全球数据安全观察

总第 103 期 2022 年第 31 期

(2022.08.22-2022.08.28)

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
1、中国证监会、财政部与美国监管机构签署审计监管合作协议.....1
2、交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》.....1
3、上海召开数据分类分级、制定重要数据目录试点工作会议.....2
4、广东省发布企业首席数据官建设指南，岗位职责涉及数据治理、数据增富、数字增值、数据安全、数据人才、数据文化.....2
5、烟台发布数据要素保障创新实施方案，加快推动数据要素市场化配置，建设完善山东数据交易平台烟台分平台.....3
技术、产品与市场.....4
1、IDC 发布 2022 年中国数据安全发展路线图.....4
2、《2022 年区域数字经济创新发展行动路线报告》：利用隐私计算技术，打造可信的数据融合环境.....5
3、微软：80%勒索软件攻击都是由于服务器错误配置导致5
4、我国将建权威可信数字身份链，加强个人数字身份认证.....6
5、美科技巨头收集了大量用户数据 其中 Google 追踪 39 种私人数据.....7
业界观点.....8
1、周汉华：继续完善细化法律制度，推动个人信息保护法更好实施.....8
2、张新宝：个人信息保护法落地可先抓大带小,重点治理大型平台企业.....9

3、专家观点：构建更安全的医保网络服务体系 10
4、隐私计算两个场景下的个人信息保护探讨——兼论匿名化问题 12
5、浅析金融业数据安全风险问题与应对策略 13
数据安全事件 14
1、因涉嫌未经同意收集人脸信息，Snap 以 2.4 亿元达成和解 14
2、法国首都一医院遭勒索软件攻击：急诊被迫停业 赎金 1000 万美元 14
3、希腊最大天然气运营商遭勒索软件攻击，多项在线服务被迫中断 15
4、LastPass 数据泄露：攻击者窃取了部分源代码 16
5、Plex 披露数据泄露并敦促重置密码 16
6、量子勒索软件攻击多米尼加共和国政府机构 17
7、数据库配置错误导致印度联邦警察和银行相关信息泄露 17
8、国际航空重要供应商遭勒索软件攻击，航空业已成为勒索主要目标 18
9、DoorDash 披露了与 Twilio 黑客有关的新数据泄露 19
10、两名快递员窃取近万条买家个人信息 19

政策形势

1、中国证监会、财政部与美国监管机构签署审计监管合作协议

近日，中国证券监督管理委员会、中华人民共和国财政部于 2022 年 8 月 26 日与美国公众公司会计监督委员会（PCAOB）签署审计监管合作协议，将于近期启动相关合作。

合作协议依据两国法律法规，尊重国际通行做法，按照对等互利原则，就双方对相关会计师事务所合作开展监管检查和调查活动作出了明确约定，形成了符合双方法规和监管要求的合作框架。

http://www.csrc.gov.cn/csrc/c100028/c5572328/content.shtml

2、交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》

8 月 26 日，为规范公路水路关键信息基础设施安全保护管理，落实关键信息基础设施安全保护工作责任， 交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》。

其中关于数据安全，重点提出“履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度”、“运营

者应当加强数据安全保护，明确重要数据和个人信息的保护措施，将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定执行”。

http://www.moj.gov.cn/pub/sfbgw/lfyjzj/lflfyjzj/202208/t20220826_462421.html

3、上海召开数据分类分级、制定重要数据目录试点工作会议

为促进数据共享应用，推进数据分类分级保护和重要数据目录制定工作，8 月 24 日，市委网信办、市政府办公厅（以下简称试点工作组）组织 16 家试点单位约 50 人召开数据分类分级、制定重要数据目录试点工作会议。

https://www.secrss.com/articles/46156

4、广东省发布企业首席数据官建设指南，岗位职责涉及数据治理、数据增富、数字增值、数据安全、数据人才、数据文化

近日，为贯彻落实国家和省有关工作部署，建设数据管理高端人才队伍，推动数字经济高质量发展，广东省工业和信息化厅组织开展了企业首席数据官专题调研，对 300 多家

企业开展了问卷摸查，广泛了解掌握国内外企业首席数据官建设情况，并形成了调研报告。广东省工业和信息化厅发布《建设指南》，主要包括建设原则、建设内容、保障措施等 3 大部分内容。其中岗位职责提到数据安全部分：贯彻执行国家数据等方面的法律、法规和政策，建立企业数据资产安全保障制度和分类分级安全管理制度，组织制定并实施企业数据安全防护方案，提升数据全生命周期安全防护能力。定期组织数据安全评估，组织基于供应链的数据安全监测，提高企业数据风险管控能力，确保企业数据隐私与安全。

