全球数据安全观察

总第 88 期 2022 年第 16 期

（2022.05.09-2022.05.15）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、国家发改委《“十四五”生物经济发展规划》：促进健康数据共享和发展

5 月 10 日，国家发展改革委印发《“十四五”生物经济发展规划》（以下简称《规划》）。《规划》指出，要推动生物信息产业发展。

一是促进**数据共享**。利用第五代移动通信（5G）、区块链、物联网等前沿技术，实现药品、疫苗从生产到使用全生命周期管理，构建药品追溯体系。整合健康可穿戴设备、互联网医疗、医疗保险等多源异构数据，实现健康态数据和主动健康产品数据互联互通。**促进区域医疗健康数据安全有序汇聚与共享**，支撑区域卫生健康大数据产业发展。

二是面向心脑血管疾病、肿瘤、呼吸系统疾病、糖尿病等重大疾病，依托人工智能技术、生物医学和健康大数据资源，发展智能辅助决策知识模型和算法，辅助个性化新药研发，为疾病诊断治疗提供决策支持。开发远程监护装备、可穿戴设备等生命支持和监护产品，发展基于智能视觉与语音交互、脑机接口等技术的新型护理和康复装备。

三是优化便民服务。发展远程医疗服务，支持发展“互联网 + 卫生健康”，建设区域性远程医疗服务中心、基因技术服

务中心、第三方影像信息中心等，完善“互联网 + 医疗服务”的医保支付政策，并以改善就医体验为重点，实现线上线下医疗服务一体化。

https://mp.weixin.qq.com/s/WYcOtJxxzttY6zuBOiOdAA

2、国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》，积极探索隐私计算等新技术在各类场景的应用潜力

近日，国家药监局关于印发《药品监管网络安全与信息化建设“十四五”规划》的通知（下文简称为《规划》）。《规划》指出强化数据资源共享与大数据应用，积极探索**大数据、人工智能、区块链、物联网、隐私计算等新技术**在审评审批、监管检查、执法取证、全链条追溯等各类场景的应用潜力。

《规划》在建设成效中指出：**强化数据资源共享与大数据应用**。全面贯彻落实国家大数据战略规划，强化药品监管数据管理与应用，建成药品监管数据共享平台，有效汇聚全国范围内的药品监管数据资源，实现国家局与省局之间的数据互联互通。探索完善药品品种档案、医疗器械唯一标识等数据应用，为监管业务提供有力的数据支撑。完善网络安全防护与信息安全建设。国家局积极建设安全管理及运营平台，并通过多种技术手段建设完善安全信任体系，构建统一的大

运维、大安全的服务管理模式。各省局积极开展网络安全等保配套建设，安全保障能力显著提升。

《规划》在基本原则中指出：业务引领，数据驱动。坚持以监管业务为中心，以监管需求为导向，正确把握监管服务与技术支撑的关系，**以数字化转型驱动智慧监管改革升级，打破信息孤岛，加强数据共享开放，构建药品全生命周期数字监管新模式**，提高监管部门的监督管理能力和政务服务水平。

《规划》在重点任务里提到：提升技术业务融合创新能力。积极探索大数据、人工智能、区块链、物联网、隐私计算等新技术在审评审批、监管检查、执法取证、全链条追溯等各类场景的应用潜力，以满足全生命周期监管、数字化监管、移动化监管、线上线下监管、全时段动态监管等创新监管的新需要。

另外，《规划》的重点任务之一是：**推进监管数据融合与驱动。一、推进数据资源汇聚共享。二、完善数据资源融合治理。三、提升数据资源应用水平。**

https://mp.weixin.qq.com/s/t_XnuBHpLIHsSxk03Fezbg

3、河南印发《河南省政务数据安全管理暂行办法》，为政务数据上“安全锁”

