全球数据安全观察

总第 100 期 2022 年第 28 期

(2022.08.01-2022.08.07)

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、《互联网用户账号信息管理规定》8 月 1 日起施行

国家网信办发布的《互联网用户账号信息管理规定》于 8 月 1 日起开始正式施行。规定明确账号信息管理规范，要求互联网信息服务提供者履行账号信息管理主体责任，建立健全并严格落实真实身份信息认证、账号信息核验、个人信息保护等管理制度。《规定》明确要求，互联网信息服务提供者为互联网用户提供信息发布、即时通信等服务的，应当进行真实身份信息认证；应当对互联网用户在注册时提交的和使用中拟变更的账号信息进行核验；应当在账号信息页面展示合理范围内的互联网用户账号的互联网协议地址归属地信息，便于公众为公共利益实施监督。

https://mp.weixin.qq.com/s/blu31sccjvogrhmxvNxlEQ

2、《北京市推动软件和信息服务业高质量发展若干措施》：有序开放公共数据，支持构建城市算力中心

近日，北京市经信局发布《北京市推动软件和信息服务业高质量发展的若干政策措施》。根据《若干措施》，北京市将支持新技术新产品研发，围绕基础软件、工业软件等重点领域开展科技攻关，实施“产业筑基工程”，通过“揭榜挂帅”

等方式支持一批关键软件产品研发，单个项目补助最高3000万元。《若干措施》其中提到:

支持创新企业参与智慧城市建设：采用数据专区等安全可信方式，有序开放公共数据，支持创新企业加速技术研发突破。建立智慧城市场景清单公开征集、评审入库、动态滚动、多方联动的迭代更新机制，鼓励创新企业采用“揭榜挂帅”“毛遂自荐”等方式承接场景开放试点,，对成效显著的优先向全市推广。

支持构建城市算力中心体系鼓励公共算力基础设施建设：探索打造市级算力网络和算力监测调度平台，优化本市公共算力资源供给，加强商业化算力资源供需对接。为本市数据(算力)中心提供免费绿色节能诊断服务。

https://mp.weixin.qq.com/s/XIIYJgh7MYuD5t1iiB65mw

3、武汉市元宇宙发展方案征求意见全文公开，加快部署大型互联网数据中心，加强城市元宇宙相关数据开放应用

8月5日，武汉市经济和信息化局发布《武汉市元宇宙产业创新发展实施方案（2022—2024年）（征求意见稿）》。**方案主要任务中提到：**要**布局核心资源平台**。加快部署大型互联网数据中心、超算中心、人工智能计算中心等平台设施，着力解决算力资源需求。**加强数据开放**。加强城市元宇宙相

关数据的开放应用，促进数据流通共享和价值传输，保障数据资产价值，破解数据资产确权难题，注重数据安全管理和隐私保护，充分发挥数据治理效用。引导和推动元宇宙产品开发者和平台运营者加强行业自律，依法打击利用元宇宙进行非法交易等违法行为，建立包容审慎、灵活敏捷的监管机制。

https://mp.weixin.qq.com/s/H48Al_pNWWg7anR5z3oZew

4、四川省发展和改革委员会等 6 部门发布《全国一体化算力网络成渝国家枢纽节点（四川）实施方案》

近日四川省发展和改革委员会等 6 部门关于印发《全国一体化算力网络成渝国家枢纽节点（四川）实施方案》。**方案重点任务提到：**

建设新型数据中心，夯实枢纽节点发展基础。（1）推动数据中心集约发展。（2）加快数据中心绿色发展。（3）提升通信网络保障能力。

加快数据开放流通，激发数据要素创新活力。（1）推动政务数据开放应用。（2）探索数据要素市场化。（3）推进数据跨境流动试点。

强化数据安全保障，增强自主可控能力。（1）推进核心技术突破与应用。（2）加快完善信创产业生态。

https://mp.weixin.qq.com/s/OUtU0NgLsdFjyrPHUGJ0tg

5、浙江省发布《关于深化数字政府建设的实施意见》

近日，浙江省政府印发了《关于深化数字政府建设的实施意见》。《意见》指出要完善环境数据全流通体系，推进数据全量归集和共享使用。发挥数据要素关键作用，推动数据全面融入生产、分配、流通、消费和社会服务管理等各个环节。率先形成数据基础制度体系。加快探索数据产权制度、数据流通和交易制度、数据要素收益分配制度、数据治理制度，全面激活要素潜能。