https://mp.weixin.qq.com/s/JqNpfiL_9438DE-ZR5yplQ

5、烟台发布数据要素保障创新实施方案，加快推动数据要素市场化配置，建设完善山东数据交易平台烟台分平台

8 月 18 日，为深入贯彻《国务院办公厅关于印发要素市场化配置综合改革试点总体方案的通知》进一步激活数据要素潜力、挖掘数据要素价值，激发数字经济活力，提高全市数字化建设水平，山东烟台市发布数据要素保障创新实施方案。方案关于推进公共数据深度应用中提到：强化数据资源平台支撑，深入开展“数源”-“数治”-“数用”行动，持续促进和规范数据开放，加快推动数据要素市场化配置。

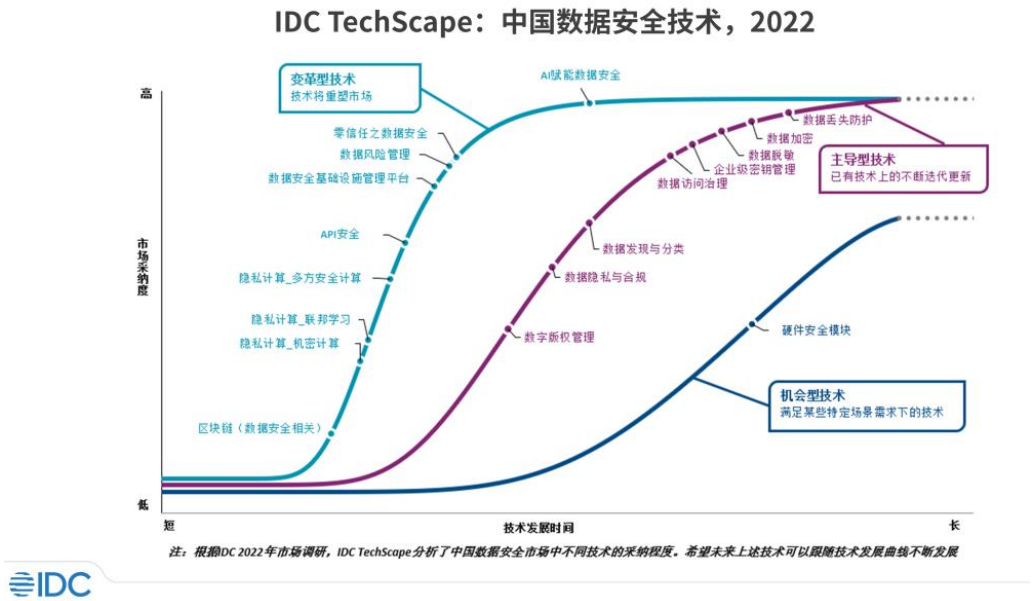
https://mp.weixin.qq.com/s/gBhP5eOo4zy7ljmWagY5mA

技术、产品与市场

1、IDC 发布 2022 年中国数据安全发展路线图

IDC 2022 CSO 全球网络安全峰会（中国站）在上海隆重开幕，会上首次发布**《IDC TechScape：中国数据安全发展路线图，2022》**。报告认为，帮助用户构建全方位数据安全治理体系将成为大趋势，各项数据安全和密码技术将在治理体系中作为重点能力模块，赋能用户实现数据安全治理目标。

本次发布的 TechScape 选取了 **18 个新兴及重要的数据安全技术**进行分析，并对数据安全技术的市场采纳度进行了可视化展示。此外，根据技术的市场影响以及各技术的发展阶段将技术分为**变革型技术**、**主导型技术**以及**机会型技术**三大类别，并给出了每项技术的三个推荐厂商。



https://www.secrss.com/articles/46255

2、《2022 年区域数字经济创新发展行动路线报告》：利用隐私计算技术，打造可信的数据融合环境

近日，华为、华信等联合发布了《2022 年区域数字经济创新发展行动路线报告》。如何加速推进区域数字经济创新发展？《报告》分析了区域数字经济创新发展面临的形势和挑战，并提出了区域数字经济创新发展的能力框架、行动路线、关键行动计划。报告指出：利用隐私计算技术，打造可信的数据融合环境。我国数字经济将进入区域加强统筹，加速落地推进的新阶段，但是仍面临着一些问题：一是数据治理水平有待进一步提高；一是数据治理水平有待进一步提高；三是缺乏场景化数据应用的标杆示范。数据治理的有力手段就是《报告》中提出的隐私计算技术，实现数据安全、数据利用的协同发展。

https://mp.weixin.qq.com/s/tI8I09FCQrC9zvKdx4pnrA

3、微软：80%勒索软件攻击都是由于服务器错误配置导致

Microsoft Security 博客官方发布的最新《Cyber Signals》报告指出，勒索软件即服务(RaaS)日益猖獗，**但是常规的软件设置就能应对，可以阻止大部分勒索软件攻击。**此外，报

