全球数据安全观察

总第 101 期 2022 年第 29 期

(2022.08.08-2022.08.14)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、银保监会发布《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》

8 月 9 日，银保监会办公厅近日向各银保监局，各大型银行、股份制银行、外资银行、直销银行、理财公司，各保险集团（控股）公司、保险公司下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》。

银保监会披露的银行保险机构侵害个人信息权益乱象主要包括个人信息收集、个人信息存储和传输、个人信息查询、个人信息使用、个人信息提供、个人信息删除以及第三方合作等 7 类，本次专项整治工作将通过自查整改、监管抽查、总结汇报三个阶段推动落实。

https://mp.weixin.qq.com/s/JGLqC0RrGpLWki9ewEIqdQ

2、科技部等六部门印发《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》

近日，科技部、教育部、工业和信息化部、交通运输部、农业农村部、国家卫生健康委六部门发布《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》。

意见提出在加强人工智能场景创新要素供给中，应采用

区块链、隐私计算等新技术，在确保数据安全的前提下，为人工智能典型应用场景提供数据开放服务。加强“数据底座”的安全保护，对个人信息、商业秘密、行业重要数据等依法予以保护。

http://www.gov.cn/zhengce/zhengceku/2022-08/12/content_5705154.htm

3、江苏开展网络安全行动，排查三类（基础电信、互联网、工业互联网）企业数据安全隐患

8 月 11 日，“铸盾 2022”江苏省信息通信行业网络与数据安全检查专项行动启动。

通过对基础电信企业、互联网企业、工业互联网企业的网络资产进行网络和数据安全的集中排查，帮助企业及时堵住漏洞、消除隐患，继续强化安全意识，筑牢我省网络与数据安全防线。

http://www.jiangsu.gov.cn/art/2022/8/12/art_60096_10572549.html

4、上海经信委印发 《2022 年上海市公共数据开放重点工作安排》，加快推进公共数据开放

为加快落实《要素市场化配置综合改革试点总体方案》

《十四五大数据产业发展规划》《上海市数据条例》等国家和本市有关部署，上海市经济信息化委发布《2022 年上海市公共数据开放重点工作安排》的通知。

以全面畅通公共数据开放渠道，全面激活社会用数活力，全面赋能城市数字化转型为目标，推动公共数据开放机制巩固深化，制定公共数据开放细则，优化完善清单开放、分级分类、协议开放等工作机制。开放服务质量有效提升，构建以需求为导向的开放数据治理机制，公共数据及时更新率达90%以上，新增建设 100 个高质量数据集，建立样本开放数据集 1000 个。开放渠道安全有序，建立需求征集与场景规划互通渠道，平均公共数据开放申请受理时间不超过 5 个工作日。融合应用创新成效显著，持续深化大数据普惠金融 2.0，加快推进公共数据开放与开发利用示范项目建设和推广，新增建设 10 个试点项目。

https://mp.weixin.qq.com/s/rV2nJ37rlkMZhfusIY49Ng

5、《哈尔滨公共数据开放管理办法》公开征求意见，全市将建设公共数据开放统一平台

为进一步强化哈尔滨公共数据管理，扩大开放规模，提高数据质量，提升政府公共服务水平，哈尔滨市工信局制定拟正式出台《哈尔滨市公共数据开放管理办法》。《办法》其

中提到:

（1）公共数据开放将遵循“统筹管理、依法采集、统一标准、有序开放、便捷高效、安全可控”原则。

（2）**开放的公共数据实行统一目录管理，实现“应开尽开”。**对非涉密但涉及敏感信息的公共数据，由各区县（市）政府、市级各公共管理和服务机构按照国家有关规定，进行脱敏、清洗后无条件开放。