https://mp.weixin.qq.com/s/o0iK9m9nw0N6O_sPCxEBkA

技术、产品与市场

1、工信部：我国算力规模排名全球第二

7 月 30 日，2022 中国算力大会在山东济南开幕。工信部相关负责人表示，我国算力产业规模快速增长，近五年平均增速超过 30%，算力规模排名全球第二。

我国已启动建设多条“东数西算”干线光缆，所有地级市全面建成光网城市，千兆光纤用户数突破 6100 万户，为算力产业发展打下了坚实基础。

目前，我国在用数据中心机架总规模超过 590 万标准机架，服务器规模约 2000 万台，数据中心存储容量年均增长速度超 50%。中国信息通信研究院测算，截至 2021 年底，我国算力核心产业规模超过 1.5 万亿元，关联产业规模超过 8 万亿。

其中，云计算市场规模超过 3000 亿元，互联网数据中心服务市场规模超过 1500 亿元，人工智能核心产业规模超过 4000 亿元。

https://mp.weixin.qq.com/s/3XUrAOQrpde4o_QyM50-fg

2、北京发布数字人产业创新发展计划，培育数字人数据要素市场，2025 年规模将达 500 亿元

近日为落实《“十四五”数字经济发展规划》战略部署，抓住以数字人为代表的互联网 3.0 创新应用产业机遇，北京市经济和信息化局发布《北京市促进数字人产业创新发展行动计划（2022-2025 年）》。**规划其中提到：**

加快共性技术平台建设。布局高精度低延迟渲染云计算平台、边缘计算设施，结合 5G 等高性能通信网络，提升数字人计算能力。建设并运营动作捕捉设备、XR 摄影棚等数据采集设施。支持搭建 DEM（数字高程模型）平台，探索开放共享真实街区、楼宇等空间数据，为数字人提供交互展示的空间数据底座。对符合新型基础设施支持政策的项目、产品，可给予一定额度资金支持。

培育数字人数据要素市场。依托国家文化专网，将数字人纳入文化数据服务平台，汇聚文化数据信息，完善文化市场综合执法体制，依法合规开展数据交易业务，强化文化数据要素市场交易监管。基于区块链技术，探索构建数字人模型、皮肤、纹理等数据要素交易平台。基于数据专区和大数据交易所，试点数字人数字资产评估工作。

https://mp.weixin.qq.com/s/gG1JrGxUEe6OU7az0_EX2A

3、IDC: 2021 年中国大数据平台公有云服务市场规模达 33.7 亿元

IDC 于近日发布了《中国大数据平台公有云服务市场份额，2021》，报告数据显示，**2021 年中国大数据平台公有云服务市场规模达 33.7 亿元人民币，相比 2020 年实现 53.8%的快速增长**。市场增长驱动力主要来自于电商行业、互联网音视频业务、政府行业政策驱动上云、抗疫公共服务、交通行业、媒体行业，其次来自金融、制造、零售和教育行业。随着数据量明显增长以及厂商对业务实时性要求提高，从数据管理到数据应用，企业对数据分析的重视程度日益提高。

IDC 认为，在大数据领域，公有云服务相比私有化部署方案可以提供更好的扩展性、更低的开发运维门槛，更能够适应今天行业用户对于大数据存储计算的需求。随着数据平台、数据湖、数据仓库的建设，组织的数据可能分散在不同的位置，在选择云服务厂商时需要关注其多云数据管理能力、数据迁移的便捷性、数据存储与使用的安全合规、计算存储资源的整体性价比。

https://www.secrss.com/articles/45429

4、2022 年全球加密趋势研究

2022 年全球加密趋势研究报告了企业面临的网络安全

挑战，以及企业如何以及为何保护其数据。主要发现包括：

拥有一致的企业级加密策略的组织从 36%增长至 57%，因为企业希望更好地控制分布在多个云环境中的数据。

报告还揭示了与 2021 年规划和执行数据加密策略相同的两大挑战，即查找数据（60%）和初步部署加密技术（34%）。虽然结果表明企业已经从评估问题转向采取行动，但它们也揭示了许多敏感数据类别之间的加密实施差距。

