全球数据安全观察

总第 93 期 2022 年第 21 期

（2022.06.13-2022.06.19）

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、网信办就《互联网跟帖评论服务管理规定（修订草案征求意见稿）》公开征求意见.....1
2、国家网信办修订发布《移动互联网应用程序信息服务管理规定》，数据安全和个人信息保护再迎监管加码.....1
3、国家发改委：数据要素基础性制度相关文件已形成初稿.....2
4、《厦门市全面提升营商环境数字化便利化水平培育和激发市场主体活力行动方案》发布！深化公共数据共享、加强数据归集应用.....3
5、《新疆维吾尔自治区关键信息基础设施安全保护条例》正式施行，健全信息通报制度、建立网络安全信息共享机制.3
技术、产品与市场.....5
1、我国数据安全产业链发展观察.....5
2、人社部公布首批 18 个新职业，包含数据安全工程技术人员、数字孪生应用技术员等.....6
3、全球网络安全行业盛会 RSAC 2022 十大热点议题.....6
4、中国信通院：八成互联网电视系统存非法采集共享用户数据问题.....7
5、勒索软件攻击中泄露的数据量和类型取决于该组织.....8
业界观点.....9
1、工信部：将实现对关键环节和在架 APP 的监管全覆盖.9
2、从数据利用视角探讨数据出境安全问题.....10
3、当心社交媒体晒照泄露隐私信息.....11
4、平衡卫生健康数据保护与产业发展，行业专家共话行业合规水位线.....12

5、智能汽车数据合规进入深水区，仍存在盲点和难点.....14
数据安全事件 16
1、圣地亚哥家庭护理公司以 100 万美元解决数据泄露集体诉讼.....16
2、前亚马逊工程师被定罪，曾盗窃曝光超 1 亿人数据...16
3、非洲最大连锁超市遭勒索团伙敲诈：600GB 数据失窃 17
4、威胁行为者利用企业滥用微软 Office 365 某功能，对企业发起勒索攻击.....17
5、数以万计开源项目开发账户遭大规模泄露.....18
6、美国 Transact Campus 配置错误泄露 3 万多学生的信息.....18
7、马来西亚软件供应商 StoreHub 泄露 100 万条客户记录.....19
8、乌干达证券交易所数据发生泄露，32GB 敏感数据曝光.....19
9、研究人员发现 BeanVPN 近 20GB 的连接日志可公开访问.....20
10、人力资源公司 Robert Half 称黑客攻击了 1000 多个客户账户.....21

政策形势

1、网信办就《互联网跟帖评论服务管理规定（修订草案征求意见稿）》公开征求意见

6 月 17 日，国家互联网信息办公室发布关于《互联网跟帖评论服务管理规定（修订草案征求意见稿）》公开征求意见的通知。《意见稿》提到跟帖评论服务提供者应当依法履行“**建立健全用户个人信息保护制度，处理用户个人信息应当遵循合法、正当、必要和诚信原则**，公开个人信息处理规则，告知个人信息的处理目的、处理方式、处理的个人信息种类、保存期限等事项，并依法取得个人的同意，法律、行政法规另有规定的除外。”的义务。

https://mp.weixin.qq.com/s/OqxYN6gJJkxg0p5FCzgpDw

2、国家网信办修订发布《移动互联网应用程序信息服务管理规定》，数据安全和个人信息保护再迎监管加码

6 月 14 日，国家互联网信息办公室发布新修订的《移动互联网应用程序信息服务管理规定》（以下简称新《规定》）。新《规定》对**数据安全和个人信息保护、未成年人保护**等管理制度进行了进一步明确和细化，并要求应用程序提供者和应用程序分发平台应当履行信息内容管理的主体责任，确保

