网信动态周报

第 10 期

2022 年

3月14日-3月19日

5G 半导体 物联网 安全

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

1 5G 行业一周要闻

- 全球首例 5G 端到端多切片并发技术方案完成现网验证
- 沃达丰英国准备在 2023 年关闭 3G 网络
- 中国电信：预计 2022 年底在用 5G 基站超 99 万站
- 中国移动四川公司携手华为建设全国首个 MetaAAU 一网两用 5G 示范区
- 沃达丰与爱立信完成英国首个网络切片试验
- IDC：2026 年 LTE/5G 专网设备收入将达 83 亿美元
- Dell'Oro 报告：2021 年全球电信设备市场收入接近 1000 亿美元 华为保持领先

■ 全球首例 5G 端到端多切片并发技术方案完成现网验证

中科创达与联通研究院泛终端研究中心、广东联通网络产品创新中心密切合作，联合广和通等伙伴共同在广州中国联通 5G 创新实验室完成了联通研究院自研行业终端，及其内置 5G 模组的端到端多切片并发技术方案现网验证。本次现网验证完成了包括注册、URSP 配置更新、PDU 会话建立、切片建立及去激活等典型流程，同时重点验证了基于 APP ID、FQDN、IP 三元组、DNN 的多类型、多并发的切片管理及业务承载功能。

■ 沃达丰英国准备在 2023 年关闭 3G 网络

沃达丰英国（Vodafone UK）正打算关闭其 3G 网络，以便为新技术腾出空间。在沃达丰英国的情况中，它将在 2023 年之前让客户为过渡做准备。

■ 中国电信：预计 2022 年底在用 5G 基站超 99 万站

2021 年，中国电信加快建设智能化综合数字信息基础设施，其中 5G 网络方面，深入推进与中国联通的网络共建共享，截至 2021 年 12 月底，在用 5G 基站数量超过 69 万站，5G 网络覆盖至全国所有市县和部分发达乡镇。同时，全网纯 SA 升级基本完成，建成全球最大

5G SA 共建共享网络。5G 资本开支为 380 亿元，同比下降 3.1%。面向 2022 年，预计年底在用 5G 基站超过 99 万站，资本开支预计 340 亿元。其中，中国电信新建17万5G基站，持续提升5G深度和广度覆盖：3.5GHz基站覆盖城区和高价值室内区域，2.1GHz 基站覆盖其他区域。同时积极推动多运营商异网漫游共建共享。

■ 中国移动四川公司携手华为建设全国首个 MetaAAU 一网两用 5G 示范区

近日，中国移动四川分公司（以下简称四川移动）携手华为在成都市天府新区率先连片部署 MetaAAU 设备，对 MetaAAU 基站设备同时开通 4G 和 5G 网络进行验证，建成全国首个一网两用 5G 示范区，实现了 4G、5G 设备一体化同覆盖的极简网络，为客户提供更加精准的高品质网络服务。

■ 沃达丰与爱立信完成英国首个网络切片试验

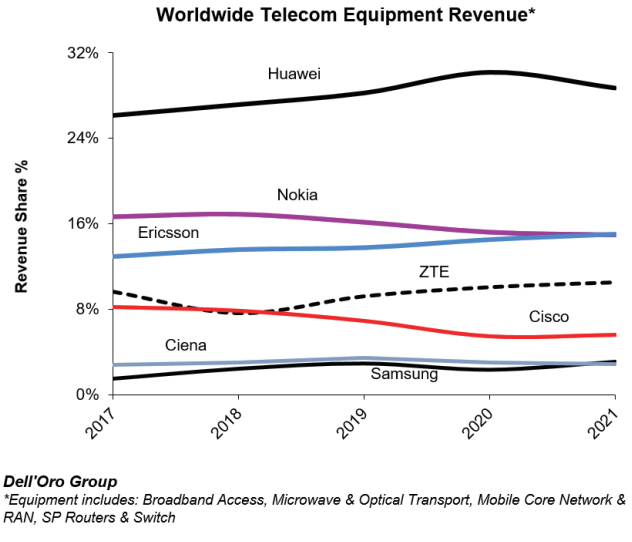
据 MobileWorld Live 报道，沃达丰英国公司与爱立信合作，完成了他们宣称的英国首个独立组网（SA）5G 网络切片试验，并展示了一个 VR 用例。在实验室演示中，他们致力于创建一个按需的 5G 网络切片，使用 RAN 切片功能进行配置，以提供零售店中 VR 用例所需的低延迟和高带宽。创建的网络片保证了 260Mb/s 的下载速度和 12.4 毫秒的延迟，从下订单到创建承载实时网络流量的网络切片的整个过程共需 30 分钟。沃达丰与爱立信宣称，此次试验证明了其“随着客户需求的变化，迅速提供自动化和定制化的连接服务”的能力。

■ IDC：2026 年 LTE/5G 专网设备收入将达 83 亿美元

根据 IDC 的研究，到 2026 年，全球专用 LTE 和 5G 无线基础设施市场的收入有望达到 83 亿美元，而 2021 年这一数字为 17 亿美元。IDC 预测，从 2022 年到 2026 年，市场的五年复合年增长率有望达到 36.7%。尽管全球 LTE/5G 无线基础设施市场在 2021 年有所增长，但研究机构指出，专用 LTE 是主要的收入来源。

■ Dell'Oro 报告：2021 年全球电信设备市场收入接近 1000 亿美元 华为保持领先

市场研究公司 Dell'Oro Group 刚刚发布了 2021 年第四季度全球整体电信设备市场报告。这份报告涵盖包括宽带接入、微波与光传输、移动核心网（MCN）和无线接入网（RAN）、SP 路由器和交换机在内的整个电信设备市场。报告数据显示，尽管去年第四季度市场总收入同比增长放缓至 2%，但这不足以破坏全年发展趋势。初步估算表明，2021 年全球整体电信设备市场增长了 7%，连续第四年实现增长，这主要得益于无线收入的飙升，以及 RAN 和宽带接入细分市场的两位数百分比增长刺激的有线相关设备的健康需求。全球电信设备市场总收入在 2021 年接近 1000 亿美元，自 2017 年来增长了超过 20%。这些报告中的分析表明，在 2020 年至 2021 年期间，领先供应商的全球总体份额保持相对稳定，Top 7 供应商占据了整个市场的 80% 左右。



2 半导体行业一周要闻

- 清华大学集成电路学院团队首次实现亚 1nm 栅极长度晶体管
- 苹果毫米波射频 RF 芯片设计完成
- 中国“小芯片”标准草案即将公示
- 三安集成或以 SAW 滤波器切入三星电子手机供应链
- 联发科计划 2022 年上市其蓝牙芯片子公司
- 传鸿海将与沙特合资建半导体工厂
- 英特尔拟在欧洲投资 890 亿美元构建完整芯片供应链
- 移远通信 LTE-A 车规级模组获全球重要认证
- SEMI：2021 年全球半导体材料市场达 643 亿美元
- 2022 年全球微处理器市场预计将达到 1104 亿美元
- 布局柔性传感器：小米入股汉威科技子公司
- 2021 年安卓智能手机 AP/SoC 市场分析：5G 芯片价格大幅下滑，海思市占率进一步萎缩

■ 清华大学集成电路学院团队首次实现亚 1nm 栅极长度晶体管

近日，清华大学集成电路学院任天令教授团队在小尺寸晶体管研究方面取得重大突破，首次实现了具有亚 1 纳米栅极长度的晶体管，并具有良好的电学性能。据介绍，目前主流工业界晶体管的栅极尺寸在 12nm 以上，日本在 2012 年实现了等效 3nm 的平面无结型硅基晶体管，2016 年美国实现了物理栅长为 1nm 的平面硫化钼晶体管，而清华大学目前实现等效的物理栅长为 0.34nm。

■ 苹果毫米波射频 RF 芯片设计完成

据业内人士爆料，一位从高通跳槽至苹果的内部人士透露，不止 Sub-6GHz，苹果的 mmWave 毫米波射频 RF 芯片也已完成设计，代号 Turaco。今年 1 月，有消息称苹果自研 5G 基带及配套射频芯片完成设计，开始试产及送样。