（3）**全市将建设公共数据开放统一平台。**各区县（市）政府、市级各公共管理和服务机构应当通过市开放平台提供公共数据开放服务，原则上不再新建独立的公共数据开放渠道。已经建成的公共数据开放渠道，应当按照有关规定进行整合、归并，将其纳入市开放平台。公民、法人和其他组织可通过市开放平台对公共数据的开放范围提出需求和建议。

https://mp.weixin.qq.com/s/KzL6EO7-Vc2TUKCTHQqPew

6、中国互联网协会发布《金融场景隐私保护计算平台技术要求与测试方法》团体标准

8 月 5 日中国互联网协会发布《金融场景隐私保护计算平台技术要求与测试方法》团体标准。

标准中提出了联邦学习参考架构、多方安全计算参考架构、可信执行环境参考架构，并从隐私保护计算能力、金融

场景应用能力、原理架构安全能力、平台管理能力等方面明确金融场景隐私保护计算平台的技术要求，同时提出了针对上述技术要求的测试方法。

https://www.isc.org.cn/article/13429117682839552.html

技术、产品与市场

1、IDC：2021 年中国数字政府大数据管理平台市场规模达 49.6 亿元

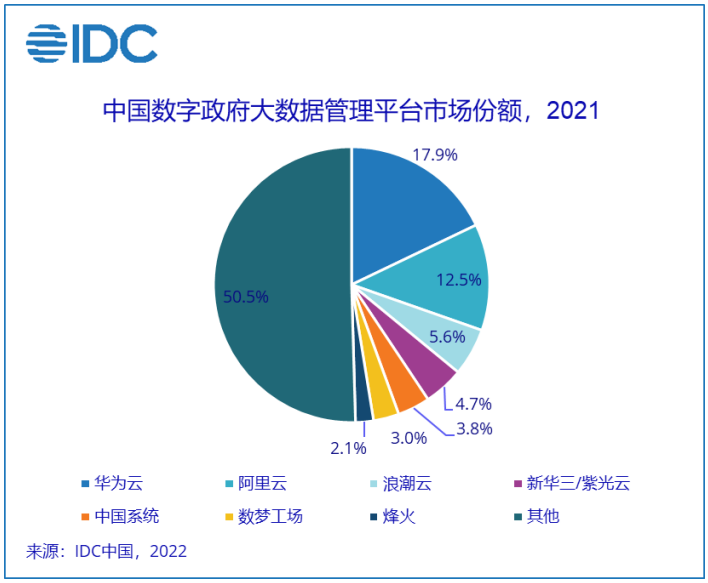
近日，IDC 发布了《中国数字政府大数据管理平台市场份额，2021》报告，报告显示，2021 年中国数字政府大数据管理平台整体规模达 49.6 亿元人民币，年复合增长率 25.3%，处于稳步增长阶段。

大数据管理平台支撑了城市运行管理指挥中心、城市治理一网统管、政务服务一网通办、城管网格化管理、智慧交通、智慧水务、智慧应急等典型场景。尤其是在疫情期间，健康码的频繁使用对大数据管理平台的稳定性、实时性、大容量提出了更高的要求。随着政务服务质量提升及安平方面的需求，对数据实时性、智能化、安全性要求越来越高。同时，大数据平台技术领域也在持续迭代演讲，如大数据 AI 一体化、跨域协同计算、可信联邦计算、轻量化部署等，这些

技术在数据加工、数据共享、业务支撑等不同层面促进政务领域的数据开发利用。

2021 年中国数字政府大数据管理平台整体规模达 49.6 亿元人民币，年复合增长率 25.3%，处于稳步增长阶段。从竞争格局来看，华为云、阿里云和浪潮云在 2021 年中国数字政府大数据管理平台市场排名前三，新华三/紫光云、中国系统、数梦工场和烽火分列第四到第七位。同时，联通数科、软通智慧、星环科技和中兴等企业都是此领域重要的参与者。

建议相关技术提供商在大数据平台建设时覆盖省市县三级，支持大数据平台的集约化建设。



https://www.secrss.com/articles/45703

2、数字中国发展报告：浙江数字化综合发展水平居全国第一

国家互联网信息办公室发布《数字中国发展报告（2021

年）》。《报告》显示，浙江、北京、上海、广东、江苏、山东、天津、福建、湖北、四川等地区数字化综合发展水平位居全国前 10 名。

《报告》指出，这些地区高度重视数字化发展整体部署和统筹推进，制定实施本地区数字化发展的整体战略规划，持续巩固数字基础设施优势，大力培育引进创新力量，积极运用数字思维、数字技术推进政府体制机制、组织架构、方式流程优化变革，不断丰富数字社会惠民为民服务，深入推进区域数字化转型发展，有力支撑经济社会高质量发展。其中，浙江全面推进数字化改革，加快建设“数字长三角”，加快公共数据资源开发利用，持续优化数字惠民服务，推动经济社会数字化转型和省域治理体系和治理能力现代化。

