网信动态周报

第 13 期

2022 年

5G 半导体 物联网 安全

4月4日-4月8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

1 5G 行业一周要闻

- 美国运营商 T-Mobile 已开始关闭 3G CDMA 网络
- 英特尔与洛克希德·马丁公司联手推进基于 5G 的军用通信系统
- 中国电信启动 2022 年自研 5G 扩展型小基站集采
- 德国电信已部署 1700 个 SA 5G 站点
- O-RAN 联盟计划今年在 ETSI 通过首批标准
- 北京联通携手华为完成 5G 室内定位能力验证
- Dell'Oro 报告：2021 年全球电信资本支出同比增长 9% 2023 年后将逐渐放缓
- 运营商沃达丰将在科隆路灯柱中集成 5G 小基站：可覆盖 400m 内用户
- 软银将筹资 2.83 亿美元用于加速 5G 网络部署

■ 美国运营商 T-Mobile 已开始关闭 3G CDMA 网络

据报道，T-Mobile 将在 60 天内迁移一些地区的客户，以确保其得到支持，3G CDMA 网络将在不晚于 5 月 31 日完全关闭。此外，T-Mobile 还计划在今年 7 月 1 日前结束自己的 3G UMTS 网络。

■ 英特尔与洛克希德·马丁公司联手推进基于 5G 的军用通信系统

据悉，英特尔的 5G 解决方案将被整合到洛克希德·马丁公司的 5G.MIL 混合基站中，该基站作为一个多网络网关，用于军事人员与当前和新兴平台（包括卫星、飞机、船舶和地面车辆）之间的持续的通信。

■ 中国电信启动 2022 年自研 5G 扩展型小基站集采

近日，中国电信发布 2022 年自研 5G 扩展型小基站集采公告，主要采购全国 31 省市自研 5G 扩展型小基站，中国电信股份有限公司广东研究院为单一来源采购供应商，单一来源采购原因是该研究院产品“需要采用不可替代

的专利或者专有技术”，依据《中华人民共和国招标投标法实施条例》的规定，属于“需要采用不可替代的专利或者专有技术”的情形，需向中国电信股份有限公司广东研究院进行采购。

■ 德国电信已部署 1700 个 SA5G 站点

德国电信近日表示，已在其 SA 5G 足迹中增添了 350 个新站点，使站点总数增加到 1700 个，目前这项技术已在 200 多个城市和地区可供使用。据悉，德国电信移动网络中约有 6.4 万个天线支持 5G 服务，同时该运营商在 2.1GHz 频段部署了动态频谱共享技术，以实现与 4G 服务共享频谱。

■ O-RAN 联盟计划今年在 ETSI 通过首批标准

据外媒报道，AT&T Labs MTS- 网络分析和自动化主管 Paul Smith 表示，O-RAN 联盟计划今年在 ETSI 标准组织通过其首批标准，从而使其标准更加正式。

■ 北京联通携手华为完成 5G 室内定位能力验证

近日，北京联通）联合华为在某半导体制造行业完成 5G 室内定位网络能力验证，并完成全国首个半导体行业工作终端应用试点，实现 2~3 米 @90% 定位精度。该功能可有效满足对工作人员快捷调度和统一指挥的需求，实现工厂内 17000 ㎡定位开通与精度测试优化。

■ Dell'Oro 报告：2021 年全球电信资本支出同比增长 9% 2023 年后将逐渐放缓

来自市场研究公司 Dell'Oro Group 的最新报告显示，初步估算表明，2021 年全球电信市场资本支出（包括无线和有线电信投资总和）按名义美元计算同比增长 9%，并有望在 2022 年增长 3%，然后在 2023 年和 2024 年逐渐下降，这证实了该公司此前传达的电信设备市场（宽带接入、微波传输与移动回传、光传输、移动核心网、无线接入网、服务提供商路由器和交换机）的积极发展势头和增长预测。

■ 运营商沃达丰将在科隆路灯柱中集成 5G 小基站：可覆盖 400m 内用户

据 Computer Base 报道，在 5G + 的品牌下，沃达丰已经开始在德国大规模推动 5G 独立部署（SA）。为了扩大规模，该网络运营商还依靠所谓的 Small Cells，例如现在首次在科隆使用的隐藏在路灯中的小基站。到 2025 年，5G 独立部署和光纤将在整个科隆普及。该网络运营商声称在德国提供了第一个独立的 5GSmall Cells。在科隆的 Heumarkt 和 Domplatte，有两个街道上的路灯，在大约六米高的地方安置了紧凑的 5G 天线，这些天线在 3.5GHz 的 n78 频段上发射信号，覆盖范围可达 400 米。沃达丰提到，Small Cells 的速度高达 1 Gbit / s。这意味着小基站将丝毫不逊于大基站，至少在峰值速度方面是如此。

■ 软银将筹资 2.83 亿美元用于加速 5G 网络部署

日本软银公司详细说明了一项借款 350 亿日元（C114 注: 约合 2.83 亿美元）用于在其本土市场建设 5G 基站的计划，它声称这些基础设施将有助于政府制定的社会倡议。其利用的名为“社会贷款（SocialLoan）”的工具将由多家投资银行提供，这笔款项将在 2031 年 1 月底前偿还。软银指出，这笔现金将用于加速其 5G 网络的部署，并以此来解决日本国内的一系列社会问题。

2 半导体行业一周要闻

- 俄罗斯计划投资 5100 万研发全新 EUV 光刻机
- 俄罗斯搜索巨头遇断供危机 服务器芯片将在 18 个月内耗尽
- 天数智芯发布国内首款通用 GPU
- 国产芯片厂商芯原股份首次加入 UCIe 封装技术联盟
- 华为芯片堆叠封装专利公开：降低硅通孔技术成本 用堆叠换性能
- 台积电将成为 2022 年英伟达 GPU 的独家合同供应商
- AMD 宣布作价 121 亿元收购 DPU 芯片厂商 Pensando
- 英特尔第一款“矿卡”细节官宣
- 英特尔宣布暂停俄罗斯业务
- 消息称 OPPO 首款自研 AP 芯片 2023 年量产，2024 年推出手机 SoC
- SIA：2 月全球半导体销售额同比增长 32.4% 中国市场继续领跑
- 机构：全球半导体供应依旧短缺，芯片交付时间延长至 26.6 周
- 电子业砍单潮蔓延至 PC 领域，2022 年上半年出货量将减少 8.5%
- 世界级超低功耗 10nA HK32L 家族已批量供货

■ 俄罗斯计划投资 5100 万研发全新 EUV 光刻机

据俄媒报道，俄罗斯莫斯科电子技术学院 (MIET) 承接了贸工部开发制造芯片光刻机的项目，首期投资 6.7 亿卢布资金（约合 5100 万元人民币）。该光刻机号称要达到 EUV 级别，但技术原理将是基于同步加速器和 / 或等离子体源”的无掩模 X 射线光刻机。据悉，X 射线光刻机使用的是 X 射线，因此光刻分辨率要更高，且 X 射线光刻机不需要光掩模版就可以直写光刻。因此，俄媒甚至称这将是当前全球最先进的 X 射线光刻机，或许比 ASML 的 EUV 光刻机性能更先进。

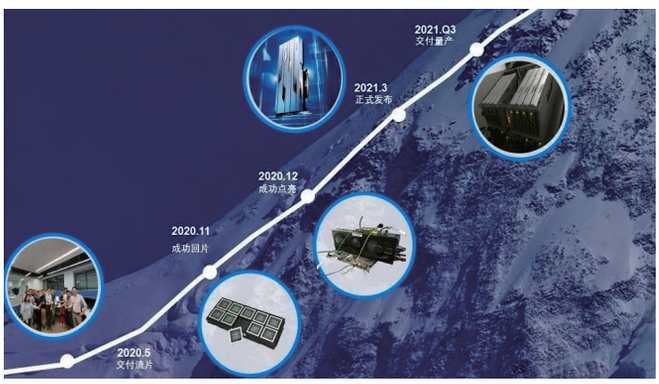
■ 俄罗斯搜索巨头遇断供危机 服务器芯片将在 18 个月内耗尽

据悉，Yandex 是俄罗斯用户最多的互联网公司，同时也是全球前十大搜索引擎公司之一。两名知情人士匿名称，由于进口限制，在 12-18 个月内，Yandex NV 的服务器用的半导体将耗尽，这些服务器能为 Yandex 的业务提供动力。此外，本次制裁主要针对军民两用技术，对 Yandex 自动驾驶汽车部门的打击最严重。

■ 天数智芯发布国内首款通用 GPU

日前，天数智芯发布了国内首款通用 GPU——天垓 100 芯片及天垓 100 加速卡，实现了国内通用 GPU 从 0 到 1 的突破。天数智芯强调，天垓 100 是目前中国唯一量产的通用 GPU 产品。此外，天垓 100 还广泛支持传统机器学习、数学运算、加解密及数字信号处理等领域，也

是唯一一家已适配 X86、ARM、MIPS 等各种类型 CPU 架构的通用 GPU 产品。

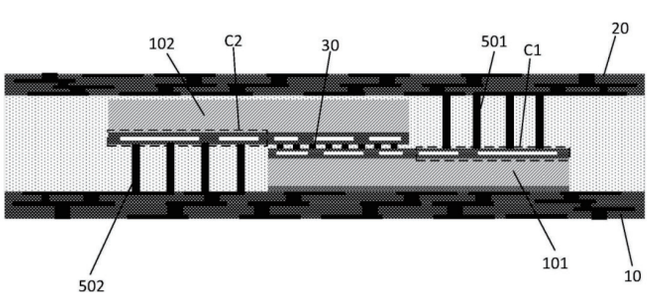


■ 国产芯片厂商芯原股份首次加入 UCIe 封装技术联盟

Chiplets 小芯片封装技术可以将不同 IP 模块封装在一起，进一步提高芯片性能，此前 AMD 及 Intel 等公司组建了 UCIe 产业联盟，现在芯原股份也加入了该联盟，成为第一个加入的国产芯片厂商，将与其他成员共同致力于 UCIe 1.0 版本规范和新一代 UCIe 技术标准的研究与应用，为芯原 Chiplet 技术和产品的发展进一步夯实基础。