■ 中国“小芯片”标准草案即将公示

据芯东西报道，国内 chiplet 标准草案现已制订完毕，即将进入征求意见阶段，预计第一季度挂网公示和意见征集，第二季度完成技术验证计划制订，年底前完成技术验证，并完成标准文本的确定，进行初版标准的发布工作，首个版本发布即可用。Chiplet 常被译为芯粒、小芯片，能将采用不同制造商、不同制程工艺的各种功能芯片像搭乐高积木般进行组装，从而实现更高良率、更低成本。

■ 三安集成或以 SAW 滤波器切入三星电子手机供应链

继切入苹果 MiniLED 供应体系后，业界传出，三安集团旗下 RF 元件大厂三安集成，将以 SAW 滤波器切入韩国龙头三星电子手机供应链，先前三安集成已经切入手机系统代工厂富智康体系。

■ 联发科计划 2022 年上市其蓝牙芯片子公司

联发科计划2022年将其蓝牙芯片子公司达发科技（Airoha Technology）上市，以筹集研发资金，并在半导体行业出现历史性的劳动力短缺之际，提高该公司在招聘方面的竞争力。达发作为联发科旗下蓝牙芯片子公司，为索尼、苹果的Beats、JBL和小米提供芯片。

■ 传鸿海将与沙特合资建半导体工厂

外媒爆料称，鸿海或将与沙特阿拉伯政府共同投资90亿美元建造一座半导体工厂，主要生产芯片、电动汽车零组件及显示器等产品。沙特政府正在评估鸿海提出在沙漠科技城NEOM建立一个用于晶圆制造和封装测试的双线半导体代工厂的提议，并表示该项目最早在去年就开始讨论，目前正就鸿海的提议进行调查。

■ 英特尔拟在欧洲投资890亿美元构建完整芯片供应链

英特尔表示，将先期斥资大约190亿美元，在德国新建两座芯片工厂。工厂选址在德国东北部城市马格德堡，预计明年开始施工，2027年开始运营。英特尔上述计划涵盖芯片供应链每个环节，包括研发、制造和封装。除德国外，上述投资将分布在法国、爱尔兰、意大利、波兰和西班牙。

■ 移远通信LTE-A车规级模组获全球重要认证

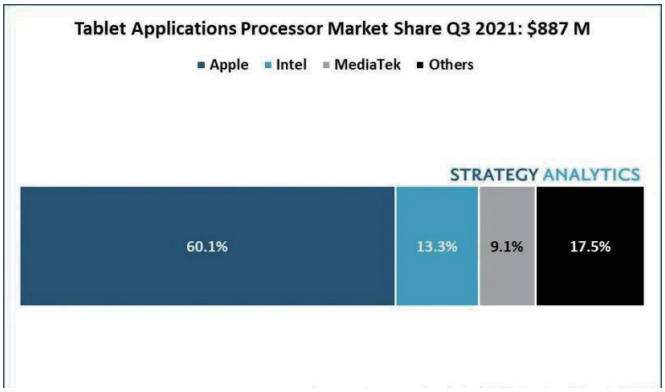
近日，移远通信宣布，其LTE-A车规级模组AG525R-GL已通过全球多个地区的强制性、一致性和运营商认证。该车规级模组基于高通SA415M芯片开发，是移远畅销全球的AG52xR系列型号之一，目前已经进入量产阶段。

■ SEMI：2021年全球半导体材料市场达643亿美元

根据国际半导体产业协会(SEMI)报告数据，2021年全球半导体材料市场收入增长15.9%，达到643亿美元，创下新高。2020年，该项数据是555亿美元。其中，晶圆制造材料和封装材料收入总额分别为404亿美元和239亿美元，同比增长15.5%和16.5%。数据显示，中国大陆2021年半导体材料市场规模为119.3亿美元，同比增21.9%。很显然，这得益于整个半导体产业的高景气。无论是芯片还是晶圆代工产业，在2021年均保持了高速增长势头。

■ 2022年全球微处理器市场预计将达到1104亿美元

IC Insights发表最新的研究报告，分析师认为2021年微处理器（MPU）继2020年增长16%后将再次实现14%的增长，达到1029亿美元。分析师预计，2022年全球微处理器总销售额增长率将达7%，MPU市场再创新高达到1104亿美元，处理器出货量增长6%，达到26亿个。微处理器市场的增长主要是因为随着用户智能手机的更新换代，支持新的5G网络、更强的摄像头和人工智能，例如具有机器学习功能的手机处理器销量增长了31%。IC Insights预测，手机应用处理器AP的销售额在2021年增长至350亿美元，而在2022年的增长率将达到10%，即384亿美元。CPU市场的销售增长在2021年将会有所放缓，预计计算机CPU微处理器的销售额将在2022年增长4%，达到创纪录的505亿美元。



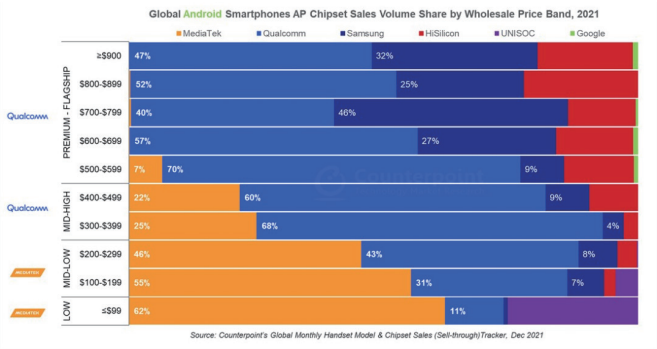
■ 布局柔性传感器：小米入股汉威科技子公司

3月14日，汉威科技公告，控股子公司苏州能斯达电子科技有限公司拟进行增资扩股并引进战略投资者湖北小米长江产业基金。小米长江产业基金以1000万元对公司控股子公司苏州能斯达进行增资，增资后将持有苏州能斯达5.21%的股权。汉威科技公告表示，控股子公司苏州能斯达电子科技有限公司拟进行增资扩股并引进战

略投资者湖北小米长江产业基金。小米长江产业基金以1000万元对公司控股子公司苏州能斯达进行增资，增资公司控股子公司苏州能斯达致力于柔性微纳传感技术的研发和产业化，为柔性传感器在物联网、智能穿戴、医疗健康、消费电子、智能汽车等领域提供完善的人机交互解决方案。

■ 2021年安卓智能手机AP/SoC市场分析：5G芯片价格大幅下滑，海思市占率进一步萎缩

Counterpoint数据显示，2021年全球安卓智能手机AP（应用处理器）/SoC（片上系统）销售额同比增长3.6%，联发科以46%的市占率成为市场第一，高通以35%份额紧随其后。由于对天玑700/800系列芯片组的强劲需求，联发科去年的大部分市场份额增长来自低于299美元批发价的中低端机型。



3 工业互联网行业一周要闻

- 艾利特机器人完成数亿元C1轮融资 达晨财智、尚珹投资联合领投
- 可骑行的机器人山羊诞生 最高可承重100公斤
- 蓝卓完成第二轮融资
- 国内工业互联网标识注册突破千亿大关

■ 艾利特机器人完成数亿元C1轮融资 达晨财智、尚珹投资联合领投

据悉，艾利特机器人成立于2016年，聚焦于平台级协作机器人研发。目前，艾利特主要推出了两个系列产品，一是面向中端和国内客户为主的EC系列，包含了从3kg到20kg负载的协作机器人；二是面向高端和海外客户的CS系列，在运行系统和编程系统等软件方面，机器人关节模组等结构及硬件方面，以及顶层算力库方面进行了全面升级。

■ 可骑行的机器人山羊诞生 最高可承重100公斤

在东京于近日举办的国际机器人展览会上，川崎公司展示了一个可骑行的四足机器人山羊--Bex。该机器人外形模仿的是一种原产于欧亚大陆和非洲部分地区的野山羊。Bex的角会发光，膝盖上有一组轮子，使其在光滑的表面上移动的速度比行走时更快，另外还可以实现让一个成年人骑在它的身上。

■ 蓝卓完成第二轮融资

本轮融资 5 亿元，由富浙资本领投，软银中国等机构跟投，资金将主要用于 supOS 工业操作系统平台的研发与创新、平台生态体系完善及开源开放生态孵化。浙江蓝卓工业互联网信息技术有限公司成立于 2018 年，专注于工业操作系统的研发与产业化，致力于打造中国自主可控的“工业安卓”。