https://mp.weixin.qq.com/s/QBe2rxPPDxrNKMQxcGtLNg

3、《2022 中国大数据产业发展地图暨中国大数据产业发展白皮书》：隐私计算呈现多元化发展态势，将在金融、政务等领域落地应用

8 月 3 日由大数据产业生态联盟联合赛迪顾问、赛迪智库、《软件和集成电路》杂志社共同编制的《2022 中国大数据产业发展地图暨中国大数据产业发展白皮书》（以下简称《白皮书》）同步重磅发布。白皮书指出：大数据发展持续演

进，激活数据要素价值成为产业关注焦点，隐私计算呈现多元化发展态势，将在金融、政务等领域落地应用。

总体看，隐私计算技术呈现多元化发展态势，包括多方安全计算、联邦学习、可信执行环境、同态加密等不同的技术路线，但商业环境尚未成熟，整体上市场还有很大上涨空间。当前，隐私计算发展呈现三大特点；**一是市场处于蓬勃发展的早期阶段，竞争格局尚未确定；二是产业发展环境、发展配套正在逐步完善；三是商业模式仍需进一步探索。**近年来，我国出台多项政策支持隐私计算发展，市场关注热度持续提升，未来几年国内隐私计算市场将迎来快速发展期。

在金融领域，金融机构借助隐私计算技术可以安全合规与相关机构打通数据，解决单个金融机构数据维度单一的问题，更加全面地分析客户情况，交叉验证相关业务背景，开展智能风控、智能营销、智能运营等业务，通过上下游间数据的安全联合统计分析提供更加完善的供应链金融服务。

在政务领域，使用隐私计算技术融合政府和企业数据进行联合统计、联合建模，推进政务数据开放共享，帮助政府精准施策，推动数据交易，让政府部门掌握的数据在保证安全的前提下，最大限度服务社会。

在医疗领域，利用隐私计算技术可实现医学数据跨机构安全匹配、安全统计、安全分析，从而助力医学联合科研、

基因关联分析、跨国联合研究和影像深度分析等。

在互联网领域，通过打通不同企业掌握的用户数据，可以建立更加立体的用户画像，制定更加精准的营销策略；通过联邦学习丰富数据库，可构建更加立体的反作弊模型，高效且合规合法识别流量质量，也可对广告效果联合归因分析。

https://mp.weixin.qq.com/s/g0gY605wnHbkMI-56C6uag

4、IDC：2026 年中国网络安全市场规模将超 318 亿美元

IDC 于近日发布了 2022 年 V2 版 IDC《全球网络安全支出指南》(IDC Worldwide Security Spending Guide)。该指南从技术、垂直行业、终端用户企业规模等多个维度回顾了 2021 年中国网络安全（Cybersecurity）市场，同时预测了市场未来五年（2022-2026）的发展情况。IDC 数据显示，2021 年全球网络安全 IT 总投资规模为 1687.7 亿美元，并有望在 2026 年增至 2875.7 亿美元，五年复合增长率（CAGR）为 11.3%。聚焦中国市场，2026 年中国网络安全 IT 支出规模将达到 318.6 亿美元，全球占比约为 11.1%，五年 CAGR 约为 21.2%。中国网络安全市场增速持续领跑全球，五年 CAGR 近全球两倍，市场前景广阔。

https://www.secrss.com/articles/45670

5、英特尔处理器曝新型架构漏洞 AEPIC Leak：可导致机密数据泄露

多所大学和企业组成的研究团队发现了一种新型的英特尔 CPU 攻击，可导致攻击者获取潜在敏感信息。

研究团队由罗马大学、奥地利格拉茨技术大学、CISPA 德国赫姆霍茨信息安全中心和亚马逊 Web 服务组建而成。这种新型攻击方法被称为“AEPIC Leak”，和高级可编程中断控制器 (APIC)有关。这个集成的 CPU 组件负责接受、优先排序和调度处理器中断。当该组件处于 xAPIC 模式时，可通过 MMIO 页面访问 APIC 寄存器。