网络安全，维护良好网络生态。新《规定》将自 2022 年 8 月 1 日起施行。

新《规定》共 27 条，包括信息内容主体责任、真实身份信息认证、分类管理、行业自律、社会监督及行政管理等条款。新《规定》要求，应用程序提供者和应用程序分发平台应当履行信息内容管理主体责任，**建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度**，确保网络安全，维护良好网络生态。

https://mp.weixin.qq.com/s/lDMFRiy7hNXAaWBeI6TwrQ

3、国家发改委：数据要素基础性制度相关文件已形成初稿

6 月 16 日上午，国家发展改革委举行六月份新闻发布会。国家发展改革委新闻发言人孟玮出席发布会，就媒体关注的推进新型基础设施建设，数据要素基础制度等方面回答了记者提问。孟玮表示发改委牵头编制数据要素基础性制度文件，围绕数据产权、交易流通、收益分配、安全治理等内容，加快构建我国数据基础制度“四梁八柱”，构建与数据生产力相适应的生产关系，目前有关文件已形成初稿。下一步，发改委将加快推动文件出台，按程序上报后印发实施。

https://mp.weixin.qq.com/s/tG9f7cb6LHxXQy0IhSrs7g

4、《厦门市全面提升营商环境数字化便利化水平培育和激发市场主体活力行动方案》发布！深化公共数据共享、加强数据归集应用

《厦门市全面提升营商环境数字化便利化水平培育和激发市场主体活力行动方案》（以下简称《方案》）于近日印发实施。市发改委表示，营商环境是企业生存和发展的土壤，事关城市核心竞争力。

根据《方案》，厦门市将聚焦营商环境数字化便利化建设的难点、堵点，启动新一轮“数字政府”强基工程，强化系统整合、标准统一、数据共享、跨域联动，倒逼政务服务方式、路径、规则、机制等重塑，大幅提升我市营商环境数字化便利化水平。

https://mp.weixin.qq.com/s/aGQAgUB61fALmy8bTUCCog

5、《新疆维吾尔自治区关键信息基础设施安全保护条例》正式施行，健全信息通报制度、建立网络安全信息共享机制

2022 年 6 月 15 日，《新疆维吾尔自治区关键信息基础设施安全保护条例》（以下简称《条例》）正式施行。

关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。制定出台《条例》，是贯彻落实国家相关法律法规的重要举措，**旨在明确各方责任，健全保障机制，**

有利于进一步健全我区关键信息基础设施安全保护法规制度体系。

《条例》明确，自治区关键信息基础设施安全保护和监督管理工作坚持党的领导，遵循综合协调、分工负责、依法保护、共同保护的原则。网信部门负责统筹协调、公安机关负责指导监督，通信、国家安全、保密、密码管理等部门在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

《条例》规定，关键信息基础设施安全保护工作执行网络安全等级保护制度、重点保护制度和安全审查制度，实行部门责任制和运营者主体责任制。网信部门会同有关部门建立网络安全信息共享、监测预警通报制度，并定期组织开展网络安全检查。

https://mp.weixin.qq.com/s/mvPQwWJmGJp0Eiz1azDWHQ

技术、产品与市场

1、我国数据安全产业链发展观察

从我国数据安全技术应用角度，可以将数据安全产业链分为上游、中游和下游。**上游市场主体为软硬件供应商，如芯片、操作系统、数据库等；中游市场主体为数据安全产品及服务提供商，如数据库安全、数据防泄漏，安全服务类别的数据安全咨询与评估服务等；下游市场主体为应用领域用户，包括最终用户、集成商和场景服务供应商。**

国内数据安全产业上游市场中，国外厂商在较长时间里占据市场优势，国内厂商在逐步追上。虽然目前国外厂商在上游产业上还占有一定优势，但国产化产品在大部分基础信息产品点位上已实现可替代。国产化产品已能满足大多数数据安全中游产品的使用需求，但在性能上还有提升空间。