■ 国内工业互联网标识注册突破千亿大关

近日，中国信息通信研究院公布了一个新数据，根据最新统计数据，截至目前，国内工业互联网标识注册量超过 1000 亿，日解析量超过 9000 万次，二级节点数达 180 个，辐射范围包括 27 个省（区、市），34 个行业，接入企业节点超过 9 万家。经过前期的快速发展，我国工业互联网标识解析体系架构实现了从 0 到 1 的突破，北京、广州、上海、武汉、重庆五大国家顶级节点持续稳定运行，南京灾备节点加速建设，整体上初步形成分层授权、“东西南北中”的一体化格局。

4 物联网行业一周要闻

- 武汉大学研发退烧手机壳
- 紫光国微发布超级钥匙解决方案
- 华为发布新一代全屋智能解决方案
- 商汤宣布渐冻症智能看护系统交付使用
- 优刻得发布三大系列 AI 智能边端产品
- 中国电信：天翼视联网已覆盖 31 省，接入终端超 2000 万
- 云米发布一站式全屋智能解决方案“1=N44”
- 2021 年可穿戴手表出货量达 3956 万台，华为、苹果持续领跑
- 三星推出 Smart Monitor M8，发力智慧屏领域

■ 武汉大学研发退烧手机壳

据报道，武汉大学动力与机械学院纳米能源实验室与 OPPO 热实验室联合开发了一款冰肤散热手机保护壳，采用 Glacier Mat 散热新材料，通过水分蒸发来带走手机背板的热量。安装散热手机壳后，手机在高负载场景下使用 1 小时，其表面温度相较于同等场景下的同款裸机低近 2~3℃。

■ 紫光国微发布超级钥匙解决方案

该解决方案可服务于家庭智能门锁，还可应用于有实名管理特殊需求的公租房、流动人口、校园宿舍管理、楼宇门锁门禁等场景。其中，紫光国微主导并完成了整体系统架构设计，同时协同紫光安芯提供智能门锁、门禁、闸机等访问控制设备的分系统解决方案，并协同中广瑞波提供超级钥匙 TSM 云服务平台、客户端 App 或小程序、超级钥匙 SuperKey SIM 卡应用。

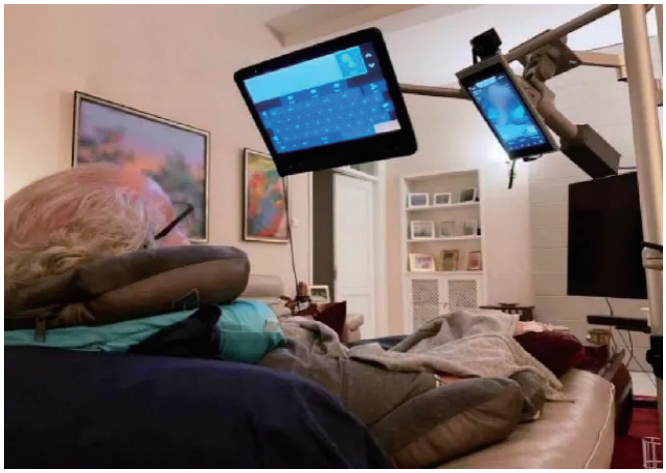
■ 华为发布新一代全屋智能解决方案

近日，在全屋智能及全场景新品春季发布会上，华为推出了新一代全屋智能解决方案。为了能更好的满足用户

的交互体验升级，2022 华为全屋智能解决方案“1+2+N”战略再升级，带来了华为全屋智能主机 SE、全屋互联和全屋中控家族以及全屋十大子系统。在售价方面，80 平的典型户型应用华为全屋智能系统 39999 元起，用户可进入官网预约线下门店体验。

■ 商汤宣布渐冻症智能看护系统交付使用

商汤科技近日宣布，公司自主开发的商汤 AI 渐冻症智能看护系统已正式交付首位患者使用。据介绍，基于计算机视觉技术，该智能看护系统能够敏锐地捕捉被看护人的痛苦表情并报警，在 3 秒内及时通知陪护人员前来处理危急情况，避免被看护人发生生命危险。同时，这套系统在体温、呼吸、心率等体征指标异常时也可发出告警，支持 24 小时无间断工作。

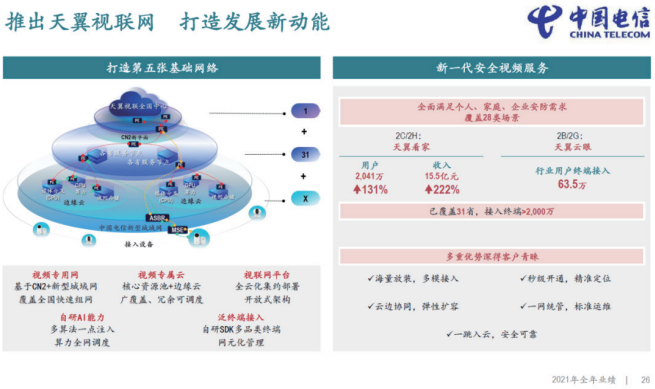


■ 优刻得发布三大系列 AI 智能边端产品

据介绍，其边缘计算 E 系列的主打产品为 UCloud 智能 AI 边缘盒子，安全卫士 G 系列包含人脸识别门禁一体机、AI 视觉芯片模组两款智能边端产品，防疫卫士 Y 系列产品包括智能防疫一体机、智能核验测温手持机。

■ 中国电信：天翼视联网已覆盖 31 省，接入终端超 2000 万

中国电信于 2021 天翼智能生态博览会上发布的第五张基础网 --“天翼视联网”，截至 2021 年底已经覆盖 31 省，接入终端超过 2000 万。天翼视联网致力于打造全球最大的运营商级别的视频回传和处理网络，构建中国电信在移动网、宽带网、物联网、卫星网之外的第五张基础网。中国电信融合云、网、AI 等能力，建设“1+31+X”架构的天翼视联平台，打造覆盖 31 省的标准化视频能力，面向个人和家庭客户推出天翼看家等标准化产品服务；面向政企客户推出标准化产品叠加行业信息化应用的定制解决方案，满足垂直行业的智能安防需求。

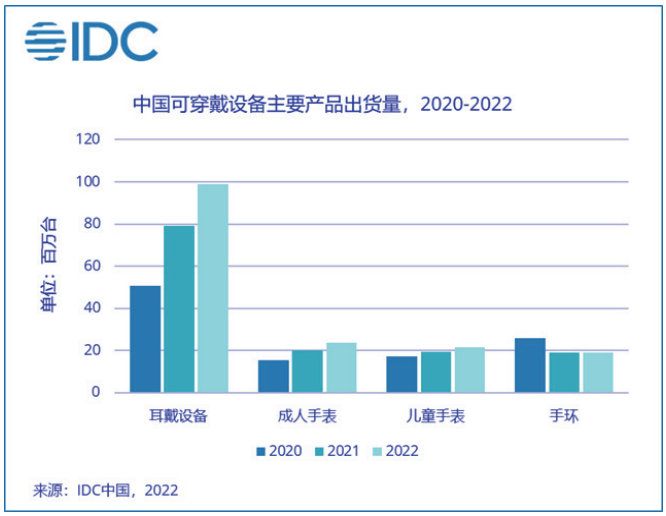


■ 云米发布一站式全屋智能解决方案“1=N44”

在云米科技 2022 春季战略新品发布会上，云米科技发布了全新升级一站式全屋智能解决方案“1=N44”，并推出 30 万元起售、亿元级别墅专享的高端全屋智能套系，旨在打造全屋畅快互联互通的高端家居生活体验，让智能变得真正“有用、好用”。“1=N44”的 1 代表“一站式全屋智能解决方案”，即家是一个整体；N 是指共计 60 多种大类的智能“全家桶”产品阵容，集合了智能家电和智能家居两大产品部门，包括空调、冰箱、洗衣机、烟灶、净水机、扫地机、智能开关、路由器等；44 则是指云米全屋智能解决方案 HomeMap 具有的 4 大能力：无感组网、主动智能、空间感知、自然交互，以及云米为用户提供的包括方案设计、OTA 持续升级智能体验、Plus 会员、增值服务在内的 4 种服务。