告中还发现客户错误配置云服务、依赖不可靠的安全软件、通过默认宏设置流量勒索软件，这导致微软制造了某种勒索软件攻击，即人为操作的勒索软件。

在报告中指出："你可能会使用某个热门应用来实现某种目的，但是这并不意味着攻击者将其武器化以实现另一个目标。其中最为常见的是，应用的'经典'配置意味着它的默认状态，允许该组织内的任意用户进行广泛访问。不要忽视这种风险，也不要担心中断而更改应用设置"。

https://www.163.com/dy/article/HFMHETUG0511BLFD.html

4、我国将建权威可信数字身份链，加强个人数字身份认证

近日，国家重点研发计划中的"揭榜挂帅"榜单项目——由公安部第一研究所牵头的"基于法定证件的数字身份区块链技术研究与应用"正式启动并进入实施阶段。"长安链"作为区块链底层平台，将支持建设高性能分布式数字身份架构，为我国可信数字身份体系建设提供技术支撑。未来，日常出行、电子支付、公共服务等方面将更加便捷，个人隐私信息也将获得更好的保护。作为我国首个自主可控的区块链软硬件技术体系，"长安链"具备全自主、高性能、强隐私、广协作的优势，上链数据可追溯、不可篡改，支持高性能隐私计算，保护个人隐私信息安全。"长安链"作为典型的隐私

计算应用，它的落地将极大促进相关研究和产业的快速发展，通过网购平台、社交网络泄露个人信息的风险将大大降低。

https://mp.weixin.qq.com/s/-wZZx-lZb65l3mRLtpUMRg

5、美科技巨头收集了大量用户数据 其中 Google 追踪 39 种私人数据

数据隐私是当今数字世界中最令人担忧的问题。有多项关于这个话题的研究显示，科技公司收集了用户的大量敏感数据。虽然人们无法控制科技巨头收集数据的行为，但可以了解这些公司从用户身上收集了什么以及有多少种数据。而这正是 StockApps 的一份新报告所揭示的内容。

根据该报告，Google 从用户那里收集的数据最多，有 39 种。接下来是 Twitter，它搜集了 24 种数据。紧随其后的是亚马逊，它从用户那里累计了 23 类数据。当用户使用他们的平台时，Meta 拥有的 Facebook 会获取 14 种数据。排名最后的是苹果，它在 12 个不同类别中保存的数据量最少。

https://www.cnbeta.com/articles/tech/1308141.htm

业界观点

1、周汉华：继续完善细化法律制度，推动个人信息保护法更好实施

8 月 20 日，《中华人民共和国个人信息保护法》颁布已一年，中国社会科学院法学研究所副所长、中国法学会网络与信息法学研究会负责人周汉华针对如“大型互联网平台的四类义务，实践中如何判定违反四类应当承担的责任？如何判断对个人信息保护情况进行监督的独立机构的‘独立性’？……”等相关制度如何落地提出建议与看法。

一是继续完善细化法律制度。特别是通过制定司法解释、行政法规、部门规章或者地方性法规，推动《个人信息保护法》有关制度的落地。

二是通过案例推进法律实施。个人信息保护的场景较多，不同场景下法律适用规则可能不完全一样，因此可能暂时难以制定明确的、体系化的司法解释或实施细则。通过个案的执法、司法明确法律适用规则，也是推进《个人信息保护法》落地的重要途径。

三是期待国家网信办出台大型平台的具体认定机制和标准、动态发布被认定为大型平台的名单，并就大型平台社会责任报告提供具体指引目录。也可以结合实践中发布社会

责任报告的情况，适时选出最佳实践予以引导和推广。

https://m.21jingji.com/article/20220823/herald/7f87b9114bb1cdfb0db11053d946b934.html