数据安全产业链中游厂商，按业务特点可划分为基础性防护、应用性防护、综合性防护平台以及数据安全保障服务四大部分。数据安全中游企业一方面需要获取上游厂商的支撑，同时要为下游用户提供服务。数据安全中游企业之间也形成了相互合作的协同关系。

数据安全下游包括最终用户、集成商和场景服务供应商，这些数据安全下游用户和厂商将数据安全集成到自身的产

品中，一方面满足合规需求，另一方面也切实提升自己产品的安全水平。

https://mp.weixin.qq.com/s/eOXNtbeLIlaqG4_E4jcoHg

2、人社部公布首批 18 个新职业，包含数据安全工程技术人员、数字孪生应用技术员等

为促进青年特别是大中专毕业生就业创业工作，近期，人力资源社会保障部将向社会公示相关新职业信息，共计 18 个新职业信息作为第一批向社会进行公示，广泛征求意见。在本次公示的新职业中，与数据相关的数字职业高达 9 个，占比 50%，它们分别是“机器人工程技术人员”“增材制造工程技术人员”“**数据安全工程技术人员**”“**数字化解决方案设计师**”“数据库运行管理员”“信息系统适配验证师”“数字孪生应用技术员”“商务数据分析师”“农业数字化技术员”等职业。

https://www.sohu.com/a/557506387_100116740

3、全球网络安全行业盛会 RSAC 2022 十大热点议题

2022 年度的全球网络安全行业盛会 RSAC 落下帷幕。RSAC 2022 的 170 余个主题演讲，主要围绕 10 大热门主题，其中包括：**数据与隐私安全（热度 14[1]）**、身份安全与零信任（热度 14）、软件供应链安全（热度 10）、勒索软件（热度

10）、AI 安全（热度 10）、威胁分析及狩猎（热度 10）、风险管理（热度 9）、云安全（热度 6）、物联网及工业安全（热度 6）、基础设施安全（热度 4）。

本届 RSAC 的**数据安全议题集中在数据保护**，如云上行业（如医疗）数据保护、企业数据保护、数据本地化保护政策，以及政府数据交易与授权访问等。在隐私安全方面，热点议题则集中在如何保障基础设施(如 5G)、设备(如汽车)，以及应用（如 AI、区块链）的隐私安全方面。

https://mp.weixin.qq.com/s/mke7Q6c6wKTVzEFtPl4j4w

4、中国信通院：八成互联网电视系统存非法采集共享用户数据问题

中国信通院联合电信终端产业协会发布的《OTT 终端数据安全和个人信息保护研究报告（2022 年）》显示，我国互联网电视用户数 10.83 亿户，并有 80% 的电视系统存在用户数据被非法采集共享的问题。

OTT 是“OverTheTop”的缩写，是指越过运营商，通过互联网向用户提供各种应用服务。OTT 终端产业迅猛发展的同时，也带来了诸多安全问题，如漏洞修补不及时、控制模块越权操控、语音控制内容被篡改、应用软件 /SDK 过度索取权限、用户数据被非法采集共享、直接采集共享 MAC 等

不可变更设备标识等。特别是在数据安全和个人信息安全方面，**互联网电视上 App 和第三方 SDK 强制授权、过度索权、超范围收集个人信息的现象大量存在。**

https://www.ithome.com/0/624/914.htm

5、勒索软件攻击中泄露的数据量和类型取决于该组织

根据 Rapid7 对两年勒索泄露网站的研究，不同的勒索软件组织对泄露哪些数据表现出不同的偏好。

报告称，Conti 在 81% 的攻击中在其首次数据转储中泄露了财务信息，而 Cl0p 仅在 30% 的攻击中泄露了财务信息。Cl0p 在其首次泄露中 70% 泄露了员工个人信息，而 Conti 仅泄露了 27%。REvil 所泄露的财务信息和个人信息占比各为约 50%。