■ 华为芯片堆叠封装专利公开：降低硅通孔技术成本 用堆叠换性能

据悉，华为近日公开了一种芯片堆叠封装及终端设备专利，专利摘要显示，该专利涉及半导体技术领域，其能够在保证供电需求的同时，解决因采用硅通孔技术而导致的成本高的问题。未来华为可能会采用多核结构的芯片设计方案，采用面积换性能，用堆叠换性能，使得不那么先进的工艺也能持续让华为在未来的产品里面，能够具有竞争力。



■ 台积电将成为 2022 年英伟达 GPU 的独家合同供应商

据报道，英伟达数据中心 GPU 将基于台积电的 4 纳米工艺制造，业内人士预计台积电将垄断英伟达在 2022 年发布的所有 GPU 的订单。据传，英伟达公司已同意向台积电支付高达 100 亿美元的费用。

■ AMD 宣布作价 121 亿元收购 DPU 芯片厂商 Pensando

据悉，AMD 继 3000 多亿成功拿下 FPGA 芯片厂商赛灵思之后，近日又收购了一家 DPU 芯片厂商 Pensando，花费 19 亿美元（约合 121 亿人民币）。收购后 Pensando 团队高管将加入 AMD 领导的数据中心解决方案部门，继续专注于执行其产品和技术路线图。

■ 英特尔第一款“矿卡”细节官宣

根据官方介绍，Intel Blockscale ASIC 采用了 Flip-chip LGA132-ball 封装样式，尺寸为 7.5×7 毫米，集成温度、电压传感器，内置了 SHA-256 硬件加速单元，比特币挖矿算力最高 580GH/s，功耗 4.8-22.7W，换算下来能效最高 26J/TH，支持最多 256 颗组成一套系统，将于第三季度起出货。

■ 英特尔宣布暂停俄罗斯业务

近日，英特尔公司就眼下在乌克兰发生的战争发表了声明，表示英特尔继续跟国际社会一道谴责俄罗斯对乌克兰的战争并呼吁迅速恢复和平，决定暂停在俄罗斯的所有业务运营。此前，英特尔曾决定暂停面向俄罗斯和白俄罗斯的客户的所有发货。

■ 消息称 OPPO 首款自研 AP 芯片 2023 年量产，2024 年推出手机 SoC

近日，据台媒报道称，中国手机大厂 OPPO 继 2021 年推出首款自行研发的影像处理神经网络运算（NPU）芯片后，旗下 IC 设计子公司上海哲库已展开应用处理器

（AP）及手机系统单芯片（SoC）研发，预计 2023 年会推出首款 AP 并采用台积电 6 纳米米制程生产，2024 年再推出整合 AP 及数据机（Modem）的手机 SoC，并进一步采用台积电 4 纳米制程投片。

■ SIA：2 月全球半导体销售额同比增长 32.4% 中国市场继续领跑

半导体行业协会（SIA）5 日报告显示，2022 年 2 月全球半导体行业销售额为 525 亿美元，较 2021 年 2 月同比增长 32.4%，较 2022 年 1 月环比增长 3.4%。销售额上看，中国地区以 166 亿美元的销售额继续领先于所有区域市场，亚太地区 / 所有其他地区（159 亿美元）紧随其后，之后是美洲（116 亿美元）、欧洲（45 亿美元）、日本（38 亿美元），排名与 2022 年 1 月保持不变。增速上看，美洲同比增长 43.2%，在所有区域市场中最高。亚太地区 / 所有其他地区（41.4%）、欧洲（29.3%）、中国（21.8%）和日本（21.6%）的均实现同比增长。亚太 / 其他地区（18.6%）和欧洲（1.4%）实现环比增长，但日本（-1.3%）、中国（-2.3%）和美洲（-3.0%）的销售额略有下降。

February 2022			
Billions			
Month-to-Month Sales			
Market	Last Month	Current Month	% Change
Americas	12.00	11.64	-3.0%
Europe	4.44	4.50	1.4%
Japan	3.89	3.84	-1.3%
China	17.04	16.64	-2.3%
Asia Pacific/All Other	13.37	15.86	18.6%
Total	**50.74**	**52.48**	**3.4%**
Year-to-Year Sales			
Market	Last Year	Current Month	% Change
Americas	8.13	11.64	43.2%
Europe	3.48	4.50	29.3%
Japan	3.16	3.84	21.6%
China	13.66	16.64	21.8%
Asia Pacific/All Other	11.22	15.86	41.4%
Total	**39.64**	**52.48**	**32.4%**

■ 机构：全球半导体供应依旧短缺，芯片交付时间延长至 26.6 周

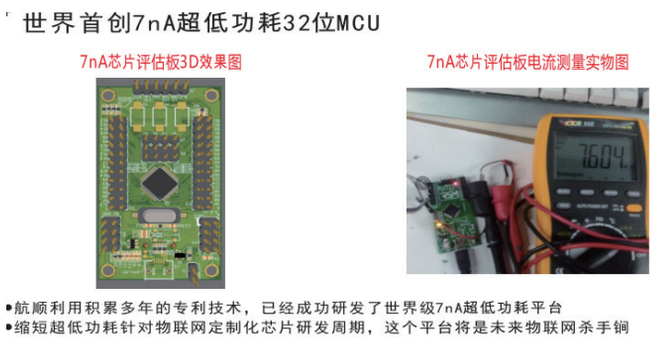
据彭博社报道，由于中国疫情和日本地震进一步阻碍了供应，3 月半导体交付的等待时间略有延长，并创出了新纪录。根据 Susquehanna 金融集团的研究，交货时间 -- 从订购芯片到交付之间的时间差 -- 在上个月增加了两天，达到 26.6 周。虽然芯片用户再次面临更长的等待时间，但交付时间增长的速度却显著低于 2021 年，当时许多行业由于缺少关键零部件而被迫削减产量。根据 Susquehanna 分析师 Chris Rolland 的报告，大多数芯片类型的交货时间都有所增加，包括电源管理、微控制器、模拟和内存。他说，俄乌冲突、中国部分地区的疫情封锁和日本地震 " 将在第一季度产生短期影响，但可能在全年对严重受限的供应链产生挥之不去的影响 "。此外，芯片行业的高管警告说，一些客户在 2023 年之前将很难获得足够的供应。英特尔等公司大规模增加的新工厂建设，最早也要到明年才能投产。

■ 电子业砍单潮蔓延至 PC 领域，2022 年上半年出货量将减少 8.5%

据台媒《经济日报》报道，俄乌战争持续加上通胀势头高涨，导致全球消费力度减弱，继非苹果手机产业传出大砍单之后，供应链最新消息指出，新一波砍单潮蔓延至 PC 业，近期几乎所有一线 PC 品牌都开始下修年度出货目标。报道称，供应链透露，联想、惠普、宏碁、华硕都在下调 2022 年订单量，降幅约二位数百分比。戴尔则因商务笔记本需求强劲，调整订单幅度相对不大。苹果也相对保持稳定。针对 PC 产业面临砍单疑虑，宏碁、华硕皆未回应。代工厂方面则维持第 2 季度出货季增长看法。市场人士分析，虽然品牌厂第 2 季开始通知供应商下修全年出货目标，但由于先前部分递延订单仍将在第 2 季持续出货，因此出现代工厂不看淡第 2 季，但对下半年出货却没把握的状况。其中仁宝预期第 2 季笔记本环比增长呈现高个位数、甚至有机会挑战双位数成长。研调机构 TrendForce 指出，2022 年上半年笔记本将垄罩在修正压力下，出货预估从原先全年 2.38 亿台出货量下修至 2.25 亿台、年减 8.5%。主要是因 Chromebook 出货动能疲软、俄乌战争影响需求，以及各笔记本品牌下修对 2022 年度出货量展望，相较年初平均约下调 10% 至 15%。

■ 世界级超低功耗 10nA HK32L 家族已批量供货

近日，航顺芯片基于 Arm® Cortex®-M0 内核国内首款 10nA 超低功耗 32 位 MCU -HK32L 家族系列迈向批量供货阶段。超低功耗以及产品的稳定性是 HK32L 家族最大的特点，航顺芯片在 2017 年就成功的研发出世界级的 7nA 超低功耗平台产品，并应用在定制化的特殊领域。正因为有了如此的硬实力，航顺芯片发展迅速，推出了多款符合市场需求，性能优越的爆款产品，其中就包括 10nA 超低 shutdown 功耗系列、业界首款 1 元以下 32 位 MCU 爆款系列、光模块专用系列、超低功耗蓝牙 BLE/SOC 系列、自主协处理器支持浮点运算系列、电机驱动专用系列等。



3 工业互联网行业一周要闻

- 多款机器人进入上海世博方舱医院
- 山西移动、华阳集团、华为合作赋能山西智慧煤矿建设
- 中国智能制造 50 强榜单出炉
- 日本研发新款机器人：3 分钟剥完一根香蕉
- 中国联通牵头编制的《钢铁行业 5G 确定性网络研究报告》发布

■ 多款机器人进入上海世博方舱医院

近日，多款机器人进入上海世博方舱医院，为新冠病毒感染者提供服务。消毒机器人在世博展览馆里边运行边喷洒雾化消毒剂；智能配送机器人为多个单元送餐、送药；人形机器人则负责为人们带路，还能随音乐翩翩起舞，给患者带来快乐。

■ 山西移动、华阳集团、华为合作赋能山西智慧煤矿建设

近日，三家公司共同签署《煤矿 5G 创新合作协议》。新场景方面，将探索煤矿 5G 专网从单一矿井建设向多矿井联合部署的新模式，聚焦 5G 矿山工业互联网平台，探索煤矿各类物联网技术的智能融合管控新场景；新技术方面，推进边缘计算能力建设，合理部署、下沉计算能力，探索井下综采、掘进面的控制中心就地实现业务数据分流；新设备方面，研究布设 5G 传输控制链路，实现对掘进机的远程控制。

