全球数据安全观察

总第 97 期 2022 年第 25 期

(2022.07.11-2022.07.17)

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、《网络数据安全管理条例》被列入国务院 2022 年度立法工作计划

7 月 14 日，国务院办公厅发布关于印发《国务院 2022 年度立法工作计划》的通知。此前曾在 2021 年 11 月由网信办发布过征求意见稿的《网络数据安全管理条例》，被明确列入 2022 年度立法项目中，由网信办组织起草。

http://www.gov.cn/zhengce/zhengceku/2022-07/14/content_5700974.htm

2、《关于加强商业银行互联网贷款业务管理提升金融服务质效的通知》发布

7 月 15 日，中国银保监会发布《关于加强商业银行互联网贷款业务管理提升金融服务质效的通知》，延续了《商业银行互联网贷款管理暂行办法》、《中国银保监会办公厅关于进一步规范商业银行互联网贷款业务的通知》一以贯之的监管原则，统筹发展和安全，对商业银行提出如下要求：

一是履行贷款管理主体责任，提高互联网贷款风险管控能力，防范贷款管理“空心化”。

二是完整准确获取身份验证、贷前调查、风险评估和贷

后管理所需要的信息数据，并采取有效措施核实其真实性。

三是主动加强贷款资金管理，有效监测资金用途，确保贷款资金安全，防范合作机构截留、挪用。

四是分类别签订合作协议并明确各方权责，不得在贷款出资协议中混同其他服务约定。对存在违规行为的合作机构，限制或者拒绝合作。

五是切实保障消费者合法权益，充分披露各类信息，严禁不当催收等行为。此外，还应加强对合作机构营销宣传行为的合规管理。

http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=1061888&itemId=917&generaltype=0

http://www.gov.cn/zhengce/2022-07/16/content_5701329.htm

3、《上海市数字经济发展“十四五”规划》印发

7 月 12 日，上海市人民政府办公厅发布关于印发《上海市数字经济发展“十四五”规划》的通知，在发展目标中指出：数据要素市场体系基本建立。

通知在重点任务中关于培育数据新要素的部分强调对数字安全的关注：加快安全技术创新突破，推动安全产品和服务的快速迭代和应用，做大做强安全产业。突破数字安全技术，深化多方安全计算、联邦计算、差分隐私等隐私计算

技术研发应用，引导密码算法、专用芯片、通信模块等关键产品突破。加快发展万物互联下的新一代身份认证技术，构建新型数字信任体系。

https://mp.weixin.qq.com/s/4HX8Hqzd2bn7wgUCNQnfkw

4、《广东省数字经济发展指引 1.0》发布

7 月 8 日，2022 中国数字经济创新发展大会在广东省汕头市举行。会上,《广东省数字经济发展指引 1.0》正式发布。指引中明确要建成数据安全保障体系。包括:

完善数据安全支撑体系。做好网络安全和**数据安全防护体系顶层**设计，落实相关法律法规和政策措施。加强**网络数据安全标准的统筹规划**，鼓励创新技术成果向标准转化，强化标准的实施与应用，加强标准的国际交流与合作，提升标准对网络数据安全保护的整体支撑作用。

加强数据安全管理能力。各行业主管部门组织开展**数据分类分级**工作，制订省市两级各部门及相关行业和领域的重要数据具体目录，对列入目录的数据进行重点保护。健全**数据隐私保护和安全审查**制度，落实政府部门、企事业单位、社会公众等数据安全保护责任。制定行业**数据安全风险评估**机制，推动有关部门、行业组织、企业、教育和科研机构、有关专业机构等围绕数据安全风险评估、防范、处置等方面

开展协作。建设**数据安全态势感知平台**，提升对数据安全隐患的监测、分析与处置能力。

https://mp.weixin.qq.com/s/Izsgdr5Vj-HqXYDOXlDMzw

5、浙江发布《互联网平台竞争合规管理规范》

浙江省市场监管局日前发布全国首个互联网平台企业竞争合规的省级地方标《互联网平台企业竞争合规管理规范》，8 月 5 日起在全省实施，旨在压实企业的竞争合规主体责任，实现政府监管模式下的平台自治。

