全球数据安全观察

总第 80 期 2022 年第 08 期

（2022.02.28-2022.03.06）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、中央网信办等四部门印发《2022 年提升全民数字素养与技能工作要点》 筑牢数字安全保护屏障

近日，中央网信办、教育部、工业和信息化部、人力资源社会保障部联合印发《2022 年提升全民数字素养与技能工作要点》（以下简称《工作要点》）。通知要求，要坚持以习近平新时代中国特色社会主义思想为指导，以满足人民日益增长的美好生活需要、促进人的全面发展和全体人民共同富裕为根本目的，坚持目标导向、问题导向、结果导向，多措并举提升全民数字素养与技能，以优异成绩迎接党的二十大胜利召开。

《工作要点》明确了工作目标：到 2022 年底，提升全民数字素养与技能工作取得积极进展，系统推进工作格局基本建立。数字资源供给更加丰富，全民终身数字学习体系初步构建，劳动者数字工作能力加快提升，人民群众数字生活水平不断提高，数字创新活力竞相迸发，**数字安全防护**屏障更加坚固，数字社会法治道德水平持续提高，全民数字素养与技能发展环境不断优化。

https://mp.weixin.qq.com/s/W5uFEUtotGEgryWTkFMyCw

2、工信部：加强个人信息保护，切实保障用户权益

2 月 28 日，国务院新闻办公室举行新闻发布会，工业和信息化部部长肖亚庆在会上介绍，过去一年，工业和信息化部做好“我为群众办实事”实践活动，着力改进影响用户感知的各环节，不断提升服务质量，同时**加强个人信息保护，切实保障用户权益**，突出解决了 APP 治理和适老化改造两方面问题。在 APP 治理方面，通过制定标准、技术检验、专项整治、行业自律等措施，大力整治违规收集使用个人信息、弹窗骚扰等行为。

该活动重点关注以下四项行为：一是聚焦用户权益，加强综合治理。持续关注用户反映的各类违规问题，深入开展 APP 整治，对移动互联网服务涉及的诸多环节进行全链条、全覆盖监管。二是聚焦服务感知，满足用户期待。**提升个人信息保护水平**，督促主要互联网企业建立客服热线，响应用户诉求。三是聚焦重点人群，推进信息普惠。再组织一批新的 APP 和网站，开展适老化和信息无障碍改造提升，打造一批适老化和无障碍改造标杆。四是聚焦长效机制，形成工作合力。围绕移动互联网服务、**个人信息保护**等重点领域，进一步完善激励机制，同时完善问责机制。

https://mp.weixin.qq.com/s/T5fk7nXb78J8Ge-4r9EO8A

3、深圳发力工业领域数据安全管理

近日，工信部印发通知部署做好工业领域数据安全管理试点工作明确在辽宁等 15 个省（区、市）及计划单列市开展试点工作，深圳市作为唯一一个计划单列市纳入试点范围。为了做好此项工作深圳市工业和信息化局遴选了 15 家优质工业企业并将在这 15 家企业重点推进以下 4 项试点内容。

一是**落实工业领域数据安全管理**。构建深圳市工业领域数据安全管理组织结构，推动试点企业开展**数据分类分级**，制定**重要数据清单**，落实数据分类分级清单、**风险信息报送与共享**通报等数据安全管理机制。二是**开展工业领域数据安全防护**。建立健全工业领域**数据安全防护标准体系**，夯实企业侧**数据安全管理制度建设**，推动试点企业联合安全企业、支撑单位制定**数据安全防护方案**。三是**推动工业领域数据安全评估**。构建**数据安全评估架构**，推动试点进行**数据安全自评估**，及时整改相关安全问题，并将评估结果及时报送主管部门。四是工业领域**数据安全产品**应用推广。组织工业领域数据安全产品、技术、服务宣贯培训，并在试点企业应用的数据安全产品解决方案中遴选一批优秀产品解决方案和应用案例宣传推广。

https://mp.weixin.qq.com/s/MZH25p250ErgSbbN7WWn9w

4、广州数据交易公司成立

3 月 4 日，广州广电运通金融电子股份有限公司（以下简称“广电运通”或“公司”）发布公告称与广州交易集团有限公司（以下简称“交易集团”）共同出资设立广州数据交易有限公司（以下简称“数据交易公司”），注册资本为 1 亿元。