2、张新宝：个人信息保护法落地可先抓大带小,重点治理大型平台企业

近日，在《中华人民共和国个人信息保护法》颁布一年之际，中国人民大学法学院教授张新宝指出，个人信息乱象的治理方面已经得到了改善，不过对于《个人信息保护法》的执法仍旧任重道远。“我觉得有两只猛虎：一是公权力；第二是大型平台。”个人作为单个主体的力量仍旧渺小，因此应警惕“猛虎”，他认为任何具备收集、处理个人信息的主体都应谨慎地行使权力。

张新宝在《个人信息保护法》对企业影响时提到：应“抓大带小”，以中等规模的企业为基础，先重点治理大型平台企业，小微企业的标准暂时放宽；相关部门接下来可以考虑是否制定关于个人行使查询、复制、删除等的相关指南。

关于后续落地《个人信息保护法》的推动抓手，张新宝提出三方面建议：

首先，过去做的很多工作仍需继续推进，比如对 App 的集中治理、常态化整治。

第二，要加强生物识别信息，比如人脸识别信息方面的监管，从装备设置、信息采集处理要全方面监管。算法推荐产生的问题仍然是需要治理的重点。

第三，在政府依法行使职权方面，把个人信息保护作为重要的内容，加强监督和处罚力度。大量个人信息掌握在政府手中，很多都是敏感个人信息，要加强对公权力的监管和约束。

http://www.21jingji.com/article/20220823/herald/6b31af2f44ec5a8f0665eaf92d57f98a.html

3、专家观点：构建更安全的医保网络服务体系

目前，全国统一的医保信息平台全面建成，拥有 13.6 亿参保人基础信息，并储存了众多医疗机构、药品信息、个人就医信息等，中央、省、市、县纵向打通，具备跨省就医、跨省结算功能，因此，该平台成为国内重要的关键信息基础设施之一，因此需从多个方面进一步深化与提升网络安全防护能力。

第一，强化网络安全法实施，提升运维安全能力建设。加快构建贯穿基础网络、数据中心、云平台、数据和应用等一体协同的全国统一医保信息平台网络安全防护体系。建立完善网络安全绩效评估体系和标准，提升网络安全运维管理

水平和应急处置能力，有效支撑全国统一的医保信息平台安全平稳高效运行。

第二，推动数据安全法落地，增强数据安全能力支撑。各级医保部门要强化网络和数据安全组织领导，压实安全责任，建立健全网络和数据安全保护规章制度。加强对各级医保平台构建统一的数据安全全生命周期防护体系，并实施重点保护。加强网络安全全域智能预警能力建设，实时监测系统运行情况，提升安全威胁信息汇集和研判能力，完善全域统一的网络和数据安全防护信息共享以及通报预警。

第三，加强关键信息基础保护，深化关键基础设施整体防御能力。加强关键核心技术应用，深入贯彻总体国家安全观，压实各方责任，持续推进安全制度体系建设。深化核心技术应用，定期开展安全检查，建立长效防御机制，确保医保信息系统安全稳定运行。

第四，夯实个人信息保护基础，持续加大投入力度。探索个人信息保护核心技术应用，逐步提升自主国产化率,；加强安全队伍建设和技术能力提升，定期开展医保数据安全检查；针对数据安全重点核心系统提升数据安全应急响应能力；建立各级网络安全防护团队，增加演习的多场景应用，逐步提升战略与战术团队整体应对能力。

http://chinasei.com.cn/zcjd/202208/t20220825_49484.html

4、隐私计算两个场景下的个人信息保护探讨——兼论匿名化问题

近年来，随着网络信息技术的迅猛发展及我国数据立法体系的不断完善，数据流通与数据保护间的张力日益突显。2019 年，党的十九届四中全会首次将数据列为新的生产要素；2021 年，国家发改委、中央网信办、工信部、国家能源局联合印发的《全国一体化大数据中心协同创新体系算力枢纽实施方案》提出，“试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率”；工信部在《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中提出，“推动联邦学习、多方安全技术、隐私计算、密态计算、安全检索、多阈协同追踪等数据安全技术研究应用”。另一方面，自 2021 年《数据安全法》《个人信息保护法》相继落地实施并与《网络安全法》共同构成我国顶层数据立法的“三驾马车“以来，各类配套法律文件也如雨后春笋般涌现，各部门、各地区的执法力度不断加大，监管强度不断收紧，企业合规压力日益突显。在此背景下，隐私计算为数据流通与数据保护间的价值平衡提供了一种可行的技术解决方案。

https://mp.weixin.qq.com/s/SkU6iYJmteHvsE6zY7eXzw

5、浅析金融业数据安全风险问题与应对策略

由于金融行业数据价值的凸显和商业利益的驱动，数据非法采集、数据贩卖、数据篡改、数据攻击、数据权限滥用等安全问题层出不穷。如何保障数据安全，促进数据合法、安全，有效流通，充分发挥数据综合价值，是金融行业面临的重要课题。现阶段金融业数据安全风险点主要分为以下 4 类:（1）**数据开放性显著增强。（2）数据安全保护意识有待提升。（3）数据安全相关法律法规不完善、不健全。（4）数据权属关系不明确。(5)新技术攻击手段多样化、层出不穷。**