该标准以互联网平台企业“自我优待”、“大数据杀熟”、算法滥用、强制“二选一”、资本无序扩张等破坏公平竞争的行为为研究对象，以发挥互联网平台企业竞争合规主体责任为出发点，从反垄断、反不正当竞争两个角度，全面梳理互联网平台企业竞争合规相关风险，明确互联网平台企业竞争合规管理活动要点。

https://mp.weixin.qq.com/s/q2kaoC8JLt9-_lNqjUKZkw

技术、产品与市场

1、2022 隐私计算十大观察

为推动隐私计算产业进一步发展，由中国通信标准化协会指导，中国信息通信研究院、隐私计算联盟主办的 2022 隐私计算大会于 7 月 13 日在北京召开，发布了 2022 隐私计算十大观察：

（1）数据产权分置，隐私计算迎来发展机遇；

（2）技术体系扩展，隐私计算概念外延深化；

（3）技术路线融合，优势互补突破应用瓶颈；

（4）平衡安全性能，安全分级灵活适应场景；

（5）支撑产品落地，技术可用性有一定提升；

（6）软件硬件协同，一体机成为产品新形态；

（7）应用落地加速，内外双向赋能数据流通；

（8）各方积极探索，合规路径亟需形成共识；

（9）激发技术创新，隐私计算积极拥抱开源；

（10）共识继续强化，互联互通加速落地实践。

https://mp.weixin.qq.com/s/KqcaCQv3FjItqln-9Pkhlg

2、Gartner 发布当前至 2024 年的五大隐私趋势

频发的安全事件对数字经济发展带来巨大挑战，全行业

从危机管理现实需求出发，正促进灾备体系向全行业广泛延伸应用。威胁加剧、灾备云化、云化应用是灾备向全行业延伸应用的关键。

根据 Gartner 的研究，随着全球隐私法规数量的不断增加，企业机构应关注五项重大隐私趋势，以应对保护个人数据和遵守监管要求方面的挑战。五大隐私趋势分别是：**数据本地化、隐私增强计算技术、AI 治理、集中式隐私用户体验和远程模式进化为“万物皆混合”**。

Gartner 研究副总裁 Nader Henein 表示：“根据 Gartner 的预测，**到 2024 年末，全球 75%人口的个人数据将得到现代隐私法规的保护**。这一监管方面的进步已成为推动企业机构加强隐私保护的主要动力。由于多数企业机构尚未形成专门的隐私保护实践，隐私保护责任落到了技术人员身上，更确切地说，落到了首席信息安全官所领导的安全团队身上。”

未来两年，几十个司法管辖区将陆续实施隐私法规，因此许多企业机构认为有必要马上启动隐私工作计划。**根据 Gartner 的预测，到 2024 年，大型企业机构的年均隐私预算将超过 250 万美元**。

https://mp.weixin.qq.com/s/qdkr8wYbLN8CExGUQuFjWA

3、身份访问管理 (IAM) 将迎来爆发式增长

根据瞻博网络上周发布的一项研究报告，**未来五年，全球在身份和访问管理(IAM)解决方案上的支出将增长 62%**，从今年预计的 160 亿美元增加到 2027 年的 265 亿美元。新增的 IAM 市场将主要基于 SaaS 模式（云 IAM），分析师认为 SaaS 正在迅速成为购买 IAM 解决方案的主要模式——预计到 2027 年，云 IAM 将占据 IAM 市场的绝大部分。

随着 SaaS 模式在 IAM 市场的激增，越来越多的小公司发现 IAM 已经触手可及，研究表明，这一趋势将以滚雪球的方式持续增长。虽然云 IAM 现在仅占市场的 60%，但研究人员预测五年后云 IAM 将占据 IAM 总体市场的 94%。

https://www.secrss.com/articles/44563

4、IDC：2021 年中国网络威胁检测与响应市场规模达 3.1 亿美元

IDC 于 2022 年 7 月正式发布了针对中国 NDR 产品的市场份额研究报告，即:《中国网络威胁检测与响应市场份额，2021：实战效果显著，市场需求明确》（# CHC48497322）。报告针对 2021 年中国网络威胁检测与响应市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。报告数据显示，中国网络威胁检测与响应市场在

2021 年实现了 36.6%的同比增长，规模达到 3.1 亿美元。
https://www.secrss.com/articles/44504

5、原语隐私计算服务平台 SaaS 版正式发布

7 月 9 日，原语科技正式对外发布 SaaS 版隐私计算服务平台，旨在让企业方便快速使用隐私计算产品。原语科技自主研发的隐私计算平台 Primihub 及管理平台 Primihub-Platform 均已在 GitHub 上开源。