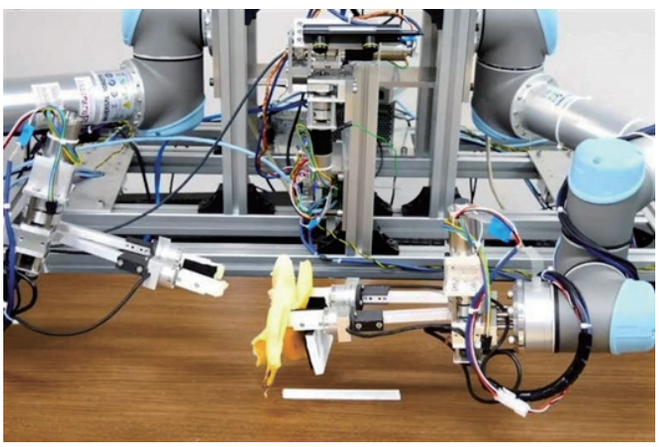
■ 中国智能制造 50 强榜单出炉

近日，中国科学院《互联网周刊》、eNet 研究院、德本咨询联合发布中国智能制造 50 强，榜单显示，海尔集团位居第一，中国航天科技集团、华为排名第二和第三，比亚迪、美的集团、京东方、中国中车、阿里巴巴集团、大疆创新、宁德时代进入前十，依次排名第 4-10 名。

2021年中国智能制造50强企业排行榜		
排名	企业	备注
1	海尔集团	家电行业智能制造
2	中国航天科技集团	工业大数据系统、机器视觉智能系统、智能设备等
3	华为	ICT（信息与通信）基础设施
4	比亚迪	研发信息化、生产数字化、产品智能化
5	美的集团	通过MBS、自动化和信息化打造智能制造工厂
6	京东方	设计制造一体化智能制造新模式
7	中国中车	轨道交通装备数字化智能化
8	阿里巴巴集团	阿里云IoT
9	大疆创新	基于无人机技术的智能化行业解决方案
10	宁德时代	电池智能制造
11	海康威视	数字安防产品智能制造
12	中国宝武钢铁集团	打造智慧钢厂
13	三一集团	离散制造业智能化、电动化、无人化
14	中国船舶	电子信息与智能装备
15	中国商飞	5G引领大飞机智能制造
16	中联重科	工程机械先进制造智慧智能
17	格力电器	数控机床、工业机器人、智能物流仓储设备等智能装备
18	潍柴动力	国六重型发动机“黑灯工厂”
19	广汽集团	广汽埃安智能生态工厂
20	烽火通信	5G通信网核心设备智能制造
21	歌尔股份	智能仓储、供应链可视化等
22	吉利控股	汽车制造引入5G、MEC、云计算和大数据等技术
23	福耀玻璃	汽车玻璃智能制造
24	TCL	显示面板智能工厂建设
25	正泰电器	跨区域数字化制造体系
26	特变电工	基于AI/AR和5G技术的智能工厂
27	长飞光纤	5G+光云工业互联网平台
28	四川长虹	“5G+工业互联网”生产线
29	科沃斯	互联家庭智能设备
30	蓝思科技	“蓝思云”工业互联网平台
31	徐工机械	智慧工业园区、5G全价值链智能工厂
32	中控技术	流程工业自动化
33	大族激光	激光、机器人及自动化领域智能制造解决方案
34	享通光电	光纤通信产业链全套智能化装备及控制软件
35	埃斯顿	工业自动化、工业机器人、工业数字化
36	科大智能	智能机器人、智能装备、智能电网终端设备等
37	新松机器人	机器人产品线及工业4.0整体解决方案
38	上海机电	机电一体化、工业自动化
39	柳工机械	“全面智能化”战略
40	楚天科技	智慧医药工厂，智能物流、智能仓储、智能信息化
41	山河智能	高端工程装备
42	同方威视	安检设备智能制造
43	康尼机电	推进智能制造与研发、管理、服务全方位融合
44	拓斯达	智能工厂整体解决方案
45	华中数控	数控系统、工业机器人
46	星网元智	智慧工厂规划、工业软件、AI工业硬件等
47	图灵智造	工业机器人生产、制造一体化
48	新时达	工业机器人
49	蓝英装备	数字化工厂、工业4.0全厂物流自动化
50	康硕集团	关键零部件领域智能制造系统解决方案
		制图：中商情报网WWW.ASKCI.COM

■ 日本研发新款机器人：3 分钟剥完一根香蕉

据介绍，这款机器人有两条手臂和两只手，可以抓住物体。为了训练机器人，研究人员将剥香蕉的过程分解成 9 个步骤，并输入指令让机器人逐步学习。仅仅经过 13 个小时的训练，机器人就可以在 3 分钟之内完整剥完一根香蕉，并确保香蕉果肉不被破坏，成功率为 57%。这项技术的目标是训练一个系统，使其能够更普遍地处理需要精细运动技能的任务。



■ 中国联通牵头编制的《钢铁行业 5G 确定性网络研究报告》发布

由中国联通牵头编制的《钢铁行业 5G 确定性网络研究报告》在 IMT-2020（5G）推进组 5G 应用工作组获得通过，并于近日正式发布。报告指出，钢铁制造过程流程长、工序多、工艺复杂、制造装备种类繁多，是典型的混合型制造流程。现代钢铁制造拥有高度自动化的工艺产线装备，具备大规模、标准化的制造过程管理体 系，对有效发挥装备产能、实现效益最大化并降低成本有着迫切需求。

4 物联网行业一周要闻

- 厦门国际健康驿站投入使用
- 北京投资 1866 亿元构建坚强韧性、绿色低碳智慧能源体系
- 三星与 ABB 合作 扩展智能家居应用
- 智能戒指制造商 Oura 完成新一轮融资
- IDC：中国物联网场景应用带动蜂窝通信模组市场快速发展
- 全球首发！新华三推出智原生 Wi-Fi 7 AP 新品

■ 厦门国际健康驿站投入使用

据介绍，厦门国际健康驿站将承担国际航班疫情防控任务，选址于高崎国际机场北侧，计划设置隔离房间 6001 间，可在未来 3-5 年满足入境人员的隔离防控需求。境外旅客从登机前即可使用小程序提前进行个人信息录入和选房缴费，到达驿站大厅后通过无感测温、行李消毒后即可刷防疫码乘坐专用电梯并进入客房。客房中配备的智能平板可以全方位满足隔离人员日常需求，事项提醒、医患沟通、健康上报、退房申请等事项一屏搞定，实现高效便捷的无接触入住体验。其中万睿科技部署的智能系统极大地提升了健康驿站的智慧化和无人化，有效降低人员接触及交叉感染的风险，同时保证隔离人员、医护人员及工作人员的生活和工作质量不受影响。

■ 北京投资 1866 亿元构建坚强韧性、绿色低碳智慧能源体系

据报道，北京提出总投资 1866 亿元的能源领域重点项目清单，通过 81 项能源发展重点任务，到 2025 年，北京天然气消费量控制在 200 亿立方米左右，应急储备能力达到 14 亿立方米左右。汽柴油总量力争较峰值下降 20%，电力占终端能源消费比重达到 29%，外调绿电量力争达到 300 亿千瓦时，可再生能源占能源消费比重力争提高 4 个百分点，达到 14.4% 以上。

■ 三星与 ABB 合作 扩展智能家居应用

据外媒报道，三星已经与 ABB 达成合作，将其 SmartThings 应用扩展到更多的家庭和建筑中。ABB 带来的 ABB-free@home 自动化系统可以控制住宅和商业建筑中的系统，包括检测、通信和气候系统。三星表示，二者的整合将为监控建筑技术创造“物联网解决方案的一站式服务”。

■ 智能戒指制造商 Oura 完成新一轮融资

在 Oura 戒指销量突破 100 万枚之后，这家智能戒指制造商宣布完成新一轮融资，目前公司总估值达到了 25.5 亿美元。在 Oura 于去年 10 月推出 300 美元的 Gen3 型号和 5.99 美元的月度订阅产品后，其销售量实现大增。

■ IDC：中国物联网场景应用带动蜂窝通信模组市场快速发展

IDC 表示，蜂窝通信模组正在向多模、智能化方向发展。中国厂商在模组市场重要性日益提升。模组市场产业链

大体由上游基带芯片、中游通信模组以下游各行业应用构成。在上游基带芯片领域，高通等国外厂商在高速的4G、5G等领域优势依然明显，但华为海思、紫光展锐、翱捷科技、移芯通信、芯翼科技等国内厂商，在借助4G Cat.1和NB-IoT的快速发展机遇，快速抢占市场。在通信模组领域，以移远通信、广和通、日海通信、美格智能等为代表的中国厂商凭借技术、成本等优势快速崛起，Sirra Wireless 、Telit、Thales、UBlox等几家传统国外领先公司，则在模组价格持续快速下降的环境下，经营压力日趋增大。模组市场整体竞争仍在加剧，厂商业绩分化，并购时有发生，鼎桥通信、联通数科等更多公司也在加入市场，市场的集中度还有望继续提升，更多中部厂商开始选择“专精化”发展，以应对激烈竞争。

■ 全球首发！新华三推出智原生 Wi-Fi 7 AP 新品

近日，紫光股份旗下新华三集团全球首发企业级智原生Wi-Fi 7 AP新品WA7638和WA7338。继2017年8月首发Wi-Fi 6 AP后，新华三再次领跑全球市场，引领WLAN正式进入Wi-Fi 7时代。由智原生技术加持的新华三Wi-Fi 7 AP将完美应对场景化新兴应用对速率、时延以及高密的严苛需求，扩展业务边界，为构建未来创新应用打开更多想象空间。

5 车联网行业一周要闻

- 比亚迪正式停产燃油车 3月销量为0
- 阳泉全域开放自动驾驶
- 宝马7系将迎来增强版停车辅助技术

- 四维图新与霍尼韦尔在汽车电子芯片等领域达成合作
- 全国首例自动驾驶重卡获得公开道路测试牌照
- 小米车辆专利获批
- 大众汽车计划 2030 年前在欧洲削减 60% 的内燃机车型
- 高通完成收购 Arriver 加码自动驾驶赛道
- 丰田自动驾驶采用摄像头 走特斯拉路线

■ 比亚迪正式停产燃油车 3 月销量为 0

近日，比亚迪公布 2022 年 3 月产销快报，3 月份比亚迪燃油汽车产量为 0。与此同时，比亚迪宣布从 2022 年 3 月起已经停止燃油汽车整车生产，专注于纯电动和插电混动汽车业务。比亚迪销量数据显示，2022 年 3 月插混车型销量为 5.07 万辆，同比增长 615.2%，纯电销量 5.37 万辆，同比增长 229.2%。2022 年 2 月比亚迪燃油车销量为 2795 辆，同比下降 84.6%，2022 年 3 月停产后燃油车销量为 0，同比下降 89.78%。