保障金融业数据安全不仅仅是用工具组合的产品解决方案，应该从法律法规到管理办法的制度保障，从技术实施到工具支持的落地应用，自上而下贯穿金融行业全方面架构的完整链条。具体数据安全防护策略有:**（1）提高数据安全意识。（2） 明确数据所属的权利和责任。（3）进一步建立和完善相关制度。（4）加强数据安全防护技术的升级与提升。**

https://www.wangan.com/p/7fy78y6bd7b94434

数据安全事件

1、因涉嫌未经同意收集人脸信息，Snap 以 2.4 亿元达成和解

2022 年 8 月 26 日报道，近日，据科技媒体 TechCrunch 报道，知名通讯软件 Snapchat 的母公司 Snap 与美国伊利诺伊州居民就一起隐私相关集体诉讼达成和解，和解金额总计为 3500 万美元（约合人民币 2.4 亿元）。

伊利诺伊州居民认为，Snapchat 的滤镜（filters）和镜片（lenses）功能收集用户面部数据，违反了伊利诺伊州的《生物信息隐私法》（Biometry Information Privacy Act，BIPA）。

据悉，伊利诺伊州曾于 2008 年通过《生物信息隐私法》。此部法律严格限制公司收集、使用和共享生物信息，禁止公司在未经用户同意的情况下收集生物信息。同时，公司需要以书面形式告知用户为什么想要收集他们的生物信息、以及存储时间。

https://www.secrss.com/articles/46298

2、法国首都一医院遭勒索软件攻击：急诊被迫停业 赎金 1000 万美元

2022 年 8 月 23 日消息，距巴黎市中心 28 公里，拥有

1000 张床位的 Center Hospitalier Sud Francilien（简称 CHSF）医院 8 月 21 日遭遇网络攻击，迫使其将患者转诊至其他机构，并推迟了手术预约。法媒《世界报》称，攻击 CHSF 的勒索软件团伙要求受害者支付 1000 万美元以换取解密密钥。https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/

3、希腊最大天然气运营商遭勒索软件攻击，多项在线服务被迫中断

2022 年 8 月 22 日消息，欧洲国家希腊最大的天然气分销商 DESFA 在 8 月 20 日证实，由于遭受网络攻击，该公司出现了一定程度的数据泄露与 IT 系统中断。

在向当地新闻媒体发布的公开声明中，DESFA 称有黑客试图渗透其网络，但因为 IT 团队快速反应而被阻断。然而，对方仍在有限范围内实施了入侵，导致部分文件和数据被访问并可能“外泄”，DESFA 为此**停用了多项在线服务**，希望保护客户数据。而且随着专家们努力进行恢复，各项服务已经逐渐恢复运行。

Ragnar Locker 勒索软件团伙在窃取数据后确认了此次攻击。该恶意黑客团伙还在其数据泄露与勒索门户上发布了

所谓被盗数据清单，展示了一小部分似乎不涉及机密信息的被盗文件。如果受害组织不满足赎金要求，该恶意黑客团伙威胁将发布整个文件树内对应的所有文件。

https://www.bleepingcomputer.com/news/security/greek-natural-gas-operator-suffers-ransomware-related-data-breach/

4、LastPass 数据泄露：攻击者窃取了部分源代码

2022 年 8 月 25 日报道，密码管理软件公司 LastPass 披露了一个安全漏洞，威胁参与者通过一个受感染的开发人员帐户访问了公司开发环境的部分内容，并窃取了部分源代码和一些专有技术信息。为应对这一事件，该公司已部署了遏制和缓解措施，并正在实施额外的增强安全措施。

https://securityaffairs.co/wordpress/134858/data-breach/lastpass-data-breach.html