SaaS 版 Primihub 隐私计算服务平台涵盖匿踪查询、隐私求交、联合建模、联合统计、审核授权、数据资源管理等主要应用服务功能。企业既能保障数据安全，又能安全合规地发挥数据最大价值，可以很好地解决业界的数据孤岛难题。
https://mp.weixin.qq.com/s/2zVPTBEgkfj21GoxS1p13A

业界观点

1、陈智敏：解决数据权属问题需要厘清五个思路

7 月 13 日，在 2022 北京网络安全大会(BCS 2022)开幕式暨战略峰会上，十三届全国政协委员、社会和法制委员会副主任，中国友谊促进会理事长，公安部原副部长、国家网信办原副主任陈智敏表示，“当前国际社会围绕数据的争夺已经成为焦点，中国作为一个数据大国，应回答好数据权属的问题，厘清主体在民、主权在国、全民共有、企业开发、共享共用这五个思路。”

主体在民是思考数据权属的逻辑起点和历史起点。陈智敏表示，数据权与公民的基本权益、个人人格权和财产权密切相关，数据权与人权、物权同等重要，共同构成公民的基本权利。

数据的**主权在国**是国家安全和社会公共安全的基本保障。数据的主权在国，是国家主权在网络空间的核心表现。维护数据主权，是网络安全的根本任务。我国作为社会主义公有制为主体的国家，数据应当**全民共有**;数据可以由**企业开发**，要保障企业的合法权利和权益，保障数据交易的公平合理;由数据产生的财富应当由全社会**共享共用**。

真正落实权属问题，需要做到四个坚持。一是要坚持党

的集中统一领导，二是要坚持法律保障，三是要坚持技术支撑，四是要坚持国际合作。

https://bcs.qianxin.com/2022/news/detail?id=62

2、邬贺铨：数据要素的开发与利用离不开数据安全

近日，在 2022 北京网络安全大会上，中国工程院院士邬贺铨详细介绍了数据要素的九大基本特征，并阐述了这九大特征与网络安全之间的内在关联。

第一大特征是**数据的可见性**。通常情况下，安全检测会使用数据可视化来发现异常，大量政企机构希望将云化的可视化工具下载到本地终端进行部署，在增加数据可见性的同时，确保数据的安全性。

第二大特征是**数据的易理解性**。邬贺铨表示，为了让计算机能更好的理解数据，工程师们会对数据进行前期的预处理，目前标注依然需要人工处理，甚至需要外包、众包的参与，这就带来了极大的用户隐私泄漏风险。

第三个特征是**数据的可链接性**。大数据技术能够将海量异构分布数据结合在一起，实现数据深度地挖掘。邬贺铨认为，跨多个应用程序和云服务存储的数据共享需要明确可共享的原则、范围、层次和内容，规定共享程序与审计。

第四是**数据互操作性**。数据要流动、要使用才能产生价

值，尤其是跨境数据流动。邬贺铨认为，数据流动的管理首先需明确并确定数据类型，以便在出境口拦截未经批准的敏感数据。其次还需还原数据路径，实施数据处理流程的全链路监控，便于事后追溯。

第五是**数据的可信性**。深度神经网络是个分类器，当事件和图像处于 AI 模型辨识分界线或被干扰时会使 AI 误判，可通过区域截图、放大缩小等预处理发现数据被投毒；在整个供应链中，数据也极易受到污染而出现失真现象，可采用区块链+隐私计算方法，整合订单、发票、物流和资金流等数据，来发现有无造假。

第六是**数据的安全性**。数据是生产要素，因此要使用加密手段防止数据被窃取或者滥用，但也需要实时对数据进行审计与版本核对，防止被恶意再加密而被控或被勒索；另一方面，可以利用多方计算技术，允许各参与方只提交密文分片的前提下，通过既定逻辑共同计算出结果，但不透露各自数据。

第七是**数据的资产性**。数据是生产要素，需要从数据采集、数据开发利用、数据鉴权、数据应用等全生命周期去保证数据资产的安全性。邬贺铨强调，在所有环节中，特别注意元数据的管理、开发过程的管理、流通过程的管理和运维过程的管理，这些过程需要采用相应的安全技术支持资产安

全管理。

第八是**数据的归属性**。毋庸置疑的是，数据本身是有归属权的，包括持有权、使用权、经营权，关系到数据使用的安全性和合法性。不同于传统资产的是，数据是可复制的，数据使用也基本上可以不留痕迹，这为数据的归属确权带来了很大的困难。