广州数据交易有限公司的大股东为广州交易集团，实控人为广州市人民政府。由此可见，广州市将建设国有控股的数据交易所，以广州市发达的数字经济发展规模及高科技企业的保有量来看，广州的数据交易所将成为北京数交所、上海数交所的有力竞争者，同时也给已经筹备完毕的深圳数交所带来很大的压力，未来广州数交所见面临前有北数所与上数所，后有深数所的竞争格局，同时也从侧面反映，发展**数据交易市场**，完善市场体系建设正一步步成为经济发达城市实现高质量发展不可或缺的重要一环。

https://mp.weixin.qq.com/s/-U3OA8f66wREFnIc_mP82g

5、首个基于“数据银行”的政务数据授权运营模式落地江西抚州

抚州市“数据银行”采用类银行的模式，对**数据进行价值挖掘应用、隐私安全保护**以及**数据产品的融通**，为数据提供者、数据需求者和生态技术服务商提供数据产品、交易撮

合和数据融通安全服务。相关负责人表示，抚州“数据银行”项目的建设，为抚州市政府的数字化治理、产业数字化转型和区域数字经济招商引资引才，提供了发展的“活水”。

当前，抚州“数据银行”平台已建设完成。“数据银行”已汇聚金融、医疗、农业、交通、文旅等运营场景所需的工商、司法、税务、社保、公积金、电力、能源等30余家政府委办局共计一千五百余张表格，约16亿条政务数据，实现了数据按日、按周、按月的稳步更新。通过政务数据深度挖掘，“数据银行”已经开始为各行业进行赋能增值，形成了数十种数据运营场景，在产业赋能、企业服务、便民服务中发挥了重要作用。

https://mp.weixin.qq.com/s/LG0U3Gqz_3Q5MR__xdUdtQ

6、贵州省大数据发展局发布《贵州省大数据战略行动2022年工作要点》

贵州省大数据发展局近日发布《贵州省大数据战略行动2022年工作要点》的相关通知及解读。据悉，2022年全省大数据工作的主要内容将从数字产业化、产业数字化、数字新基建、数字化治理、数据价值化、支撑保障6大方面，部署30项重点工作、130项具体任务。

其中提出：着力做实数据价值化，加快打造国家数据生

产要素流通核心枢纽。实施数据要素大开发行动，加快公共数据高质量归集和共享开放，推动教育、医疗、供水、供电、供气、交通等行业公共数据归集，在省属国有企事业单位建立数据专员机制。推进数据流通交易，优化提升贵阳大数据交易所，完善数据流通交易服务中心组织架构，搭建数据流通交易平台，在政务、金融、通信、电力、交通、信用等领域，培育引进一批专业“数据商”，培育数据集成、数据经纪、资产评估、定价评估、安全评估等第三方专业服务机构。开展数据要素市场化配置改革行动，探索数据市场化交易机制，研究出台支持数据要素市场培育财政制度，推进“场外交易”逐步转入“场内交易”。力争集聚数据商 300 家，形成数据产品 500 个，数据流通交易走在全国前列。

https://mp.weixin.qq.com/s/Q1fGeo0t_7kHTBtzy4xJgQ

技术、产品与市场

1、360 企业安全云免费助力中小微企业数字化转型，护航数字安全战略

3 月 1 日，360 推出“360 企业安全云”，面向中小微企业免费开放。360 企业安全云是专注于企业级数字化安全与管理 SaaS 套装，在 360 安全大脑的全面赋能下，360 企业安全云基于即用即懂的可视化安全控制中心和管理功能，面向中小微企业免费提供终端、网络、软件、数据、资产及防勒索等全方位数字化安全与管理服务。

360 集团创始人周鸿祎表示，要再掀起一次“免费安全新浪潮”，为受资金、技术、人才限制的中小微企业提供免费、全方位的数字安全管理服务，确保中小微企业实现数字化转型没有后顾之忧，在数字安全时代“不掉队”，护航国家数字安全战略。

http://stock.jrj.com.cn/2022/03/01150734507842.shtml

2、联邦生态系统：隐私计算的终极愿景

联邦学习首创团队带头人、谷歌研究院副总裁 Blaise Aguëra y Arcas 博士，与联邦学习亚洲奠基人杨强教授两位顶尖学者提出了一种新的构想，即用现有的数据来训练许多

