全球数据安全观察

总第 123 期 2023 年第 4 期

(2023.01.30-2023.02.05)

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、工信部发布 52 个工业互联网标准项目确定

2022 年 12 月 30 日，工信部发布《2022 年第三批行业标准制修订和外文版项目计划》的通知（以下简称《项目计划》），工业互联网被划分进新型基础设施标准项目计划表，共计 52 个项目，涉及工业互联网平台、工业互联网安全、工业互联网标识解析、5G+工业互联网应用、时间敏感网络、边缘计算等方向标准的制定。

https://mp.weixin.qq.com/s/_qkKBH07SYORsLNrcAuYRQ

2、工信部等十七部门联合印发《“机器人+”应用行动实施方案》

工业和信息化部、教育部、公安部等十七部门近日印发《“机器人+”应用行动实施方案》，提出到 2025 年，制造业机器人密度较 2020 年实现翻番，服务机器人、特种机器人行业应用深度和广度显著提升，机器人促进经济社会高质量发展的能力明显增强。聚焦 10 大应用重点领域，突破 100 种以上机器人创新应用技术及解决方案，推广 200 个以上具有较高技术水平、创新应用模式和显著应用成效的机器人典型应用场景。

https://mp.weixin.qq.com/s/yHSIgtf5KFr0T5io40rLLw

3、上海市网信办发布数据出境安全评估申报工作实务问答（二）

为更好服务上海市数据处理者开展数据出境安全评估申报工作，根据《数据出境安全评估办法》和《数据出境安全评估申报指南（第一版）》，上海市网信办结合近期咨询情况及完备性查验常见问题，从形式查验、内容查验、等方面发布实务问答。

https://mp.weixin.qq.com/s/4lYcOmFNVOOtn_YqS6v3HA

4、杭州市经信局发布关于摸排全市数字工程服务企业的通知

根据《杭州市推进软件和信息技术服务业高质量发展的若干政策》，为加快培育发展数字工程服务产业，精准制订相关扶持政策实施细则，持续提升数字化服务能力，经研究，决定开展全市数字工程服务企业摸排工作。

https://mp.weixin.qq.com/s/pVkXMxE_c-Phf9tmlekX1A

5、美国发布 AI 风险管理框架，引导 AI 技术安全发展

美国国家标准与技术研究院（“NIST”）于 2023 年 1 日

26 日发布了人工智能风险管理框架 （AI RMF 1.0）（“AI RMF”），这是一份指导文件，供设计、开发、部署或使用人工智能 （“AI”） 系统的组织自愿使用，以帮助管理 AI 技术的风险。NIST 特别指出随着技术的不断发展，AI RMF 旨在适应 AI 领域，并被组织使用，以便社会可以从 AI 技术中受益，同时免受其潜在危害。

https://mp.weixin.qq.com/s/whxsG5kcbENqskZJG4KrKQ

技术、产品与市场

1、《数据安全风险治理成熟度评价模型》发布

2023 年 1 月 5 日，在第二届数据安全治理峰会上，《数据安全风险治理成熟度评价模型》标准正式发布。《数据安全风险治理成熟度评价模型》将企业的数据安全风险治理按照风险治理的阶段分为 5 大能力域：分别是风险准则确立、风险要素识别、风险评估分析、风险处置解决、风险治理改进，并进一步细分成 15 个能力项。

评价模型的等级设置依据组织数据安全风险治理的覆盖范围、支撑力度进行划分。

第一级“初始级”指组织的数据安全风险治理主要依靠突发事件或临时需求驱动，具有明显的滞后性缺乏数据安全

风险治理的目标、规划、依据、资源保障。

第二级“基础级”指组织的数据安全风险治理主要体现在个别业务活动或项目活动中，能主动识别法律法规与外部监管要求，使个别业务活动或项目活动中可以满足组织的数据安全保护与合规需求。

第三级“已定义级”指组织的数据安全风险治理主要体现在组织整体层面，考虑了法律法规和外部监管要求下，兼顾了组织内部发展需求，建立了覆盖数据安全风险识别、评估、处置、监控等标准化管理机制、技术和运营体系，能够保障组织数据安全风险治理工作的有序开展与规范化落地。

