全球数据安全观察

总第 75 期 2022 年第 03 期

（2022.01.10-2022.01.16）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、国务院印发《“十四五”数字经济发展规划》

1月12日，国务院印发了“十四五”数字经济发展规划，是我国数字经济领域的首部国家级专项规划。《规划》明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。

《规划》部署了八方面重点任务：一是优化升级数字基础设施。二是充分发挥数据要素作用。三是大力推进产业数字化转型。四是加快推动数字产业化。五是持续提升公共服务数字化水平。六是健全完善**数字经济治理体系**。强化协同治理和监管机制，增强政府**数字化治理能力**，完善多元共治新格局。七是着力强化**数字经济安全体系**。增强网络安全防护能力，提升数据安全保障水平，有效防范各类风险。八是有效拓展数字经济国际合作。围绕八大任务，《规划》明确了信息网络基础设施优化升级等十一个专项工程。

https://mp.weixin.qq.com/s/WFigCPoaene_3bWU87GcRQ

2、工信部网安局：奋力推动工信领域网络和数据安全工作再上新台阶

全国工业和信息化工作会议近日召开，会议强调，工信领域要以党的二十大网络安全保障为主线、网络设施安全为

基础、**数据安全为重点**、安全产业为依托，不断提升网络和数据安全综合保障能力，助力筑牢国家安全屏障，护航工业和信息化高质量发展。并提出了六个方面的重点工作：一、深耕关键信息基础设施网络安全。二、健全新型融合性网络安全保障体系。三、全面推进工信领域**数据安全管理**，研究制定**数据安全重点标准**，组织开展工信领域**数据安全风险信息报送和共享**工作。四、纵深推进防范治理电信网络诈骗工作。五、大力升以技管网硬实力，加强网络和数据安全技术手段建设。六、推进网络和数据安全产业高质量发展，推动建设**数据安全创新体系**。

https://mp.weixin.qq.com/s/PhfINvcnwL9DQEaWWIxdNg

3、湖南大数据交易所试运营

1 月 11 日，湖南大数据交易所在长沙市天心经开区进入试运营，该交易所也将成为继贵州、陕西咸阳、北京、上海之后的全国第五家、中部唯一的新型大数据交易所。

目前，该交易所仅 2 个月时间开发上线并发布可供交易数据商品共 103 个，应用行业分布金融、保险、物流、地理信息等领域。交易所采取会员制规则，数据资源提供商、数据技术服务商、数据产品供应商及数据需求方均可申请注册成为交易所会员，入驻交易所平台，目前已经吸纳意向会员

单位 150 余个。

交易所着力打造三大平台：数据交易市场平台、会员和生态联盟服务平台、数据融合价值中心平台。发挥四大功能：数据的安全监管、质量标准认定审核、价值和初始价格的认定、交易过程管理。为确保交易数据的安全，湖南省大数据交易所在省行业主管部门的指导下制定了大数据交易所的交易规划，确定了八项运营业务规则，出台监管办法。同时交易所引入隐私计算公司华控清交，公司可运用多种密码学等隐私计算技术，做到“数据可用不可见、使用可控可计量”；可以在严格管控多方数据融合计算目的和方法（用途用量）前提下，实现数据特定使用价值（使用权）的安全流通和安全使用。

https://mp.weixin.qq.com/s/j8u2Ixa3GyoCsN2C8johcw

4、《信息安全技术 重要数据识别指南（征求意见稿）》公开征求意见

1 月 13 日，全国信息安全标准化技术委员会秘书处发布了《信息安全技术 重要数据识别指南（征求意见稿）》，并面向社会公开征求意见。

该指南为 2021 年 9 月 23 日公开的标准草案《信息安全技术 重要数据识别指南（征求意见稿）》的修订版本，在

框架上，新版的《指南》将旧版中“重要数据的特征”和“重要数据识别流程”合并为“重要数据的识别因素”。在内容上，新版的《指南》没有详细描述重要数据特征的小类，指提出了重要数据的十四项识别因素；此外，在识别重要数据的基本原则中，新版的《指南》将旧版中第二项“促进数据流动”原则替换为“突出保护重点”。