不同类型的信息会给公司带来不同的压力。泄露的员工或客户的个人信息可能会造成繁重的通知要求、重要群体之间的愤怒以及集体诉讼的风险。财务信息给投资者带来压力，并可能导致公司泄露的商业信息令人尴尬。

https://www.scmagazine.com/analysis/ransomware/what-data-will-get-leaked-it-depends-on-the-ransomware-group?&web_view=true

业界观点

1、工信部：将实现对关键环节和在架 APP 的监管全覆盖

6 月 14 日，中共中央宣传部举行了党的十八大以来工业和信息化发展成就发布会。会上有媒体提出“在专门立法背景下，工信部在个人信息保护方面的工作重点和变化有哪些”的问题。工业和信息化部总工程师韩夏对此进行了回答。

一是**主动适应技术发展变化，及时研究健全法规制度体系**。2013 年，我部出台了国内第一部针对个人信息保护的部门规章，也就是《电信和互联网用户个人信息保护规定》，去年我部组织起草了《移动互联网应用程序个人信息保护管理暂行规定》。目前，工信部正在对 2013 年出台的《电信和互联网用户个人信息保护规定》进行修订，强化应用程序关键责任链的管理，进一步健全个人信息保护制度体系。

二是**以群众关切为重点，加强电信和互联网行业个人信息保护突出问题的治理**。连续组织开展 APP 侵害用户权益专项整治，后续将围绕“全流程、全链条、全主体”监管，实现对各类终端、应用商店、软件开发工具 SDK 等关键环节和在架的 APP 的全覆盖，全方位保护用户权益。

三是**以深化科技为手段，加快提升治理能力**。组织建设全国 APP 技术检测平台，累计完成 322 万款 APP 的检测。

下一步，将打造面向移动互联网程序的检测和认证公共服务平台，着力提升自动化检测、大数据分析、监测预警、认证签名和公共服务能力，为行业治理提供更加有力的支撑。

四是**以协同共治为方向，营造良好的治理环境**。工信部与各有关部门加强协同，发挥社会各界的积极作用，形成了政府监管、企业自律、社会监督、用户参与的共治格局。今后将不断研究新情况新问题，总结新的实践经验，参照国际成功做法，加强监督检查，督促企业落实主体责任，提高合规水平，营造安全、健康、有序的信息通信应用环境。

https://finance.eastmoney.com/a/202206142411937497.html

2、从数据利用视角探讨数据出境安全问题

在经济全球化与数字化的大背景下，数据流通共享成为数据要素价值充分释放的关键，必然包含国际间的数据合作。然而，数据出境在实现全球数字经济持续性增长的同时，也可能会给一个国家、企业和个人带来很大的安全风险。因此，各国非常关注数据安全，纷纷发布数据出境安全的法规条例。

大数据协同安全技术国家工程研究中心专家研究分析了我国、欧盟、俄罗斯、美国等典型国家地区的数据出境管理做法，认为当前数据出境及出境安全面临的困难主要包括：**数据出境被狭义理解为数据跨境流动、确需跨境数据流动的**

情形有待澄清、对重要数据的定义及范围识别难等。

针对上述问题和困难，需要在保障数据安全和促进全球数据开放利用协调发展的原则指导下，充分利用数据安全技术进步带来的支撑，加强安全监管审计，促进全球数据合作。

（1） 加强安全评估，严控数据复制转移出境

（2） 用隐私计算技术实现数据出境合规利用

（3）加强安全监管，确保数据出境依法合规安全：一是建设数据出境安全监管审计平台。二是建立专门的数据出境安全监管队伍，并要求企业设立数据安全官岗位，负责与监管部门的对接和沟通。三是建立数据出境认定的“白名单”机制。

https://www.secrss.com/articles/43484

3、当心社交媒体晒照泄露隐私信息

近日，“发原图或暴露隐私”话题冲上微博热搜。一时间，保护个人隐私信息再次得到广泛关注。当我们以原图或者原文件的形式发送信息时，Exif 信息会一并发送出去，这与是否使用微信发送无关。