第四级“量化级”指在第三级的基础上对组织的数据安全风险治理效率、效果能量化分析和监控。

第五级“卓越级”指组织的数据安全风险治理成为行业标杆并推广至行业。

https://www.secrss.com/articles/51469

2、2023 年态势感知与安全运营十大技术趋势展望：面向数据安全的态势感知将成为新热点

伴随着数字化转型，数据在推动数字经济高速发展的同时，数据滥用、数据泄露等安全事件频繁发生，数据安全风险日益凸显。

国际著名咨询机构提出建议，用户必须在整个数据生命周期中规划和缓解管理风险，从而解决数据安全性，隐私性，信任与道德、数据所有权，数据恢复等一系列问题。2021 年 9 月 1 日，《中华人民共和国数据安全法》正式实施，数据安全上升到我国国家安全战略高度，并加速了数据安全体系建设。

在数据安全体系落地实践中，组织的数据安全风险迫切需要依赖系统化、产品化技术手段实现数据安全全生命周期管控，全面感知、分析、呈现数据安全风险的态势感知应运而生。

面向数据安全的态势感知围绕数据安全全生命周期管理，将数据安全技术、流程、产品和人有机的结合，融合数据资产梳理和发现、数据风险检测识别、数据风险集中分析、数据风险响应处置、数据风险态势呈现等能力，实现数据安全风险可感知、可溯源、可研判、可处置、可呈现，为数据安全运营提供基础。随着数据安全体系建设不断发展演进，面向数据安全的态势感知势将成为新热点，推动数据安全建设，助力数据安全治理 。

https://mp.weixin.qq.com/s/LKzs7rGVhNJ72mrW8nB9hw

3、IDC 发布中国 API 安全市场洞察报告

IDC 认为，API 作为数据流转和使用的重要通道，承载着十分重要的责任。同时，API 的多样性、复杂性在不断增加，传统基于网络和主机边界安全的防护技术无法充分应对云计算和微服务技术下不断弹性部署的业务安全需要，许多用户在攻击事件发生后才意识到 API 风险。因此，API 资产的全面梳理和安全防护成为市场的迫切需求，API 的安全建设也成为企业数字化创新的基础保障。

IDC 将 API 安全定义为专门为保护 API 通信免受误用、滥用和漏洞利用而设计的解决方案，其所提供的功能包括 API 资产发现、验证和执行，动态和自适应的流量监测和模式分析、检测和阻止威胁，例如恶意软件、漏洞利用、代码注入、机器人流量、DDoS 攻击、欺诈和滥用等。目前 API 安全多以 API 安全网关、API 安全管理平台等产品形式进行交付。

IDC 认为，API 的安全防护市场在中国还处于初步发展阶段，产品和技术能力还需进一步加强。目前，国内众多网络安全厂商、数据安全厂商、云计算服务商、专业的 API 安全厂商纷纷布局 API 安全市场，且各个厂商结合自己的技术积累和行业优势推出了各具特色的产品和解决方案。

https://mp.weixin.qq.com/s/eYC2WW192EHWulBWERHvmw

4、调查：美国报告的数据泄露事件接近历史新高

据 Identity Theft Resource Center 的研究报告显示，2022 年，美国组织共发出了 1,802 份数据泄露通知，报告了影响超过 4 亿人的记录或个人信息。

2022 年发生已知最大数据泄露事件的组织包括：Twitter，泄露了 2.22 亿条记录；Neopets，有 6900 万受害者；AT&T Data，有 2300 万受害者；和 Cash App Investing，有 820 万受害者。

调查显示，最常暴露的数据属性是受害者姓名，其次是社会安全号码、出生日期、当前家庭住址、驾照或州身份证号码、医疗详细信息和银行帐号。此外，不同种类的“在线攻击”是 2022 年导致数据泄露的罪魁祸首，其次是网络钓鱼或商业电子邮件泄露，然后是勒索软件和恶意软件。

https://www.bankinfosecurity.com/reported-data-breaches-in-us-reach-near-record-highs-a-21018?&web_view=true