https://mp.weixin.qq.com/s/0l7WbATWBx-UZtYJFt3Olw

5、美国佛罗里达州参议院提出隐私保护法案

1 月 7 日，佛罗里达州参议院提交了关于《佛罗里达州隐私保护法》的第 1864 号参议院法案（SB）。除其他事项外，第 1864 号法案将：(1) 要求控制者实施合理的安全制度流程和实践做法；(2) 禁止控制者在某些情况下处理某些敏感的消费者数据；(3) 在出售消费者个人信息方面为其提供某些权利，允许数据主体选择退出此类出售和处理行为；(4) 为未成年人及其个人信息的处理提供某些保护；以及(5)要求收集消费者个人信息的控制者提供某些通知。此外，第 1864 号法案不会为消费者提供私人诉讼权依据，但将授权司法部对被认为实施了不公平和欺骗性贸易行为的控制者和处理者采取行动，同时还授权总检察长对违法行为追讨律师费及其他费用。

https://mp.weixin.qq.com/s/3QVPvqUuK_mLLqH4wuYbSg

技术、产品与市场

1、2022 年中国未来数字化基础架构十大预测

IDC FutureScape 对未来数字化基础架构的预测如下:

（1）敏捷业务战略：到 2023 年，中国 500 强企业将更优先考虑业务目标而非基础设施选择，30%新的工作负载将使用解决方案提供商特定 API 来部署，这些 API 将会增加价值，但同时降低工作负载的可移植性。

（2）供应链完整性：到 2024 年，超过 50%的中国 500 强企业将考虑到业务韧性，将基础设施供应链完整性作为选择厂商的评估标准。

（3）数据安全治理：到 2023 年，随着网络安全隐患的不断增加，大规模数据面临风险，大多数最高层领导者将实施与数据可用性、数据保护和数据治理相关的 KPI，这些 KPI 对企业来说至关重要。

（4）环境、社会和公司治理（ESG）：到 2025 年，鉴于 CIO 依赖基础设施厂商来帮助实现其 ESG 目标，50％中国 500 强企业的数字基础设施方案征询书（RFP）将要求 IT 厂商能用数据来证明企业在 ESG/可持续运营方面的成效。

（5）边缘数据优先：到 2025 年，随着边缘数据的爆炸式增长，超过 50％的中国 500 强企业将把边缘优先数据管理、

安全和网络实践嵌入到数据保护计划之中。

（6）工作负载激增：到 2025 年，高依赖性工作负载将激增 5 倍，这将促使 40％的中国 500 强企业使用前后一致的架构治理框架，以此来确保基础设施报告和审计的合规性。

（7）即服务：到 2025 年，50％的中国企业将通过营运开支（opex）预算来为业务线（LOB）和 IT 项目提供经费，并与 KPI 准确对接。

（8）创新基础架构：到 2025 年，60％的中国企业将采用创新计算技术，通过缩短价值生成时间（time to value）来促进业务差异化。

（9）AIOps：到 2026 年，60％的中国 500 强企业将使用 AIOps 解决方案来推动自动化和工作负载分配决策，包括定义成本和绩效指标，以提高韧性和敏捷性。

（10）以应用为中心：到 2026 年，中端市场企业将把 40％的基础设施开支从传统渠道转向更加以应用为中心的技术合作伙伴。

https://mp.weixin.qq.com/s/Sqtfwd0nJJ2MRROZNYblwQ

2、数据库技术七大发展趋势

大数据时代，数据量不断爆炸式增长，数据存储结构也越来越灵活多样，日益变革的新兴业务需求催生数据库及应

用系统的存在形式愈发丰富，这些变化均对数据库的各类能力不断提出挑战，**推动数据库技术不断向着模型拓展、架构解耦的方向演进，与云计算、人工智能、区块链、隐私计算、新型硬件等技术呈现取长补短、不断融合的发展态势**，总结起来体现为如下三个方向、七大趋势。

三个方向：1）多模数据库实现一库多用、利用统一框架支撑混合负载处理、运用 AI 实现管理自治，提升易用性、降低使用成本；2）充分利用新兴硬件、与云基础设施深度结合，增强功能、提升性能；3）利用隐私计算技术助力安全能力提升、区块链数据库辅助数据存证溯源，提升数据可信与安全。