■ 阳泉全域开放自动驾驶

地处山西东部的“煤城”阳泉近年来携手百度、智行者等科技企业启动车城网建设，带动全域自动驾驶商业化运营及相关产业生态的集聚，目前已成为中国首个全域开放自动驾驶的城市。阳泉市车城网 - 车路智行新生态项目共规划有 3 条自动驾驶公交车测试线路，自 2021 年 12 月以来已完成城区大连路 - 平阳路路网线路的调试，在测试过程中克服了阳泉复杂交通路况和道路坡度大等技术困难，实现 L4 级自动驾驶功能，近期该线路将对公众开放试乘。

■ 宝马 7 系将迎来增强版停车辅助技术

据报道，宝马停车辅助功能可以记住 820 英尺的行驶距离并沿着相同的路径自动倒车，驾驶者只需控制油门和刹车。更新后的系统在这一技术的基础上得到了改进，其允许司机在车内或车外控制车辆的运行。倒车助手专业版、停车助手专业版和远程操控助手功能都将在 4 月 20 日亮相的新 7 系上提供。

■ 四维图新与霍尼韦尔在汽车电子芯片等领域达成合作

四维图新发布公告称，与霍尼韦尔传感控制（中国）有限公司签署《战略合作框架协议》，双方将在汽车电子芯片、自动驾驶、智能网联方向深化业务合作，构建战略合作伙伴关系。

■ 全国首例自动驾驶重卡获得公开道路测试牌照

近日，全国第一张针对公开道路入厂物流场景的自动驾驶重卡测试牌照在柳州发出，获得自动驾驶公开道路测试牌照的东风柳汽乘龙 H5 智能网联电动物流车，是专门针对入厂物流、园区转运等场景开发的智能电动卡车。车上配备摄像头、雷达、5G-OBU 等设备，在单车智能基础上，还具备 V2X 车路协同、5G 远程平行驾驶、云端智能调度等功能。

■ 小米车辆专利获批

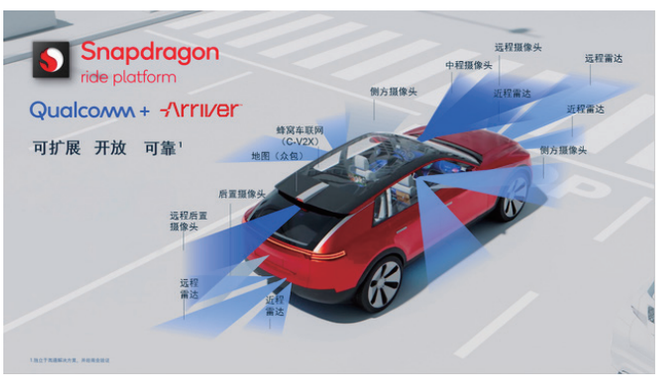
近日，北京小米移动软件有限公司“车辆”专利获授权。摘要显示，本公开涉及一种车辆，包括车身和安装于车身顶部、并用于采集目标方向图像信息的第一摄像头模组，该摄像头模组包括至少两个视场角范围不同的摄像头。通过该方案，能够提高车辆采集图像信息的清晰度和准确性。

■ 大众汽车计划 2030 年前在欧洲削减 60% 的内燃机车型

据报道，大众汽车首席财务官安特利茨表示，大众将在 2030 年前放弃数十个内燃机车型，并减少汽车的总体销量，以集中精力生产利润更高的优质汽车。安特利茨表示，大众将在未来 8 年内将其在欧洲的汽油和柴油汽车阵容（包括几个品牌的至少 100 个型号）减少 60%。

■ 高通完成收购 Arriver 加码自动驾驶赛道

高通公司近日宣布已完成收购 Arriver（安致尔）的交易，将把 Arriver 的计算机视觉、驾驶策略和驾驶辅助资源整合进其 Snapdragon Ride 平台产品组合。据悉，该平台是面向高性能中央计算与视觉系统解决方案的完整产品组合。



■ 丰田自动驾驶采用摄像头 走特斯拉路线

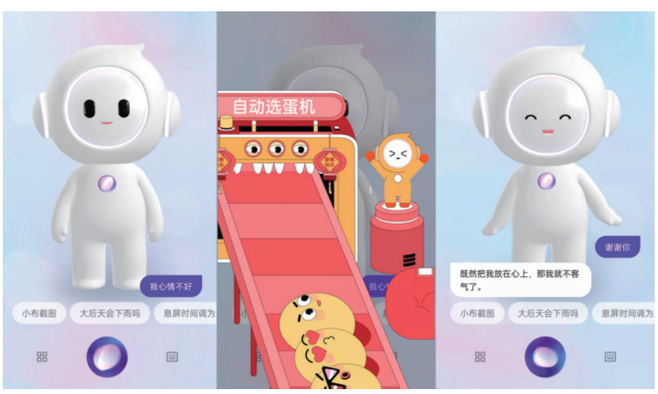
近日，丰田旗下的子公司 Woven Planet 宣布将以低成本摄像头为硬件基础研发自动驾驶技术。该公司表示，收集驾驶数据对提升自动驾驶系统至关重要，但使用激光传感器成本高昂，难以大规模安装。丰田使用的摄像头比先前使用的传感器便宜 90%，可以轻易安装于不同类型轿车，但其无人驾驶出租车等其他种类的自动驾驶汽车仍将使用激光雷达等传感器。

6 科技行业一周要闻

- OPPO 上线小布数字人 3D 互动式聊天
- 华为举行第二批军团组建成立大会
- 阿联酋电信宣布与 Meta 合作
- 亚马逊签署发射协议，将组建卫星互联网
- 谷歌联合埃森哲等多家巨头成立数据云联盟
- 全国一体化算力网络宁夏枢纽建设方案出炉
- 集微咨询：2022 年折叠屏手机出货将翻倍成长，达 1800 万部
- 法国最高行政法院撤销 SpaceX 星链频谱牌照
- 被罚 1.63 亿美元 谷歌在法国输掉反垄断案

■ OPPO 上线小布数字人 3D 互动式聊天

小布助手通过打造 3D 场景以及 AI 驱动的数字人与故事设定，让用户获得以聊天互动为主兼具游戏娱乐的沉浸式聊天新体验，并支持智能 AI 驱动来感知用户情绪，比如开心、难过、夸赞、生气等，带给用户更加生动、自然的交互体验，让用户面对智能助手能够聊得下去、聊得舒服。



■ 华为举行第二批军团组建成立大会

华为近日在深圳华为坂田基地举行第二批军团组建成立大会。第二批十个军团包括：电力数字化军团、政务一网通军团、机场与轨道军团、互动媒体军团、运动健康军团、显示新核军团、园区军团、广域网络军团、数据中心底座军团与数字站点军团。

■ 阿联酋电信宣布与 Meta 合作

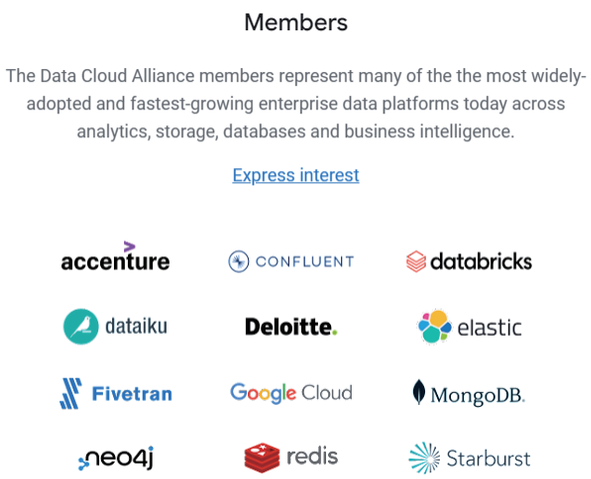
据报道，阿联酋电信已与 Meta 签署制定了“战略合作伙伴关系路线图”，将在其数字通信计划中，整合 Meta 最新的产品和解决方案，在消费者渠道数字化、AR、VR 以及对话式商务应用等方面进行合作。

■ 亚马逊签署发射协议，将组建卫星互联网

亚马逊与三家公司签署火箭发射协议，准备投资数十亿美元发射卫星，组建太空互联网卫星群，类似于 SpaceX 星链，该项目名叫 Project Kuiper。按照计划，2022 年年底之前 Project Kuiper 将会发射两颗原型卫星。

■ 谷歌联合埃森哲等多家巨头成立数据云联盟

据悉，数据云联盟致力于共同提供 API 和集成支持，通过允许平台之间的数据可移植性和可访问性，让成员客户的日常工作流程能够更加轻松通畅 —— 无论这些平台是在本地使用，还是构建于私有云、公共云、或混合云。需要指出的是，该联盟的大多数成员都没有直接竞争关系，而是提供相辅相成的服务。



■ 全国一体化算力网络宁夏枢纽建设方案出炉

根据《方案》，宁夏枢纽节点建设将分为起步区建设阶段（2021 年 -2023 年）、全面建设阶段（2024 年—2025 年）。宁夏枢纽全面建成后，标准机柜总数将达到 72 万架，总体投资超 7000 亿元，拉动大数据及相关产业规模达到万亿级。其中起步区建设谋划了七大工程 46 个重大项目，总投资超 3000 亿元。

■ 集微咨询：2022 年折叠屏手机出货将翻倍成长，达 1800 万部

集微咨询（JWInsights）指出，三星将折叠屏智能手机 Galaxy Z Flip 3 价格降至 1 万元以内，激发了海外消费者的购买欲望，加速了全球折叠屏智能手机的发展进程，2021 年全球折叠屏智能手机出货达 800 万部。2022 年可折叠 OLED 屏幕手机出货量有可能翻倍成长，超过 1800 万部。Stone Partners 预计，2022 年全球折叠屏手机出货量达到 1780 万部。

2022年折叠屏智能手机出货预测	
品牌	2022年
三星	13.9
小米	0.8
OPPO	0.3
vivo	0.2
华为	0.7
荣耀	1
其他	0.9
总计	17.8
来源：Stone Partners，单位：百万部	