5、2022 年中国数据中台行业研究报告

狭义来看，数据中台是一套实现数据资产化和服务复用的工具；广义来看，数据中台是一套运用数据推动企业数字化转型升级的机制和方法论。数据中台始于业务数据的沉淀积累，用于数据的收集、整合、分析及应用，循环往复，形

成生态闭环。

2021 年数据中台市场规模达到 96.9 亿元。在供给侧，行业的生态化合作趋势明显；在需求侧，企业对数据中台的关注点从中台本身转向了最终的数据变现能力。行业集中度和成熟度持续上升，整体规模稳步增长，增速趋于平稳，预计将在 **2024 年达到 187.4 亿元**。

当前数据中台的行业集中度仍保持较低水平，行业的活跃参与者大致分为平台生态厂商、解决方案厂商和独立中台厂商三类，行业格局由竞争转向竞合，以协同生态为核心，集众所长，将成熟的技术方案与行业服务经验结合，协同拓展应用解决方案的广度和深度，深耕于金融、泛零售、政务、制造、工业等多行业应用场景。

云原生是当下最为确定的技术趋势，存算分离、微服务、ServerLess 等核心技术要素驱动数据中台走向云原生。数智融合理念将 AI 算法模型植入数据治理，高质量数据反哺 AI 开发能力，让数据和 AI 开发高效互通。泛中台化趋势明显，业务场景需求的解决方案/产品趋于“中台化”，以数据中台为基础的中台体系不断丰富。

https://mp.weixin.qq.com/s/v_6vDjVX2Qjxhrm6cRCOgw

业界观点

1、人民政协网：牢牢抓住数字经济发展新机遇

北京市政协委员、民建北京市委会副主委、中央财经大学中国银行业研究中心主任郭田勇在调研中发现，数字经济发展在全国领先的北京，其数字金融以及平台经济的发展依然存在一些短板和问题。如，数字金融基础有待进一步夯实，北京市关于金融科技创新发展的政策有待进一步优化，数字金融产业发展有待进一步推进，发展平台经济的各项支持政策有待进一步完善。

为此，郭田勇建议：

一是应进一步夯实数字金融基础。充分发挥北京金融行业聚集的优势，不断加强数字金融基础设施建设与相关支撑布局，夯实数字金融的发展基础。

二是依托数字金融的产业聚集效应，推动标杆产业发展。优先聚焦以数字金融产业为首的相关产业聚集与上下游产业发展，加快推进相关领域的产业布局，稳妥推进数字人民币场景试点应用，推动数字人民币在金融领域的改革试验与测试应用落地。

三是应紧抓数字经济发展新机遇，推动平台经济发展。利用平台企业数字化技术优势为传统产业赋能，充分发挥平

台企业对经济高质量发展的积极作用，同时要引导平台企业在常态化监管下合法合规经营，保障平台企业劳动者的合法权益，促进平台经济健康持续发展。

https://mp.weixin.qq.com/s/FqNP2BIEl1JCjvtGgWLfTQ

2、畅通数据要素“双循环” 完善全球数据“定价链”

近日，《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据 20 条”）正式出台，对于新发展格局下推动数据要素市场化配置具有重要意义：加速政企数据融合对接，充分释放数据要素发展潜力；破除行业和区域壁垒，构建超大规模数据市场；推动数据要素高水平开放，助力数字丝绸之路建设。

当前三类市场主体内部和三类市场主体之间的典型数据跨境应用场景值得重点关注：

（一）市场主体内部，当前存在三类典型数据跨境流通应用场景。一是海外企业“走进来”，即境外跨国公司在境内业务布局涉及的数据流动。二是中国企业“走出去”，即境内企业在海外布局业务引发的数据流动。三是企业“走出去”，数据“走进来”，即境外企业在海外业务产生数据的离岸托管需求。

（二）市场主体之间，三类数据跨境流通应用模式值得

重点关注。一是跨境数据交易模式。二是“来数加工”模式。三是科研数据共享模式。

为加快构建全国统一数据大市场，有效提升数据要素跨境流通和数据资产全球化定价效率，现阶段宜快速推进以下重点工作。

（一）尽快建立数据要素市场顶层统筹和生态体系，畅通内循环。一是布局若干政府主导、社会参与的国家级数据交易所，探索完善区域数据交易中心和行业交易平台体系；二是不断强化数据要素生态培育，发展壮大供需两侧市场主体；三是依托全国一体化大数据中心体系，建设国家数据要素基础设施。