为最近侧信道攻击发布的缓解措施并无法防御 AEPIC Leak 攻击。英特尔已推出微码更新和 SGX SDK 补丁修复该

漏洞。

https://www.secrss.com/articles/45681

业界观点

1、李凤华：隐私数据共享和泄露间的矛盾永恒存在，隐私计算必将越来越成熟

中国中文信息学会大数据安全与隐私计算专委会主任委员、研究员李凤华是国际上率先提出隐私计算（Privacy Computing）的学者，他在接受 21 世纪经济报道记者专访时表示，当前，国内个别机构、少数企业为了蹭“隐私计算”热度，将密码学领域学者提出的同态加密、安全多方计算等技术纳入隐私计算范畴，误导大家认为所谓的隐私计算技术存在对算力要求过高等问题，同时隐藏了这些技术只适用于局部场景的隐私保护缺陷，并没有普适性地、全生命周期地保护好隐私数据。

隐私计算涵盖了信息搜集者、发布者和使用者在信息产生、感知、发布、传播、存储、处理、使用、销毁等全生命周期过程的所有计算操作，并包含支持海量用户、高并发、高效能隐私保护的系统设计理论与架构。同态加密、安全多方计算等密码学领域学者提出的技术并不属于隐私计算。这

些技术只适用于局部场景的隐私保护，并没有普适性地、全生命周期地保护好隐私数据；同时还误导大家，引发了所谓的隐私计算技术对算力要求过高等问题。

隐私计算未来需要从六个方面完善和发展：一是要研究隐私计算的基础理论，包括隐私计算模型、安全保障模型、隐私计算的数学基础等；二是隐私智能感知与动态度量，包括包含文本、图片、视频等多模态数据的隐私信息抽取与感知、适应不同场景的隐私动态度量、隐私度量的量化指标等；三是隐私保护算法，包括隐私脱敏的基本操作算法、隐私保护算法框架、隐私保护算法的保护能力量化指标等；四是隐私保护效果评估，包括效果评估指标、效果评估自动化、基于大数据隐私挖掘的隐私保护效果评估等；五是隐私侵权行为判定与溯源，包括侵权行为判定方法、隐私信息流转全过程的审计和存证机制、隐私信息流转的延伸控制机制、隐私侵权行为的追踪溯源等；六是隐私信息的完备删除，包括隐私信息传播过程中多副本的完备发现、删除指令的通知与确认，删除效果评估等。

https://www.wangan.com/p/7fy78y1c75a8de27

2、袁燕龙：打造安全可信存储，守护数据安全的最后防线

7 月 28 日，由中国信息通信研究院（以下简称“中国信

通院”）安全研究所主办、数据安全共同体计划、大数据应用及安全创新实验室承办的“数据安全峰会 2022”在京成功召开。

华为技术有限公司数据存储产品线副总裁、首席安全官袁燕龙分享了华为如何构建数据安全的“三不两永远”目标，让数据始终处于保护且合规使用的状态，并提出对于数据安全保护意识应该以标杆示例，让企业和使用者能体会到数据安全建设带来的价值。

同时，袁燕龙倡议落实数据分级分类保护体系，建设“存、算、备”均衡的新型数据中心；加快数据存储的可信安全认证和测评机制，数据作为关键生产要素，做好数据保护才能更好的保障我国数字经济的高速、平稳、健康发展。

https://topics.gmw.cn/2022-08/10/content_35945534.htm

3、秦海林：中小微企业如何应对数字安全挑战

近日，工信部赛迪研究院研究员秦海林就中小微企业如何应对数字安全挑战主题参加了专访。

秦海林表示，中小微企业在数字化转型中，一方面要面临企业“上云”带来的外部环境风险，以及数字化升级后部门管理方法陈旧、对数字化理解不深、思想意识薄弱带来的

内部管理风险，另一方面要面临着恶意软件入侵、勒索病毒攻击、数据泄露、邮件或者钓鱼网站等软硬件，以及数据篡改和泄露带来的技术风险。伴随着云计算等技术的不断发展，数字化转型加速推进，中小企业的数字安全风险将不断增加，特别是数据泄露等风险问题将更加突出。