近日，河南省政府办公厅发布《河南省政务数据安全管理暂行办法》（以下简称《暂行办法》），明确了河南各级政务部门**非涉密政务数据收集、存储、传输、共享、开放、使用、销毁等行为及相关管理工作要求，进一步健全政务数据安全防护体系，为政务数据上一把“安全锁”**。

《办法》中指出，在职责分工中需要：会同本级网信、公安等部门按照职责研究解决涉及政务数据安全的重大事项，建立政务数据安全监测预警、信息通报和应急处置机制，检查、评估政务部门政务数据安全工作，指导政务部门建立政务数据应急管理制度；建立完善政务数据安全防护体系，制定政务数据安全事件应急预案，定期开展应急演练。

《办法》还指出，在建设与运行中需要：在政务数据收集、共享交换、开放等环节，政务部门应制定政务数据安全传输策略，利用安全可信通道或者采取加密等措施，确保传输过程可信可控；对关键传输链路、重要设备节点实行冗余建设，保障数据传输可靠性和网络传输服务可用性。政务部门应**履行数据安全审查职责，按照数据安全、保护隐私有关要求和使用需求确定本部门政务数据开放范围**。

https://mp.weixin.qq.com/s/EgnZ_GX2Dlew-shHVi8OEg

4、陕西加快推进数字经济产业发展，培育数据要素市场，建设数据产品超市

近日，陕西省人民政府办公厅关于印发加快推进数字经济产业发展实施方案（2021—2025 年）的通知（下文简称《方案》）。

《方案》指出重点任务有加强数字技术创新应用、壮大数字产品制造业、做强数字技术应用业、培育数据要素驱动业、推动制造业数字化转型、培育数据要素市场六个方面。其中，重点任务之一是培育数据要素市场。建立数据确权、价值评估、交易流通、数据传输和安全保护等基础制度和标准规范，健全数据产权交易和行业自律机制，探索建立数据产权保护和利用制度。推动陕西数据产品超市平台建设，构建规范化数据产品交易渠道。推进政府数据开放共享平台建设，支持大型工业企业、互联网平台企业等行业龙头企业与公共数据运营机构合作，开展数据汇聚与融合应用试点，创新数据合作新模式。

《方案》中提到的重大工程有数字产业培育工程，提出建设数据产品超市。搭建陕西数据产品超市平台，遴选优秀大数据场景化应用案例，多形式开展数据产品、算法、数字软件、解决方案及存储能力、计算能力的供需对接，积极探索新型数据产品交易方式。

《方案》在保障措施中指出：**强化数据安全。完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。健全数据安全风险评估、信息共享、监测预警和应急处置机制。制定数据隐私保护制度和安全审查制度。**

https://mp.weixin.qq.com/s/PPjo2CGQ9dw3XYJK4Lbu9A

5、深圳市探索开展数据交易工作方案

据深圳市发改委消息《深圳市探索开展数据交易工作方案》（以下简称《方案》），将构建数据交易系统、数据商务服务系统、综合运营管理系统、全局信息存证系统、数据安全保障系统，“五位一体”的新型数据交易信息化平台，激活释放数据活力，推动数字经济高质量发展。

《方案》是从建设原则、建设内容、建设计划三个方面进行说明。《方案》在建设内容上提出：**建设新型数据交易信息化平台；培育高频标准化交易产品和场景；制定数据交易制度规则和技术标准；构建完善的数据交易服务体系；稳步推进数据资产化、资本化；强化数据交易全过程监督。**

《方案》还提出，将要注册成立深圳数据交易有限公司，作为数据交易平台的运营主体，按着四个阶段，分阶段逐步推进建设。到 2022 年底，新型数据交易体系框架初步形成，

到“十四五”期末，初步形成全球数据交易市场枢纽，打造 5 家左右知名跨境数据商，培育 100 家以上具有技术优势及特色应用的中小型数据商。

https://mp.weixin.qq.com/s/TWDhnFHy9RLn9f_lb5VeiA

6、江西省数据条例公开征求意见：聚焦公共数据体系构建，探索建立容错免责机制

江西省近日就《江西省数据条例》向社会公开征求修改意见（以下简称《征求意见稿》）。《征求意见稿》为八章六十条，对于公共数据、非公共数据、数据要素市场、数据开发利用、数据安全以及相关法律责任有明确要求。