安天移动安全资深安全专家潘博文表示，每一张数码照片中都有一组可交换图像文件格式的信息，简称 Exif，它是照片在拍摄时生成的自带信息，主要包括拍摄时的准确位置

和时间，以及拍摄设备的唯一 ID 号。这些信息在使用智能手机或者数码相机拍摄照片时会自动生成。

对于社交平台而言，为帮助用户避免照片原图暴露隐私，可以在用户选择上传图片或者分享图片时，给予前置性的检查功能，当检测到存在疑似敏感信息时，提醒用户安全风险的存在，或者对其进行删除。当然，为了提高交互性体验，社交平台也可提供内置的自动删除图片 Exif 信息的功能。

对于普通用户来说，在分享、上传和个人隐私相关的照片之前，应务必检查自己所使用的社交平台的访问权限设置，将社交平台的“隐私和权限”设置为仅朋友可访问；如果存在分享时间的设置，尽量设置短一点。另外，如果拍摄的照片存在明显的位置标识，可以选择裁掉再发送。

http://finance.people.com.cn/n1/2022/0614/c1004-32445637.html

4、平衡卫生健康数据保护与产业发展，行业专家共话行业合规水位线

近日，由中国法学会网络与信息法学研究会主办、南财合规科技研究院承办的“卫生健康数据合规 实践与前瞻”研讨会召开。

多位专家学者、医疗机构、相关企业代表，围绕数据安

全相关法律法规及监管政策在实践中的落地情况，认为目前健康医疗大数据产业缺乏具体可操作的法规细则，以及数据确权难等问题，是企业们所面临的共同瓶颈。

北京市中伦律师事务所合伙人蔡鹏则认为卫生健康数据中所涉及的敏感个人信息在某些场景下很难获得单独同意，导致流动困难，可以从匿名化处理的角度去寻求解决方案。

锘崴科技董事长王爽表示，很多医院、科研机构和第三方检测机构的卫生健康数据具有极高的学术价值，可用于科学研究或支持药物研发，但由于数据存在所有权不明确等问题，导致这些数据的使用出现合规性瓶颈。还从隐私计算的角度提出了思路。他建议通过充分知情授权，以区块链技术记录数据使用全过程，运用隐私计算等技术保证全过程不会出现超范围使用，减少泄露风险，促进医疗数据在可管可控的前提下实现安全合规共享使用。

阿里健康高级法务专家常帅指出，个人信息保护是医疗健康数据处理和共享所面临的重大挑战，主要体现在个人授权同意及相关医学研究的伦理审查方面。他建议，对医疗健康数据进行合理的分类分级，并非该领域所有的数据都应划分为敏感个人信息；同时，在平衡个人信息保护和医疗健康数据有序流动的基础上，进一步完善医疗健康数据合理融合、

共享与开放。

http://www.21jingji.com/article/20220615/herald/fdb0acae94d0bf6e8beb8c15f3fa1b33.html

5、智能汽车数据合规进入深水区，仍存在盲点和难点

目前智能汽车的新挑战是“数据无处不在，安全迫在眉睫”，包括汽车数据成为新型的资源进而面临更大的挑战，公众与隐私保护的担忧在增加，以及数据过度采集、数据孤岛、数据权责不清、存储方式不当、使用流程不安全、缺乏溯源能力、敏感数据隐私数据和其他数据交织在一起等问题被屡屡提及，这些都意味着数据安全防护存在巨大的挑战。

中国电子信息产业发展研究院副总工程师安晖从评测机构的角度提出了智能网联汽车合规体系的三个方面：**组织架构、流程制度和技术保障**。首先要建立分层次的组织架构，明确各层级的人员角色与分工；其次要建立数据安全流程制度，将数据安全的制度体系融入到现有的研发流程中，以数据的分类分级管理为基础，覆盖智能网联企业产品的典型业务场景；最后需要采用防护技术和安全检测监测等方面的工具平台，来实现数据全生命周期的技术保障。