小的模型，这些小的模型在物理上隔离，但是可以通过某种技术联系起来，形成一个庞大的包含许许多多小模型的虚拟网络来更好的服务全社会，这个虚拟网络不属于任何一个个体，而是整个人类的财产。这些小的模型会不停的学习进化，时刻保持最优的模型效果，当某个任务在虚拟网络中被执行时，相应的小模型能够参与其中协助完成任务，实现联邦学习。

这一技术能够很好地解决当前数据隐私安全对模型有效性及计算效率的限制，不仅能够降低联邦学习的成本，甚至可以从根源上解决数据隐私安全的问题，是联邦学习未来发展的必然趋势。

https://mp.weixin.qq.com/s/pX-VbjEaTufTBv5cL1FYZA

3、隐私计算技术解读：可信执行环境（TEE）概要及应用

作为基于密码学的隐私保护技术的一种替代方案，可信执行环境（Trusted execution environment，TEE）基于硬件安全的 CPU 实现了基于内存隔离的安全计算，可在保证计算效率的前提下完成隐私保护的计算。

TEE 是一种具有运算和储存功能，能提供安全性和完整性保护的独立处理环境。其基本思想是：在硬件中为敏感数据单独分配一块隔离的内存，所有敏感数据的计算均在这块

内存中进行，并且除了经过授权的接口外，硬件中的其他部分不能访问这块隔离的内存中的信息，以此来实现敏感数据的隐私计算。

TEE 强大的数据安全和隐私保护能力，使其成为隐私计算主要技术流派之一，比 REE 得到了更广泛的应用。但目前 TEE 技术还无法作为通用的安全技术进行应用，主要原因在于其安全性一定程度上依赖于对硬件厂商的信任，同时攻击面较多、安全边界定义不清晰，这都成为了限制其大规模应用的重要因素。对于用户而言，在 TEE 技术的应用过程中，需要清晰地了解其应用场景和局限性，以免造成不可预知的安全问题和财产损失。

https://mp.weixin.qq.com/s/zYSFpfoLk5v_H9Vqq-gBRA

4、[调研]敏感数据泄露事件持续上升

3 月 3 日，GitGuardian 发布报告称，2021 年企业泄露了超过 600 万个密码、API 密钥和其他敏感数据（统称开发“秘密”），泄密量是上一年的两倍。报告表明，推送到存储库的代码有所增加，并且可用的检测功能也更强大了。

GitGuardian 发现，平均而言，2021 年每 1000 个 GitHub 提交就有 3 个泄露秘密，这一频率比 2020 年高出 50%。超过一半的秘密包含访问数据存储服务、云提供商、私有加密

密钥或开发工具所需的凭证，另外 10%则含有用于消息传递系统和版本控制平台的凭据。

GitGuardian 开发人员倡导者 Mackenzie Jackson 表示，敏感访问信息泄露给潜在的攻击者会破坏公司网络和基础设施的安全性。此处的“秘密”一词指的是“授予服务、系统和数据访问权限”的任何数字身份验证凭证，包括 API 密钥、应用或服务凭证，以及安全证书。

https://mp.weixin.qq.com/s/dopLMoQXmxV5h3Bfhf5VUg

5、数据分深度应用、广泛共享、探索交易产生更复杂的安全态势

数字时代，数据资产化的趋势凸显，数据资产安全开始呈现流动性的新需求。传统的数据安全，聚焦在数据访问，以加密、防泄漏和备份为主要思路的静态安全思想，虽然能在一定程度上解决数据安全问题，但却极大地牺牲了数据作为生产资料的流动性。未来的数据安全防护思路，将会把重点放在数据资产的访问保护和共享保护上。由静态的安全防护逐渐向动态、流通的安全防护演进。目前行业对数据安全和数据交易的动态平衡进行了诸多探索，例如零信任、访问安全、隐私计算等新技术的探索，都是基于这个迫切的痛点给出的解决方案。他们在一定程度上解决了静态安全防御思

路的缺陷，2022 年这一趋势将会继续。

https://mp.weixin.qq.com/s/_9unhdwSVsUCXJSBMhb4fQ

业界观点

1、周鸿祎两会提交多份提案，关注数字安全、智能网联车、中小企业等

3 月 4 日，全国政协十三届五次会议开幕会举行，全国政协委员、360 创始人周鸿祎携多份提案上会，内容聚焦数字安全、智能网联汽车安全、开源软件安全以及中小企业安全。