《征求意见稿》对公共数据体系、分级分类以及平台建设等进行了规定，同时提出**推动非公共数据共享，鼓励非公共数据向公共数据汇聚**。此外，《征求意见稿》还提到将聚焦数据开发利用，鼓励数字经济监管模式创新，探索建立容错免责机制。

《征求意见稿》提到，医疗卫生、养老服务、文化教育等涉及**个人信息和隐私的公共数据经过匿名化处理后无法识别特定个人且不能复原的，应当向全省统一的数据共享交换平台汇聚，推动公共数据开发利用**。《征求意见稿》还规定，公共数据和管理机构应当加强公共数据应用的管理，并

及时向省数据资源管理部门反馈公共数据应用成效。

https://mp.weixin.qq.com/s/FUwHT1B-2F4KIDB_P-6yEw

7、英国拟出台区别于 GDPR 的《数据改革法案》，这可能影响会欧盟的充分性保护决定

2022 年 5 月 10 日，英国举行国家议会开幕式。《数据改革法案》是今年女王讲话中的内容之一。脱欧后，英国政府提出了一项实施 GDPR 的法案，但前首相鲍里斯-约翰逊在 2020 年宣布他希望在欧盟框架外制定单独的数据法律。脱欧一年后，欧盟通过了数据充分性决定，裁定英国目前的数据保护足以继续欧盟-英国的数据传输。但是，欧盟制定了一些措施，允许委员会在英国政策发生重大变化时推翻这一决定。例如 "日落条款"，该条款将使数据充分性决定在 2024 年自动失效，届时是否续期将取决于英国的数据保护标准。英国表示希望与美国、澳大利亚、韩国和新加坡等国家建立新的数据流，欧盟担心这可能导致欧盟个人的数据被转移到隐私标准不完善的第三国。

改革细节尚未公布，但政府在去年的公众咨询中表示：它旨在提供一个数据保护制度，以尽量减少"负责任的数据使用的不必要障碍 ";减少企业的"不适当的不确定性或风险";使信息专员办公室（ICO）能够在一个更加强调数据驱动的

环境中进行监管。

https://mp.weixin.qq.com/s/9V754KeGn2E0Dpm9-5TTGA

技术、产品与市场

1、隐私保护计算（PPC）入选 IDC TechScape 报告“变革型”技术曲线

隐私保护计算（Privacy-Preserving Computation）入选《IDC TechScape：全球行业生态使能技术，2022》（IDC TechScape: Worldwide Future of Industry Ecosystems Enabling Technologies, 2022，Doc # US47437921）报告“变革型”技术曲线。。

IDC TechScape 报告对特定业务或场景可采用的相关技术通过可视化曲线的方式进行了展示，根据技术对组织的影响将技术分为三大类：**变革型、增量型、机会型**，并评估它们在各自类型曲线的相对成熟度。

作为入选六大“变革型”技术之一的隐私保护计算（PPC），IDC 认为该技术仍处于从概念验证到规模化推广的阶段，应用推广的速度中等，影响其应用成功落地实施的风险等级中等，并且具有很高的市场热度。而来自中国的隐私计算厂商也在报告中与 Meta、Google 及 AWS 并列为该领域值得关注

的技术提供商。

https://mp.weixin.qq.com/s/LWF255XKNeKuVKRT1bwWGA

2、2022 年企业需要关注的十二项数据和分析趋势

俄罗斯和乌克兰所引发的地缘政治危机对于遭受新冠疫情长期肆虐的世界无疑是雪上加霜。今年数据和分析领导者的工作重点之一是管理由此引发的持续不确定因素和波动性。现在应该根据关键数据和分析技术趋势对于业务优先事项的紧迫性和匹配性来监测、尝试或积极投资于这些趋势，以此预测、调整并扩大数据和分析战略的价值。今年的主要数据和分析趋势主要关注以下三大主题:

- **激活多样性和活力。**使用自适应 **AI 系统**推动增长和创新，同时应对全球市场的波动。
- **增强人员能力和决策，**以提供由业务模块化组件创建的丰富的、情境驱动的分析。
- **将信任制度化，**以大规模地实现数据和分析的价值。管理 AI 风险并实施跨分布式系统、边缘环境和新兴生态系统的互联治理。

https://mp.weixin.qq.com/s/9szAF9fySTtBSEbZVnVH2g

3、2022 谷歌 I/O 大会丨如何缓解用户对隐私问题的担忧成为一道必解题

Google I/O 2022 开发者大会在北京时间 5 月 11 日凌晨正式开幕，隐私是大会的关键词之一。谷歌与隐私管理相关的改变主要聚焦在 3 个方向：安全，更好的隐私设计以及提高用户控制权。

作为一家互联网公司，隐私管理和谷歌所有的产品和服务息息相关，这也是谷歌一直以来不得不面对的敏感领域：

如何缓解用户对隐私问题的担忧成为一道必解题。谷歌强调自己在隐私保护上，从“产品”到“保护性计算工具包”，再到“让用户有更多控制权”，Google 都在努力让全球用户的隐私和网络安全获得更好的保护。

https://mp.weixin.qq.com/s/cfXFSGq8inVA-8cg5FHOeA

4、卡巴斯基发布《2022 年勒索软件威胁趋势报告》

2022 年，勒索软件的活跃程度不亚于以往，世界范围内的企业饱受着勒索软件的威胁。与此同时，恶意软件的旧变种、新变种也卷土袭来，网络安全格局变幻莫测。近日，卡巴斯基研究人员从技术和地缘政治层面分析了 2021 年末和 2022 年发生的攻击事件，为打击网络犯罪及时的提供了威胁情报，分析了未来几个月可能出现的勒索软件威胁趋势：

趋势 1：威胁参与者正在尝试开发跨平台勒索软件

由于多年来越来越流行的大型游戏狩猎 (BGH) 计划，网络犯罪分子已经渗透到运行各种系统的越来越复杂的环境中。为了造成尽可能多的损害并使恢复变得非常困难，攻击者开始转向尝试加密尽可能多的系统。同时，这也意味着他们的勒索软件应该能够在不同的架构和操作系统组合上运行。克服这个问题的一种方法是使用“跨平台编程语言”（例如 Rust 或 Golang）编写勒索软件。

趋势 2: 勒索软件生态系统正在演变并变得更加“工业化”

就像合法的软件公司一样，网络犯罪组织也在不断地开发他们的工具包，重新命名他们的勒索软件，在此过程中改变点点滴滴，逐渐转向“工业化”。Lockbit 的演变，自 2019 年以来最成功的 RaaS 之一。

趋势 3: 勒索软件团伙在地缘政治冲突中偏袒一方

在全球 Covid-19 大流行的初始阶段可以清晰的看到 Covid-19 相关的垃圾邮件和网络钓鱼电子邮件激增;2022 年乌克兰的地缘政治冲突也是如此。通常在这样的地缘政治冲突中，人们会将网络攻击的来源与国家支持的威胁行为者联系起来，但网络犯罪组织和勒索软件团体也会“积极”采取行动。Conti 就在近期俄乌战争中选择了明确一方站队。

https://securelist.com/new-ransomware-trends-in-2022/106457/

5、企业 SaaS 应用中的十大数据访问风险

软件即服务（SaaS）应用可以给企业数字化发展带来很多便利，能够帮助用户实现更具性价比的实时工作协同，提升业务效率。但是，当企业频繁通过 SaaS 应用进行日常文件和业务数据交换时，如果缺少精细化的安全访问控制措施，将会让企业面临严重的数据泄漏风险。以下梳理汇总了企业在使用 SaaS 系统时，经常会发生的十种数据安全风险:

（1）SaaS 应用的访问权限缺乏时效性管理;

（2）企业员工个人身份信息过度曝光;

（3）第四方外部人员（企业第三方合作伙伴的外部供应商）的安全风险无法评估;

（4）员工在开放的环境下过度共享加密信息;

（5）多个 SaaS 应用程序的权限管理难以统一;

（6）对 SaaS 数据共享缺少监管;

（7）离职员工的恶意使用行为;

（8）安全团队缺乏对业务安全需求的了解;

（9）员工通过 SaaS 系统访问有潜在风险的第三方应用程序;

（10）不安全的内部访问权限设置与共享。

https://www.secrss.com/articles/42330

业界观点

1、沈艳：数据不用就安全了吗？

目前市值最大的苹果、微软、亚马逊、Alphabet(谷歌)、Meta(脸书)，他们的发展历程中都不乏数据安全事件。那么，雪藏不用，是不是数据就最安全？北京大学国家发展研究院教授、北大数字金融研究中心副主任沈艳认为，为了保护数据安全而雪藏数据，反而可能是最不安全的安排。至少有如下几个原因：

第一，如果数据丰富的企业不使用数据，就无法了解数据特征，就不知道数据的缺点、弱点在哪里。第二，不使用数据不利于发挥数据丰富企业的自身数据优势，甚至是放弃了核心竞争力。第三，不使用数据难以“知彼”，无法通过实战学习应对攻击的措施，并作出有力防范。第四，即便不使用数据保障了数据安全，但有数据生产要素却不运用的代价是无法通过发展获取数字红利。

事实上，无论是《意见》还是《数据安全法》，指出的方向都是“以发展促安全”，而不是“为安全不发展”。

（1）推动公共数据有序开放共享和安全利用，使数据需求方无需或仅支付成本价格，从而降低交易成本和合规成本。

（2）从技术上解决安全问题，实现“数据可用不可见”，

例如采用基于密码算法及协议的隐私保护技术，或构建可信执行环境(Trusted execution environment，TEE)，实现基于硬件安全的内存隔离的安全计算。

（3）要求平台明确对不同利益相关方的由算法所体现的利益分配机制，并要求平台报告对算法训练和算法评估及选择中用到的数据来源和质量、算法预测或优化目标、算法使用的技术、算法运行效果等。通过对算法的评估，在风险到来之前对于平台企业算法的安全性有更全面的掌握。

（4）以发展促数据安全，在激励机制上，需要有一定的容错率，但需要从机制上明确相关主体责任，尽量避免数据安全漏洞和风险。不能以保障数据安全为由而固步自封，也不能因鼓励创新而疏于监管机制建设和模糊责任担当。

https://www.bimba.pku.edu.cn/wm/xwzx/xwlx/jsgd/523077.htm

2、汤珂：数据交易的难点与解决之道

近日，清华大学社会科学学院经济所教授、所长汤珂在演讲中分享了对数据交易的难点与解决之道的看法。

汤珂认为，数据交易的难点和痛点存在于，第一，在交易前，数据权属是否存在不确定性；交易的数据是否合规。第二，在交易中，数据传输的安全性是否得以保障；是否存在交易所不见数据的问题。第三，在交易后，数据送达和争

议解决；以及买方未经卖方许可，是否存在转卖、倒卖其购买的数据等问题。

汤珂表示，可以从政策、技术和监管三个方面得出可行的解决方案。

（1）政策及制度配套：明确什么样的数据可以交易，明确谁可以交易（交易卖方），明确数据持有者的责任和义务（交易买方），需按照持有者权属（使用权等）进行保护，做到使用的“场景公正”。