国家智能网联汽车创新中心安全产品业务线总监靳龙辉认为，数据安全防护体系的建设要遵循整体建设思路，从

车端、路侧、云端、通讯数据，形成整体的安全治理和防护体系。并从上而下建立国家层面、属地层面、企业层面，车内到车外，事前、事中、事后的一体化监管体系。

https://www.lehuiche.com/400397.html

数据安全事件

1、圣地亚哥家庭护理公司以 100 万美元解决数据泄露集体诉讼

2022 年 6 月 16 日，据外媒报道，圣地亚哥家庭护理(SDFC) 以 100 万美元解决了与 2020 年数据泄露有关的集体诉讼。该事件涉及了所有在 2021 年 5 月收到违规通知的 SDFC 患者（或其父母/监护人）。

SDFC 为患者提供初级保健服务以及牙科和心理保健，在圣地亚哥设有八个保健中心。2020 年 12 月，SDFC 成为数据泄露的受害者，导致未经授权披露了姓名、出生日期、社会安全号码、帐号、治疗信息、保险数据和其他敏感的患者数据。此次违规是由于 SDFC 的技术托管服务提供商的安全保护措施松懈所致。

https://www.natlawreview.com/article/san-diego-family-care-settles-data-breach-class-action-1-million?&web_view=true

2、前亚马逊工程师被定罪，曾盗窃曝光超 1 亿人数据

2022 年 6 月 19 日消息，美国西雅图陪审团裁定，前亚马逊软件工程师 Paige Thompson 被指控在 2019 年从 Capital One 窃取数据，犯有电信欺诈罪和五项未经授权访问

受保护计算机的罪名。

Capital One 黑客攻击是美国最大的安全漏洞之一，该事件导致 1 亿美国人和 600 万加拿大人的数据泄露，包括姓名、出生日期、社保号码、电子邮件地址和电话号码。Thompson 于当年 7 月被捕，当时一名 GitHub 用户看到她在网站上分享有关从存储 Capital One 信息的服务器窃取数据的信息。

https://mp.weixin.qq.com/s/8RFacSz41eisk4qg78kFYg

3、非洲最大连锁超市遭勒索团伙敲诈：600GB 数据失窃

2022 年 6 月 17 日消息，非洲最大连锁超市 Shoprite 披露了一起安全事件，部分地区客户受影响，姓名、身份证号等信息失窃；勒索软件团伙 RansomHouse 声称对此负责，称已窃取 600GB 数据，要求支付赎金。

https://www.secrss.com/articles/43667

4、威胁行为者利用企业滥用微软 Office 365 某功能，对企业发起勒索攻击

安全研究人员警告称，威胁行为者可能会劫持 Office 365 账户，对存储在 SharePoint 和 OneDrive 服务中的文件进行加密，以获得赎金，很多企业正在使用 SharePoint 和 OneDrive

服务进行云协作、文档管理和存储，如果数据没有备份，那针对这些文件的勒索软件攻击可能会产生严重后果，导致所有者和工作组无法访问重要数据。

https://www.freebuf.com/news/336489.html

5、数以万计开源项目开发账户遭大规模泄露

2022 年 6 月 14 日，安全研究人员发现流行的持续集成开发工具 Travis CI 发生大规模账户泄露，超过 7.7 亿条 Travis CI 免费版用户日志数据以明文方式泄露，其中包含大量敏感机密信息（开发令牌、云服务凭证等），包括 Github、Docker 的数以万计的开源项目开发账户受到影响。

https://www.secrss.com/articles/43505

6、美国 Transact Campus 配置错误泄露 3 万多学生的信息

2022 年 6 月 15 日报道，SafetyDetectives 发现了一个配置错误的 Elasticsearch 服务器，其中包含 Transact Campus 的应用程序的数据。该应用用于高等教育机构的学生的支付流程，此次事件泄露了约 100 万条记录，涉及 3 至 4 万名学生。值得注意的是，用户名和密码等登录数据均以纯文本格式存储，且泄露的信用卡信息包括银行识别号、信用卡号的前六位和后四位和到期日期等。目前，数据库已被保护起来，但