第九是**数据的开放性**。邬贺铨认为，原则上不涉及国家安全、企业秘密和个人隐私的政务数据，都应该向社会开放，才能发挥更大的价值。但政务数据开放要特别注意个人身份识别和地理位置等隐私保护，在大数据技术日益发达的今天，通过混合不同数据集进行关联分析，可以间接地追踪到个人工作生活等隐私，因此需要进行匿名化等脱敏处理。

https://bcs.qianxin.com/2022/news/detail?id=75

3、何良生：要充分发挥密码在保障网络安全中的重要作用

国家密码管理局副局长何良生表示，密码是维护网络安全的核心技术和基础支撑，要充分发挥密码在保障网络与信息安全的重要作用，不断推动我国密码事业高质量发展，需要全社会的参与。

何良生从坚持以人为本、融合应用、科技创新、依法管理四个方面提出建议：

一是坚持以人为本，筑牢国计民生密码安全防线。密码发展始终围绕着人民福祉。亿万民众的身份证、银行卡、社保卡、公交卡，家家户户的智能电表、智能机顶盒，面向百姓的政务服务、社区服务、纳税缴费等等，都有密码在保驾护航。特别是2020年以来，面对突如其来的新冠肺炎疫情，密码更是发挥了重要作用，全国各级疫情数据的报送传输，人人出门必备的“健康码”，居家办公所需的视频会议，看病就医的电子病历等等，都离不开密码。可以说密码已经进入千家万户，与老百姓的生活息息相关，事关人民的切身利益。

二是坚持融合应用，赋能数字经济高质量发展。密码是保护数据安全最经济、最可靠、最有效的手段，对消除数据孤岛、发挥数据价值有着不可替代的重要作用，能够实现数据所有权、使用权、管理权有效分离和保护，可以让数据安全可靠地跑起来、用起来、活起来。推动密码与数字基础设施体系建设深度融合，将为数字经济高质量健康发展提供有力支撑。

三是坚持科技创新，谱写密码高水平自立自强新篇。密码高水平自立自强的关键在于密码基础理论引领研究的原创能力，和密码关键核心工程与应用技术领先研发的攻坚突破能力。我国密码科技在国家密码发展基金等国家级科技计划项目的引导和支持下，取得了一系列具有国际一流水平的

创新成果。何良生介绍，我国自主研制的 SM2 椭圆曲线公钥密码签名算法、SM3 密码杂凑算法、SM4 分组密码算法、ZUC 序列密码算法、SM9 标识密码算法均已成为 ISO/IEC 国际标准。密码科技创新任重道远，需要政产学研用各方持续用力，久久为功，才能真正做到密码高水平自立自强。

四是坚持依法管理，共建密码行业发展良好生态。《中华人民共和国密码法》实施两年多来，我国密码工作的规范化、科学化、法治化水平得到显著提升，全社会密码安全和应用密码的意识普遍增强。值得关注的是，近年来，各地区各有关部门陆续出台了一系列促进商用密码产业发展的政策措施，在资金补助、创新研发、人才引进、成果转化等方面给予实打实的支持，不断优化产业生态，商用密码正在迎来依法治理、供需互促、创新发展的新阶段。

https://bcs.qianxin.com/2022/news/detail?id=56

4、张劲松：推动网络安全高质量发展，护航中国数字经济“北京样板”

7 月 13 日，北京市经济和信息化局局长张劲松在 2022 北京网络安全大会线上致辞时表示，北京要在网络安全人才建设、基础技术攻关等方面提升网络安全技术实力。在数据安全方面更要做好保护支撑，推动产业的整体升级。

张劲松表示，推动网络安全高质量发展应当从以下三方面入手：

首先，应**提升网络安全技术实力，以谋划数字经济新发展布局**。在统筹做好新型数字化基础设施，及时出台政策规范融合网络安全发展的同时，还应加强网络安全人才建设，保障人才储备，开展基础技术攻关。

其次，应**做好数据安全保护支撑，着眼新型数字生态构建**。去年北京落地了国际大数据交易所，加快了数据汇集、流转，未来，需要建立更加可信可控的网络安全体系，以充分释放数据资源要素潜力。