（1）把网络安全升级为数字安全，筑牢数字安全屏障。

瞄准产业数字化新场景，同步规划建设行业数字安全体系，保障传统产业数字化转型；要面向新型数字技术和应用场景，研究建设前瞻性的数字安全平台体系；以城市为主体，由政府统筹打造城市级数字空间安全基础设施和应急体系，保障经济社会稳定发展。

（2）建立智能网联汽车 “数字空间碰撞测试”长效机制。

建立智能网联汽车“数字空间碰撞测试”机制和相关标准，保障汽车出厂安全和持续检测；建议规范汽车安全漏洞

的上报行为，不得恶意炒作和违规披露；打造以安全大脑为核心的智能网联汽车行业态势感知体系，建立汽车安全监管长效机制。

（3）鼓励帮扶中小微企业构建数字安全能力。

建议出台专项政策明确中小微企业应具备的数字安全能力要求；借鉴免费杀毒的模式，鼓励大型安全企业提供中小微企业的轻量化免费安全服务，让中小微企业数字安全不掉队。

（4）加强我国开源软件安全风险方法之力。

开展对开源代码的系统性漏洞挖掘，构建开源代码的安全风险评估机制；建立软件企业安全责任制，明确软件企业承担开源软件的全生命周期安全管理；积极参与国际开源社区，促进国际开源软件的漏洞挖掘。

https://mp.weixin.qq.com/s/DaxSwRNrOJFT9ZRJiyPOTA

2、两会前的政协委员热议：数字经济发展与数据安全兼顾

全国两会召开前，业界专家和委员们对于数字经济发展进行点评，其中多位专家对数字经济发展与数据安全兼顾提出了各自见解。

全国政协委员、原中国保监会副主席周延礼指出，目前在数字经济发展的制度建设方面，国家先后出台了一系列具

体政策、法律法规，对于维护健康数字经济市场秩序发挥了重要作用。他强调，数据的安全问题不但需要制度，更需要技术，这两方面都需要权衡好关系。

蚂蚁集团研究院院长李振华支出，数据要素发展和数据安全之间的平衡是保障数字化进程中兼顾保护个人信息的重要挑战和方向。以隐私计算为代表的技术创新是其中重要的探索。同时，他认为今年无论从法规要求还是技术成熟度上，整个数据流通领域将告别数据明文时代，开启“数据密态时代”的新征程。

锘崴科技创始人、董事长王爽针对关于加强数据安全、推进隐私保护计算技术，提三点建议：第一，健全完善数据流通和分享的政策监管体系，鼓励应用隐私保护计算的创新，鼓励在合法合规的基础上使用隐私保护计算挖掘数据价值，促进数据要素市场化的发展；第二，促进建立隐私保护计算技术与应用标准和产品认证体系，规范行业发展；第三，建立统一的数据行业监管平台，使用隐私保护计算作为数据行业的监管工具，依据法律法规对数据资源和算法资源进行监管，在安全可控的基础上促进数据要素化的发展。

http://www.cppcc.gov.cn/zxww/2022/03/01/ARTI1646112846258511.shtml

3、工信部肖亚庆：深入开展 APP 整治，实现三个“全覆盖”

工信部部长肖亚庆在国新办新闻发布会上透露，深入开展 APP 整治。肖亚庆表示，这项工作永无止境，今年还要继续做好。

一是聚焦用户权益，加强综合治理。持续关注用户反映的各类违规问题，深入开展 APP 整治，对移动互联网服务涉及的诸多环节进行全链条、全覆盖监管。主要实现三个“全覆盖”：即对手机、平板各类终端全覆盖；对应用商店、第三方软件开发工具包、预置预装等关键的责任链环节全覆盖；对 APP 技术检测全覆盖，让用户权益得到全方位保护。