该公司声称服务器不在他们的控制之下且数据是假的。但研究人员表示经过开源工具的检查，这些数据属于真实的用户。

https://www.hackread.com/elasticsearch-database-expose-login-pii-data-students/

7、马来西亚软件供应商 StoreHub 泄露 100 万条客户记录

2022 年 6 月 16 日报道，据研究人员称，他们在马来西亚的软件供应商 StoreHub 所运行的 Elasticsearch 服务器上发现了近百万条客户记录。

报告指出，StoreHub 服务器存储了大量未加密的数据。因此，这家安全公司的研究人员能够进入并访问 17 亿条记录，这些记录描述了近 100 万人的事务，这些记录总计超过 1TB。StoreHub 的商品提供销售点和在线订购，因此供应商存储有关经营其产品的企业和个人买家活动的数据。客户全名、电话号码、实际地址、电子邮件地址，甚至设备类型都在暴露的数据中。

https://www.theregister.com/2022/06/16/storehub_data_leak/?&web_view=true

8、乌干达证券交易所数据发生泄露，32GB 敏感数据曝光

2022 年 6 月 13 日，据外媒报道，乌干达证券交易所（USE）被发现暴露了其互联网上的全球客户、商业实体的

财务等敏感数据，这些数据量达 32GB。其中泄露的数据包括全名、用户名、完整地址、出生日期、访问令牌、 电话号码、电子邮件地址、明文密码、用户 ID 号、银行等详细信息。据称，乌干达证券交易所数据泄露是源于其在线服务门户 Easy Portal 配置错误的数据库暴露在互联网上，且允许公众访问，导致大规模数据泄露。截至目前，乌干达证券交易所、乌干达 CERT（计算机应急响应小组）和其他几个政府机构尚未出面回应此次数据泄露事件。在此期间内，服务器暴露在互联网数天。

https://www.hackread.com/scoop-uganda-security-exchange-leaking-sensitive-records/

9、研究人员发现 BeanVPN 近 20GB 的连接日志可公开访问

2022 年 6 月 15 日消息，Cybernews 的调查发现提供商 BeanVPN 18.5 GB 的连接日志可被公开访问。该缓存日志包括超过 2500 万条记录，涉及用户设备和 Play 服务 ID、连接时间戳和 IP 地址等。研究人员表示，Play 服务 ID 可用于查找用户登录设备时使用的电子邮件地址。此外，该提供商表示不收集用户 IP 地址、传出 IP 地址、连接时间戳和会话持续时间等信息。但这一说法与泄露的信息并不一致，后者几乎包含了 BeanVPN 声称不会收集的所有数据。目前，泄露的

数据已被保护起来。

https://www.infosecurity-magazine.com/news/beanvpn-leaks-user-records/

10、人力资源公司 Robert Half 称黑客攻击了 1000 多个客户账户

2022 年 6 月 17 日，据外媒报道，人力资源咨询公司 Robert Half 已开始通知客户，在黑客攻击他们的 RobertHalf.com 帐户后，他们的个人和财务信息可能已被泄露。

该公司向缅因州总检察长提供的信息显示，威胁行为者在 4 月 26 日至 5 月 16 日期间以 Robert Half 为目标开展了攻击。该事件于 5 月 31 日被发现，影响了 1058 人。目标账户存储包括诸如姓名、地址和社会安全号码等信息，以及工资和税收信息。该公司指出，直接存款的银行帐号存储在这些账户中，但只有最后四位数字可见。

https://www.securityweek.com/staffing-firm-robert-half-says-hackers-targeted-over-1000-customer-accounts?&web_view=true