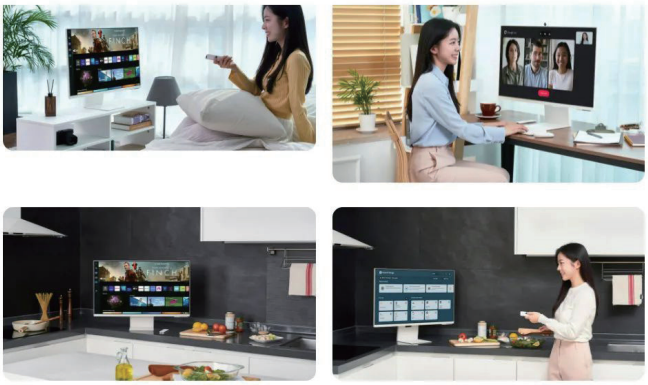
■ 2021 年可穿戴手表出货量达 3956 万台，华为、苹果持续领跑

IDC 近日发布的《中国可穿戴设备市场季度跟踪报告，2021 年第四季度》报告显示，2021 年可穿戴手表市场出货量 3956 万台，同比增长 21.4%。厂商格局出现了较大变化，但整体上华为和 Apple 领跑的局面仍然持续。数据显示，2021 年中国可穿戴市场出货量近 1.4 亿台，同比增长 25.4%。2021 年可穿戴手表市场出货量 3956 万台，同比增长 21.4%。其中，成人手表出货量 2,013 万台，同比增长 31.0%。2021 年儿童手表出货量 1,943 万台，同比增长 12.8%；此外报告指出，2021 年手环市场出货量 1,910 万台，同比下降 26.3%。



■ 三星推出 Smart Monitor M8，发力智慧屏领域

据 SamMobile 报道，三星宣布在韩国推出 SmartMonitor M8，售价 850000 韩元（约合 691 美元），并将于 3 月 15 日在韩国各地线上和线下商店发售。据报道，Smart Monitor M8 是一款 32 英寸 4K 显示器，采用 QLED 显示屏，支持 HDR10+ 视频播放，具有 99% 的 sRGB 色域，同时采用了 Eye Saver 技术。音响方面，它采用 2.2 声道立体声扬声器，并支持 Adaptive Sound+。此外，该显示器的厚度只有 11.3 毫米。这款显示器运行 Tizen OS，可运行音频和视频流媒体服务，配备语音助手 Bixby 和可拆卸的 SlimFit 摄像头，支持 SmartThings IoT Hub 和 Samsung Health。另外，这款显示器还支持蓝牙、Wi-Fi 5、Wireless DeX 和 Apple AirPlay 2，以及视频会议的自动缩放和面部跟踪功能。



5 车联网行业一周要闻

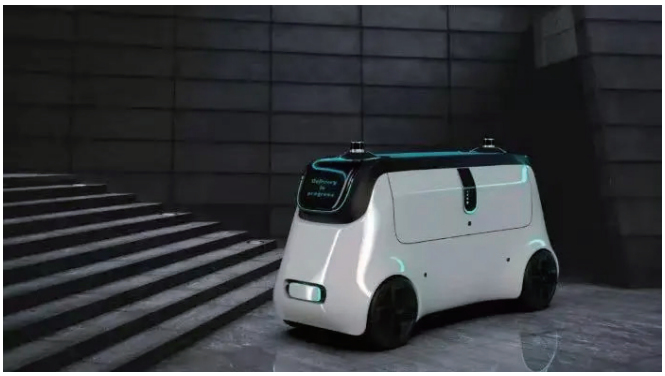
- 华为、宁德时代、长安联手打造的阿维塔 11 实车亮相
- 自动驾驶创企惠尔智能完成 Pre-A 轮融资
- 自游家 NV 将于 3 月 31 日发布并开启预订
- 全球首款自动驾驶水陆两用巴士在日本试运营
- 白犀牛通过首个 L4 级自动驾驶系统国际标准的场景评估测试
- 广汽埃安将适时启动 A 轮融资并择机 IPO
- 美的集团：MCU 出货量达千万颗 2024 年量产汽车芯片

■ 华为、宁德时代、长安联手打造的阿维塔 11 实车亮相

近日，阿维塔 11 出现在了工信部新车申报目录中。在 2021 年 11 月 15 日，阿维塔品牌全球首发，首款情感智能电动汽车阿维塔 11 也同步亮相。阿维塔是长安汽车、华为、宁德时代组成中国队造车，联合推出的高端品牌。其将会整合三家在整车制造、智能汽车解决方案和电池能源的独特优势。

■ 自动驾驶创企惠尔智能完成 Pre-A 轮融资

据介绍，惠尔智能成立于 2018 年，是一家专注于研发自动驾驶的科技公司，最初致力于研发乘用车 L4 级自动驾驶方案，并成功向国内不少高校、科研机构及 Tier1 交付了自动驾驶整车方案，后将 L4 级乘用车自动驾驶技术平移到无人配送车上，瞄准公路级无人车配送的市场。



■ 自游家 NV 将于 3 月 31 日发布并开启预订

新造车企业自游家汽车宣布，公司旗下的智能电动 SUV 自游家 NV 将于 3 月 31 日发布并开启预订。据官方介绍，自游家 NV 定位于高端中大型 5 座电动 SUV，基于 GEMINI 双子动力模块系统打造而成，可全面兼容纯电系统和增程系统。新车自游家预计于今年 9 月交付首批用户。

■ 全球首款自动驾驶水陆两用巴士在日本试运营

2020 年 12 月，日本开始试验全球首款自动驾驶水陆两用巴士，经过一年多试验，这款两用巴士近日在日本长野县八场水库进行了实验性运营，并计划在 2022 年正式投入商业运行。这辆无人驾驶巴士是由埼玉工业大学自动驾驶技术开发中心参与研发，搭载有日本最新研发的

传感器系统、雷达系统、风速自控系统和 5G 信号系统，能够实现路径和航路的自动规划设定、障碍物回避、水下水面自动避航、出入水自动控制。

■ 白犀牛通过首个 L4 级自动驾驶系统国际标准的场景评估测试

白犀牛无人车在第三方检测、检验和认证机构德国莱茵 TUV 的见证下，通过一系列严格的测试验证后，成为大中华区第一家通过 L4 级自动驾驶系统国际标准 ISO22737 场景评估测试的自动驾驶企业。

■ 广汽埃安将适时启动 A 轮融资并择机 IPO

广汽集团全资子公司广汽埃安已完成共计 25.66 亿元融资。本次增资扩股后，广汽集团通过直接或间接共持股广汽埃安 93.45% 股权。广汽方面透露，埃安将适时启动其股份制改造及 A 轮融资，进一步引入战略投资者，未来积极寻求适当时机上市。

■ 美的集团：MCU 出货量达千万颗 2024 年量产汽车芯片

日前，美的集团在互动平台表示，2020 年至 2021 年主要投产 MCU 芯片，并于 2021 年开始量产，全年量产规模约 1000 万颗。2024 年，美的可实现汽车芯片的量产，并首先应用于新能源汽车水泵的控制。

6 科技行业一周要闻

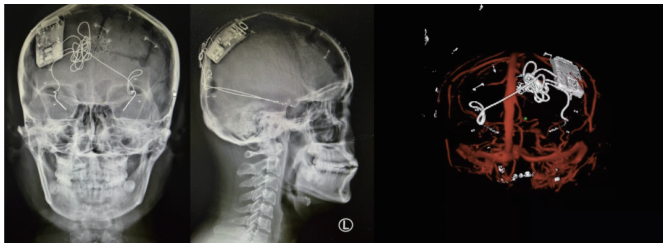
- 我中兴推出鼠标大小的电脑：仅重 55 克 可塞进衣服口袋
- 中国首例“脑机接口”反应性闭环神经刺激系统植入成功
- 骨龄 AI 技术研究新成果公布
- 英国电信与谷歌云合作以增强 AI 能力
- 我国大推力氢氧发动机完成 2022 年首次试车
- 研究人员发明可以让人用衬衫接电话的声学织物
- 中国智能手机在俄销量翻倍
- Counterpoint：2022 年 1 月份全球 5G 手机渗透率达 51%，预计全年出货量超 8 亿部
- SpaceX 星链在 15 国平均下载速度超 100 兆 最高逼近 200 兆