二是聚焦服务感知，满足用户期待。提升个人信息保护水平，督促主要互联网企业建立客服热线，响应用户诉求。

三是聚焦重点人群，推进信息普惠。再组织一批新的 APP 和网站，开展适老化和信息无障碍改造提升，打造一批适老化和无障碍改造标杆。

四是聚焦长效机制，形成工作合力。围绕移动互联网服务、个人信息保护等重点领域，我们将进一步完善激励机制，同时也完善问责机制，强化技术手段，激发企业自身改进服务、提高水平的动能。

https://mp.weixin.qq.com/s/RiTsSL0UGflOn0tEIqy4Ng

4、全国政协委员皮剑龙：建议制定数字经济促进法、数据产权法

2022 年全国两会期间，全国政协委员、北京金台律师事务所主任皮剑龙指出，我国数字经济发展存在缺乏统筹设计，法律制度供给不足，立法结构和体系过于分散，数字经济管理体制机制不健全等问题，并带来相关提案。

皮剑龙建议设立“国家数字经济工作局”，作为中央统筹数字经济发展的管理协调机构，统筹谋划全国数字经济发展，组织实施数字经济建设等。他还在提案中指出，为了打破数字经济的政策障碍和体制瓶颈，亟需出台《数字经济促进法》，进一步鼓励创新，推动合理竞争。

同时，皮剑龙建议加快制定《数据产权法》，在其中明确合法、公平、效率等原则，确定数据所有权、支配权、使用权、收益权等权利的归属，与数据产权的流通和交易规范，以此增强市场主体对数据利益的可期待性和市场信心。

他还建议，加大关键核心技术的司法保护力度，健全大数据、人工智能、基因技术等新领域新业态知识产权司法保护规则；妥善审理涉数据交易、数据市场不正当竞争等案件，完善数据产权、数据隐私等司法保护机制，推动平台经济规范健康发展。

https://mp.weixin.qq.com/s/JNVRhz-7Bnzs9_xh-vTrGw

5、工信部田玉龙：将积极培育数据要素市场，支持北京、上海建设数据交易所

2022 年 2 月 28 日，工业和信息化部总工程师、新闻发言人田玉龙在国新办新闻发布会上表示，我国制造业数字化转型呈现加快发展态势，创新活动呈现出良好态势。主要体现在三个方面：一是数字化转型的基础不断夯实；二是转型范围不断拓展；三是转型程度不断提升。

田玉龙表示，下一步工信部将延续前期工作，重点抓好三个方面：一是要突出重点，增强企业数字化能力；二是要扩大应用，丰富产品供给；三是要建生态，优化数字化改造环境。

https://mp.weixin.qq.com/s/77Ffd5WqRCdfIqKzhZ8WIA

数据安全事件

1、加利福尼亚州律师协会的机密信息被网站泄露

2022 年 3 月 2 日报道，存储在 judyrecords.com 网站上的加利福尼亚州和不同司法管辖区的 260,000 起律师记录案件的敏感信息被泄露。泄露内容包括案件编号、有关各种案件和状态的信息、受访者、文件日期和证人被删除的名字。https://www.cysecurity.news/2022/03/state-bar-of-californias-confidential.html?utm_source=dlvr.it&utm_medium=twitter

2、英伟达在最近的网络攻击后披露数据泄露

2022 年 3 月 2 日，据报道，芯片制造商巨头英伟达在最近披露的安全事件中专有信息被盗后证实了数据泄露。勒索软件团伙从英伟达的网络中窃取了 1 TB 的数据并在网上泄露了大约 20GB 的数据，包括所有英伟达员工的凭据。https://securityaffairs.co/wordpress/128573/data-breach/nvidia-data-breach.html

3、“匿名者”组织宣称侵入俄罗斯太空研究网站并泄露任务文件

2022 年 3 月 4 日消息，作为俄乌冲突抗议活动的后续，“匿名者”组织刚刚宣称破坏了一个属于俄罗斯空间研究所

（IKI）的网站，并在推特上发布了指向俄罗斯联邦航空局（Roscosmos）泄露数据的缓存页面的链接。Vice 报道称，黑客似乎侵入了 IKI 网站的一个子域，同时其它子域仍处于正常在线的状态。

https://www.cnbeta.com/articles/tech/1243147.htm

4、乌克兰研究人员泄露了 Conti 勒索软件的源代码

2022 年 3 月 2 日，据报道，一名乌克兰研究人员在宣布支持俄罗斯后，泄露了 60,694 条属于 Conti 勒索软件操作的内部聊天消息。他能够访问 Conti 组的数据库 XMPP 聊天服务器。显然，针对 Conti 勒索软件的攻击和数据泄露是对其支持俄罗斯入侵乌克兰的报复。

https://securityaffairs.co/wordpress/128563/data-breach/conti-ransomware-source-code-leaked.html