他认为，面对数字安全挑战，中小微企业与大型企业相比，风险重点源于以下几个方面：一是安全意识薄弱，重视程度不够。二是在数字安全方面，中小微企业资金投入、建设基础和后期运营管理都存在较大不足。三是数字化转型不是一次性投入，数字安全也不是一次性投入，需要长期运营维护，大部分中小微企业没有专业运维人员，后期运营维护问题较大。

秦海林建议提升中小微企业的数字安全能力要做好以下两方面工作：从**意识端**来看，加强中小微企业对数字安全的重视程度，通过增加安全专业培训，让企业从认知上清楚，在数字经济时代，未来数字安全问题会不断增加，风险会不断加大，要做好数字安全防范工作。从**技术端**来看，中小微企业不同于大企业，在数字化转型中，面临的数字安全问题主要是以合规和满足安全的基本要求为主，因此结合不同中小微企业的特点和目前“云”的布局和发展，研发出轻量化、低价格平台型产品是破题关键；从安全运维方面，要结合中

小微企业安全运维人员缺乏甚至缺失的问题，提出云服务的服务模式。

http://theory.people.com.cn/n1/2022/0811/c40531-32499898.html

4、专家建议制定数据安全基线要求和标准

8 月 4 日下午，中国信息通信研究院（以下简称“中国信通院”）安全研究所联合中国互联网协会数据安全与治理工作委员会举办“数据要素安全治理”系列学术沙龙第一期—“数据要素市场化背景下数据安全新挑战”研讨会。

专家普遍表示，现阶段企业数据流通场景仍以业务运营合作为主，企业数据流通安全保障中主要面临以下挑战：一是数据流通中非结构化数据体量较大，自动化识别难度高，分类分级管理措施难以落地；二是数据流转场景增加，多方主体参与，安全可控性降低，加剧数据泄露风险；三是数据流通链路复杂，安全责任难以清晰划分。

与会专家建议，在数据要素流通过程中，应平衡好数据流动与数据安全的关系，加强法律法规和配套标准的落地和细化，针对不同企业和不同应用场景，制定数据安全基线要求和标准，明确数据流通中各数据主体的安全责任，加强关键数据安全技术产品测评和认证，共同推进数据要素安全有

序流通。

http://www.ourxun.com/fk/2022/0809/1000031921.html

5、专家：智能学习硬件产品规范和安全使用不可忽视

近日，有网友发帖称，“暑假期间一学校专为学生发放了‘点阵笔’，并要求必须用这支笔来写暑假作业，学生的书写数据将由该笔实时传输给老师。”

江苏理工学院计算机工程学院范洪辉教授认为：“对教学质量进行有效和个性化的评价是基于大量精准、完整、规范的数据。从数据收集、分析和整理的角度，引入人工智能技术手段，有利于促进教育教学评价的开展。然而，人工智能技术的潜在危险是数据泄露的风险，还需要进一步的标准化、提前安排和慎重处理。”

范洪辉建议，政府相关职能部门要及时制定有关的政策和法规，来规范智能学习硬件的市场，并要加强监督与管理，对于有风险的智能学习硬件产品及时发布预警信息，避免造成重大危害。

江苏理工学院计算机工程学院何胜教授表示，智能学习硬件产品不可避免搜集学生个人信息，应该从多方面和多渠道来保证智能学习硬件的规范和安全使用。学校在购买智能学习硬件时，要通过正常渠道招标购买，并对购买的设备进