（二）分步推动数据跨境流通“增容扩圈”，激活外循环。一是规划建设全国数据跨境流通示范区，开展“数据海关”制度等试点；二是有序推动离岸数据服务外包和离岸数据交易定价中心建设；三是探索以“以双边带多边、以区域带整体”的推进策略。

https://mp.weixin.qq.com/s/hyv8VajTqxM51yotRDu8VQ

3、企业数据合规重中之重：个人信息

纵观最近几年各地互联网法院公布的个人信息保护典型案例，安全风险主要来源于以下几方面：内部人员权限管

理混乱、大量数据处理活动频繁、事后难以溯源并整改。

关于企业如何守护个人信息安全，主要包括以下两方面:

个人信息识别梳理。作为开展各种个人信息保护活动的前提，企业首先需要弄清楚到底哪些数据属于个人信息。

个人信息全生命周期管理。全生命周期管理是企业开展数据合规工作的重要指导原则之一，涉及个人信息的各类处理活动均需遵守相应的法律规定，确保个人信息安全，而不应狭隘地认为数据合规仅仅或者主要是指初始收集阶段的合规。为了在各个数据处理环节提升安全水位，企业从技术和管理层面同步进发，比如:

1) 权限管控，针对不同访问需求，规范数据访问权限，并严格记录访问情况，实现内部数据操作行为的有效控制与监管;

2) 脱敏流转，在数据使用流转过程，遵循数据最小使用原则，去标识、去隐私，实现数据的安全高效利用，在安全的前提下提升数据的使用价值;

3) 密文存储，落实重要数据识别和分类分级保护要求，对重要的核心数据加密存储，守护数据安全;

4) 数据审计，详细记录应用用户访问数据的日志，包括时间戳、应用与数据库用户、访问路径、数据源、数据位置、访问类型、SQL 请求、数据量、敏感数据相关信息等;

5) 应急处置机制，一旦发生安全事件，确保企业有完善的应急预案和应对处理机制，防止事态进一步扩大。

https://www.infosws.cn/20230201/60420.html

4、王建冬：数据要素市场化改革要抓“棋眼”

2023 年，数据要素制度创新大幕全面拉开，我国构筑数字经济新优势迎来强大动能。发改英才”、国家发改委价格监测中心副主任王建冬表示，数据和数字化技术已经成为驱动经济增长的主要动力。

对于如何加快数据要素与实体经济深度融合，王建冬建议，可从三个方面加强布局：一是加快推动重点行业数据要素流通交易平台建设；二是构建面向重大区域战略的数据要素流通平台；三是加快推动跨境数据安全有序流通应用。

王建冬认为，当前数据要素市场化配置改革的“棋眼”，是加快形成面向全社会数据资产的全链条管理体系，从数据资产的确权、登记、评估、定价、入表等环节入手构建一个全流程的政策闭环。“只有真正形成闭环，整个数据资产的商品化、市场化、要素化才能真正见到成效。”

如何抓住“棋眼”构建数据资产全链条管理体系？王建冬提出五大建议：

一是数据产权界定。在《民法典》和《数据安全法》《个

人信息保护法》框架下，构建完善数据资源持有权、数据加工使用权和数据产品经营权“三权分置”的数据产权制度框架。

二是数据资产登记。搭建国家数据资产登记存证平台，未来可作为支撑数据要素产权界定的重要基础设施，将数据来源、提供者、权利人、使用期限、使用次数、使用限制、安全等级、保密要求等作为事实确认下来。