■ 中兴推出鼠标大小的电脑：仅重 55 克 可塞进衣服口袋

近日，中兴通信介绍了旗下一款薄到可以塞进衣服口袋的电脑产品——中兴太极云电脑 W100D，其重量仅 55 克，集轻巧、便捷、高效、极简、易用于一体，简单连接即可访问云端桌面系统。云电脑最大的痛点在于延迟，中兴云电脑号称可在 100Kbps~20Mbps 的带宽范围内自适应控制桌面码，保障用户体验，节约带宽。

■ 中国首例“脑机接口”反应性闭环神经刺激系统植入成功

据介绍，3 月 9 日，首都医科大学宣武医院院长赵国光教授、神经外科单永治教授带领的神经外科立体定向与功能性脑疾病组团队成功为一名难治性癫痫患者施行了闭环反应性神经刺激系统 Epilcure ™注册临床试验植入手术，术后重建显示电极位置精准，脑电信号清晰。闭环反应性神经刺激系统为“脑机接口”在临床领域的重要应用，该技术通过将人工智能芯片植入颅骨，颅内电极植入脑内，昼夜无间断监测脑电节律，一旦预测到即将发生的癫痫，即启动外源性干扰节律，直接阻断致痫灶内的癫痫形成，精准的控制环路的活动。



■ 骨龄 AI 技术研究新成果公布

据介绍，“承影 -05z”由喜高科技独立研发，突破已有算力和模型发展限制，采用 AI 算法技术—喜高”AI-China-05“, 性能优越, 超过了国际其他自动化骨龄系统, 具有准确率高、稳定性强、速度快、自动学习能力强的特点, 为中国儿童生长发育评价提供快速而准确的骨龄。

■ 英国电信与谷歌云合作以增强 AI 能力

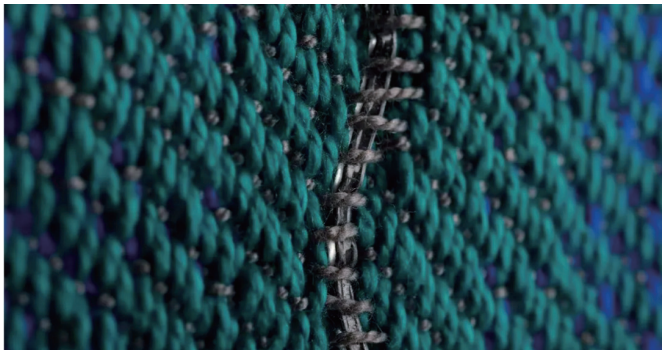
英国电信集团与谷歌云签署了一项为期五年的合作协议，以访问其各种服务，因为该运营商希望在自身的运营和产品范围内加强人工智能和机器学习的使用。根据协议，英国电信将使用谷歌云的基础设施、ML 和 AI 平台、安全系统、数据分析和 API 管理，旨在降低成本并创造新的收入来源。

■ 我国大推力氢氧发动机完成 2022 年首次试车

日前，我国新一代运载火箭长征五号使用的大推力氢氧发动机，完成了今年的首次试车，试车圆满成功。大推力氢氧发动机用于长征五号系列运载火箭的芯一级，是目前我国已投入型号应用的性能最先进的低温液体火箭发动机。后续，大推力氢氧发动机还将在今年通过 20 多次试验任务，进一步验证发动机的可靠性。

■ 研究人员发明可以让人用衬衫接电话的声学织物

据报道, 科学家们正在颠覆裤子、T 恤衫和夹克衫的用途, 他们发明了一种能够检测并产生声音的“声学织物”，由这种材料制成的衣服将有可能通过接收人们皮肤上的振动来持续监测心脏或呼吸频率，还可以提供接听电话的功能，甚至可以作为助听器。

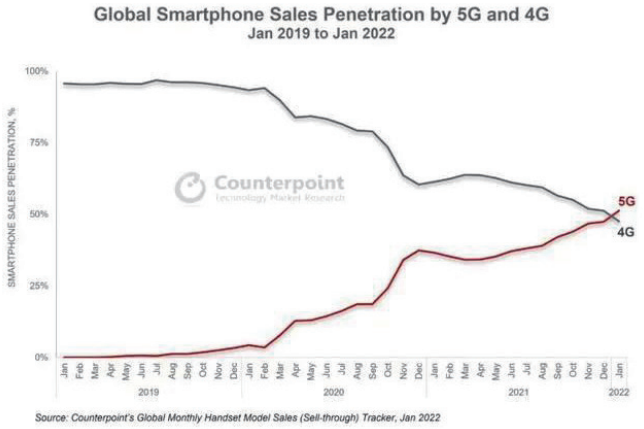


■ 中国智能手机在俄销量翻倍

据俄罗斯卫星通讯社称，俄罗斯移动网络运营商 MTS 发布消息，从 2 月 28 日到 3 月 13 日，中国智能手机的销量比此前两周增长一倍。其中，华为智能手机销量增长 300%，Vivo 和 Oppo 手机增长 200%，中兴手机增长 100%，Realme 增长 80%。

■ Counterpoint：2022 年 1 月份全球 5G 手机渗透率达 51%，预计全年出货量超 8 亿部

市场调研机构 CounterpointResearch 报告显示，2022 年 1 月全球 5G 智能手机的销售渗透率达到 51%，首次超过 4G 智能手机的渗透率。从地区来看，中国、北美和西欧是 5G 手机渗透率增长的最大推动力。其中，中国 1 月份的 5G 普及率全球最高，达到了 84%，中国电信运营商对 5G 的推动以及 OEM 厂商向消费者推出了更具价格优势的 5G 智能手机促成了这一增长。北美和西欧的 5G 智能手机普及率分别达到 73% 和 76%，原因是苹果在北美和西欧占据主导地位，销售份额分别超过 50% 和 30%。苹果于 2020 年 10 月通过 iPhone 12 系列转向 5G 之后，北美和西欧 5G 智能手机的销售渗透率随之提升。



■ SpaceX 星链在 15 国平均下载速度超 100 兆 最高逼近 200 兆

全球宽带网络速度测试网站 Speedest.net 运营商 Ookla 发布最新数据显示，尽管 SpaceX 旗下星链卫星互联网服务刚刚完成测试阶段，但其现在在 15 个国家的平均下载速度超过 100Mbps。

7 安全一周要闻

- 315 晚会重点关注两大信息安全
- 2025 年中国网络安全市场规模预计超 214 亿美元
- 2021 年中国 IT 安全硬件市场规模达 37.7 亿美元，同比增 15.2%
- 国家计算机病毒应急处理中心披露美国安局网络间谍木马！
- 对 Ragnar Locker 勒索软件攻击美国关键基础设施的分析与思考
- 美国 NIST 发布关于保护非机密信息增强安全要求的指南
- NIST 发布制造业工业控制系统环境下信息和系统完整性指南
- 美国通过“改变游戏规则”的网络事件报告立法
- 美国退役网军受雇佣监控全球，“制裁”来了！
- 美国警告俄罗斯利用 MFA 协议进行攻击，PrintNightmare 漏洞
- 美国 NIST 发布关于保护非机密信息增强安全要求的指南

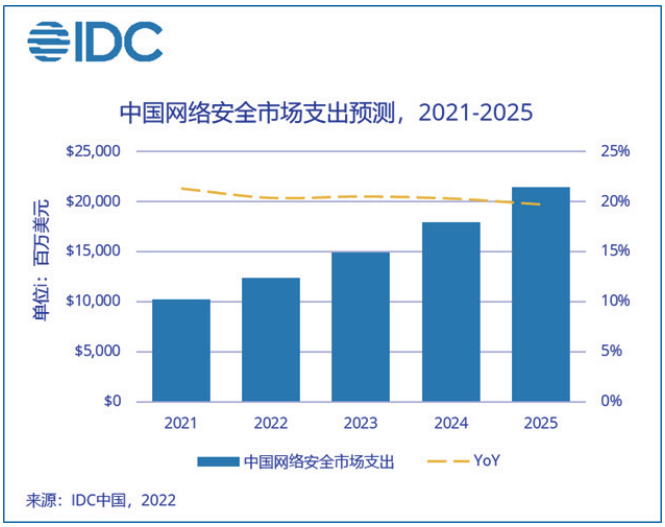
- “放箭”俄罗斯让中国背锅？ 美国才是最大黑客帝国！
- 中国网安企业曝光美方网络攻击特点 ：当年攻击伊朗核设施前，美国曾准备了 4 年多
- 美国安局网络间谍主力装备曝光 控制全球海量互联网设备
- 中国互联网遭境外网络攻击，主要来自美国
- 独家揭秘美国国安局全球网络攻击手法：全球数亿公民隐私和敏感信息犹如“裸奔”
- 微软发布安全更新
- 黑客组织 Lapsus$ 发起投票：根据结果公开公司数据
- 招商证券 APP 因系统故障上热搜：券商 IT 与数字服务能力崛起，更随时面临考验
- 全球最大轮胎制造商之一普利司通遭数据泄露，并被喊话支付赎金
- 研究结果：七分之一的勒索软件勒索攻击会泄露关键的运营技术数据
- “最成功勒索软件团伙”如何运营武器库：Conti 泄露数据分析
- 神误报！微软卫士称 Office 更新是勒索软件

