对激进革命的快乐渴望的地区参与不同形式的抵抗，”他们说。

https://www.secrss.com/articles/45413

■ 美国众议院通过了《勒索软件法案》主要应对俄罗斯、朝鲜、伊朗在内的多国勒索软件攻击

近日，美国众议院通过了《报告来自被选为监督和监控网络攻击和勒索软件的国家的攻击法案》（也称为《勒索软件法案》）据悉，美国众议佛罗里达州共和党众议员 Gus Bilirakis 的说法，《勒索软件法案》将使美国更容易应对来自外国对手的勒索软件攻击。拟议的立法将通过强制报告与勒索软件和其他攻击有关的跨境投诉来修订 2006 年美国安全网络法案。《勒索软件法》主要针对俄罗斯、中国、朝鲜和伊朗，在提到涉嫌勒索软件攻击者时，特别指出了这些国家。它针对那些被指控对美国实施勒索软件攻击的国家的个人、政府或其他组织。根据该法律，联邦贸易委员会 (FTC) 将每两年向众议院能源和商业委员会以及参议院商业、科学和运输委员会提交一份报告。该报告将概述 FTC 收到的跨境投诉，并按被指控的攻击者进行细分。描述了其使用和体验 2006 年美国安全网络法案（公法 109-455）授予的权限以及该法案所做的修正。报告包括以下内容：该报告将包括涉及勒索软件的投诉数量，以及 FTC 已采取或未采取行动的投诉清单。在该法案中，Bilirakis 呼吁 FTC 确定与其合作的外国机构，以及它取得的成果。它还将确定它在外国法院购买的任何诉讼，并注明结果。“我们看到针对美国人的网络犯罪有所增加，”Bilirakis 在宣布该法案时说。“这些事件凸显了加强和现代化我们的关键基础设施以防止和应对网络攻击的重要性。”据悉，Bilirakis 于 2021 年 7 月提出了这项名为 HR

4551 的立法。它现在必须通过参议院才能到达总统的办公桌。

https://mp.weixin.qq.com/s?__biz=MzUzNDYxOTA1NA==&mid=2247530083&idx=3&sn=d95717d14b13779d9f947fbccfd7782a&scene=21#wechat_redirect

■ Magecart 对餐厅订餐系统进行攻击

研究人员发现，Magecart 的攻击活动一直在利用三个在线餐厅订餐系统盗取那些毫无戒心的顾客的支付卡凭证，并且攻击影响了大约 300 家使用这些服务的餐厅，迄今已泄露了数万张卡的信息。多次进行攻击的 Magecart 团伙将 e-skimmer 脚本注入到了使用这三个独立平台的在线订购门户。来自 Recorded Future 的研究人员在本周的一篇博文中透露，针对 MenuDrive、Harbortouch 和 InTouchPOS 进行的攻击，一个似乎在去年 11 月开始的，另一个是在 1 月。Recorded Future's Insikt Group 的研究人员在报告中写道，这三个平台上，至少有 311 家餐厅被 Magecart 感染，随着更深入的分析，这个数字可能会继续增加。Magecart 是一个网络犯罪集团的总称，他们会使用盗卡技术从销售点（POS）或电子商务系统使用的支付卡中窃取凭证。并且他们通常最终会在暗网的黑客论坛上出售这些被盗的凭证。研究人员指出，在 Recorded Future 观察到的两个攻击活动中，那些受影响的餐馆网站往往会导致客户的支付卡数据和 PII（他们的账单信息和联系信息）发生泄露。他们说，到目前为止，研究人员已经从暗网上发布的活动中发现了 5 万多条被破坏的支付记录，他们预计未来会有更多被盗数据被发布出来。研究人员发现，MenuDrive 和 Harbortouch 是同一个 Magecart 攻击者的攻击目标，这一攻击活动导致 80 家使用 MenuDrive 的餐馆和 74 家使用 Harbortouch 的餐馆感染了 e-skimmer 病毒。他们在帖子中指出，这个攻击活动可能是不晚于 2022 年 1 月 18 日开始的，截至本报告发布，仍然有一部分餐馆受到了感染。然而，研究人员确定该攻击活动的恶意域名为 authorizen[.]net，5 月 26 日以来就已经被封锁。研究人员说，一个单独的、不相关的 Magecart 攻击活动甚至在更早就针对 InTouchPOS 进行了攻击，此活动最迟在 2021 年 11 月 12 日开始。在那次攻击活动中，有 157 家使用该平台的餐馆被感染 e-skimmers，而且与该攻击活动有关的恶意域名 bouncepilot[.]net 和 pinimg[.org 仍然十分活跃。此外，据 Recorded Future 称，针对 InTouchPOS 的攻击活动使用的策略和破坏指标与自 2020 年 5 月以来，针对 400 个从事不同类型交易的电子商务网站的其他网络犯罪活动非常相似。研究人员说，截至 6 月 21 日，相关攻击活动中的 30 多个受影响的网站仍然在受到不同程度的影响。