■ 法国最高行政法院撤销 SpaceX 星链频谱牌照

近日，法国最高行政法院撤销了此前电子通信和邮政监管局向 SpaceX 低地轨道卫星宽带服务星链授予频段的决定，理由是该监管机构向 SpaceX 星链的授权没有执行正确程序。电子通信和邮政监管局曾于 2021 年 2 月授权 SpaceX 星链两个使用频段，帮助后者开展基于卫星的宽带服务。不过，在 4 月 6 日的公开裁决中，法院指出这一授权由于没有举行公开听证会，因此判定为不合法。据了解，SpaceX 星链被授权使用的一个是频段是 10.95GHz 至 12.70GHz，主要用于进行太空对地球的传输，另一个频段是 14GHz 至 14.5GHz，主要用于进行地球对太空传输。此外，法院还指出向星链发放牌照的决定“可能会冲击高带宽联网市场并最终影响用户的利益”。

■ 被罚 1.63 亿美元 谷歌在法国输掉反垄断案

谷歌在法国输掉了一场 1.63 亿美元的反垄断上诉案，被指利用在搜索市场的主导地位，为其在线广告平台设置不公平规则。2019 年 12 月，法国反垄断部门宣布对谷歌处以 1.5 亿欧元（约合 1.63 亿美元）的罚款，原因是谷歌存在不公平竞争行为，包括利用其在搜索市场的主导地位，为其广告平台 Google Ads 设置不公平条款。谷歌不服提起上诉。近日，巴黎上诉法院驳回了谷歌的上诉，维持原判。此外，法国反垄断机构“竞争管理局”（FCA）去年 6 月还宣布，已对谷歌处以 2.2 亿欧元（约合 2.67 亿美元）的罚款，原因是谷歌滥用其在网络广告市场的主导地位。

7 安全一周要闻

- 微软称已控制俄罗斯黑客的域名，帮助乌克兰免受网络攻击
- 俄罗斯外卖应用的泄露数据中包含 GRU 特勤人员的用餐习惯
- 国际电子邮件营销巨头 MailChimp 遭黑，沦为钓鱼工具
- 为应对网络攻击，德国风电设备巨头 Nordex 关闭 IT 网络
- Stuxnet 攻击再现？罗克韦尔自动化 PLC 曝出严重漏洞
- GitLab 存在漏洞，允许攻击者接管用户账户
- Wyze 摄像头曝出大漏洞，近三年时间才修复
- IT 服务巨头遭勒索软件攻击，损失超 4200 万美元
- 苹果发布紧急补丁以修复被积极利用的零日漏洞
- Meta 雇佣公司攻击 TikTok 引发数据隐私担忧；Spring 漏洞补丁已更新
- OpenSSL 无限循环漏洞影响威联通 NAS 设备
- CNVD 收录 Spring 漏洞，补丁发布；Facebook 算法漏洞持续半年

- Lapsus 勒索团伙声称攻击 IT 巨头 Globant
- 监控软件公司 FinFisher 宣布破产
- 部分本田车型存在漏洞，黑客可远程启动车辆
- 黑客组织宣称攻击了微软公司和 Okta 公司
- 黑客假冒 Instagram 技术支持人员钓鱼保险公司
- Wyze 摄像头曝出大漏洞，近三年时间才修复
- IT 服务巨头遭勒索软件攻击，损失超 4200 万美元
- 黑了微软、三星、英伟达的神秘黑客组织曝光，背后竟是 16 岁英国少年，还招内鬼帮忙
- 苹果发布紧急补丁以修复被积极利用的零日漏洞
- “透明部落”APT 组织正在大肆攻击印度官员

■ 微软称已控制俄罗斯黑客的域名，帮助乌克兰免受网络攻击

据 Neowin 报道，微软透露，它已经控制了由与俄罗斯有关的黑客实体 Strontium 控制的七个互联网域名。微软称，这些域名被用于针对乌克兰机构（如媒体组织）以及美国和欧盟参与外交政策的政府机构和智囊团的网络攻击。这些域名是在微软于 4 月 6 日获得法院命令后被没收的。微软长期以来一直在应对 Strontium，并且已经制定了一个流程，可以快速获得法院命令以对该组织的黑客活动采取行动。通过对域名的控制，微软已将其重新定向到它运行的一个 sinkhole，以确保用户安全并通知攻击的受害者。

■ 俄罗斯外卖应用的泄露数据中包含 GRU 特勤人员的用餐习惯

据 TheVerge 报道，根据 Bellingcat 的调查结果，俄罗斯外卖平台 Yandex Food 的一次大规模数据泄漏暴露了属于那些与俄罗斯秘密警察有关的递送地址、电话号码、姓名和配送指示。

■ 国际电子邮件营销巨头 MailChimp 遭黑，沦为钓鱼工具

近日，电子邮件营销公司 MailChimp 披露其遭到黑客攻击，黑客利用内部客户支持和账户管理工具窃取用户数据，并进行网络钓鱼攻击。当日，许多 Trezor 硬件加密货币钱包所有者发推特称，收到了关于该公司遭到数据泄露的网络钓鱼通知。这些邮件促使 Trezor 客户下载可以窃取加密货币的恶意软件来重置他们的硬件钱包 pin。随后，Trezor 表示，MailChimp 已经被针对加密货币行业的威胁行为者攻破，借此进行了网络钓鱼攻击。

■ 为应对网络攻击，德国风电设备巨头 Nordex 关闭 IT 网络

德国风电设备巨头 Nordex 遭遇网络攻击，被迫关闭 IT 网络应对；近半年来，全球多个风电上下游厂商因网络攻击导致业务受影响，网络安全已成为风电行业重大风险。

■ Stuxnet 攻击再现？罗克韦尔自动化 PLC 曝出严重漏洞

近日，网络安全公司 Claroty Team82 的研究人员在罗克韦尔自动化（Rockwell）的可编程逻辑控制器 (PLC) 平台中发现了两个高危漏洞，攻击者可以（远程）利用这些漏洞修改自动化流程，破坏工厂运营、对工厂造成物理损坏或采取其他恶意行为。在本周发布的安全报告中，

研究人员指出其中一个漏洞的危险性堪比 Stuxnet（震网病毒），因为它们允许攻击者在 PLC 上运行恶意代码而不会触发任何明显的异常行为。罗克韦尔自动化已经为其客户发布了这两个漏洞的安全公告（链接在文末）。美国网络安全和基础设施安全局 (CISA) 本周四也发出安全警报，指出使用受影响组件的企业采取缓解措施和应对威胁的检测方法。CISA 表示，这些漏洞影响了全球各地的关键基础设施，并指出这些漏洞的攻击复杂性低，其中一个可被远程利用。可远程利用漏洞其中可被远程利用的漏洞 (CVE-2022-1161) 的严重性等级高达 10，并且广泛存在于在罗克韦尔的 ControlLogix、CompactLogix 和 GuardLogix 系列控制系统上运行的 PLC 固件中。据 Claroty 透露，这些都是罗克韦尔的主要 PLC 产品线。“这些设备在几乎所有垂直领域都很常见，包括汽车、食品和饮料以及石油和天然气，”Claroty 指出：“我们能想到的唯一一个幸免的行业是输电和配电。”Claroty 表示，该漏洞与罗克韦尔的 PLC 将可执行文件（或字节码）和源代码（也称为文本代码）存储在 PLC 上不同位置有关。这为攻击者提供了一种在不更改源代码的情况下修改字节码的方法。“PLC 不需要两者兼容，”Claroty 指出：“当工程师连接到 PLC 时，他们会看到运行的文本代码并无异常，而被更改的字节代码会导致恶意代码在没有任何篡改迹象的情况下运行。”Claroty 确定共有 17 个罗克韦尔 PLC 型号受到影响。代码注入漏洞第二个漏洞 (CVE-2022-1159) 存在于罗克韦尔的 Studio 5000 Logix Designer 中，这是工程师用来对其 PLC 进行编程的软件。该软件允许工程师开发、编译并将新开发的逻辑传输到可编程逻辑控制器系列中。OT 环境中的工程师通常会对 PLC 中的复杂逻辑进行升级，以改进、调整或修改 PLC 控制的任何过程。Studio 5000 Logix Designer 中的漏洞允许已经在运行该软件的工作站上具有管理访问权限的攻击者劫持编译过程并注入恶意代码，然后他们可以在 PLC 上执行这些代码而不会触发任何警报。“CVE-2022-1159 使攻击者能够在用户不知情的情况下更改正在编译的代码，”Claroty 指出：“这可能会导致工程师无法意识到传输到 PLC 的逻辑被篡改。”此漏洞的严重性等级为 7.7（满分 10），这意味着该漏洞有着高缓解优先级，但不一定是严重漏洞。类似 Stuxnet 攻击的可能性这两个漏洞都存在于不同的罗克韦尔自动化组件中。都可以被攻击者用来改变 PLC 中的逻辑流程，将新命令发送到系统控制的物理设备中。例如，Claroty 研究人员表示，攻击者可将某些标签（或自动化过程变量）更改为不同的值，在现实中，这意味着攻击者可以控制设备（例如发动机转速），从而对自动化过程造成重大损害。“这是一种类似Stuxnet的攻击, 它能在PLC上隐藏已执行的字节码, 同时让工程师相信正常代码已被执行, ”Claroty 指出:“在 Stuxnet 的案例中，这导致离心机的旋转速度超过了预期，并导致了意想不到的结果。”对 ICS 安全性的担忧绝非新鲜事。Claroty 最近的一项研究发现，与 2020 年相比，2021 年报告的 ICS 漏洞增加了 52%。与 2019 年至 2020 年期间披露的ICS漏洞增加25% 相比, 这一增长要高得多。2021 年 ICS 产品发现漏洞的 82 家供应商中 ,21 家之前没有报告任何漏洞，这意味着研究人员已经开始更广泛地寻找 ICS 漏洞。Claroty 去年发布的一份报告显示，2021 年前六个月披露的 ICS 漏洞中有 90% 的攻击复杂性较低，71% 的严重等级为“高”或“严重”。超过六成 (61%) 可以远程执行，74% 不需要任何权限即可执行。