行详细的安全论证。同时，学校要加强对教师安全意识方面的培训。

https://news.voc.com.cn/article/202208/20220814122001719219.html

数据安全事件

1、网络巨头思科遭数据勒索：VPN 访问权限被窃取，2.8GB 数据泄露

2022 年 8 月 10 日消息，恶意黑客声称窃取到思科 2.75GB 数据，约 3100 个文件，其中不少文件为保密协议、数据转储和工程图纸。攻击者窃取一名员工的谷歌账号，通过浏览器同步的账密获得了思科内网 VPN 账号，利用复杂语音钓鱼电话获得了该员工的二次验证码，从而进入内网实施窃密；思科公司证实，“阎罗王”（音译，原名 Yanluowang）勒索软件团伙在今年 5 月下旬入侵了其企业网络，攻击者还试图公布被盗文件以要挟索取赎金，少量非敏感数据泄露，并公布了攻击过程复原。

https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

2、LockBit 团伙攻击阿根廷卫生服务网站并勒索 30 万美元

2022 年 8 月 9 日称，LockBit 团伙攻击了阿根廷的 OSDE。OSDE 是阿根廷的医疗服务和供应商网络，目前拥有超过 200 万会员、8000 多家药店和近 400 个中心。据悉，这次攻击导致 OSDE 在几个小时内无法使用。OSDE 在 6 月 27 日承认了此次攻击，但没有确认这是一起勒索攻击事件。7 月 22 日，LockBit 将 OSDE 添加到其数据泄露网站，并勒索 300000 美元来购买或删除所有被盗数据，截止日期为 8 月 6 日。8 月 8 日，LockBit 回复了 DataBreaches 的询问，称其窃取了 139.07 GB 文件。

https://www.databreaches.net/argentinian-health-services-plan-hit-by-lockbit/

3、因在收集个人位置数据方面误导用户，谷歌在澳大利亚被罚款约 4 亿元

2022 年 8 月 12 日消息，据澳大利亚联合通讯社报道，在与澳大利亚竞争监督机构的法律斗争中，谷歌已经同意支付 6000 万美元（约 4.04 亿元人民币）的罚款，原因是该科技巨头在收集个人位置数据方面误导了用户。

去年 4 月，澳大利亚联邦法院发现谷歌违反了消费者法律，误导一些用户相信该公司没有通过安卓操作系统的移

动设备收集有关他们位置的个人数据。当用户的位置记录被设置为“关闭”，但他们在网络和应用程序上的活动是“启用”的，并且正在使用其应用程序时，谷歌会继续收集和访问位置数据。

在澳大利亚联邦法院举行的简短听证会上获悉，双方已就 6000 万美元的罚款达成了“公正合理”的共识。

https://www.ithome.com/0/634/711.htm

4、因违反 GDPR 或被罚六千万欧元，法国广告巨头回应称坚决反对

2022 年 8 月 9 日报道，近日，致力于全球隐私保护的非政府组织“隐私国际”（Privacy International）在推特上透露，法国数据保护监管机构（French Data Protection Authority，CNIL）在接受其起诉并展开调查两年后，认定法国广告巨头 Criteo 违反了欧盟《通用数据保护条例》（GDPR）的相关规定，计划对 Criteo 处以约 6000 万欧元的罚款。其后，Criteo 方回应称该拟议处罚与指控罪名不匹配，坚决反对调查结果。

作为一个广告平台，Criteo 为营销人员和发行商提供包括客户获取、受众匹配、广告分析和设计等服务，其声称可获取 72%全球在线消费者的身份信息和偏好数据，拥有超过 14 亿月度活跃消费者的分析数据。“隐私国际”提交的诉状

显示，Criteo 等公司收集、传输、处理个人数据过程的透明度很低，“人们不知道谁在处理他们的数据，如何处理以及出于什么目的处理。”此外，Criteo 的自动化决策过程不透明，其擅自通过行为跟踪和数据处理生成用户画像并推送个性化广告的行为缺乏法律依据。诉状认为，这些行为违反了 GDPR 的多项核心原则。

https://www.secrss.com/articles/45606

5、全国第一案！一科技公司因侵害儿童个人信息被判赔 150 万最高检发布涉及互联网企业数据合规典型案例

2022 年 8 月 18 日，作为全国第一家集中审理涉网案件试点法院的杭州互联网法院，将迎来成立 5 周年的日子。其中，全国首例儿童个人信息、网络安全保护民事公益诉讼案，引起了大家的关注。