研究人员指出，虽然像 Uber Eats 和 DoorDash 这样的集中式餐厅订餐平台在这类系统的市场中占主导地位，而且比受这些活动影响的平台要知名得多，但互联网上数百个为当地餐厅服务的小型平台仍然是网络犯罪分子的重要攻击目标。他们说，即使是小规模的平台也可能有数以百计的餐馆作为客户，这意味着针对一个较小的平台攻击就可以泄露出数十种在线交易和支付卡的信息。事实上，这些平台对攻击者来说是非常有吸引力的，研究人员指出，他们更倾向于用最少的工作量寻求最高的回报。一位安全专家指出，一般来说，电子商务网站在安全方面一直面临着很大的挑战，而且往往会包含来自第三方或供应链合作伙伴的代码，这些代码很容易被攻击者破坏，并可能对下游产生更大的影响。网络安全公司 PerimeterX 的首席营销官在给媒体的一封电子邮件中写道，这是用来解释网络攻击生命周期的一个很好的例子，由于网络攻击的周期性和连续性，导致网站的数据被大量泄露，这也就是 Magecart 攻击的结果，这也为另一个网站的刷卡、凭证填充或账户接管攻击提供了资源。

https://threatpost.com/magecart-restaurant-ordering-systems/180254/

■ 欧洲能源网安警报！卢森堡电力和天然气管道公司遭 BlackCat 勒索攻击恐遭大规模数据泄露

ALPHV 勒索软件团伙，又名 BlackCat，声称对上周针对中欧国家天然气管道和电力网络运营商 Creos Luxembourg SA 的网络攻击负责。Creos 的所有者 Encevo 于 7 月 25 日宣布，他们在 7 月 22 日至 23 日遭受了网络攻击，该公司在五个欧盟国家经营能源供应商。Creos Luxembourg SA 在卢森堡拥有并管理电力网络和天然气管道。公司规划、建设和维护其拥有或负责管理的高、中、低压电网和高、中、低压天然气管道。虽然网络攻击导致 Encevo 和 Creos 的客户门户不可用，但所提供的服务并未中断。7 月 28 日，该公司发布了网络攻击的最新消息，他们的初步调查结果表明，网络入侵者已经从被访问的系统中窃取了“一定数量的数据”。当时，Encevo 无法估计影响的范围，并恳请客户耐心等待调查结束，届时每个人都会收到个性化的通知。由于没有在 Encevo 的媒体门户上发布进一步的更新，因此该程序可能仍在进行中。Encevo 说，当有更多信息可用时，它将发布在网络攻击的专用网页上。目前，建议所有客户重置他们用于与 Encevo 和 Creos 服务交互的在线帐户凭据。此外，如果这些口令在其他网站上相同，客户也应该在这些网站上更改他们的口令。Encevo 表示已向大公国警察局报告，并已通知卢森堡国家数据保护委员会、卢森堡监管研究所和其他“主管部门”。