（2）技术：对于数据交易中不涉及隐私的数据，公钥密码学非常重要。对于很难发生权属转移的隐私数据需要使用隐私计算技术如联邦学习、多放安全计算、可信执行环境等技术。此外，博弈论（机制设计）、人工智能、区块链等技术也是支持数据交易的重要技术。

（3）监管：监管的重要性首先在于打击非法活动，特别是打击黑市交易等。其次是明确执法机构；以及依法规制泄露数据行为，打击数据交易中的刷单等交易；建立仲裁机制，特别是监管方需要提供证据以明晰交易中买卖双方的责任；同时，运用区块链、人工智能等新型监管技术，建立监管沙箱。

https://mp.weixin.qq.com/s/aVtzH22plnGKKSNV2bOQpg

3、专家观点：公共数据资源开发利用网络安全保障模型研究

公共数据资源开发利用对提升政府治理能力和治理体系现代化、推动数字经济高质量发展、提升政府公共服务水平具有重要意义。

公共数据资源开发利用面临的风险和挑战主要包括：公共数据资源开发利用面临合规性挑战，公共数据资源开发利用安全监管难度大，公共数据资源面临恶意篡改等多重威胁，公共数据资源开发利用基础设施易遭受攻击。

对此，专家提出以下安全保障建议：规范公共数据资源开发利用生命周期，厘清公共数据资源开发利用责任主体，强化公共数据资源开发利用制度建设，打造公共数据资源开发利用监管平台。

http://www.sic.gov.cn/News/91/11523.htm

4、人民日报：个人信息要多加几道保护锁

不久前，中消协发布的《APP 个人信息泄露情况调查报告》（以下简称《报告》）发现，个人信息泄露的两条最主要途径，一是经营者未经本人同意暗自收集个人信息，二是经营者或不法分子故意泄露、出售或者非法向他人提供个人信息，这两者均超过调查总样本的 60%。

个人信息泄露的源头是什么？“问题出在过度采集上。”

陈音江说，“合法、正当、必要”六字是目前相关法律对个人信息采集和使用的规定，必须贯彻落实，同时要尽快明确，哪些事项必须通过实名制注册或办理，哪些事项无需实名，避免信息采集主体过多、实名登记事项过度。

“如何引导行业对于个人信息进行分类，构建分级分类保护体系，这是当前个人信息防泄露问题要着重考虑的一项。”腾讯守护者计划安全专家马瑞凯说。

受访专家表示，个人信息获取、存储和利用的环节众多，许多信息的传播又具有隐蔽性和复杂性，做到切实保障公民个人信息安全，需要公民、信息采集机构、技术人员和有关部门协同共治。就企业管理层面而言，要推动数据防窃密、防篡改、防泄露等安全技术的研发和部署，有效降低不法分子窃密风险；就监管部门而言，要进一步加大对电信诈骗、网络诈骗等违法犯罪活动的打击力度，持续形成高压态势，保护消费者的合法权益。

http://gzhuids.com/?p=5774

5、医疗机构如何构建个人信息保护合规体系？

医疗健康信息作为我国重要的基础性战略资源，加之本身具有隐私性与高价值性，使得医疗机构个人信息面临着外部威胁组织化、内部机制有待完善的双重安全威胁。

鉴于医疗健康信息的隐私性、高价值性以及成熟的监管环境，个人信息保护的落地需具备“系统”视角，从组织、制度、资产、技术等方向协同发力：

（1）建立组织以明确职能分工有效实现部门协同；

（2）完善体系以建立系统化的个人信息保护规章制度；

（3）梳理资产以形成个人信息资产清单持续动态更新；

（4）技防落地，采用合适的技术落地安全策略。

https://www.cn-healthcare.com/article/20220509/content-569345.html

数据安全事件

1、ElasticSearch 服务器配置错误，暴露 579GB 用户网站记录

2022 年 5 月 12 日，hackread 资讯网站消息，**两台配置错误的 ElasticSearch 服务器共暴露了约 3.59（35 9019902）亿条记录**，这些记录在 SnowPlow Analytics 开发的数据分析软件帮助下收集而来。Website Planet 的 IT 安全研究人员发现了两台暴露的 ElasticSearch 服务器，经过研究，确定服务器使用的是软件供应商 SnowPlow Analytics 开发的开源数据分析软件，尚不清楚属于哪个组织。