出处：https://claroty.com/2022/03/31/blog-research-hiding-code-on-rockwell-automation-plcs/

■ GitLab 存在漏洞，允许攻击者接管用户账户

Bleeping Computer 网站披露，GitLab 出现一个严重的漏洞（CVE-2022-1162），该漏洞可能允许远程攻击者使用硬编码密码接管用户账户，影响到 GitLab 社区版（CE）和企业版（EE），目前漏洞问题已解决。据悉，该漏洞由 GitLab CE/EE 基于 OmniAuth 的注册过程中，意外设置的静态密码造成。GitLab 团队发布安全公告表示，在 GitLab CE/EE 14.7（14.7.7 之前）、

14.8（14.8.5 之前）和 14.9（14.9.2 之前）版本中，使用 OmniAuth 提供程序（如 OAuth、LDAP、SAML）注册的账户被设置了硬编码密码，允许攻击者接管账户。先前提交的一份代码显示，GitLab 删除了 "lib/gitlab/password.rb " 文件，该文件用于为 "TEST_DEFAULT " 常量分配一个弱的硬编码密码。GitLab 敦促用户应立即将所有 GitLab 安装升级到最新版本（14.9.2、14.8.5 或 14.7.7），以阻止潜在的网络攻击。重置部分 GitLab 用户的密码 GitLab 强调，超过 10 万个组织使用其 DevOps 平台，在全球 66 个国家拥有 3000 多万注册用户，为缓解 CVE-2022-1162 带来的恶劣影响，重置了部分 GitLab.com 用户的密码。另外，GitLab 表示没有证据表明攻击者利用这一硬编码密码安全漏洞入侵了任何账户，但仍需要为用户的安全采取预防措施。当被问道重置密码的 Gitlab.com 用户数量时，GitLab 发言人分享了一些公告中已有的信息，并告诉 Bleeping Computer，只为部分用户做了密码重置。发布识别脚本虽然 GitLab 称，目前为止没有用户账户被入侵，但该公司已经创建了一个脚本，实例管理员可以使用脚本识别可能受 CVE-2022-1162 影响的用户账户，在确定可能受影响的用户账户后，会建议管理员重置用户的密码。

出　处：https://www.bleepingcomputer.com/news/security/critical-gitlab-vulnerability-lets-attackers-take-over-accounts/

■ Wyze 摄像头曝出大漏洞，近三年时间才修复

近日，某畅销的摄像头品牌 Wyze Cam 被曝存在三个严重的安全漏洞，黑客利用这些漏洞可以执行任意代码，完全控制摄像头，并且访问设备中的视频资源。更糟糕的是，这些漏洞是在三年前被发现的，最后一个漏洞直到近段时间才完成修复。这三个安全漏洞的具体信息如下：漏洞一：CVE-2019-9564，可绕过身份安全验证；漏洞二：CVE-2019-12266，基于堆栈的缓冲区溢出，可远程控制摄像头漏洞三：无编号，可远程接管设备，并访问 SD 卡中的视频资源；如果黑客将以上三个漏洞综合利用，那么就可以轻松绕过设备的身份验证，入侵目标摄像头，最终实现实时监控摄像头。这意味着，使用者的一举一动都会清晰的出现在黑客的视野中，再无任何的隐私。罗马尼亚网络安全公司 Bitdefender 发布的报告显示，安全研究人员最早发现了这些漏洞，并在 2019 年 5 月就向供应商报告了漏洞详情，Wyze 分别在 2019 年 9 月和 2020 年 11 月发布了修复 CVE-2019-9564 和 CVE-2019-12266 的补丁。2022 年 1 月底，Wyze 终于发布了固件更新，解决了攻击者不经身份验证，即可访问 SD 卡内容的问题。安全专家表示，目前这些漏洞会影响三个版本的 Wyze Cam 摄像头，其中第一个版本已经停产，因此不会收到解决上述漏洞问题的安全更新。这意味着，正在使用且未来继续使用第一个版本的 Wyze Cam 摄像头将会一直处于风险之中，安全性无法得到保证。这对正在很多用户都将会是一个灾难，尤其是家庭用户，他们所有的隐私都有可能被黑客窃取。因此，Bitdefenders 表示，家庭用户应密切关注物联网设备，并尽可能将它们与本地或访客网络隔离开来。这可以通过专门为物联网设备设置专用 SSID 来完成，或者如果路由器不支持创建额外的 SSID，则将它们移动到访客网络。

出　处：https://securityaffairs.co/wordpress/129677/hacking/wyze-cam-flaws-allow-takeover.html

■ IT 服务巨头遭勒索软件攻击，损失超 4200 万美元

近期，西班牙一家领先的业务流程外包 (BPO) 服务提供商表示，因遭遇勒索软件攻击导致其损失超过数千万美元。作为全球前五的客户关系管理 (CRM) 和 BPO 提供商，Telefonica Atento 在拉丁美洲拥有强大的基础。然而去年 10 月，它声称其巴西子公司 IT 系统遭遇了“网络攻击”。不过公司已经第一时间做出了响应，“快速识别”出威胁、且隔离受影响的系统并暂停与客户的连接。虽然公司表示在之后的 24 小时内，服务开始恢复在线，不到一周后，数据中心的运营已经恢复。然而近期发布的 2021 财年财

务报告显示，勒索攻击对公司的影响比最初想象的要大得多。根据报告可以得出，由于“巴西业务中断”，第四季度收入损失了 3480 万美元，另外还有 730 万美元用于与攻击相关的“保护、检测和补救措施”。Atento 的首席财务官兼首席执行官在一份联合声明中说，“与当今时代的许多公司一样，包括一些世界技术领导者，我们受到了网络攻击，这当然也影响了我们第四季度的业绩。该事件的复杂性和对我们的影响，都远大于我们的预期。据当地报道，该公司没有向勒索者付款，而发起勒索攻击的黑客组织据说是近期高调的 LockBit 组织。对此，Atento 声称已经设立了最佳的应对方案，除了提高其保护、检测和补救能力——包括与 CrowdStrike 和 Mandiant 签署的新协议，现在正与“防御团体和机构”更密切地合作，以提高应对威胁的准备。不过，基于近期勒索事件频发，Atento 也会被添加到勒索软件攻击后遭受极高损失的公司名单中，名单中包括法国 IT 服务公司 Sopra Steria（6000 万美元）、铝业巨头 Norsk Hydro（4100 万美元）和 IT 服务公司 Cognizant（7000 万美元）。

出　处：https://www.infosecurity-magazine.com/news/services-42m-fallout-ransomware/

■ 苹果发布紧急补丁以修复被积极利用的零日漏洞

近日，苹果发布了一个紧急安全补丁，以解决两项被积极利用以入侵 iPhone、iPad 和 Mac 的零日漏洞。这两项漏洞均由匿名研究人员发现并报告，苹果公司表示在 iOS 15.4.1、iPadOS 15.4.1 和 macOS Monterey 12.3.1 的发布中已解决了该两项漏洞，并建议用户尽快安装安全更新。除此之外，苹果方面没有透露任何关于在这些漏洞被如何利用的具体细节。第一项漏洞是存在于英特尔显卡驱动程序中的超权限读取问题，追踪代码为 CVE-2022-22674，该漏洞允许恶意应用程序读取内核内存。这一漏洞的积极利用引起了苹果公司的注意，公司最近发布的一份报告中称，超权限读取问题可能会导致内核内存的泄露。在报告也同时提到了公司的对应建议：“可以通过改进的输入验证来解决该漏洞。”第二项漏洞是一个越界写入问题，影响 AppleAVD 媒体解码器，追踪代码为 CVE-2022-22675。该漏洞同样允许恶意应用程序读取内核内存，从而使应用程序能够使用内核特权执行任意代码。对此，报告给出建议：“通过改进的边界检查可以解决越界写入问题。”其实，自 2022 年 1 月以来，苹果公司已经解决了三个被积极利用的零日漏洞。1 月，公司解决的两项零日漏洞追踪代码分别为 CVE-2022-22587 和 CVE-2022-22594，攻击者可以利用其在受攻击的设备上运行任意代码。2 月，解决的是 WebKit 中一个影响 iOS、iPadOS、macOS 和 Safari 的零日漏洞，追踪代码为 CVE-2022-22620，可以通过处理恶意制作的网页内容触发，从而导致任意代码执行。

出　处：https://securityaffairs.co/wordpress/129672/security/apple-emergency-patches-zero-days.html

■ Meta 雇佣公司攻击 TikTok 引发数据隐私担忧；Spring 漏洞补丁已更新

国家信息安全漏洞共享平台收录 Spring 框架远程命令执行漏洞，安全补丁更新

出处：https://www.freebuf.com//news/326992.html

■ OpenSSL 无限循环漏洞影响威联通 NAS 设备

据 The Hacker News 消息，中国台湾公司威联通（QNAP） 本周透露，旗下部分网络附加存储 (NAS) 设备正受到最近披露的开源 OpenSSL 加密库中的一个漏洞影响。据报道，该漏洞被跟踪为 CVE-2022-0778（CVSS 评分：7.5），是 OpenSSL 中的一个无限循环漏洞，其原因与解析安全证书以触发拒绝服务条件，并远程使未打补丁的设备崩溃时出现的错误有关。如果被利用，该漏洞允许攻击者进行拒绝服务攻击。目前威联通仍在调查受影响的产品型号，但已确定会影响以下系统版本：QTS 5.0.x 及更高版本 QTS 4.5.4 及更高版本 QTS 4.3.6 及更高版本 QTS 4.3.4 及更高版本 QTS 4.3.3 及更高版

本 QTS 4.2.6 及更高版本 QuTS hero h5.0.x 及更高版本 QuTS hero h4.5.4 及更高版本 QuTScloud c5.0.x 迄今为止，没有证据表明该漏洞已在野外被利用。一周前，威联通发布了 QuTS hero 安全更新（版本 h5.0.0.1949 build 20220215 及更高版本），以解决影响其设备的“ Dirty Pipe ”本地权限提升漏洞。QTS 和 QuTScloud 操作系统的补丁预计将很快发布。

出　处：https://thehackernews.com/2022/03/qnap-warns-of-openssl-infinite-loop.html#google_vignette