■ 315 晚会重点关注两大信息安全

2022 年的“315 晚会”首设 315 信息安全实验室，并重点关注网络信息安全和儿童互动产品的信息安全。节目中，央视对外曝光了部分免费 WiFi 软件不仅应用内诱导用户下载其他应用程序，且私自大量收集用户信息用以推送广告。比如一款叫“雷达 WiFi”的应用程序，一天之内收集测试手机的位置信息竟然高达 67899 次。另外，还有多家企业抓取网上数据，进行推销电话、骚扰电话、大数据的精准推送等行为，即便用户浏览网站并未留下电话，也能通过手机上对应的 MAC 号（手机识别码）匹配到这个手机。

■ 2025 年中国网络安全市场规模预计超 214 亿美元

IDC 于近日发布了《2022 年 V1 全球网络安全支出指南》。IDC 数据显示，2021 年全球网络安全相关硬件、软件、服务总投资规模有望达到 1,519.5 亿美元，预计在 2025 年增至 2233.4 亿美元，五年复合增长率（CAGR）将达 10.4%。IDC 数据显示，2021 年中国网络安全相关支出有望达到 102.6 亿美元。预计到 2025 年，中国网络安全支出规模将达 214.6 亿美元。在 2021-2025 的五年预测期内，中国网络安全相关支出将以 20.5% 的年复合增长率增长，增速位列全球第一。



■ 2021 年中国 IT 安全硬件市场规模达 37.7 亿美元，同比增 15.2%

IDC 日前正式《2021 年第四季度中国 IT 安全硬件市场跟踪报告》。2021 年第四季度中国 IT 安全硬件市场厂商整体收入约为 15.4 亿美元，规模增长不及预期，同比涨幅仅为 9.25%。综合全年，2021 全年中国 IT 安全硬件市场规模达到 37.7 亿美元，同比增长约 15.2%。

■ 国家计算机病毒应急处理中心披露美国安局网络间谍木马!

近日，国家计算机病毒应急处理中心对名为“NOPEN”的木马工具进行了攻击场景复现和技术分析。该木马工具针对 Unix/Linux 平台，可实现对目标的远程控制。根据“影子经纪人”泄露的 NSA 内部文件，该木马工具为美国国家安全局开发的网络武器。“NOPEN”木马工具是一款功能强大的综合型木马工具，也是美国国家安全局接入技术行动处（TAO）对外攻击窃密所使用的主战网络武器之一。

出处：安全内参

■ 对 Ragnar Locker 勒索软件攻击美国关键基础设施的分析与思考

2022 年 3 月 8 日，美国联邦调查局（FBI）、网络安全和基础设施安全局（CISA）联合发布警告称，Ragnar Locker 勒索软件正大规模入侵美国关键基础设施。截至 2022 年 1 月，联邦调查局已在 10 个受该勒索软件影响的关键基础设施部门确定了至少 52 个实体，包括关键制造业、能源、金融服务、政府和信息技术部门的实体。

出处：安全内参

■ 美国 NIST 发布关于保护非机密信息增强安全要求的指南

美国 NIST 发布了关于保护非机密信息的指南 -(SP)800-172A 美国国家标准与技术研究院 3 月 15 日发布了特别出版物 (SP) 800-172A，题为“评估受控非机密信息的增强安全要求”的程序，可以针对自我、第三方或政府赞助的评估进行定制。美国 NIST IT 实验室开发了这些程序，以便处理政府受控非机密信息 (CUI) 的机构和供应商，可以衡量他们实施 SP 800-172 中引入的保护措施的进度。未经适当机构（如管理和预算办公室）批准，该指南仍不适用于国家安全系统，并且对行业而言是可选择的。SP 800-172 解释了如何确保与高价值资产或关键程序相关联的 CUI 的机密性、完整性和可用性。SP 800-172A 包括如下内容：识别安全和风险管理计划中的差距；发现信息系统及其环境中的漏洞；优先考虑风险缓解；确认漏洞已得到解决；支持持续监控；提供信息安全态势感知。

出处：路云天网络安全研究院

■ NIST 发布制造业工业控制系统环境下信息和系统完整性指南

当地时间 3 月 16 日，美国国家标准与技术研究所 (NIST) 的国家网络安全卓越中心 (NCCoE) 与 NIST 的工程实验室 (EL) 和网络安全技术提供商合作推出了一份文件，以解决制造业面临的网络安全挑战。该文档提供了以数据为驱动的见解，并基于对几个基本制造系统测试平台的实验室测试分析。NIST 联合 MITRE 以及 Microsoft、Dispel、Forescout、Dragos、OSIsoft、TDi Technologies、GreenTec、Tenable 和 VMware 共同合作，制定了题为《NIST 特别出版物 (SP) 1800-10，保护工业控制系统环境中的信息和系统完整性》的指南。该文件就制造商如何加强运营技术 (OT) 系统以降低 ICS 完整性风险并保护这些系统处理的数据提供经过审查的信息和指导。

出处：网空闲话

■ 美国通过“改变游戏规则”的网络事件报告立法

拜登总统于本周签署“改变游戏规则”的立法，要求关

键基础设施实体和联邦机构必须在 72 小时内向网络安全和基础设施安全局（CISA）报告重大网络事件，并在 24 小时内向 CISA 报告勒索软件攻击。美国众议院通过了 2022 年关键基础设施网络事件报告法案的关键条款，该法案要求关键基础设施运营部门在遭到黑客攻击或向威胁行为者支付赎金时向政府发出警报。这是众议院周三通过的 1.5 万亿美元综合支出法案的一部分，该法案为联邦政府提供了今年剩余时间的资金。该法案中包含的事件报告条款是更广泛的加强美国网络安全法案的一部分, 去年未能成为法律, 但于 3 月 1 日在参议院一致通过。拜登总统于本周签署。该立法是在勒索软件攻击和其他关键基础设施组织面临的网络威胁激增的情况下起草的，而当前的俄罗斯 - 乌克兰冲突加剧了这一威胁。除了阻止组织进行勒索软件付款外，这些措施还旨在为网络攻击和威胁参与者计划提供更多情报。反过来，这将有助于司法部 (DoJ) 和 FBI 等联邦机构之间的信息共享，帮助确保有一种标准化的方法来处理关键基础设施网络攻击。新的报告要求将适用于属于 CISA 定义的 16 个美国关键基础设施部门的组织。这些公司必须报告“重大”网络事件，例如对操作系统或流程的安全性和弹性造成危险或扰乱商业或工业运营的事件。

出处：天极智库

■ 美国退役网军受雇佣监控全球，“制裁”来了！

美国颁布一项新法，禁止国家间谍人员在离职后立即为外国政府工作。本周二（3 月 15 日），此法案由拜登总统正式签署为法律。作为 1.5 万亿美元支出法案的一部分，这项新法对掌握间谍活动与国家安全机密的情报官员做出限制，禁止其在离职后的 30 个月内为其他国家提供雇佣服务。一位国会助理表示，这项立法由民主党众议员 Joaquin Castro 提出，希望解决 2019 年路透社一份调查报告中提出的问题。在长达一年的系列调查中，路透社发现前国家安全局黑客曾帮助阿联酋, 监视记者、政治异见者及多位美国公民。阿联酋的这次间谍行动名为“乌鸦计划”（Project Raven），曾入侵了目标人物的脸书与谷歌账户，以及数千部苹果 iPhone 手机。根据人权组织的跟进，这些活动人士随后被捕并遭受酷刑折磨。