Bleeping Computer 已联系 Creos，要求提供有关网络攻击影响的更多信息，但该公司发言人现阶段拒绝发表任何评论。ALPHV/BlackCat 勒索软件组织 7 月 30 日将 Creos 添加到其勒索网站，威胁要发布 180,000 个被盗文件，总大小为 150GB，包括合同、协议、护照、账单和电子邮件。虽然没有宣布实现这一威胁的确切时间，但黑客们发誓要在 8 月 1 日（周一）晚些时候进行披露。ALPHV/BlackCat 最近推出了一个新的勒索平台，让访问者可以搜索被盗数据，目的是增加受害者的压力，让他们支付赎金。在 2022 年 7 月 10 日下午 15:35 在 Dark Web 发布的最新帖子中，“ALPHV”不仅通过文本签名引入了搜索，而且还支持用于搜索密码和泄露 PII 的标签。似乎一些被盗文件仍在索引中，但大部分已可用于快速导航。已识别出超过 2,270 个包含明文访问凭证和密码信息的索引文档，以及超过 100,000 包含机密标记的文档，包括索引的电子邮件通信和敏感附件。虽然 BlackCat 继续创新数据勒索，但他们似乎从未从错误中吸取教训，并继续针对可能使他们成为国际执法机构瞄准目标的知名公司。BlackCat 被认为是重新命名的 DarkSide， 在对 Colonial Pipeline 的广为人知的勒索软件攻击后，在执法部门的压力下关闭。关闭 DarkSide 后，他们重新命名为 BlackMatter 以逃避执法，但随着该团伙再次关闭，压力仍在继续。自 2021 年 11 月威胁行为者以 BlackCat/ALPHV 的形式重新启动以来，威胁行为者倾向于避开美国的大型目标，转而瞄准欧洲实体，如 奥地利国家、 意大利时装连锁店和 瑞士机场服务提供商。然而，他们似乎没有从错误中吸取教训，继续攻击关键基础设施，例如 2 月份的德国石油供应公司 Oiltanking 和现在的 Creos Luxembourg。BlackCat 也称为“ALPHV”或“AlphaVM”和“AphaV”，是用 Rust 编程语言创建的勒索软件系列。该组织的领导人在暗网论坛上的通讯中具有相同的别名，将 Rust 描述为与 Lockbit 和 Conti 相比美，Rust 是他们的储物柜的竞争优势之一。尽管 Blackcat 和 Alpha 在 TOR 网络中具有完全不同的 URL，但它们页面上使用的脚本场景是相同的，并且可能由相同的参与者开发。欧盟网络安全局 7 月 29 日发布了一份报告，其中分析了 2021 年 5 月至 2022 年 6 月期间欧盟发生的 623 起事件。报告发现，在勒索软件攻击期间，每月有 10TB 的数据被盗和外泄，而超过 60% 的组织可能已经支付了赎金。https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