5、Plex 披露数据泄露并敦促重置密码

2022 年 8 月 24 日，据外媒报道，流媒体平台 Plex 公司披露了在威胁行为者可以访问存储在受损数据库中的有限数据子集后的数据泄露事件。暴露的数据包括电子邮件、用户名和加密密码。针对未经授权访问其数据库的情况，该公司敦促其所有用户立即重置帐户密码并注销与其服务连接

的所有设备。

https://securityaffairs.co/wordpress/134814/data-breach/plex-data-breach.html

6、量子勒索软件攻击多米尼加共和国政府机构

2022 年 8 月 24 日，多米尼加共和国的多米尼加农业研究所遭到了 Quantum 勒索软件的疯狂攻击，该勒索软件加密了整个政府机构的多项服务和工作站，导致部分工作暂时停滞。

调查发现 Quantum 勒索软件操作是这次攻击的幕后黑手，最初要求该机构支付 650,000 美元的赎金。威胁参与者声称已经窃取了超过 1TB 的数据，并威胁说如果不公开支付赎金，就会将其释放。

https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-disrupts-govt-agency-in-dominican-republic/

7、数据库配置错误导致印度联邦警察和银行相关信息泄露

Cybernews 在 8 月 24 日称其发现了一个公开的 Elasticsearch 数据库，其中包含属于印度联邦警察的金融欺诈调查记录等数据。该数据库约 24 GB，总共包含 3350 万条记录，涉及银行账户持有人姓名、余额、帐号、交易类型、

金额和印度中央情报局(CBI)处理的案件。更糟糕的是，研究人员在数据库中还发现了 200 多家银行的记录。目前尚不清楚该数据库的持有者，但其中信息的性质表明它可能由印度法院或私人的欺诈调查机构持有。

https://cybernews.com/privacy/federal-police-and-banking-records-exposed-by-database-leak-in-india/

8、国际航空重要供应商遭勒索软件攻击，航空业已成为勒索主要目标

2022 年 8 月 25 日报道，服务美英等国主要航空公司的技术供应商 Accelya 透露，近期遭遇勒索软件攻击，部分系统已经受到影响；Accelya 公司主要负责为各大航空零业企业提供客运、货运与行业分析平台，与 9 个国家共 250 多家航空企业保持着合作关系。

据悉，AlphV/BlackCat 勒索软件团伙公布了据称窃取自 Accelya 的数据。该团伙称窃取的数据包含电子邮件、员工合同等内容。航空产业已经成为勒索软件团伙的一大主要攻击目标，今年 5 月，印度香料航空、加拿大战斗机培训服务商均曾遭遇勒索软件攻击。

https://www.secrss.com/articles/46226

9、DoorDash 披露了与 Twilio 黑客有关的新数据泄露

2022 年 8 月 26 日报道，食品配送公司 DoorDash 披露了一项数据泄露事件，该事件暴露了与最近对 Twilio 的网络攻击有关的客户和员工数据。

在周四下午发布的安全公告中，DoorDash 表示，攻击者使用从有权访问其系统的第三方供应商处窃取的凭据获得了对公司内部工具的访问权限。黑客利用这种对 DoorDash 内部工具的访问权限来访问消费者和员工的数据。

暴露的信息包括消费者的姓名、电子邮件地址、送货地址和电话号码。此外，对于一小部分客户，黑客访问了基本订单信息和部分信用卡信息，包括卡类型和卡号的最后四位数字。虽然 DoorDash 没有提及第三方供应商的名称，但其表示该漏洞与最近对 Twilio 的网络攻击相同的威胁行为者有关。

https://www.bleepingcomputer.com/news/security/doordash-discloses-new-data-breach-tied-to-twilio-hackers/?&web_view=true

10、两名快递员窃取近万条买家个人信息

2022 年 8 月 26 日报道，老李（化名）是一个仓库老板，从事第三方仓储业务，为网络电商提供货物仓储、打包服务。

近来，有客户向老李反映，有多名网店买家投诉称接到诈骗电话，怀疑个人信息被泄露。

经调查发现，某快递公司快递员刘某在 2018 年通过手机聊天软件认识了上家“老蔡”，向他贩卖快递面单上的买家个人信息。在这期间，刘某利用揽收快递的工作便利，用自己的手机偷拍快递面单，窃取网店买家的收件信息，并出售给“老蔡”。仅在 2021 年 8 月 23 日至 31 日 9 天时间里，刘某与朱某就用这种方式窃取买家个人信息 8614 条。近日，杭州市余杭区人民检察院以侵犯公民个人信息罪对刘某提起公诉。目前案件正在法院审理中。

https://www.secrss.com/articles/46268