几乎一半的受访者（43%）承认，他们的企业将敏感或机密数据传输到云端，无论这些数据是否经过加密或通过诸如标记化或数据屏蔽等其他机制变得不可读。另有 44%的受访者预计会在未来一到两年内这样做。

在威胁来源方面，受访者认为员工错误是可能导致敏感数据泄露的最大威胁（46%），来自临时工或合同工的威胁排名第二（41%）。其他排名最高的威胁是黑客（34%）和第三方服务提供商（27%）。

https://mp.weixin.qq.com/s/kCg6QjoYWXd2z8lBqfK5FQ

5、现在采集，以后解密：真随机数应对量子计算威胁

加密有两个重要问题：密钥及其分发。分发通常通过非对称加密完成，但分发可以被拦截，非对称加密会被破解。这一问题到今天仍然存在，而且随着量子计算机的到来，破

解问题将变得更加严重。非对称加密首当其冲（Shor 量子算法已被证明有效）。这导致了一种新的攻击手段，**“现在采集，以后解密”**。

攻击者，尤其是国家支持的网络黑客，目前正在设法收集加密数据，期望将来能够解密。量子解密已不是技术问题，只是时间迟早的问题。

针对这一未来的威胁，量子安全公司 Qrypt 发布了一款产品“Qrypt 密钥生成”，旨在消除传统密钥分发的需要，从而消除非对称加密。方法是删除加密公式中的密钥分发部分，并使用量子方法生成真正的随机数，以产生更安全的密钥。

https://www.secrss.com/articles/45495

业界观点

1、周鸿祎：在数字安全时代，“看见”是安全的分水岭

7 月 30 日，第十届互联网安全大会（ISC2022）在北京国家会议中心开幕，本届大会以“护航数字文明、开创数字安全新时代”为主题，三六零公司创始人周鸿祎发表主题演讲时表示，在数字安全时代，“看见”是安全的分水岭，回避“看见”谈安全都是假把式，只是隔靴搔痒。正因为“看见”，我们才知道，网络攻击时时刻刻都在发生，并且所及之处一片狼藉，比如城市断水断电，企业受到勒索，损失动辄上百万。

周鸿祎表示，针对数字化过程中的安全挑战，数字化的内在脆弱性导致安全风险更大，同时外部威胁也在不断升级，在内外部双重安全挑战之下，风险遍布数字化的所有场景，倒逼网络安全升级为数字安全。

目前，外部威胁不断升级。“过去的‘小毛贼’已经鸟枪换炮，升级为专业化的网络犯罪组织，技术能力不亚于安全公司。”周鸿祎指出，勒索攻击、挖矿攻击、供应链攻击、DDoS 攻击、网站攻击等新攻击手段层出不穷，国家背景的 APT 攻击已经成为大国对抗的主流，网络攻击目标、手法、产生的破坏都突破常规。

数字安全时代的最大痛点就是“看不见”。为解决这一“卡

脖子”难题，近 20 年间，360 投入了 200 亿，聚集了 2000 名安全专家，积累了 2000PB 的安全大数据，建立了一套以“看见”为核心的数字安全大脑框架，帮助国家感知风险、看见威胁、抵御攻击，并将服务国家的能力服务于政企客户、中小微企业，守护数字经济发展。

http://www.news.cn/info/20220730/527e0d94bf7d4ec48a161ff21dcf1fd7/c.html

2、李京春：数据分类分级需要同时考虑分类安全与发展两个视角

当数据确权的讨论还在学术理论界争执不下时，数据分类分级的实践早已在各行各业遍地开花。数据安全需要采用分类分级安全管理，按重要级别备份/恢复，按数据类别进行强制访问控制、身份识别等密码措施加以保护。国家信息技术安全研究中心总师组专家李京春采访时表示，**为保证数据质量和高效利用，数据本身必须治理，数据分类分级就是数据治理的重要内容，需要站在不同的视角多维度管理和利用。**比如，监管部门或数据安全企业可能会更多地关注在数据处理活动当中是否合法、正当、必要，是否合规。毕竟数据关乎国家安全和经济发展，关乎公共利益，关乎我们每个人的隐私安全，所以说**安全是数据分类分级需要考虑的重要因素。**