■ 中欧天然气管道公司疑遭勒索软件攻击，150GB 数据失窃

ALPHV 勒索软件团伙威胁称，已成功入侵中欧地区天然气管道与电力网络运营商 Creos，并窃取 150GB 数据；Creos 母公司确认遭到网络攻击，导致客户服务网站无法访问，数据失窃，但服务运营没有中断；ALPHV 团伙此前恶迹累累，其前身 DarkSide 曾在 2021 年 5 月入侵科洛尼尔致使美国东部输油管道停运多天。8 月 2 日消息，ALPHV 勒索软件团伙（又名 BlackCat）声称，对上周中欧地区天然气管道与电力网络运营商 Creos Luxembourg S.A. 遭受的网络攻击负责。Creos 母公司 Encevo 在 7 月 25 日证实，在 7 月 22 日至 23 日遭受了网络攻击。Encevo 在欧盟五个国家拥有能源经营业务。虽然网络攻击致使 Encevo 和 Creos 的客户门户网站无法访问，但其服务运营并未中断。7 月 28 日，Encevo 公司发布关于网络攻击的最新消息，称初步调查结果表明，网络入侵者已经从被访问系统中窃取到“一定数量的数据”。Encevo 还坦言，他们暂时无法估量影响的具体范围，并恳请客户耐心等待调查结束，届时将分别发送个性化事件通报。目前 Encevo 的媒体门户上仍未发布进一步更新，因此调查程序可能仍在进行当中。Encevo 表示在掌握更多情报时，会将消息发布在专门的网络攻击页面上。眼下，他们建议所有客户重置用于 Encevo 和 Creos 服务交互的线上账户凭证。此外，如果在其他网站上使用到相同的密码内容，客户也应相应修改这些密码。外媒 Bleeping Computer 已经联系 Creos，并提出关于此次网络攻击影响的置评请求，但该公司发言人现阶段拒绝发表任何评论。

https://mp.weixin.qq.com/s?__biz=MzkyMzAwMDEyNg==&mid=2247529725&idx=2&sn=da08d7a5ca5101d86df1ab6ffa867511&scene=21#wechat_redirect

■ 航天工业五个重大网络安全事件

针对国际太空计划的破坏性网络攻击和数字间谍活动呈现令人担忧的增长趋势。在过去五年中，国际太空计划和卫星关键基础设施遭受的一系列重大网络攻击已经成为太空网络安全态势的转折点。近年来，太空数字关键基础设施的军民融合趋势正在提速。例如 SpaceX、BlueOrigin 和波音公司的成功发射，SpaceX 通过 Starlink 为乌克兰提供关键通信基础设施，以及太空部队和太空 ISAC 的创建。太空网络安全威胁也随着地缘政治紧张局势而升级，俄罗斯已经宣布将退出国际空间站（ISS）。最早的太空网络安全事件报道可追溯到 2008 年，在国际空间站从 Windows XP 切换到 Linux 之前，据西方媒体报道，俄罗斯宇航员将一个受感染的 USB 设备引入了空间站上的计算机，导致国际空间站上的宇航员使用的基于 Windows XP 的笔记本电脑感染了一种名为 W32.Gammima.AG，一种窃取密码的计算机病毒。美国国家航空航天局（NASA）官员当时将这种病毒描述为“令人讨厌的东西”。补充说它“不是经常发生，但这不是第一次”。最近，威胁情报结构 BushidoToken 盘点了航天工业近年来遭遇的五个重大太空网络安全事件，具体如下：卫星通信（SATCOM）可以提供电视广播和远程访问互联网。然而，这种基于卫星的互联网访问被称为下行链路。2015 年 9 月，卡巴斯基实验室披露了一个名为 Turla 的俄罗斯高级持续威胁 (APT) 组织（又名 Snake 或 VenomousBear）利用了这些卫星互联网连接的弱点。Turla 将监视下行链路，识别活动 IP 地址，在入侵期间选择一个作为源 IP 地址，并通过在发送到卫星和从卫星发送的数据包中隐藏恶意代码来劫持它。被 Turla 入侵的系统还会将数据泄露到常规卫星互联网用户的 IP 地址。Turla 使用这种特殊技术针对中东和非洲的政府、大使馆、军事实体、教育机构、研究组织和制药公司的系统。Estonian 情报部门将 Turla 的业务与俄罗斯联邦安全局 (FSB) 联系在一起。2022 年 2 月，德国调查记者披露了两名 Turla 开发商的身份以及他们与俄罗斯 FSB 的关系。2020 年 12 月，与 Nobelium APT 组织（又名 APT29、CozyBear 或 DarkHalo）