三是数据资产评估。完善数据资产评估体系，把好数据资产的“安全关”“合规关”“质量关”和“价值关”。

四是数据资产定价。围绕数据的资源化、资产化和资本化构建一套全新的适应数据资产特性的估值和定价逻辑。

五是数据资产入表。在当前数据日益成为企业核心资产的背景下，探索研究将数据资产纳入会计核算体系，加快推动相关法规政策完善和会计准则调整，将有助于数据要素交易流通，也是做大做强数据要素市场的关键举措。

http://www.echinagov.com/viewpoint/335325.htm

5、郭启全：多措并举 全面提升政务安全防御能力

公安部网络安全保卫局一级巡视员、副局长郭启全在题为《提档升级重要举措，全力保障电子政务安全》的主题报告中，就当前网络安全形势进行了分析。

郭局长指出，当前数据安全问题隐患突出，应该引起我

们认真反思和应对。而问题产生的原因主要集中在三个方面：一、数据大集中、大流动、大应用，客观上造成了重要数据保护困难，易遭受网络攻击。二、有些政府部门总体上安全意识不强，主管责任、监管责任落实不到位，特别是数据处理者，主体责任落实不到位，安全服务商责任和措施落实不到位。三、有些地方部门不按照上级要求开展网络系统建设，不落实安全责任，造成重大数据泄露事件高发、频发。

基于此，郭局长表示，在数字政府建设中要加强网络与数据安全顶层设计和统筹规划，要坚持电子政务网络安全工作原则，加强组织领导和统筹规划，落实安全责任。郭局长强调，加强数字政府网络安全保护、保障和保卫工作，大力提升电子政务网络安全综合防御能力，需做好以下工作：一要强化落实重要保护措施，提升综合防御能力；二要强化电子政务网络安全保障，提升综合保障能力；三要加强电子政务网络安全保卫工作，提升保卫能力。

https://www.infoobs.com/index.php/article/20221116/56023.html

数据安全事件

1、联邦调查局对 Banner Health 处以 125 万美元的违规罚款

2 月 2 日，据外媒报道，在 2016 年黑客入侵事件影响近 300 万人后，联邦监管机构对多州医院系统 Banner Health 处以 125 万美元的 HIPAA 罚款。

据悉，大约 281 万人的 PHI 在该事件中遭到泄露，包括患者姓名、医生姓名、出生日期、地址、社会安全号码、临床详细信息、服务日期、索赔信息、实验室结果、药物、诊断和条件以及健康保险信息。这是自 2021 年 1 月以来卫生与公共服务部民权办公室在 HIPAA 违规案件中首次达成七位数的罚金。

https://www.bankinfosecurity.com/feds-smack-banner-health-125-million-fine-in-breach-a-21096?&web_view=true

2、GoodRx 与 Google 和 Facebook 共享健康数据，被罚 150 万美元

美国联邦贸易委员会周三指控药品费用和远程医疗平台 GoodRx 与谷歌和 Facebook 等第三方共享消费者的个人健康信息。

根据 FTC 的投诉，GoodRx 出于广告目的提供了有关其用户的处方药和健康状况的信息。该机构还表示，GoodRx 允许第三方将这些数据用于他们自己的内部目的，歪曲其 HIPAA 合规性，并且未能制定关于如何保护其用户个人健康信息的政策。

GoodRx 同意支付 150 万美元的罚款来了结此案，但承认没有任何不当行为。除了付款之外，美国联邦贸易委员会表示，其拟议的法院命令将永久禁止 GoodRx 共享广告健康数据，在出于其他目的与第三方共享信息之前需要用户同意，指示第三方删除以前共享的数据，限制 GoodRx 的期限可以保留患者信息并迫使公司制定隐私保护计划。

https://mp.weixin.qq.com/s/gbMfEjjLAnDQiksTGwBZ-Q

3、BlackCat 勒索软件攻击国防承包商，窃取武器数据

2 月 1 日，据外媒报道，BlackCat (ALPHV) 勒索软件组织声称已经入侵了工业炸药制造商 Solar Industries India Limited，并窃取了超过 2 TB 的关键数据，包括当前使用的武器设计。

BlackCat 已将 Solar Industries India Limited 添加到其 Tor 泄漏站点，并显示数据泄露影响了该组织的所有机密文件和产品的消息。据称，被盗数据包括公司员工和客户的详

细信息、军备供应链以及公司其他合作伙伴和承包商的信息，还包括公司产品的技术文档、武器蓝图，以及有关这些武器的审计和检测到的缺陷和漏洞的报告，以及有关未来发展的详细信息等等。

https://cyware.com/news/blackcat-ransomware-hits-defence-contractor-steals-weapons-data-87376d21