数据分类分级需要同时考虑到安全与发展，两个视角观察世界。

https://mp.weixin.qq.com/s/yjSY5u35RrClJ3ANuaePlw

3、左晓栋：对数据出境安全管理制度的几点思考

当前，我国政策并未明确强调要实施数据本地化存储。对数据出境施加一些条件要求甚至是条件限制，并不等于不让数据出境，也不等于数据必须存在境内。在数据管理方面，我国正在建立重要数据出境安全监管制度，相关政策仍处于动态调整阶段。特别是，对重要数据的定义存在不一致是该阶段的特定现象，未来将逐步达成共识。

理解我国当前的数据出境安全管理制度，主要有以下几个要点：

一是当前我国政策并未明确强调要实施数据本地化存储。对数据出境施加一些条件要求，甚至有时候是条件限制，并不等于不让数据出境，也不等于数据必须存在境内。必须看到，除了《网络安全法》外，后续出台的法律法规的确没有再强调数据本地化存储的概念。在个别场合下，可能数据还是要坚持本地化存储，但这一定是某种特定的数据，而不是针对所有的数据。

二是对数据出境安全管理政策的认定，不是所有的数据

出境都按现在的数据出境条件来实施。《网络安全法》和《数据安全法》明确了重要数据的出境条件，即必须经过网信部门组织的安全评估，《个人信息保护法》与《网络安全法》也明确了个人信息出境的条件。

个人信息出境有四条不同的途径，不属于规定的情况，按照目前法律法规规定，这是可以自由出的（涉密信息或行业有特殊要求的除外）。大家的注意力都被前一阶段国家政策的数据出境安全要求吸引过去了，误以为数据必须这么出境。实际上还有相当多的数据是不必通过以上路径就可以出境，即，既非重要数据也非个人信息。目前的法律没有规定所有的数据出境都必须经过评估、标准合同或者认证。当企业进行数据出境时，可以对数据进行梳理，将重要数据、个人信息与其他出境数据分类处理。

https://mp.weixin.qq.com/s/DTx0RDg3nLcly_zV4toPVw

4、潘剑锋：真正的 EDR 是“看见”威胁的眼睛

“真正的 EDR 是看见威胁的眼睛，需要具备看见的能力。”360 集团副总裁兼首席科学家潘剑锋在第十届互联网安全大会（ISC 2022）未来峰会上谈到。

数字时代大量设备入网、业务和数据上云背后，是终端作为数字化基础节点面临对抗加剧、安全挑战严峻的现状。

“看见是检测的基础。只有快速、完整地理解网络攻击事件发生的全部情节，跟踪攻击事件每一步，才能以有效的方式做出响应。真正的 EDR 是看见威胁的眼睛。”潘剑锋表示，想要看见高级威胁攻击、勒索攻击、供应链攻击等各类威胁事件，需要具备全球视野、海量云端大数据的存储及处理能力、高质量事件的捕获能力、AI 分析技术及实战经验丰富的安全专家团队。

终端安全往往被视为最后一道防线，面对穷凶极恶的攻击者，终端防御方案“木桶效应”明显。EDR 必须同时在全球视野、云端分析能力、高级端点能力、AI 分析技术、实战专家五个方面具备顶尖实力，才能真正解决数字时代终端高级威胁防护难题，实现安全能力从被动式单点防护到主动式纵深防御的演进。

http://www.news.cn/info/20220801/481f0b72dab54749a4d88de33aa8b530/c.html

5、唐建国：基于区块链技术进行数据确权 探索数据合理化定价机制

北京市大数据中心副主任唐建国表示，当前数据要素市场面临着四个瓶颈问题。一是如何通过确权拉动海量数据的供给；二是如何为数据资产评估定价，促进高价值数据的有

序流动；三是如何在保护数据内容安全的前提下，促进数据背后的计算价值得以释放；四是在服务数据跨境流通的活动中维护国家的主权。

“通过一年多的实践我们在上述四个问题方面有了一些初步的回答。”唐建国介绍，一是**基于区块链技术进行登记实现数据资产的唯一性确权**。数据确权是数据交易的前提，数据交易中心、交易中介服务机构具有数据确权的天然职能。二是**基于资产评估破冰数据资产化改革，探索数据的合理化定价机制**。在工信部、财政部的支持下，2021 年 11 月，经信局会同相关单位率先启动了数据资产评估工作。参考国家即将发布的团体标准和行业规范，形成了首批六个单位的数据资产评估报告，探索了数据资产的评估的方法，量化了数据资产的价值。此外，还推动三家专业化的数据资产评估机构在城市服务中心率先落地。