■ CNVD 收录 Spring 漏洞，补丁发布；Facebook 算法漏洞持续半年

Facebook 因算法漏洞连推糟糕内容，一直持续半年 Facebook 动态消息（News Feed）因为存在重大排序错误，过去 6 个月一直推送“糟糕”内容。由于排序算法存在漏洞，动态消息抬高了虚假、暴力信息的权重。

出处：https://www.freebuf.com//news/326960.html

■ Lapsus 勒索团伙声称攻击 IT 巨头 Globant

近日，勒索团伙 Lapsus$ 声称其侵入了 IT 巨头 Globant 公司，并在网络上泄露了大约 70GB 的被盗数据。事后，该团伙声表示，Globant 公司实施的安全措施实在糟糕至极，使得他们能够轻易地攻击其基础设施。“对所有 Globant.com 糟糕的安全措施感兴趣的人，我们将公开全部的 DevOps 平台的管理凭证”，Lapsus$ 团过甚至将这条消息发布了在 Telegram 频道上。据该团伙透露，本次攻击中被盗的数据主要是客户的源代码，而他们已经在网络上公开披露了一份访问该公司使用的源代码共享平台的凭证清单，包括 GitHub、Jira、Crucible 和 Confluence。就在 Globant 遭到黑客攻击的几天前，伦敦警方宣布逮捕了 7 名涉嫌为 Lapsus$ 勒索团伙成员的少年。警方的证据显示，一名来自牛津的 16 岁少年极有可能是这个臭名昭著的勒索团伙的头目之一。而外界普通认为该犯罪团伙的总部设在南美洲。在过去的几个月里，Lapsus$ 犯罪团伙入侵了许多知名公司，如 NVIDIA，Samsung，Ubisoft，Mercado Libre 和 Vodafone。就在上周，该组织还了宣布对微软和 Okta 进行了黑客攻击。

出　处：https://securityaffairs.co/wordpress/129615/cyber-crime/lapsus-gang-hacked-globant.html

■ 监控软件公司 FinFisher 宣布破产

据彭博社和 Netzpolitik 周一消息，总部位于慕尼黑的间谍软件公司 FinFisher 已于上个月宣布破产，有关部门正对其业务交易进行调查。之前，这家公司因为向专制政权出售监视间谍软件而备受争议，这些软件被用来争对持不同政见者、活动家和记者。FinSpy 是该公司最赚钱的间谍软件，一些非政府组织提起刑事诉讼声称 FinSpy 被出售给土耳其政府并用于 2017 年针对反政府抗议者的行动中。2019 年，德国开始对 FinFisher 展开调查。根据无国界记者组织、Netzpolitik、民权协会和欧洲宪法与人权中心提出的申诉，指控 FinFisher 没有遵守欧洲的出口规定，包括要求获得联邦经济和出口管制办公室（BAFA）给予的对非欧盟国家的贸易许可。FinSpy 问世于 2016 年，并与埃及、巴林、孟加拉国、埃塞俄比亚、阿曼、沙特阿拉伯和委内瑞拉政府在内的客户建立了合作关系，其产品特性是具有高侵入性，本质上为用户提供了对选定目标设备（包括聊天和电话对话）以及设备摄像头和麦克风的所有访问权限。根据非政府组织的调查，FinFisher 在未经德国联邦政府批准的情况下，将间谍软件 FinSpy 出售给了土耳其政府，从而助长了对土耳其反对派人士和记者的监控，2020 年 10 月，德国当局突袭了 FinFisher 公司办公室、两家关联企业以及董事和高管的住所，并最终促成 FinFisher 在近期宣布破产。慕尼黑检察院的一位发言人告诉彭博社，尽管调查正在进行，但因 FinFisher 的破产，检察院无法扣押他们涉嫌非法获得的资产。

出　处：https://therecord.media/surveillance-software-firm-finfisher-declares-insolvency/

■ 部分本田车型存在漏洞，黑客可远程启动车辆

The Hacker News 网站披露，研究人员发现一个影响部分 Honda（本田） 和 Acura（讴歌）车型的重放攻击漏洞（CVE-2022-27254），黑客能够利用该漏洞解锁汽车、甚至启动汽车引擎。据悉，发现漏洞问题的是达特茅斯大学两个学生 Ayyappan Rajesh 和 Blake Berry。Blake Berry 在 GitHub 帖子中表示，黑客可以通过该漏洞获得锁定、解锁、控制车窗、打开后备箱和启动目标车辆发动机的访问权限，防止攻击的唯一方法是永远不要使用遥控钥匙，或者在被攻击后，从汽车经销商处重新设置新的钥匙。受影响车型的遥控钥匙向汽车传输相同的、未加密的无线电频率信号（433.215MHz）时，攻击者能够拦截并重新发送，以无线方式启动发动机，并锁定和解锁车门。漏洞主要影响 2016 年至 2020 年生产的本田思域 LX、EX、EX-L、旅行版、Si 和 Type R 等车型。本田汽车出现过类似漏洞值得一提的是，这不是第一次在本田汽车中发现此类漏洞， 2017 年本田 HR-V 车型中出现了一个相关漏洞（CVE-2019-20626，CVSS 评分：6.5）。Rajesh 强调，汽车制造商必须实施滚动代码，也就是所谓的跳转代码, 这是一种常用的安全技术, 为远程无钥匙进入（RKE）或被动无钥匙进入（PKE）系统的每次身份认证提供一个新的代码，来确保汽车安全。

出 处：https://thehackernews.com/2022/03/hondas-keyless-access-bug-could-let.html

■ 黑客组织宣称攻击了微软公司和 Okta 公司

目前，微软公司和 Okta 公司都在调查核实黑客组织 Lapsus$ 早先宣称破坏攻击他们系统的说法是否真实。黑客组织 Lapsus$ 声称自己获得了访问 Okta 公司内部系统的“超级用户 / 管理员”权限。并且还在 Telegram 频道发布了近 40GB 的文件，其中包括了据说来源于微软内部项目以及系统的屏幕截图和源代码。这则令人震惊的消息最早由 Vice 和路透社报道。Okta 公司周二证实，该公司确实遭受了网络黑客的攻击，且一些用户也受到了不同程度的影响。尽管此次网络安全漏洞的范围尚未明晰，但不容乐观的是漏洞可能是巨大的。根据该公司的说法，他们正在为数亿用户提供网络平台服务，其中就包括了联邦快递、穆迪公司 (债权评级机构)、T-Mobile 公司 (德国电信的子公司)、惠普公司和 GrubHub 公司 (美国大型食品配送公司) 等数千家大型公司的员工。一位微软公司的发言人告诉 Threatpost，在公司内部调查时发现一个具有访问权限的公司账户被盗。微软公司的网络安全响应团队正在迅速地对被盗账户进行补救，亡羊补牢，犹未为晚，以防止黑客组织利用该账户进行下一步的活动。该发言人同时表示他们并不将代码的保密性作为唯一地网络安全防范措施，查看源代码的行为与公司内的风险提升并无直接的联系。微软的威胁情报团队在周二发布了一个博客，详细介绍了其观察 Lapsus$ 的活动，微软将其标记为 DEV-0537。

出　处：https://threatpost.com/lapsus-data-kidnappers-claim-snatches-from-microsoft-okta/179041/

■ 黑客假冒 Instagram 技术支持人员钓鱼保险公司

研究人员透露，最近的一场网络钓鱼活动以 Instagram 技术支持为诱饵，意图窃取总部位于纽约的一家知名美国人寿保险公司的员工的登录凭证。根据 Armorblox 周三发布的一份报告，这次攻击将品牌冒充与社会工程攻击相结合，并通过使用一个有效的域名设法绕过了谷歌的电子邮件安全，最终拿到了数百名员工的邮箱。诈骗所用的网站与 Instagram 完全相同网络攻击从一封简单的电子邮件开始。它伪装成是来自 Instagram 技术支持团队的告警，表示收件人的账户正面临着被停用的风险。根据分析，这样说的目的是为了创造一种紧迫感，同时使受害者提高对发件人的信任度。电子邮件的内容这样写到，你已经被警

告了，因为你的账号中分享了虚假的内容。你必须验证你的账号资格。如果你不能在 24 小时内完成验证，那么你的会员资格将会从我们的服务器中永久删除。 这条信息营造了一种紧迫感，诱使那些毫无戒心的用户点击一个恶意的账户验证链接。最终用户会被引诱到一个登录页面上，他们会被要求提交他们的Instagram账户登录信息。当然，这些信息会被直接传给恶意攻击者，而被害人自己并不知情。研究人员指出，这些步骤中任何一点对普通终端用户来说都没有任何恶意，而且在每个过程中，从电子邮件到账户验证表，都含有 Meta 和 Instagram 的品牌和标志。攻击者在攻击的过程中必然会留下线索。他们在钓鱼邮件的正文中犯了语法、拼写和大小写等相关错误。在发件人栏中，"Instagram 支持 " 中的 "I " 实际上是 "L"。而电子邮件域名本身是 membershipform@outlook.com.tr，这显然不是来自于 Instagram。不过，域名本身是完全合法的，这也就可以使它绕过传统的垃圾邮件过滤器。而且，研究人员解释说，发件人还精心设计了一个很长的电子邮件地址，这意味着许多移动用户只会看到 '@' 符号之前的字符，在这种情况下 'membershipform' 就是一个不会引起怀疑的字符。如何保护自己的信息安全就在几周前，网络攻击者通过冒充 DocuSign 公司的电子签名软件，从一家美国支付解决方案公司窃取了微软的账户凭证。在那个案例中，也是由于攻击者巧妙地利用了品牌冒充、社会工程和能够绕过传统安全措施的有效电子邮件域名，从而导致了数百名员工的信息被泄露。也许这两个活动被发现并已经被阻止了，但下一个攻击活动呢？或者之后的那个？还有哪些其他没有被安全团队成功识别，以至于我们没有听说过的攻击活动呢？Armorblox 在报告中提出了员工可以关注的四个主要领域，可以保护自己免受网络钓鱼的侵害。 避免打开你所不熟悉的电子邮件加强原生电子邮件的安全性，阻止社会工程学的攻击注意有针对性的攻击 遵循多因素认证和密码管理的原则 KnowBe4 的研究人员通过电子邮件写道，为了防止这些攻击，员工应该接受安全教育，了解他们的电子邮件账户的价值。此外，员工还需要了解到使用重复密码的危险性，使用强健的密码来保护个人和组织内的账户。即使是一个员工的失误也会给整个组织带来严重的问题，然后是供应链上的其他组织。Armorblox 研究人员写道，在使用商业凭证登录多个应用程序时要谨慎，特别是在那些个人使用的社交应用程序中。这种行为可能看起来很方便，但是，只需要一次，你的敏感的个人信息和商业数据就会有被泄露的风险。