相关的 SolarWinds 供应链攻击内幕被披露。它涉及 SolarWinds Orion 平台的恶意软件更新，已被超过 1.8 万名 SolarWinds 客户下载。Nobelium 设法入侵了 SolarWinds 软件构建环境，并使用名为 SUNSPOT 的软件来加载 SUNBURSTOrion 软件更新后门。据报道，入侵始于 2019 年 9 月，并于 2019 年 10 月首次尝试添加测试代码并将其推送给 SolarWinds 客户。为了使其更难被发现，SUNBURST 的代码是使用从 Orion 平台窃取的证书进行签名，并且它的命名约定与 Orion 的代码相同，因此 SolarWinds 开发人员会将其误认为是他们自己的。安装后，SUNBURST 将休眠 12-14 天，然后通过 DNS 联系 C&C 服务器。SUNBURST 的流量还使用 Orion 改进计划协议 (OIP) 来混入合法的 SolarWinds 活动。然后，Nobelium 会使用 SUNBURST 部署其他恶意软件，例如 TEARDROP、RAINDROP 和其他一些恶意软件。根据美国国家安全局 (NSA) 的声明，大约 100 个非政府实体收到了后续活动，其中包括几个美国联邦政府机构和 NASA。2021 年 1 月，美国国家情报总监办公室（ODNI）正式发表声明称这次攻击是由俄罗斯外国情报局（SVR）策划的。分析：

尽管太空探索和研究涉及国际太空机构之间的大量合作，但一些情报机构在这些协议之外运作并无视这些协议。Turla 和 Nobelium 都属于高级持续性威胁，但并未窃取知识产权信息。

此类活动本质上是传统间谍活动的网络版本，将始终发生在民族国家的竞争对手之间。很难将这些类型的入侵称为“攻击”，因为没有破坏性组件。然而，在这些网络间谍活动中收集的信息可能会支持未来的破坏性进攻行动。降低 IT 系统和网络性能的网络攻击更有可能来自网络犯罪威胁团体，而不是民族国家的 APT 组织。2020 年 7 月下旬，美国宇航局的 Ingenuity Mars 直升机使用的导航设备和智能设备的主要制造商 Garmin 遭到 WasedLocker 勒索软件的攻击。Garmin 的云服务，包括飞行员使用的设备同步和地理定位仪器一度无法使用。Garmin 在其官方声明中证实遭受网络攻击，导致在线服务中断，一些内部系统被加密。Garmin 报告说，没有证据表明任何人在事件期间未经授权访问了用户数据。一位熟悉该事件的匿名 Garmin 员工透露，勒索赎金要求为 1000 万美元。在全球服务中断四天后，Garmin 突然宣布他们已向网络犯罪分子支付赎金以获得解密器后开始恢复服务。值得注意的是，WastedLocker 由于与 eCrime 威胁组织开发的其他勒索软件系列 DoppelPaymer 和 BitPaymer 的相似性而被归因于 EvilCorp。2019 年 12 月，EvilCorp 被列入造成 1 亿美元经济损失的美国 OFAC 制裁名单。因此，向 EvilCorp 支付赎金可能会导致 Garmin 被美国政府处以巨额罚款。太空领域最具破坏性的网络攻击之一是在俄罗斯入侵乌克兰当晚针对欧洲卫星通信网络发动的攻击。美国和欧盟声称，2022 年 2 月 24 日，俄罗斯对属于 Viasat 的名为 KA-SAT 的商业卫星通信网络发起了网络攻击。网络攻击旨在破坏乌克兰的指挥和控制行动，并对包括德国、希腊、波兰、意大利和匈牙利在内的其他欧洲国家造成重大溢出影响。直到一个月后，欧洲卫星宽带服务才从事件中恢复。据 Viasat 称，数以万计的 SATCOM 调制解调器被毁坏，不得不更换。据报道，攻击者能够通过利用“配置错误的 VPN”获得访问权限，并横向移动到 KA-SAT 网络的管理部分。随后，攻击者执行命令来清除调制解调器的内存，使它们无法使用。有趣的是，来自网络安全供应商 SentinelOne 的研究人员发现了一种名为 AcidRain 的擦除恶意软件，该恶意软件专为 SATCOM 调制解调器使用的 MIPS 固件而设计，可能用于 KA-SAT 攻击。SentinelOne 研究人员认为，AcidRain 是由与 VPNFilter 相同的恶意软件作者开发的，VPNFilter 被正式归因于俄罗斯主要情报局 (GRU)，更具体地说是 GTsST Unit 74455，即著名的沙虫团队。对航天工业发起破坏性网络攻击并不限于国家资助的 APT 团体和有组织的网络犯罪分子。2022 年 3 月，一个名为 Network Battalion 65（又名 NB65）的