https://www.bbtnews.com.cn/2022/0729/446074.shtml

数据安全事件

1、Robinhood 因违反纽约网络安全法规被罚款 3000 万美元

2022 年 8 月 3 日报道，Robinhood 的加密货币部门因违反网络安全和洗钱法规而被纽约金融服务部罚款 3000 万美元。纽约金融服务部的声明表示，Robinhood Crypto 网络安全计划存在问题，没有完全解决 RHC 的运营风险，并且该计划中的具体政策不完全符合网络安全和虚拟货币法规的几项规定，且该公司的合规计划和交易监控系统中的存在缺陷。除了 3000 万美元的罚款外，该公司还需要聘请一名独立顾问来全面评估 Robinhood Crypto 法规的遵守情况，并修复已发现的缺陷和违规行为。

https://www.securityweek.com/robinhood-crypto-penalized-30m-violating-ny-cybersecurity-regulations

2、2.88 亿条印度养老基金持有人的身份数据被暴露在互联网

2022 年 8 月 3 日报道，一个包含印度养老基金持有人全名、银行账户号码等信息的巨大数据缓存已在网上浮出水面。安全研究员 Bob Diachenko 发现两个独立的 IP 地址存储了超过 2.88 亿条记录——其中一个 IP 地址下有约 2.8 亿条记录，

约 840 万条是第二个 IP 地址的一部分。该研究人员说，这两个 IP 地址都公开向互联网暴露数据，但没有密码保护。

这些记录是名为"UAN"的集群指数的一部分，这显然是指该国国有雇员公积金组织（EPFO）分配给养老基金持有人的通用账户号码。Diachenko 表示:"据我所知，数据库中的信息可能被用来拼凑出一个印度公民的完整档案，使他们成为网络钓鱼或诈骗攻击的目标。"

每条记录都包括详细的个人信息，包括他们的婚姻状况、性别和出生日期。还有一些细节主要与他们的养老基金账户有关，包括 UAN、银行账户号码和就业状况。除了泄露持有养老基金账户的个人身份信息（PII）外，这些记录还暴露了其办理人的详细信息。

https://www.cnbeta.com/articles/tech/1300399.htm

3、健康保险公司 Aetna 报告一起影响近 326,000 人的数据泄露事件

2022 年 8 月 2 日，据外媒报道，健康保险公司 Aetna ACE 向联邦监管机构报告了一起影响近 326,000 人的健康数据泄露事件，这与涉及 OneTouchPoint 的勒索软件事件有关，OneTouchPoint 是一家为保险公司的供应商提供打印和邮寄服务的分包商。

在上周二的一份声明中，Aetna 表示受影响的信息可能包括姓名、地址、出生日期和有限的医疗信息。保险公司通常持有大量对黑客有价值的个人可识别数据，涉及健康保险公司的违规行为对其成员的受保护健康信息构成了重大的隐私和安全问题。

https://www.bankinfosecurity.com/aetna-reports-326000-affected-by-mailing-vendor-hack-a-19691?&web_view=true

4、数以千计的 APP 正在泄露 Twitter 的 API 密钥

2022 年 8 月 4 日报道，来自印度 CloudSEK 的安全研究人员表示，他们已经确定共有 3207 个移动应用程序泄露了有效的 Twitter 用户密钥和密钥信息。大约 230 个应用程序被发现泄露了 OAuth 访问令牌和访问机密。

这些信息为攻击者提供了访问用户 Twitter 帐户并执行各种操作的机会，包括：阅读信息、代表用户转发点赞或删除消息、删除关注者或关注新帐户、修改账户设置。

研究人员将该问题归因于应用程序开发人员在开发过程中将身份验证凭据保存在其移动应用程序中，以便与 Twitter 的 API 进行交互。后者为第三方开发人员提供了一种将 Twitter 的功能和数据嵌入到他们的应用程序中的方法。因为用户授权移动应用程序使用他们的 Twitter 账户，从而将自