在一起猥亵儿童刑事案件中，公益诉讼起诉人发现，某科技公司运营的短视频 APP，存在侵害众多不特定儿童个人信息的侵权行为。

这一短视频 APP 没有对儿童用户采取区分管理措施，默认用户点击“关注”后，就可以和儿童账户私信联系，获取地理位置、面部特征等个人信息。在没有征得儿童监护人授权同意的情况下，运用后台算法，向具有浏览儿童内容视频

喜好的用户直接推送含有儿童个人信息的短视频，从而让犯罪分子有机可乘。

https://www.163.com/dy/article/HEE8OSE90514CN9Q.html

6、Twilio 透露其员工遭到钓鱼攻击，导致客户数据泄露

2022 年 8 月 8 日消息，云通信公司 Twilio 部分客户的数据已经泄露。Twilio 表示，他们在 8 月 4 日发现其员工遭到了复杂的钓鱼攻击后凭据泄露，然后攻击者利用窃取的凭据访问了公司的内部系统，以及部分客户的数据。攻击者冒充 Twilio 的 IT 部门，要求目标点击包含 Twilio、Okta 和 SSO 关键字的 URL，并将他们重定向到伪造的 Twilio 登录页面。Twilio 已撤销了攻击期间被盗的员工账户，但尚未确定攻击者身份，目前正在与执法部门合作对此事展开调查。

https://securityaffairs.co/wordpress/134147/data-breach/twilio-discloses-data-breach.html

7、调查发现全球超 9000 台 VNC 服务器存暴露风险

2022 年 8 月 14 日报道，研究人员通过调查发现了至少 9000 个暴露的 VNC（虚拟网络计算）端点，这些端点能在没有认证的情况下进行访问，从而使攻击者能够轻松进入内部

网络。

VNC（虚拟网络计算）是一个独立于平台的系统，旨在帮助用户连接到需要监控和调整的系统，通过网络连接的RFB（远程帧缓冲协议）提供对远程计算机的控制。

“攻击者可能会滥用 VNC，以登录用户的身份进行恶意操作，如打开文档、下载文件和运行任意命令，"一位 Cyble 研究员表示道“攻击者可以利用 VNC 来远程控制和监控一个系统，以收集数据和信息，从而向网络内的其他系统进行渗透。”

https://www.freebuf.com/news/341900.html

8、黑客正在从分类信息网站上窃取信用卡

2022 年 8 月 10 日，据 Bleeping Computer 网站披露，新加坡正在发生一场新的信用卡窃取活动，攻击者通过精心设计的网络钓鱼伎俩，“抢夺”分类网站上卖家的付款信息。更糟糕的是，攻击者还试图利用银行平台上的一次性有效密码（OTP）将资金直接转入其账户上。

Classicscam 是一个全自动的“诈骗即服务”平台，一般以分类网站用户（这些用户试图出售或购买网页上所列物品）为主要攻击目标。除此之外，该诈骗计划还针对银行、加密货币交易所、快递公司、搬家公司和其他类型的服务提供商，

侧面反映了其目标范围甚广。据悉，Classicscam 主要依靠其 Telegram 频道（目前依旧有 90 个活跃频道）进行诈骗宣传和运营协调，自 2019 年以来，估计已经造成了超过 2900 万美元的损失。

https://www.wangan.com/p/7fy78y7b6d06d7aa

9、PlatformQ 暴露 100,000 名美国医护人员的个人数据

2022 年 8 月 9 日，据外媒报道，VPNOverview 安全研究团队发现了一起数据泄露事件，该事件可能危及在美国各大医院工作的近 100,000 名医生、护士和其他医疗保健专业人员。

PlatformQ 是医疗保健和教育行业的数字解决方案提供商，其在无意中发布了存储在配置错误的 AWS S3 存储桶中的数据库备份。根据调查结果，安全研究团队发现了存储在备份数据库和数千个其他文件中的大量敏感个人数据，这些信息与某种用于治疗和预防胃溃疡的仿制药的营销有关。泄露的敏感信息包含美国各地医院的医生、护士和其他医护人员的全名、电子邮件地址、职称、工作地址、电话号码、医护标识符 (NPI) 编号等。

https://vpnoverview.com/research/platformq-exposes-personal-info-of-nearly-100000-us-healthcare-workers/?web_view=true