4、欧洲汽车经销商巨头遭勒索攻击，客户个人数据全部泄露

安全内参 2 月 3 日消息，英国汽车零售商 Arnold Clark 日前通知客户，其个人信息可能因网络攻击而失窃。已经有勒索软件团伙表示对此负责，并声称掌握了数 GB 敏感信息。

Arnold Clark 是欧洲汽车零售行业中的龙头企业，其在 2022 年 12 月 23 日沦为网络攻击目标。调查显示，恶意黑客可能已经窃取到客户个人数据，包括姓名、联系方式、出生日期、车辆信息、护照/驾照、国民保险号和银行账户等详细信息。

Play 勒索软件团伙已经在其 Tor 泄密网站上，宣布对此次攻击负责。目前，他们已发布了 31 个大小为 500 Mb 的归档文件，总计约 15 Gb。他们声称窃取到“隐私及个人数据”，包括护照和 ID 复印件、机密合同、协议、租赁合同以及财务相关文件。

https://www.secrss.com/articles/51553

5、乌克兰 IT 军队从俄罗斯能源巨头 Gazprom 获得了 1.5GB 的档案

1 月 31 日，据外媒报道，IT Army of Ukraine（乌克兰 IT 军队）声称已经破坏了俄罗斯能源巨头 Gazprom 的基础设施，并获得了 1.5 GB 的档案数据。

该黑客组织声称该档案包含俄罗斯天然气工业股份公司集团公司的 6,000 多份文件。档案包含该企业与金融和经济活动相关的信息，以及关于 Koviktinsky 油井（俄罗斯联邦最大的气田之一）自动化系统的测试和钻井、实施和调整的报告。

https://securityaffairs.com/141640/hacktivism/it-army-of-ukraine-hacked-gazprom.html?web_view=true

6、美国涉恐禁飞名单被公开泄露

1 月 31 日消息，近日，美国交通安全管理局（TSA）两个包含超过 150 万条涉恐禁飞人员和 25 万条“二级安检选中者”人员信息的禁飞名单被黑客在论坛公开泄露。

据报道，一位瑞士年轻女黑客 maia arson crimew 使用知道创宇的钟馗之眼（Zoomeye）搜索 Jenkins 服务器时偶然发

现了一个配置错误的亚马逊 AWS 服务器，其中包含 2019 年版 TSA 禁飞名单。

这些数据库是秘密的，即使不算“机密”，也被认为是非常敏感的信息，因为它们在协助国家安全和执法任务方面发挥着至关重要的作用。

https://www.secrss.com/articles/51430

7、JD Sports 泄露 1000 万用户信息

2 月 1 日，据报道，JD Sports 近日披露了一次涉及 1000 万客户数据的网络攻击，这些客户的个人和财务信息可能已被攻击者访问。

JD Sports 是英国著名运动连锁服饰零售商，在全球 32 个地区经营着 3402 家门店。此次攻击影响范围包含了 2018 年 11 月至 2020 年 10 月期间在 JD、Size、Millets、Blacks、Scotts 和 MilletSport 品牌下订单的客户——估计有“1000 万独立客户”。被泄露的信息包括姓名、地址、电子邮件帐户、电话号码、订单详细信息和银行卡的最后四位数字。

然而，JD Sports 称访问的数据“有限”，并解释道他们不存储完整的支付卡详细信息。因此，它不认为帐户密码已被泄露。

https://www.wangan.com/p/11v72bdc1fa17956

8、日本多个中央部门电邮地址遭泄露

1 月 30 日报道，共同社记者日前采访日本内阁官房情报安全中心（NISC）等处获悉，日本厚生劳动大臣加藤胜信的电子邮箱地址被泄露到了暗网。这是日本众院事务局分派的电邮地址，被用于注册推特账号。除加藤外，NISC 还发现多个中央部门的电邮地址泄露。

报道称，美国推特被报道有至少 2.3 亿个用户电邮地址疑似泄露。NISC 表示：“网络攻击可能会增加，希望相关人员注意。”

https://mp.weixin.qq.com/s/H1pGyxSSDCd8z32uMl2_Pw

9、小米汽车“设计文件”泄密，供应商被罚 100 万元!