已也置身于应用程序所面临的风险中。此类密钥泄露也为许多可能的滥用和攻击场景创造了可能性。

https://www.secrss.com/articles/45422

5、阿联酋零售商 Spinneys 客户数据泄露

2022 年 8 月 4 日，据外媒报道，阿联酋主要零售商 Spinneys 声称，一个勒索软件组织已从其内部服务器访问客户数据，并且该勒索软件组织可能已于 2022 年 7 月 16 日就从其内部服务器泄露了被黑客入侵的数据。

黑客访问了包含客户数据的内部服务器，包括姓名、联系电话、电子邮件地址、送货地址和以前的订单信息。该公司表示，“我们可以确认没有个人银行信息被泄露，因为我们不会在我们的服务器上存储银行详细信息。”。

https://securereading.com/uae-spinneys-customer-data-leak/?web_view=true

6、黑客组织公开 2TB 电子邮件，揭露南美洲多家矿业公司内幕

2022 年 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，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。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。

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

7、神经病学诊所遭受勒索攻击，泄露 363,000 人敏感信息

2022 年 8 月 4 日，据外媒报道，印第安纳州的一家神经病学诊所已通知近 363,000 人，他们的敏感信息在最近的勒索软件攻击中遭到破坏，并且他们的一些数据已发布在暗网上。

勒索软件组织 Hive 声称与本次攻击有关，该事件中受影响的信息包括姓名、出生日期、地址、电话号码、电子邮件地址、病历号码、患者帐号、诊断和治疗信息、医生姓名、保险信息、服务日期和社会安全号码。“虽然我们没有迹象表明有敏感个人信息因本次事件而被不当使用，但我们确实知道攻击者获得的一些信息在暗网上可以使用大约 10 天，”通知信说。

https://www.bankinfosecurity.com/neuro-practice-tells-363000-that-phi-was-posted-on-dark-web-a-19706?&web_view=true

8、德国半导体巨头赛米控遭勒索软件攻击

2022 年 8 月 3 日报道，德国电力电子制造商赛米控（Semikron）近日披露遭到勒索软件攻击，部分公司网络被加密。

赛米控在德国、巴西、中国、法国、印度、意大利、斯洛伐克和美国的 24 个办事处和 8 个生产基地拥有 3000 多名员工，2020 年的营业额约为 4.61 亿美元。

根据赛米控集团本周一发布的声明，攻击者从其系统中窃取了数据，“这次攻击还导致了我们的 IT 系统和文件的部分加密。目前正在研究和调整整个网络的取证。”根据德国联邦信息安全办公室发出的警报，勒索软件运营商正在勒索该公司，并威胁要泄露据称被盗的数据。

虽然赛米控没有透露攻击者的任何信息，但是根据流出的勒索软件声明，这是一次大规模数据勒索软件攻击，攻击者声称窃取了多达 2TB 的文件。

https://www.bleepingcomputer.com/news/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack/

9、中欧天然气管道公司疑遭勒索软件攻击，150GB 数据失窃

2022 年 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 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。Encevo 公司初步调查结果表明，网络入侵者已经从被访问系统中窃取到“一定数量的数据”。

而 ALPHV/BlackCat 勒索软件团伙上周六已经将 Creos 添加至勒索网站，并威胁要发布总计 150 GB 大小的 18 万个被盗文件，具体涵盖合同、协议、护照、账单及电子邮件。
https://mp.weixin.qq.com/s/CeGGxXss5UktXObnfjjzmg

10、在涉嫌数据盗窃后，黑客试图勒索调查公司 QuestionPro

2022 年 8 月 4 日，据外媒报道，有黑客声称窃取了在线调查平台 QuestionPro 包含受访者个人信息的数据库后，试图对该公司进行勒索。

QuestionPro 公司提供在线服务，允许企业创建和进行调查以进行市场研究。该公司确认他们遭受了勒索，威胁者要求支付比特币以不发布数据。据称被盗的数据库包含大约 2200 万个唯一电子邮件地址的记录。

https://www.bleepingcomputer.com/news/security/hackers-try-to-extort-survey-firm-questionpro-after-alleged-data-theft/?&web_view=true