亲乌克兰黑客组织通过 Twitter 分享说，它对俄罗斯航天局 Roscosmos 发起了攻击。Roscosmos 总干事德米特里·罗戈津（Dmitry Rogozin）后来在推特上表示 NB65 的说法“不真实”，并称他们为“小骗子”。不过，NB65 分享的截图据称属于俄罗斯卫星成像软件和车辆监控系统。Roscosmos 事件最终被俄官方否认，NB65 也未能提供足够有效证据。同样在 3 月，一个据称与黑客组织 Anonymous 有关的推特帐户透露另一个名为 v0g3lSec 的黑客组织破坏了一个属于俄罗斯空间研究所 (IKI) 的网站，并泄露了据称属于俄罗斯航天局 Roscosmos 的文件。其中一份被盗文件讨论了月球南极潜在着陆点的位置。这与俄罗斯当局已经宣布的南极地点相吻合，这可能会增加这些文件被成功窃取的可信度。NB65 和 v0g3lSec 攻击俄罗斯航天局分析：虽然不常见，但纯粹的破坏性网络攻击往往是最令人恐惧的。数据丢失和对系统的非法访问可能会造成数百万美元的损失，并使运营延迟数月或数年。最具破坏性的攻击通常会使用数据加密勒索软件或数据破坏擦除器。沙虫团队实施的进攻性网络行动是世界上最危险的行动之一。它是少数成功发起多次网络攻击的 APT 组织之一，这些攻击具有破坏性影响，主要针对乌克兰。针对太空组织和卫星网络的攻击技术往往是最先进的，但最危险的对手也许不是民族国家和网络犯罪威胁团体，而是黑客活动团体上。与通常试图秘密获取和维持访问权限的国家黑客或希望将访问权限货币化的网络犯罪分子不同，黑客活动主义者往往试图通过破坏网站、通过 DDoS 攻击关闭网站或泄露数据的方式来羞辱对手，支持其活动主张。航天工业的威胁模型与许多其他垂直行业大不相同。攻击面涉及许多先进技术，例如卫星通信网络。现代航空供应商往往无力保护这些技术，需要定制安全解决方案。例如，物联网 (IoT) 设备的端点安全性目前远不及现代工作站的水平，这使得航天产业对高级持续威胁的准备严重不足。