出　处：https://threatpost.com/phony-instagram-support-staff-emails-hit-insurance-company/178929/

■ Wyze 摄像头曝出大漏洞，近三年时间才修复

近日，某畅销的摄像头品牌 Wyze Cam 被曝存在三个严重的安全漏洞，黑客利用这些漏洞可以执行任意代码，完全控制摄像头，并且访问设备中的视频资源。更糟糕的是，这些漏洞是在三年前被发现的，最后一个漏洞直到近段时间才完成修复。这三个安全漏洞的具体信息如下：漏洞一：CVE-2019-9564，可绕过身份安全验证；漏洞二：CVE-2019-12266，基于堆栈的缓冲区溢出，可远程控制摄像头；漏洞三：无编号，可远程接管设备，并访问 SD 卡中的视频资源。如果黑客将以上三个漏洞综合利用，那么就可以轻松绕过设备的身份验证，入侵目标摄像头，最终实现实时监控摄像头。这意味着，使用者的一举一动都会清晰的出现在黑客的视野中，再无任何的隐私。罗马尼亚网络安全公司 Bitdefender 发布的报告显示，安全研究人员最早发现了这些漏洞，并在 2019 年 5 月就向供应商报告了漏洞详情，Wyze 分别在 2019 年 9 月和 2020 年 11 月发布了修复 CVE-2019-9564 和 CVE-2019-12266 的补丁。2022 年 1 月底，Wyze 终于发布了固件更新，解决了攻击者不经身份验证，即可访问 SD 卡内容的问题。安全专家表示，目前这些漏洞会影响三个版本的 Wyze Cam 摄像头，其中第一个版本已经停产，因此不会收到解决上述漏洞问题的安全更新。这意味着，正在使用且未来继续使用第一个版本的 Wyze Cam 摄像头将会一直处于风险之

中，安全性无法得到保证。这对正在很多用户都将会是一个灾难，尤其是家庭用户，他们所有的隐私都有可能被黑客窃取。因此，Bitdefenders 表示，家庭用户应密切关注物联网设备，并尽可能将它们与本地或访客网络隔离开来。这可以通过专门为物联网设备设置专用 SSID 来完成，或者如果路由器不支持创建额外的 SSID，则将它们移动到访客网络。

出 处：https://securityaffairs.co/wordpress/129677/hacking/wyze-cam-flaws-allow-takeover.html

■ IT 服务巨头遭勒索软件攻击，损失超 4200 万美元

近期，西班牙一家领先的业务流程外包 (BPO) 服务提供商表示，因遭遇勒索软件攻击导致其损失超过数千万美元。作为全球前五的客户关系管理 (CRM) 和 BPO 提供商，Telefonica Atento 在拉丁美洲拥有强大的基础。然而去年 10 月，它声称其巴西子公司 IT 系统遭遇了“网络攻击”。不过公司已经第一时间做出了响应，“快速识别”出威胁、且隔离受影响的系统并暂停与客户的连接。虽然公司表示在之后的 24 小时内，服务开始恢复在线，不到一周后，数据中心的运营已经恢复。然而近期发布的 2021 财年财务报告显示，勒索攻击对公司的影响比最初想象的要大得多。根据报告可以得出，由于“巴西业务中断”，第四季度收入损失了 3480 万美元，另外还有 730 万美元用于与攻击相关的“保护、检测和补救措施”。Atento 的首席财务官兼首席执行官在一份联合声明中说，“与当今时代的许多公司一样，包括一些世界技术领导者，我们受到了网络攻击，这当然也影响了我们第四季度的业绩。该事件的复杂性和对我们的影响，都远大于我们的预期。据当地报道，该公司没有向勒索者付款，而发起勒索攻击的黑客组织据说是近期高调的 LockBit 组织。对此，Atento 声称已经设立了最佳的应对方案，除了提高其保护、检测和补救能力——包括与 CrowdStrike 和 Mandiant 签署的新协议，现在正与“防御团体和机构”更密切地合作，以提高应对威胁的准备。不过，基于近期勒索事件频发，Atento 也会被添加到勒索软件攻击后遭受极高损失的公司名单中，名单中包括法国 IT 服务公司 Sopra Steria(6000 万美元)、铝业巨头 Norsk Hydro(4100 万美元) 和 IT 服务公司 Cognizant(7000 万美元)。

出 处：https://www.infosecurity-magazine.com/news/services-42m-fallout-ransomware/

■ 黑了微软、三星、英伟达的神秘黑客组织曝光，背后竟是 16 岁英国少年，还招内鬼帮忙

大数据文摘出品之前，一个神秘的黑客组织攻击了微软、英伟达和三星，轰动一时。这个组织名为 Lapsus$，在攻击了英伟达和三星后，还将一些数据公布于众，很多人都在猜测这个神秘黑客组织的身份，现在这件事有了眉目。网络安全研究人员调查了一系列和 Lapsus$ 有关的攻击事件，发现攻击源竟然来自一名 16 岁的少年，他住在英国牛津附近的母亲家中。彭博社报道，代表被攻击公司调查黑客组织 Lapsus$ 的四名调查人员表示，他们认为这名少年是主谋。并且，该组织还在招募大公司内部人员作为攻击的卧底。

出 处：https://netsecurity.51cto.com/article/705583.html

■ 苹果发布紧急补丁以修复被积极利用的零日漏洞

近日，苹果发布了一个紧急安全补丁，以解决两项被积极利用以入侵 iPhone、iPad 和 Mac 的零日漏洞。这两项漏洞均由匿名研究人员发现并报告，苹果公司表示在 iOS 15.4.1、iPadOS 15.4.1 和 macOS Monterey 12.3.1 的发布中已解决了该两项漏洞，并建议用户尽快安装安全更新。除此之外，苹果方面没有透露任何关于在这些漏洞被如何利用的具体细节。第一项漏洞是存在于英特尔显卡驱动程序中的超权限读取问题，追踪代码为 CVE-2022-22674，该漏洞允许恶意应用程序读取内核内存。这一漏洞的积极利用引起了苹果公司的注意，公司最近发布的一份报告中称，超权限读取问题可能会导致内核内存的泄

露。在报告也同时提到了公司的对应建议：“可以通过改进的输入验证来解决该漏洞。”第二项漏洞是一个越界写入问题，影响 AppleAVD 媒体解码器，追踪代码为 CVE-2022-22675。该漏洞同样允许恶意应用程序读取内核内存，从而使应用程序能够使用内核特权执行任意代码。对此，报告给出建议：“通过改进的边界检查可以解决越界写入问题。”其实，自 2022 年 1 月以来，苹果公司已经解决了三个被积极利用的零日漏洞。1 月，公司解决的两项零日漏洞追踪代码分别为 CVE-2022-22587 和 CVE-2022-22594，攻击者可以利用其在受攻击的设备上运行任意代码。2 月，解决的是 WebKit 中一个影响 iOS、iPadOS、macOS 和 Safari 的零日漏洞，追踪代码为 CVE-2022-22620，可以通过处理恶意制作的网页内容触发，从而导致任意代码执行。

出　处：https://securityaffairs.co/wordpress/129672/security/apple-emergency-patches-zero-days.html

■ “透明部落”APT 组织正在大肆攻击印度官员

据 The Hacker News 消息，具有巴基斯坦国家背景的，名为“透明部落 (Transparent Tribe)”的 APT 组织，正在利用一个基于 Windows 的 CrimsonRAT 远程访问木马大肆发起网络攻击活动，目标直指印度官员。思科 Talos 安全研究人员表示，“自 2021 年 6 月以来，透明部落在印度网络空间中一直非常活跃，他们攻击的主要目标是阿富汗和印度的政府官员、军事人员等，此次攻击活动让他们离这一目标更近一步，且已经建立起了向核心目标发起长期网络攻击的准备。”2016 年 2 月，ProofPoint 首次发现了透明部落 APT 组织，其 IP 地址位于巴基斯坦，具有明显的政府色彩。该组织运用了网络钓鱼、水坑攻击、远程访问木马等多重复杂手段，向印度驻沙特阿拉伯和哈萨克斯坦使馆的外交官和军事人员发起攻击。如今，透明部落再一次活跃了起来。2022 年 2 月，高级持续性威胁扩展了其恶意软件工具集，通过名为 CapraRAT 的后门入侵 Android 设备，该后门与透明部落使用的 CrimsonRAT 木马高度“交叉”。在报告中，思科 Talos 详述此次攻击活动，在新一系列的攻击中，黑客利用“伪装成合法政府和相关组织的虚假域来传播恶意软件的有效载荷，包括一个基于 python 的存储器，用于安装基于 .NET 的网络侦察工具和 RATs，以及一个基于的 .NET 的植入木马，以便在受感染的系统上运行任意代码。”除了不断优化部署策略和恶意功能外，透明部落还大力发展各种交付方法，例如模拟合法应用程序安装程序、存档文件和武器化文档的可执行文件，以便更好地针对印度官员和军事人员。其中一个下载器可执行文件伪装成 Kavach(在印地语中意为“盔甲”)，这是一种印度政府强制要求的两因素身份验证解决方案, 用于访问电子邮件服务, 以传递恶意工件。透明部落还使用了以 COVID-19 为主题的诱饵图像和虚拟硬盘文件 (又名 VHDX 文件)，它们被用于远程命令和控制服务器 (例如 CrimsonRAT)，用于收集敏感数据并建立对受害者网络的长期访问权限。思科 Talos 安全研究人员表示：“透明部落正在使用多种类型的运载工具，和可以轻松修改以进行敏捷操作的新型定制恶意软件，表明该组织具有攻击性、持久性、敏捷性，更重要的是，他们还在不断进行发展和优化，值得引起相关人员的警惕。”

出　处：https://thehackernews.com/2022/03/new-hacking-campaign-by-transparent.html

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