https://www.secrss.com/articles/42394

2、俄克拉荷马城印第安诊所数据泄露影响近 40,000 人

2022 年 5 月 12 日，据外媒报道，俄克拉荷马城印第安诊所 (OKCIC) 本周宣布，它经历了一次数据泄露事件，泄露了近 40,000 人的个人身份信息 (PII)。

为了调查此事件，OKCIC 寻求第三方法证公司的帮助。随后的调查证实，未经授权的一方访问并可能保留了敏感的客户信息。OKCIC 透露，被泄露的文件包括客户的姓名、出生日期、处方信息、医疗记录、医生信息、健康保险单号码、

电话号码、社会安全号码和驾驶执照号码等。据报道，多达 38,239 人受到了违规行为的影响。

据了解，3 月，美国通过立法，强制关键基础设施公司在 72 小时内向网络安全和基础设施安全局 (CISA) 报告网络事件。医疗保健是 CISA 定义的 16 个关键基础设施部门之一。

https://www.infosecurity-magazine.com/news/oklahoma-city-indian-clinic-data/?&web_view=true

3、南非公司 Dis-Chem 遭到攻击泄露超过 360 万人的信息

2022 年 5 月 11 日报道，南非最大的药品零售商之一 Dis-Chem 已泄露超过 360 万人的信息。据该公司称，此次事件是由其第三方服务提供商遭到网络攻击导致的，涉及客户的姓名、邮件地址和手机号码等信息。泄露发生在 4 月 28 日，在 5 月 1 日才被发现。近期，攻击者越来越多地针对南非的组织，2 个月前，美国消费者信用报告机构 TransUnion 称其位于南非的服务器被入侵，泄露了 5400 万用户的信息。

https://www.itweb.co.za/content/PmxVE7KEABOqQY85

4、约 2100 万个 VPN 用户的个人信息在 Telegram 上被公开

据 VPNMentor 在 5 月 9 日的报道，约 2100 万个 VPN 用

户的个人信息已被泄露。该 SQL 转储于 5 月 7 日在 Telegram 上发布，大小为 10 GB，包括 GeckoVPN、SuperVPN 和 ChatVPN 等多个 VPN 服务的用户的信息，涉及邮件地址、用户名、姓名、国家、密码字符串、结算明细和状态等。研究人员指出，VPN 用户更重视隐私和匿名性，因此他们的数据更有价值，当其个人信息泄露时，他们更可能遭到勒索攻击。

https://www.vpnmentor.com/blog/vpns-leaked-on-telegram/

5、研究人员在暗网上发现 31,000 个富时指数公司的登录凭证

2022 年 5 月 10 日，据外媒报道，Outpost24 的安全专家警告英国富时指数公司（FTSE 100），在暗网上发现其数以万计的公司登录凭证，他们可能会在不知不觉中受到严重威胁。

据调查，Outpost24 使用其威胁监控工具 Blueliv 搜索网络犯罪网站以查找被泄露的凭据，找到属于 FTSE 100 公司的 31,135 个用户名和密码。这些凭据中约有四分之三 (75%) 被认为是通过常规数据泄露窃取的，而大约四分之一是通过单独针对性的恶意软件感染获得的。Outpost24 表示，大部分 (60%) 被盗凭证来自三个监管最严格的行业——IT/

电信 (23%)、能源和公用事业 (22%) 以及金融 (21%)。

https://www.infosecurity-magazine.com/news/researchers-31000-ftse-100-logins/?&web_view=true