来源：GoUpSec

■ 奇安信集团董事长齐向东：以“零事故”为目标护航 5G 融入千行百业

中国经济新闻网哈尔滨讯（杨同玉）8 月 10 日，在 2022 世界 5G 大会主论坛上，奇安信集团董事长齐向东表示，5G 应用发展加速了各行各业的数字化转型，同时也面临着更加复杂的网络安全挑战。当前，我国 5G 应用正处于规模化快速发展的关键阶段，要以“零事故”为目标，护航 5G 融入千行百业，筑牢安全底板。5G 正式商用已经三年，截至 2022 年 6 月，我国 5G 基站数达到 185.4 万个，已部署 5G 行业虚拟专网 6518 个，5G 应用创新案例超过 2 万个。齐向东表示，5G 正成为推动经济社会数字化转型的重要引擎，也面临新的网络安全挑战，主要体现在新设备、新技术、新应用三个方面。在新设备方面，5G 网络接入终端设备种类多数量大，防护“盲点”激增。据 Gartner 预测，到 2030 年，全球物联网设备连接数预计将接近 1000 亿个，其中我国将超过 200 亿个。而管控策略不完善、安全监测不到位、升级维护不及时等安全短板，给 5G 安全防护带来巨大挑战。在新技术方面，新技术的广泛应用引入了新的安全风险。网络功能虚拟化，不仅模糊了传统网络边界，还引入了开源软件的漏洞风险；网络切片相比行业专网更为开放，更容易成为攻击跳板，网络接口也更容易被利用；边缘计算则增大了核心网的攻击面，并增加了数据保护难度。在行业应用方面，各行业安全需求差异大，个性化方案匹配难。随着我国积极推进 5G 融入千行百业，智慧能源、智慧交通、智慧医疗、智慧金融等不同行业应用在环境、业务、资产、运营等层面具有不同的特征，需要从行业视角进行整体规划设计，针对行业的差异化需求进行安全能力的个性化匹配，以有效提高防护能力。齐向东表示，冬奥网络安全保障的结果已证明，网络安全“零事故”是可以实现的目标，奇安信也以“零事故”为目标，梳理 5G 应用的共性网络安全需求，融合形成了统一的安全架构，助力 5G 应用快速发展，护航 5G 融入千行百业。而实现“零事故”目标，需满足“联合作战、精准

防护、深度运营”三大要求。具体来看，首先，可通过全流量检测 + 态势感知实现联合作战：核心网全流量威胁检测将信令面和数据面流量分析相结合，全面监测异常行为，防止终端恶意接入；相比传统网络流量监测，能够对网络安全态势作出更准确的评估，并提供针对性的预防建议；一体化安全态势感知将 CT 侧的信令安全、IT 侧的边缘计算平台安全和 OT 侧的工业应用安全相结合，通过网络行为与业务应用行为的对比分析，能够精准、快速定位威胁。其次，用零信任实现精准防护。零信任是将用户的身份信息、行为操作、终端信息等，和业务访问有机结合起来，构建用户、终端、网络、服务之间统一的信任体系。零信任与 5G 相结合，能够将核心网对设备的认证与行业侧对业务的认证相结合并持续进行信任评估，极大地提高防护精度，确保合适的人、在合适的时间、以合适的方式，访问合适的业务数据。第三，用合规检测实现深度运营。5G 应用在国家整体政策法律要求下，既要符合通信行业的标准规范，又要符合应用行业的标准规范。因此要建立新的合规检测与评价体系，针对 5G 应用场景，梳理识别 5G 网络中的安全资产，分析安全威胁风险，并借助专业工具进行实战化的攻防测试，检验 5G 应用整个系统应对各种类型攻击的实际效果，及时消除隐患，不断提升安全防御能力。

https://www.cet.com.cn/dfpd/jzz/hlj/hlj/3222140.shtml

■ 海莲花组织 (APT32) 针对我国关基单位攻击活动分析

2022 年 5 月，绿盟科技伏影实验室与运营能力中心梅花 K 战队共同于国家某关基单位发现异常外联 IP，通过攻击活动中捕获的攻击流量分析，确认此次攻击活动是由境外 APT 组织 APT32 所发起。

绿盟科技伏影实验室与运营能力中心梅花 K 战队利用主机行为监控技术对攻击者攻击活动进行了全周期监控，并对其攻击活动进行阻断。在监控过程中，观察到攻击者活动持续至 7 月中下旬，时间长达 2 个月。攻击者针对关基单位负责重点课题的研究员发起 APT 定向攻击，瞄准文档类资料进行窃取，以窃取机密资料和重要文件为目标。如攻击者窃取成功，将造成严重损失。

通过流量分析，发现国内某核心制造业厂商也同样遭受该组织攻击，并持续处于活跃状态，经过处置，已成功阻断该组织攻击活动。

https://www.secrss.com/articles/45496

本期编辑：于寅虎

排版设计：赵景平

出　　品：中国电子信息产业集团有限公司第六研究所信息服务部