七大趋势：1）多模数据库实现一库多用；2）统一框架支撑分析与事务混合处理；3）运用 AI 实现管理自治；4）充分利用新兴硬件；5）与云基础设施深度结合；6）隐私计算技术助力安全能力提升；7）与云基础设施深度结合。

https://mp.weixin.qq.com/s/qFugTh0V0z2HGx2leN9U6Q

3、展望：2022 年端点安全十大发展趋势

2021 年网络安全行业发生了众多变化，联软科技结合过去一年全球网络安全市场的变化以及自身对企业端点安全的理解，对 2022 年端点安全进行了以下趋势预测：

（1）远程办公常态化，将加剧企业对 BYODPC 的安全投资；

（2）EDR 将成为 EPP 持续增长的重要推手；

（3）企业数字化转型将揿下零信任部署“加速键”；

（4）ZTNA 作为 SASE 的核心能力之一，将保障企业网络边缘安全接入；

（5）**数据安全产业将迎来“黄金”发展期；**

（6）信创产业从“分散”到“集中”；

（7）端点攻击复杂性持续增长，将炒热 XDR 市场；

（8）企业选择 VDI/DaaS 解决方案时，需同时考虑其带来的安全问题；

（9）构建一体化安全能力&注重用户体验，是零信任落地有效的催化剂；

（10）UEM+UES 将是端点安全发展方向。

https://www.secrss.com/articles/38185

4、Facebook 推出“隐私中心”，教育用户了解数据收集和隐私选项

近日，前身为 Facebook 的 Meta 公司宣布推出一站式“隐私中心”，旨在教育用户在使用其社交媒体应用程序时，收集和处理个人信息。隐私中心主要由五大板块组成，分别是

共享、安全、数据收集、使用和广告。

目前，隐私中心仅面向美国本土 PC 端用户开放，未来数月内可能将该功能推向其他地区用户和 App 端。参与试点的用户将能够通过在桌面版 Facebook 上导航到“设置和隐私”来访问隐私中心。

https://www.freebuf.com/news/319325.html

5、首个隐私保护机器学习国际标准正式推行

2022 年 1 月 11 日消息，近日，IEEE 标准委员会正式发布并推行了基于可信执行环境的隐私保护机器学习的国际标准（IEEE Std 2830™）。**这也是国际上首个基于可信执行环境的隐私保护机器学习技术框架与要求的国际标准**。由蚂蚁集团联合国内外共知名高校、研究机构共同立项、筹备、制定。该标准的设立通过规范隐私计算的技术标准，为保护数据隐私和释放数据价值提供了可落地的技术标准方案。

此标准的制定可用以指导规避隐私计算技术体系中存在的风险，促进多个数据提供方在满足数据安全、隐私保护和监管合规等要求下，实现基于数据协同和授权共享的数据聚合和计算，在保护保护数据隐私的基础上释放数据价值。

https://mp.weixin.qq.com/s/LOA02ToGXTTnxkwojOoDXA

业界观点

1、张小军：数据安全是区块链应用的根本

在中国科协企业创新服务中心和中国通信学会承办的2021“科创中国”企业创新大家谈第二期活动上，华为区块链首席战略官张小军就“区块链构筑数据要素的可信流转”为主题进行分享。

张小军认为，现在的区块链需要有前端的录入，在2018年时，关于区块链在应用中提出最主要的问题是上链数据是假的怎么办？问题出在哪里，就要从哪儿解决。因此他提出区块链+IOT（物联网），借助IOT实现可信信息上链，同时对于关键机密信息，可以实现数据采集并加密直接上链，从而保障数据在上链前的可靠性。区块链是保障上链后的数据的安全流转，在流转中需要网络的转发，因此区块链需要多技术加持，方能保障数据要素从上链前、上链中、上链后期的数据采集、流转、分析的全封闭安全闭环。

张小军表示，不管是政务还是金融应用数据的安全性在这两个领域首当其冲，不仅需要BaaS平台的安全保障，更需要从硬件、网络、软件平台多级的安全防护，方能促成应用的大面积商用。

https://tech.gmw.cn/2022-01/07/content_35432193.htm

2、中国政法大学发布“个人信息保护和数据安全”专题调查报告：满意度呈“三三分”

近日，在中国政法大学举办的《2021 全国网民网络安全感满意度调查“个人信息保护与数据安全”专题调查报告》（以下简称《专题报告》）发布会上，网民对我国个人信息保护现状的满意度呈现“三三分”态势，即 37.52%受访人群评价“比较好”“非常好”，35.86%受访人群评价“一般”，26.62%受访人群评价“不太好”“非常不好”。

针对个人信息泄露的感受状况，《专题报告》显示，23.08%受访人群“没有遇到”“很少遇到”个人信息泄露，35.66%受访人群“有一些”信息泄露遭遇，41.25%的受访人群遭遇“比较多”“非常多”信息泄露。