5、黑客泄露了 190GB 的三星数据和源代码

2022 年 3 月 6 日报道，Lapsus$数据勒索团伙今天泄露了一大批机密数据，该组织声称这批数据来自韩国电子巨头三星。

Lapsus$发布了描述即将泄密的声明，称含有闯入后获取的“机密的三星源代码”，包括安装在三星的信任区

（TrustZone）环境中的每个可信任小程序（TA）的源代码、用于授权和验证三星帐户的技术的完整源代码等等。如果上述信息准确无误，说明三星已遭受重大数据泄露，可能对公司造成巨大损害。

Lapsus$将这批泄露的数据拆分成三个压缩文件，这些文件总共近 190GB 的容量，做成了大受欢迎的 torrent 种子文件来提供，已有 400 多个同行分享了内容。该勒索团伙还表示，它会部署更多台服务器，以提高下载速度。

https://mp.weixin.qq.com/s/sPMv2Vcyj96UemTlJQ_E_Q

6、Chrome Skype 扩展程序被发现泄露用户信息

2022 年 3 月 1 日，据外媒报道，微软修复了 Chrome 的 Skype 扩展程序中的一个隐私漏洞，该漏洞使数百万用户面临账户信息泄露的风险。安全研究员 Wladimir Palant 发现了一个“微不足道”的错误，该隐私漏洞会将用户的 Skype 帐户信息泄露给任何感兴趣的网站。据研究人员称，该漏洞存在于扩展程序的身份跟踪功能中，该功能可以确定用户是否登录了 Microsoft 帐户。

https://portswigger.net/daily-swig/private-chat-chrome-skype-extension-with-9m-installs-found-to-be-leaking-user-info?&web_view=true

7、Adafruit 披露了前员工 GitHub 储存库中的数据泄露

2022 年 3 月 6 日报道，纽约市开源硬件组件的供应商 Adafruit 披露了一个数据泄露事件，这个事件是由于一个可公开查看的 GitHub 存储库引起的。该公司怀疑这可能允许攻击者对 2019 年或之前对某些用户的信息进行“未经授权的访问”。

数据泄漏并不是来自 Adafruit 的 GitHub 存储库，而是来自一位前雇员。一名前雇员在他们的 GitHub 储存库中使用真实的客户信息进行培训和数据分析操作。该公司解释说：“Adafruit 在得到关于意外泄露信息的通知后 15 分钟内，就与这名前雇员取得联系，删除了相关的 GitHub 存储库，Adafruit 团队开始了检测程序，以确定是否有任何访问权限，以及哪类数据被影响了。”目前，Adafruit 并不知道这些暴露的信息被对手滥用，并声称其披露这一事件是为了“透明度和责任感”。

https://www.bleepingcomputer.com/news/security/adafruit-discloses-data-leak-from-ex-employees-github-repo/

8、申请系统漏洞 日本 6 万人份外籍入境者信息遭泄露

据日本共同社 3 月 2 日报道，鉴于日本政府放宽新冠病毒边境口岸措施，在线办理技能实习生和留学生等入境申请

手续的厚生劳动省专用系统“ERFS”存在漏洞，最多约 6 万人份的外籍入境者姓名、出生年月日、护照号码一度处于入境申请者可以阅览的状态。

http://d.youth.cn/shrgch/202203/t20220304_13497978.htm

9、医疗保健公司 Mon Health 披露第二起数据泄露事件

2022 年 3 月 3 日报道，医疗保健公司 Mon Health 在 2021 年 12 月 18 日发现遭受了第一次网络攻击，当时它的一些 IT 系统被中断，但几周后才得知潜在的数据被盗。2021 年 3 月初，Mon Health 披露了第二次数据泄漏，受影响的数据包括姓名、地址、出生日期、社会安全号码、健康保险索赔号码、病历号码、患者帐号、医疗信息和各种其他数据，大约影响 40 万人。

https://www.securityweek.com/healthcare-company-mon-health-discloses-second-data-breach

10、勒索软件组织 Conti 几乎所有的专有基础设施都已泄露

2022 年 3 月 1 日，推特账号 DarkOwl（@darkowlcyber）发布推文表示：勒索软件组织 Conti 几乎所有的专有基础设施都已泄露。

https://twitter.com/darkowlcyber/status/1498461185653411840