张劲松呼吁，在两个百年接力的时代坐标上，万物互联为行业带来新机遇新挑战。网络安全产业的企业家、技术专家、业内精英，应抓住北京“两区”建设和全球数字经济标杆城市建设的机遇，来京创业，在京发展，共同谱写网络安全高质量发展新篇章，为建设网络强国贡献北京力量。

https://bcs.qianxin.com/2022/news/detail?id=60

5、丁晓东：数据交易如何破局——数据要素市场中的阿罗信息悖论与法律应对

数据交易是数据要素市场建构的关键一环，但是数据交易所的交易却困难重重。数据确权能否解决数据交易的阿罗

信息悖论？能否避免公地悲剧、解决“搭便车”问题？数据能否借鉴证券交易所采取标准化的合同交易模式？对此，中国人民大学法学院丁晓东副教授在《数据交易如何破局——数据要素市场中的阿罗信息悖论与法律应对》一文中，从基础产权理论出发，认为数据具有价值不确定性、非排他性和非竞争性，数据确权无法解决数据交易中的阿罗信息悖论。

数据交易面临阿罗信息悖论：交易需要披露信息，但披露信息即意味着数据价值的丧失。有观点认为，应通过数据产权保护消解阿罗信息悖论，避免相关的公地悲剧、“搭便车”与激励问题。但数据具有价值不确定、一定程度的非竞争性与非排他性，数据产权并不能解决阿罗信息悖论，也不会克服公地悲剧，反而可能造成公共资源私有化、溢出效应丧失、普遍违法等问题。数据交易与产品流通型交易不同，具有服务合作型特征，其可通过部分逐步公开与有限控制，实现数据交易双方的互动型合作，或者借助信用品的声誉机制、合作机制，克服阿罗信息悖论。因此大数据交易应以婚姻介绍所为模型，成为撮合数据交易、提供安全认证的机构，而非以商场或证券交易所为模型。法律应设置大数据交易所的安全保障义务，积极利用知识产权、合同制度，同时审慎应用反不正当竞争制度保护数据交易。

https://mp.weixin.qq.com/s/uyhAkZwJAr46U3bsPB1eJA

数据安全事件

1、意大利监管机构警告 TikTok 涉嫌违反欧盟隐私规定

2022 年 7 月 11 日，意大利数据保护机构表示，已经正式警告 TikTok 涉嫌违反欧盟的用户隐私保护规则。该监管机构称，TikTok 在最近几周告知用户，将从 7 月 13 日起向他们提供有针对性的广告，而未在征求用户同意的情况下，使用他们设备中存储的数据。监管机构还表示，如果 TikTok 不撤回该政策变化，当局将保留对其施加不明确限制的权利。

https://mp.weixin.qq.com/s/QspkYr4ZpdHGpwkdo5KBEg

2、印度地方洪水监测系统遭勒索软件攻击，水文数据全部被加密

2022 年 7 月 12 日报道，印度果阿邦的洪水监测系统遭到勒索软件攻击，攻击者要求支付加密货币，以解密洪水监测站的数据。

位于帕纳吉的数据中心服务器存储了果阿州主要河流 15 个地点的洪水监测系统的数据，以监测河流的水位。该系统作为灾害管理的一部分，以便控制洪水的情况。

在向果阿警方网络小组的投诉中，一直在维护数据的州政府水资源部表示，所有文件已被加密，无法再被访问。**数**

据的完整性已被改变，使其无法备份以前的数据。执行工程师 Sunil Karmarkar 提交的投诉显示："该服务器在 24x7 的互联网线路上工作，由于没有杀毒软件且防火墙已过时，攻击者轻易得手了。"

https://www.secrss.com/articles/44630

3、热门游戏《老头环》发行商万代南官梦遭勒索软件攻击

2022 年 7 月 13 日，据外媒报道，今年最热门的游戏之一《艾尔登法环》（Elden Ring）的发行商万代南梦官（Bandai Namco）成为了勒索软件攻击的受害者。

根据 vx-underground（专门收集分享恶意软件样本、信息的团体）周一发布的推文，ALPHV 勒索软件团伙（又名 BlackCat）声称对万代南梦官进行了攻击勒索。万代南梦官是一家国际视频游戏发行商，拥有的视频游戏专营权包括皇牌空战、黑暗之魂系列等。据爆料，一张疑似万代南梦官 2023 财年发行计划的图片也被泄漏。