网民认为，数据安全保护现阶段存在的问题主要体现在市场现状、数据结构和标准规范等方面。其中，数据市场交易市场混乱，以及数据不规范是目前最突出的问题。其次，数据安全标准规范建设滞后、数据应用程度较低、中介服务供应不足、政府数据不开放等问题也是数据安全方面存在的重要问题。

https://mp.weixin.qq.com/s/QMLc7emlqtgXN0EKJZXlmw

3、新时期个人数据保护政策与技术研讨

近日，由中国科学院(以下简称中科院)计算机网络信息中心主办的“新时期个人数据保护政策与技术”学术研讨会在京举办。会议强调指出，在数字经济迅猛发展的背景下，以个人数据为中心的大数据时代将加速到来，其底层逻辑将更加要求数据的私密性、安全性、不可被利用和篡改性。

会上，中科院计算技术研究所洪学海研究员指出，大数据时代的个人数据保护，需要一定的技术手段来解决法律法规实施过程中的操作实践问题。我们希望业界开放合作，凝练个人数据保护中的科学问题，进而去推导和解决其中的技术问题，通过各领域专家的跨学科协作，探索各应用场景下个人数据保护落地方案的创新。

中国人民大学孟小峰教授从技术发展角度，指出传统互联网体系结构在身份认证与数据权属的设计上存在先天不足，有必要在新时期数字经济发展的大环境下重新定义和设计数据基础设施。产业界要用发展的眼光看待和解决目前个人数据保护领域的相关产业政策和法律法规问题，既不能无视个体的权益诉求强化平台的绝对优势，也不能作茧自缚错失大数据发展红利，让我们在世界新经济竞技场中错失良机。

https://finance.eastmoney.com/a/202201102241900612.html

4、iLAW 合规创研院发布 2021 年数据隐私合规行政处罚研究报告

2021 年出台并施行的《数据安全法》《个人信息保护法》对数据违法行为规定了多项行政处罚条款，对不履行规定保护义务、交易来源不明的数据、拒不配合国家机关进行数据调取、违反国家核心数据管理制度及数据出境管理要求等行为，均设定了严格的罚则：对单位最高可罚 5000 万元，并可以视违法程度责令违规企业暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对个人最高可罚 1000 万元，并可以对其采取“职业禁入”限制，对构成违反治安管理行为的给予治安管理处罚，相关违法行将记入信用档案并予以公示。

iLAW 合规创研院由 2021 年的数据隐私合规行政处罚案例出发，收集数据隐私合规相关行政处罚数据共 234 起，其中，**工信部共罚款 30 次，各地市监局共罚款 128 次，各地网信部门共罚款 67 次**。2021 年度三部门做出**罚款金额共计 36,856,671 元**，其中，网信部门共罚款 2,790,000 元，市监局共罚款 6,706,671 元，工信部门共罚款 2,250,000 元。江苏、北京、上海所发生行政处罚数量最多，分别为 83 起、72 起、29 起。

https://mp.weixin.qq.com/s/y1M5aeKCLkmGDine8TdH7g

5、环球律师事务所数据合规团队发布 2021 中国数据合规年度报告

2021 年，见证了《数据安全法》和《个人信息保护法》两部数据领域核心法律的出台，与《网络安全法》并驾齐驱；见证了监管机构配套政策有条不紊地推陈出新，也为产业界将数据运用在各行业各领域的高速发展把住了方向盘；见证了全国信息安全标准化技术委员会发布的各项国家标准并不断成熟丰富，给企业提供了更有操作性的合规指引；见证了用户个人信息保护意识的显著提升，隐私保护理念渐入人心；也见证了企业对数据合规监管要求与落地思路的逐渐熟悉、适应和重视，对数据合规工作有了更细致、更深入的了解，也产生了更迫切的需求。

报告指出，我国规制企业拟赴境外/国外上市的监管态度逐渐清晰：首先，《网络安全审查办法》第七条明确要求，掌握超过 100 万用户个人信息、赴国外上市的网络平台运营者必须向网络安全审查办公室申报网络安全审查—申报后可能有以下三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。其次，《网络数据安全管理条例（征求意见稿）》针对赴境外上市的数据处理者有数据安全评估及年度上报义务，并专门做出