出处：互联网安全内参

■ 美国警告俄罗斯利用 MFA 协议进行攻击，PrintNightmare 漏洞

美国网络安全和基础设施安全局 (CISA) 和 FBI 周二警告组织，俄罗斯国家支持的威胁参与者通过利用默认的多因素身份验证 (MFA) 协议和称为 PrintNightmare 的 Windows 漏洞获得了对网络和系统的访问权限。根据这些机构的说法，这个未具名的威胁组织早在 2021 年 5 月就针对一个非政府组织，利用设置为默认 MFA 协议的错误配置帐户来访问受害者的网络。攻击者随后利用 PrintNightmare 漏洞 (CVE-2021-34527) 以提升的权限执行任意代码。该漏洞已被各种威胁行为者利用，第一次攻击显然是在微软于 2021 年夏天设法发布补丁之前开始的。在攻击消息出现后不久，CISA 指示所有联邦机构立即采取行动解决安全问题缺陷。在 CISA 和 FBI 的最新公告中描述的攻击中，攻击者主要滥用了已存在于受感染系统上的合法 Windows 实用程序。黑客的目标显然是从云存储和电子邮件帐户中获取文件。

出　处：https://www.securityweek.com/us-warns-about-russian-attacks-exploiting-mfa-protocols-printnightmare-flaw

■ 美国 NIST 发布关于保护非机密信息增强安全要求的指南

美国国家标准与技术研究院 3 月 15 日发布了特别出版物 (SP) 800-172A，题为“评估受控非机密信息的增强安全要求”的程序，可以针对自我、第三方或政府赞助的评估进行定制。美国 NIST IT 实验室开发了这些程序，以便处理政府受控非机密信息 (CUI) 的机构和供应商，可

以衡量他们实施 SP 800-172 中引入的保护措施的进度。未经适当机构（如管理和预算办公室）批准，该指南仍不适用于国家安全系统，并且对行业而言是可选择的。SP 800-172 解释了如何确保与高价值资产或关键程序相关联的 CUI 的机密性、完整性和可用性。

出处：安全内参

■“放箭”俄罗斯让中国背锅？ 美国才是最大黑客帝国！

俄乌冲突全面爆发后，美国曾多次宣称不会派兵对俄作战。但战争不止于兵戎相见，在互联网领域，美国已经直接或间接地通过黑客组织对俄罗斯发起了多轮攻击，并试图将这些行为嫁祸给中国，以此挑拨中俄关系。据国家互联网应急中心公布的消息，2 月下旬以来，陆续有境外组织攻击并控制我国境内计算机，进而对俄罗斯和白俄罗斯等国家的目标展开网络攻击。

出处：央视新闻客户端

■ 中国网安企业曝光美方网络攻击特点：当年攻击伊朗核设施前，美国曾准备了 4 年多

14 日，国家计算机病毒应急处理中心曝光了美国对外攻击窃密所使用的主战网络武“NOPEN”。持续多年跟踪分析全球 APT（高级持续性威胁）攻击活动的安天科技集团 15 日接受《环球时报》记者采访时进一步曝光了美国网络攻击活动的十大作业特点，披露美方将网络空间仅视为达成窃密的通道之一，美方采用人力、电磁、网空作业三结合的方式，达到其最优攻击效果，面对美方攻击能力，没有安全的系统。美国国家安全局（NSA）打造了体系化的网络攻击平台和制式化的攻击装备库，美国国家安全局下的特别行动办公室（TAO）是这些攻击装备的主要使用者，该办公室下设 5 个部门，包括高级网络技术部门 (ANT)、数据网络技术部门 (DNT) 等。安天科技集团副总工程师李柏松对《环球时报》表示，其中 ANT 部门拥有不少于 48 种网络攻击装备，“ANT 攻击装备家族是美方在 2008 年前后陆续批量列装的攻击装备体系，基本覆盖了主流的桌面主机、服务器、网络设备、网络安全设备、移动通讯设备等。装备形态包括恶意代码载荷、计算机外设、信号通讯设备等。这些装备可以组合使用，以达成复杂攻击作业目标。其中，软件装备主要用于向各类 IT 设备系统中植入持久化后门，其目的以长期驻留潜伏、窃取信息为主；硬件装备有的伪装成计算机外设，有的以独立的硬件设备形态出现，用以进行恶意代码注入、建立第二控制和信息回传信道等。”另外一个部门 DNT 的攻击装备则包括 Fuzzbunch 漏洞攻击平台和 DanderSpritz 远控平台，“这些攻击装备涉及大量系统级 0day 漏洞利用工具和先进的后门程序，体现了美方的超级 0day 漏洞储备能力和攻击技术水平。”李柏松表示，“美方在网络攻击装备的上的优势，源自于其试图覆盖所有主流 IT 场景的作业目标，多年持续性巨量的资金投入，并获得美主要 IT 企业的深度信息共享支持。”根据对美方相关武器和攻击行动的分析，安天总结出美方网络攻击作业的十大特点，就其中一些特点，李柏松进行了具体阐述。首先，进行全面的前期侦查与信息搜集。例如在 2010 年 7 月“震网”(Stuxnet) 蠕虫攻击事件中（Stuxnet 是一个面向工业系统进行攻击的病毒，采用构造阀门超压和改变转速方式破坏铀离心装置系统，是世界上首个网络“超级破坏性武器”，据称造成了超过 2/3 的伊朗离心机损坏，后续还扩散感染了全球超过 45000 个网络端点），美方经历了超过 4 年的准备过程，在攻击伊朗核设施之前，美方已经完全渗透了伊朗的基础工业机构，包括设备生产商、供应商、软件开发商等，完整研究与模拟了伊朗核工业体系，知己知彼后才实施最后攻击。其次，超强的边界突防能力，美方针对网络防火墙、路由器、交换机、VPN 等网络设备 0day 漏洞储备丰富，能隐蔽打入控制边界和网络设备，进行流量转发，并将此作为持续攻击内网目标的中继站。（例如在对中东最大 SWIFT 服务提供商 EastNets 攻击中，美方就先后入侵了外层的 VPN 防火墙和内层企业级防火墙，并在防火墙上安装了

木马。）第三，美方攻击手段已经实现人力、电磁、网空作业三结合，美方将网络空间仅视为达成窃密的通道之一，组合人力手段和电磁手段达到最优攻击效果。例如：代号为水蝮蛇 I 号的设备，就融合了基于 USB 接口的木马注入和数据无线回传机制，根据资料，最大通讯距离可达 8 英里。第四，超强的突破物理隔离网络能力。美方基于物流链劫持、人工带入等方式，借助外设和辅助信号装置，实现建立桥头堡、构建第二电磁信道等方式，突破物理隔离网络。例如在震网攻击中，根据相关信息，由荷兰情报机构人员进入到现场，将带有震网病毒的 USB 设备接入到隔离内网发起攻击。第五，恶意代码载荷基本覆盖所有操作系统平台。在已曝光的美方攻击行动中，已发现各类操作系统平台样本，如 Windows、Linux、Solaris、Android、OSX、iOS 等。可以说面对美方攻击能力，没有安全的系统。第六，广泛采用无文件实体技术，采用直接内存加载执行或建立隐藏磁盘存储空间等方式隐蔽样本，同时通过固件等方式实现更隐蔽的持久化。例如，DanderSprit 木马框架中就包括写入硬盘固件的组件，在攻击过程中，针对符合预设条件的主机，将木马写入到硬盘固件中。即使用户重新安装系统，木马依然能重新加载。李柏松表示，网络安全防护工作必须正视威胁、直面对手，要充分认识到网络安全所面临风险挑战的高度严峻性，深入贯彻总体国家安全观，以捍卫国家主权、安全和发展利益的高度开展网络安全防御工作。

出处：环球时报

■ 美国安局网络间谍主力装备曝光 控制全球海量互联网设备

美国国家安全局（NSA）组织针对全球数亿公民及行业龙头企业长达十余年的网络攻击前不久被曝光后，NSA 网络攻击武器库中的又一种主力装备露出马脚。国家计算机病毒应急处理中心 14 日正式发布 NSA 专用“NOPEN”远程木马技术分析报告，将美国情治部门的网络间谍手段揭露在世人面前。相关网络安全专家对《环球时报》记者表示，“NOPEN”远程木马一旦被植入受害者计算机，就会成为“潜伏者”，随时向攻击者敞开“金库大门”，各种机密数据、敏感信息“一览无余”。有证据显示，该款木马已经控制全球各地海量的互联网设备，窃取了规模庞大的用户隐私数据。