6、攻击者伪造 WhatsApp 语音通知来窃取信息

2022 年 5 月 15 日报道，研究人员发现，恶意攻击者在钓鱼活动中伪造了来自 WhatsApp 的语音信息通知，并且利用了合法的域名来传播恶意软件窃取信息。

研究人员说，到目前为止，攻击者发送的邮件数量已经达到了 27,660 个，该攻击活动通知受害者有一个来自 WhatsApp 聊天应用程序的 "新的私人语音邮件"，并附加了一个链接，并声称允许他们播放该语音。研究人员说，攻击的目标组织包括医疗保健、教育和零售行业。攻击者的诈骗策略包括在那些发送的电子邮件中获得用户信任来进行社会工程学攻击；通过伪造 WhatsApp 合法品牌，利用合法的域名来发送电子邮件。

https://mp.weixin.qq.com/s/n3hPDVtbRobANrTIJJhDIQ

7、哥斯达黎加多个政府机构遭到 Conti 勒索软件攻击，全国进入紧急状态

2022 年 5 月 9 日，据外媒报道，哥斯达黎加多个政府机

构遭到 Conti 勒索软件组织攻击，全国进入紧急状态。其中财政部、卡塔戈省电力服务行政委员会（Jasec）、国家气象研究所 (IMN) 、Radiográfica Costarricense S.A. (Racsa)、哥斯达黎加社会保障基金 (CCSS)等机构均受到 Conti 勒索软件攻击的影响。由于政府程序、签名被打乱，财政部的数字服务一直无法使用，这严重影响了政府部门运营。随后，哥斯达黎加政府宣布进入国家紧急状态。

据外媒报道称，Conti 勒索软件团伙疑似向政府索要 1000 万美元的赎金，在政府拒绝支付后，勒索软件组织公开了 672GB 转储的数据，其中疑似包含哥斯达黎加政府机构的数据。

https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/

8、加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据

2022 年 5 月 11 日报道，专门为空军提供战斗机培训服务的的加拿大公司 Top Aces（顶级王牌）表示，已经遭到勒索软件攻击。该公司在周三（5 月 11 日）的一份声明中证实，正在对攻击事件开展调查。Top Aces 公司总部位于蒙特利尔，是“**加拿大与德国武装部队的独家空中对抗演习供应商**”，而

它的名字已经出现在 LockBit 勒索软件团伙的泄密网站上。

https://therecord.media/top-aces-ransomware-attack-lockbit/

9、Colonial Pipeline 因违反安全规定被罚款近 100 万美元

据媒体 5 月 10 日报道，因违反联邦安全法规，Colonial Pipeline 被美国运输部管道和危险材料安全管理局(PHMSA)罚款 986400 美元。2021 年 5 月初，美国最大燃料管道运营商 Colonial Pipeline 遭到 DarkSide 的勒索攻击，导致天然气供应中断，使 17 个州进入紧急状态。PHMSA 表示该公司未对手动关闭和重新启动其管道系统做好充分的计划，其管道在 2021 年 5 月的攻击后无法使用时，对全国造成了严重影响。

https://thehackernews.com/2022/05/us-proposes-1-million-fine-on-colonial.html

10、乌克兰黑客因在暗网上出售账户凭证而被判入狱

2022 年 5 月 15 日报道，美国司法部 (DoJ) 表示，来自乌克兰切尔诺夫策的 Glib Oleksandr Ivanov-Tolpintsev 因操作旨在暴力攻击服务器的僵尸网络而被判处联邦监狱监禁。根据美国司法部的文件，Ivanov-Tolpintsev 的僵尸网络被用来“同时解密大量计算机登录凭据”。在鼎盛时期，每周大约

有 2,000 台机器成为目标并受到攻击。从 2017 年到 2019 年，网络攻击者在暗网上经营一家商店，并出售数千份被黑的凭证。

https://www.wangan.com/p/7fy7f68455c5b8b8