了规定。其中第三十二条指出，处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门。这两份文件的发布进一步反映我国对于赴国外/境外上市企业所涉及数据安全问题的关注。尤其考虑到企业国外上市后，可能受制于当地监管部门管辖从而需要向国外传输中国境内相关数据，有可能受到外国政府影响、控制或恶意利用，我国有必要加强对拟国外上市企业的监管力度。结合早先网络安全审查办公室对“某知名互联网出行企业”突发实施的网络安全审查的急行动、重举措，监管机构的态度和国家政策导向可见一斑。

https://mp.weixin.qq.com/s/x0Ip-utTvlAYv4tTcJag3g

数据安全事件

1、央行新年首张千万罚单，东亚银行因违反信用信息采集被罚

2022 年 1 月 12 日报道，近日，央行开出 2022 年首张千万级别罚单。据中国人民银行上海分行网站发布行政处罚信息显示，因违反信用信息采集、提供、查询及相关管理规定，东亚银行（中国）有限公司被责令限期改正并处罚款人民币 1674 万元。

因违反信用信息采集、提供、查询及相关管理规定而被处罚的银行等金融机构不在少数，监管部门正不断加强对个人信息安全和消费者权益的保护。

https://mp.weixin.qq.com/s/7Bt1-ANXXdojk6VKsXu4ew

2、隐私计算领域第一个安全漏洞被爆出

2022 年 1 月 13 日，微众银行 FATE 联邦学习项目官方进行了声明：关于 RIAC 同态加密算法的相关说明。

据悉，微众银行 FATE 框架自研的同态加密算法存在安全漏洞，已经第一时间上报给监管部门，请大家立刻停止使用 RIAC 同态加密算法。

这是我国隐私计算领域第一个安全漏洞。简单地说，

RIAC(或者叫迭代仿射变换) 被破解，指的是可以解密，迭代仿射变换和仿射变换都有问题，不迭代的话攻击难度更低。

https://mp.weixin.qq.com/s/fDXipvAT_nY8crPqYuUThA

3、美国医学评论研究所披露 134,000 人的数据泄露事件

2022 年 1 月 11 日，据外媒报道，美国医学评论研究所(MRIoA) 于上周五发布数据泄露通知，超过 134,000 人受到该事件的影响。

对该事件的调查显示，受保护的被盗健康信息包括了姓名、性别、地址、电子邮件、电话号码、出生日期、社会安全号码、完整的临床信息（包括诊断、治疗、病史和实验室测试结果）)和财务信息（例如健康保险单）。MRIoA 表示已采取措施加强安全性，实施了额外的多因素身份验证保护，用新的服务器替换了原先的设备，部署了一个强化的备份环境，修改了它的网络安全政策，并加强了员工培训。

https://www.securityweek.com/mrioa-discloses-data-breach-affecting-134000-people?&web_view=true

4、化妆品公司娇韵诗遭遇数据安全事件，可能涉及新加坡客户的个人信息

2022 年 1 月 11 日报道，法国化妆品公司娇韵诗遭遇数

据安全事件，由于该事件可能涉及新加坡客户的个人信息安全，该公司向新加坡个人数据保护委员会 (PDPC) 通报了安全漏洞。

娇韵诗在其网站上的一份声明中表示，该事件是由 Log4j 漏洞导致。虽然该漏洞在安全补丁发布后的几个小时内得到了及时修补，但在漏洞公开后，服务器似乎已经受到攻击，被访问的数据可能包括客户的姓名、地址、电子邮件、电话号码和娇韵诗忠诚度计划状态等。

https://headtopics.com/sg/cosmetics-company-clarins-hit-by-data-security-incident-may-involve-singapore-customers-personal-23358610

5、大量美国和加拿大人的财务数据遭曝光

2022 年 1 月 12 日报道，Website Planet 的 IT 安全研究人员发现了一个配置错误的数据库，该数据库由位于佛罗里达州杰克逊维尔的运输行业商业信用报告机构 TransCredit 拥有。据称，该数据库包含客户敏感财务和个人数据，其中涵盖了加拿大和美国的货运和运输公司。该错误配置的数据库共暴露了 822,789 条记录，其中 600,000 条是客户的信用记录，其他暴露的信息包括：姓名、税号、电子邮件地址、银行信息、社会安全号码 (SSN)、内部登录 ID 和密码、EIN