https://www.secrss.com/articles/44678

4、PFC 承认遭勒索软件攻击，191 万患者信息被泄露

2022 年 7 月 14 日报道，PFC（Professional Finance Company,Inc.）是一家总部位于美国科罗拉多州的债务催收

公司，其承认过去数月持续遭到勒索软件攻击。由于该公司服务于数百家美国医院和医疗机构，因此本次勒索攻击可能成为今年美国历史上最大规模的私人和健康信息泄露事件。

PFC 表示本次数据泄漏将影响 650 家医疗提供商，黑客获取了患者名称、家庭住址、尚未偿还的结算金额和其他金融信息。PFC 表示部分数据还涉及患者的出生日期、身份证号码、医疗保险、药物救治等信息。在提交给美国卫生与公众服务部的文件中，PFC 确认本次勒索软件攻击至少影响了 191 万患者。

https://www.cnbeta.com/articles/tech/1292183.htm

5、新的 0mega 勒索软件针对企业进行双重勒索攻击

一个名为“0mega”的新勒索软件正在针对全球组织进行双重勒索攻击，并要求受害企业支付数百万美元赎金。

经研究人员分析后发现，0mega 是 2022 年 5 月出现的一项新勒索软件操作，自那时以来已经攻击了许多受害者。目前，研究人员还没有发现 0mega 操作的勒索软件样本，因此没有太多关于文件如何被加密的信息。但是，研究人员发现该勒索软件在加密文件的名称上附加了.0mega 扩展名，并创建了名为 DECRYPT-FILES.txt 的赎金记录。

https://hackernews.cc/archives/39883

6、Kaiser 医疗集团泄露了近 7 万份医疗记录

2022 年 7 月 13 日报道，Kaiser 公司本月早些时候透露，由于 4 月 5 日的电子邮件泄露事件，该公司遭受了一次大规模的数据泄露，可能泄露了近 7 万名患者的医疗记录。

该公司透露，攻击者获得了华盛顿 Kaiser 基金会健康计划公司一名雇员的电子邮件的访问权限，其中包含大量的受保护的健康信息。攻击者一直未授权访问该邮箱长达数个小时，该事件影响了 69,589 个人。

到目前为止，该公司表示，还没有任何证据能够表明攻击者盗窃或滥用受保护的健康信息是由于漏洞引起的。这一事件也再次揭示了企业一直以来面临的最大的安全风险——人为的错误。

https://app.myzaker.com/news/article.php?pk=62ccf21db15ec01ce930957b

7、英国招聘机构 Morgan Hunt 证实遭到数据泄露

2022 年 7 月 15 日报道，英国招聘机构 Morgan Hunt 证实，该公司遭遇了数字盗窃，入侵者窃取了其账簿上一些自由职业者的个人数据。该公司在致承包商的一封信中表示，公司的一个数据库受到影响，未经授权的第三方访问了公司的系统。数据库中被访问的信息包括承包商的姓名、联系方

式、身份证件、地址证明文件（包括提供的任何银行或建筑协会声明）、国民保险号和出生日期。

https://www.theregister.com/2022/07/15/digital_burglary_at_recruitment_agency/

8、Uniswap 在大规模网络钓鱼攻击中被盗 800 万美元

2022 年 7 月 13 日报道，在一次复杂的网络钓鱼攻击中 Uniswap 公司损失了价值近 800 万美元的以太坊。黑客利用免费 UNI 代币（空投）的诱惑来诱骗受害者授予交易，使其能够完全访问钱包。收到空投时，请确保在单击任何按钮之前验证所有内容，从登录的网站的域名开始,保护隐私安全。

https://www.bleepingcomputer.com/news/security/8-million-stolen-in-large-scale-uniswap-airdrop-phishing-attack/

9、黑客通过“面试”从 Axie Infinity 窃取 6.2 亿美元

近日，根据 The Block 的报道，朝鲜黑客通过“面试”目标企业员工的方式从全球最热门的加密货币游戏 Axie Infinity 窃取了 6.2 亿美元加密货币。了解此次攻击的消息人士称，黑客伪造了一家公司，并冒充雇主通过 LinkedIn 以高薪招聘的名义联系了 Axie Infinity 的开发商 Sky Mavis 的一位高级工程师。面对诱人的高薪，Axie Infinity 的这位高级工

程师对“工作机会”表现出兴趣，并经历了多轮“面试”。在其中一次“面试”中，工程师收到了一份 PDF 文件，其中包含有关工作的详细信息。然而，该文件为黑客打开了进入 Ronin 区块链系统（支撑 Axie Infinity 的 NFT 在线视频游戏的以太坊侧链）的入口。该员工在公司的计算机上下载并打开了文件，启动了一个感染链，使黑客能够侵入 Ronin 系统并控制了四个令牌验证器和一个 Axie DAO 验证器。

https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/