出处：中国青年网

■ 中国互联网遭境外网络攻击，主要来自美国

国家互联网应急中心监测发现，2 月下旬以来，我国互联网持续遭受境外网络攻击，境外组织通过攻击控制我境内计算机，进而对俄罗斯、乌克兰、白俄罗斯进行网络攻击。经分析，这些攻击地址主要来自美国，仅来自纽约州的攻击地址就有 10 余个，攻击流量峰值达 36Gbps，87% 的攻击目标是俄罗斯，也有少量攻击地址来自德国、荷兰等国家。

出处：新华社

■ 独家揭秘美国国安局全球网络攻击手法：全球数亿公民隐私和敏感信息犹如“裸奔”

《环球时报》记者近日独家从 360 公司获悉，2008 年开始，360 云端安全大脑整合海量安全大数据，独立捕获大量高级复杂的攻击程序，通过长期的分析与跟踪并实地从多个受害单位取证，结合关联全球威胁情报，以及对斯诺登事件、“影子经纪人”黑客组织的持续追踪，确认了这些针对系列行业龙头企业长达十余年的攻击属于美国国家安全局（NSA）组织。《环球时报》记者了解到，除严重威胁电力、水利、交通、能源等关键基础设施外，NSA 还将通信行业视为重点攻击目标，长期“偷窥”及收集关于通信行业存储的大量个人信息及行业关键数据，导致大量网民的公民身份、财产、家庭住址、甚至通话录音等隐私数据面临着恶意采集、非法滥用、跨境流出的严重威胁。在 NSA 组织的监视下，全球数亿公民隐私和敏感信息无处藏身犹如“裸奔”。

出处：环球时报

■ 微软发布安全更新

微软周二发布了另一个相对较轻的安全更新，披露了 71 个漏洞，包括对 Azure 和 Office 产品套件中问题的修复。三月份的补丁星期二只包括两个关键漏洞，这是值得注意的，因为在二月份的安全更新中没有任何关键问题。这一轮漏洞是 Xbox 有史以来第一次安全更新。游戏主机容易受到特权提升攻击，这似乎是周二补丁中包含的第一个 Xbox 特定的安全问题。

出　处：https://blog.talosintelligence.com/2022/03/talos-threat-source-newsletter-march-10.html

■ 黑客组织 Lapsus$ 发起投票：根据结果公开公司数据

在攻破 NVIDIA 之后，嚣张的黑客组织 Lapsus$ 近日在 Telegram 上发出投票帖，通过投票结果来决定接下来公开哪家公司的数据。在投票选项中包括运营商 Vodafone 的源代码、Impresa 的源代码和数据库、MercadoLibre 和 MercadoPago 的数据库。投票将于 3 月 13 日结束。

出　处：https://www.cnbeta.com/articles/tech/1245685.htm

■ 招商证券 APP 因系统故障上热搜：券商 IT 与数字服务能力崛起，更随时面临考验

恰逢深圳因疫情按下“暂停键”，招商证券 APP 因系统故障也登上了热搜榜。事实上，近一两年券商 APP 宕机事件出现并不罕见，每次宕机事件出现，都会给同行敲一敲警钟。昨日午间收盘后，招商证券已正式回应称，问题是出在“成交回报处理延迟”，且经过加紧修复后，问题已有所缓解，系统其他功能正常。不过截至发稿前，“招商证券崩了”的微博话题仍然破了 2700 万阅读量。

出处：https://www.secrss.com/articles/40258

■ 全球最大轮胎制造商之一普利司通遭数据泄露，并被喊话支付赎金

近日，LockBit 勒索软件团伙声称已经破坏了最大的轮胎制造商之一普利司通美洲公司的网络，并窃取了该公司的数据。普利司通美洲企业家族在美洲拥有 50 多个生产设施和 55,000 名员工。如果公司不支付赎金，Lockbit 计划在 2022 年 3 月 15 日 23:59 之前释放被盗数据。NewsChannel5 发布的普利司通的完整声明：“普利司通美洲公司目前正在调查一起潜在的信息安全事件。自 2 月 27 日凌晨得知可能发生的事件以来，我们已展开全面调查，以迅速收集事实，同时努力确保我们的 IT 系统的安全性。出于谨慎考虑，我们将拉丁美洲和北美的许多制造和翻新设施与我们的网络断开连接，以遏制和防止任何潜在影响。在我们从这次调查中了解更多信息之前，我们无法确定任何潜在事件的范围或性质，但我们将继续努力解决任何可能影响我们的运营、我们的数据、我们的团队成员和我们的客户的潜在问题。”

链　接：https://mp.weixin.qq.com/s/HZZos9tXt1fBaQMsu3X0Og

■ 研究结果：七分之一的勒索软件勒索攻击会泄露关键的运营技术数据

2021 年勒索软件和多方面勒索的增加导致了运营技术的惊人风险。Mandiant Threat Intelligence 的一项新研究显示，在勒索软件勒索网站上发布的工业组织泄漏的信息中，每七分之一可能会暴露敏感的 OT 文档。在这项研究中，Mandiant 观察到被盗的敏感文档，包括网络和工程图、操作面板图像、第三方服务信息等。利用 OT 环境的敏感细节，攻击者可以更容易地以这些系统和网络为目标进行重复攻击。

出　处：https://www.mandiant.com/resources/research-findings-1-7-ransomware-extortion-attacks-leak-critical-operational-technology

■ “最成功勒索软件团伙”如何运营武器库：Conti 泄露数据分析

勒索软件攻击初期，攻击者的勒索方式主要是对企业的数据进行加密，然后要求对方支付赎金换取解密密钥。但自 2020 年以来，勒索软件攻击团伙开始执行一种被称为“双重勒索”（double extortion）的新战术。Conti 是最早使用“双重勒索”的网络攻击团伙。他们会要求受害公司支付双份费用。一份用来赎取解开被加密系统的数字密钥；另一份是所谓的“封口费”，即保证公司被窃取的数据会被销毁，不会被公开或出售。Conti 通常会给受害者一个暗网链接，打开后可以看到一个计时器画面，受害者如果在计时器归零前没能满足赎金要求，其失窃或被加密的内部数据就将自动向外界发布。“我们正在等待你们在 2 月 5 日前支付上述金额。我们会信守承诺。不过如果到期没能看到钱，我们将会上传这些数据。”这是 Conti 团伙发给受害公司的典型勒索信息。对 Conti 团伙来说，“双重勒索”的好处显而易见——即使受害者对本公司解开并恢复被团伙加密的系统信心十足，但也不得不考虑支付一笔“封口费”，确保本公司数据不外泄、形象不受损。

出处：安全内参

■ 神误报！微软卫士称 Office 更新是勒索软件

3 月 16 日，微软卫士终端版（Microsoft Defender for Endpoint）的一波误报令 Windows 系统管理员们大惊失色。在对系统进行勒索软件扫描时，Office 更新居然被标记为恶意活动。根据 Windows 系统管理员们的上报来看，几小时内这一问题已经遍地开花，引得“勒索软件警报此起彼伏”。随着报告数量的激增，微软确认称，这次 Office 更新由于误报而被错误标记成了勒索软件活动。微软还称，工程师们已经更新了云端逻辑，消除了原有误报，并避免未来再出现类似的警报。微软在收到用户报告后表示，“自 3 月 16 日上午开始，客户可能经历一系列检测误报。这些检测旨在识别文件系统内的勒索软件活动。管理员们看到的误报标题为「在文件系统中检测到勒索软件活动」，触发警报的是 OfficeSvcMgr.exe。”“我们在调查中发现，检测勒索软件警报服务组件新近部署了一项更新，正是这项更新引入了代码问题，导致可能在没有问题时触发警报。我们已经发布代码更新纠正了问题，并确保后续不会出现新的警报提醒。我们也重新处理了积压警报，希望彻底消除此次意外造成的影响。”云端逻辑更新之后，勒索软件活动误报确实不再出现。而且无需管理员干预，所有误报记录将会自动从门户中消除。

出处：互联网安全内参

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