2 月 2 日，小米汽车针对此前的“设计文件泄露”事件做出最终的处理结果：将依照《保密协议》处以 100 万元的经济赔偿，责成其对下游供应商加强信息安全管理，并对泄密人进行处理。

根据小米内部的通报处理结果，小米汽车“设计文件泄密”事件的起因是合作方北京北汽模塑科技有限公司因对其下游供应商管理不善，泄露了小米汽车前后保险杠某个版本的过程稿。

https://www.freebuf.com/news/356343.html

10、拳头公司《英雄联盟》及反作弊平台源代码泄露，黑客以百万美元价格打包拍卖

2 月 1 日报道，近日，某个暗网论坛上，一份关于拳头游戏公司 Riot Games 的热门游戏《英雄联盟》及其 Packman 反作弊平台的源代码正在以百万美元的价格被拍卖。

上周五，Riot Games 官方账号发布推文证实，其开发环境已被黑客入侵，攻击者能够窃取《英雄联盟（League of Legends）》《云顶之弈（Teamfight Tactics）》以及该公司的 Packman 反作弊平台的源代码。他们已经收到了攻击者的勒索信，黑客在信上向他们索要 1000 万美元，否则就将公开这份盗窃得手的敏感数据。

为证实真实性，黑客向 Riot Games 提供了一个一千页的 PDF 文档，据称该文档包含 72.4 GB 被盗源代码的目录列表，能够证明他们确实拥有对该公司源代码的访问权。对此，Riot Games 表示拒绝支付赎金，因为没有玩家数据或玩家个人信息受到损害。

https://www.wangan.com/p/11v7263ef2bba889

11、Google Fi 遭到破坏，客户数据遭重大泄露

2 月 1 日报道，美国移动电话运营商 Google Fi 近日表示，客户数据遭黑客泄露。此次事件可能与 1 月 19 日最近发生的 T-Mobile 数据泄露事件有关，该事件涉及超过 3700 万 T-Mobile 客户。

Google Fi 周一向其客户发送了一封电子邮件，解释说他们的主要网络提供商已通知他们“涉及第三方客户支持系统和有限数量的 Google Fi 客户数据的可疑活动”。

被访问的信息包括电话号码，帐户何时激活的信息、SIM 卡序列号、帐户状态以及有关移动服务计划的有限详细信息以及您的 Google Fi 服务提供的选项（例如无限短信或国际漫游）。据悉，此次事件引起了广大 Google Fi 客户的不满。

https://www.freebuf.com/articles/356199.html

12、TruthFinder、Instant Checkmate 确认数据泄露影响了 2000 万客户

2 月 3 日消息，TruthFinder 和 Instant Checkmate 背景调查服务的所有者 PeopleConnect 证实，在黑客泄露了包含数百万客户信息的 2019 年备份数据库后，他们遭遇了数据泄露。

1 月 21 日，Breached 黑客和数据泄露论坛的一名成员泄露了据称截至 2019 年 4 月 16 日使用该服务的 2022

万 TruthFinder 和 Instant Checkmate 客户的数据。在 2019 年 4 月 16 日创建备份之前，被盗数据共享为两个仅包含客户信息的 2.9 GB CSV 文件。暴露的客户信息包括电子邮件地址、散列密码、名字和姓氏以及电话号码。

https://www.bleepingcomputer.com/news/security/truthfinder-instant-checkmate-confirm-data-breach-affecting-20m-customers/

13、英国 Planet Ice 的系统被黑超过 24 万人的信息泄露

媒体 2 月 1 日报道，英国 Planet Ice 称黑客入侵其系统并窃取了 240488 个客户的详细信息。上周初，用户在网上订票时收到了一条简短的消息，解释说 Planet Ice 的服务器正在经历计划外的停机。之后，部分客户收到来自 Planet Ice 的邮件，透露它的 Ice Account 系统遭到攻击，未经授权的各方可访问系统的非财务信息。该公司已将此次违规事件通知 ICO，并对其展开调查。

https://www.bitdefender.com/blog/hotforsecurity/planet-ice-hacked-240-000-skating-fans-details-stolen/

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/