（雇主识别号码）等。

https://www.hackread.com/transcredit-exposed-financial-data-americans-canadians/

6、新的 ZLoader 恶意软件活动袭击了 111 个国家的 2000 多名受害者

2022 年 1 月 10 日报道，Check Point Research 的专家在 2021 年 11 月上旬发现了一个新的 ZLoader 恶意软件活动。截至 2022 年 1 月 2 日，该恶意软件活动仍然活跃，威胁行为者已经窃取了 111 个国家/地区的 2000 多名受害者的数据和凭据。

https://securityaffairs.co/wordpress/126513/malware/zloader-new-campaign.html

7、不安全的 Amazon S3 存储桶暴露了 50 万名加纳毕业生的个人数据

2022 年 1 月 10 日报道，vpnMentor 的研究人员表示，他们在亚马逊网络服务(AWS)的一个存储桶中发现了大量与加纳国家服务秘书处(NSS)相关的未加密数据。在与 NSS 的工作相关并保存在 AWS S3 存储桶中的 300 万份文件中，有一些文件受到密码保护，但许多文件并未受到密码保护——从

2018 年 3 月到 2021 年底，这一疏忽暴露了大约 500,000-600,000 人的数据，包括个人信息、身份证和照片的扫描以及就业记录。vpnMentor 报告称，该实例配置错误，并且密码保护应用不一致，因此可以在其他目录中访问受密码保护的敏感文件的打开版本。

https://portswigger.net/daily-swig/insecure-amazon-s3-bucket-exposed-personal-data-on-500-000-ghanaian-graduates

8、印度时装公司 ABG 遭到攻击，客户和员工数据已被盗

2022 年 1 月 11 日报道，印度时装公司 Aditya Birla Group(ABG)遭到网络攻击。12 月初，ShinyHunters 表示其已入侵该公司的网络，直到现在仍然可以访问其客户和员工的敏感数据。研究人员曾多次就此事联系 ABG，但未收到回复。1 月 11 日，ShinyHunters 称其和 ABG 之间的谈判失败，将直接公开或出售这些信息。

https://www.databreaches.net/major-indian-fashion-retailer-hacked-and-data-leaked/

9、松下称黑客在网络攻击中获取了求职者的个人资料

2022 年 1 月 11 日报道，日本科技巨头松下公司证实，黑客在 11 月的网络攻击中获取了属于求职者和实习生的个

人信息。该公司在 11 月 26 日首次确认了数据泄露事件，当时该公司无法说明黑客是否获取了任何敏感信息。然而，在 1 月 7 日发布的更新中，松下公司表示：与申请就业或在公司某些部门参加实习的候选人有关的一些个人信息在此次事件中被获取。

该公司在外部安全顾问的帮助下进行的调查结果证实：第三方通过一家海外子公司的服务器非法访问了日本的一台文件服务器。松下公司说，在发现非法访问后，它 “立即实施了额外的安全对策”，包括加强来自海外的访问控制，重新设置相关密码和加强服务器访问监控。松下公司表示，它正在加强安全措施，以防止再次发生攻击。

https://mp.weixin.qq.com/s/A3xF0e1TAYptwhFJhza3WQ

10、黑客入侵了加密货币交易所 LCX 并窃取了近 700 万美元

2022 年 1 月 10 日报道，黑客侵入了基于 LCX 的比特币交易所 LCX 的热钱包。在攻击期间，ERC-20 代币被盗。调查期间，平台资金存取已暂停。据 PeckShield 分析师称，黑客从平台上移除了价值 680 万美元的资产，其中包括 343 万美元的美元硬币（USDC）稳定币和 222 万美元的 LCX 原生代币。

https://www.wangan.com/p/7fy7fgb8ff370fce

11、黑客从 Lympo NTF 平台窃取了 1870 万美元

2022 年 1 月 11 日报道，体育 NFT 铸造平台、Animoca Brands 子公司 Lympo 遭遇热钱包安全漏洞，损失 1.652 亿个 LMT 代币，在黑客入侵时价值 1870 万美元。Lympo 团队在 Medium 上发布的简短更新称，1 月 10 日，黑客成功进入了 Lympo 的热钱包，并“从里面偷走了总共约 1.652 亿个 LMT。”据该帖子称，有 10 个不同的项目钱包在这次攻击中入侵。似乎大多数被盗的代币都被发送到一个地址，在 Uniswap 和 Sushiswap 上被换成 ETH，然后被发送到了其他地方。

https://securityaffairs.co/wordpress/126766/cyber-crime/lympo-ntf-platform-hacked.html