网络安全电子期刊

Security Awareness

4月
2024

全民国家安全教育

- 网信办公布《促进和规范数据跨境流动规定》
- 划重点！2024年我国数据工作明确8大重点任务
- 首个公开针对AI工作负载的大规模攻击：数千台服务器被黑
- 415·国家安全教育日|新时代，新考验，国家安全，你我共筑

Contents 目·录

1 业界动态

2 信息安全在身边

3 警钟长鸣

业界动态

没有网络安全就没有国家安全

网信办公布
《促进和规范数据跨境流动规定》

◉ **关键词：**数据安全；数据出境；个人信息保护

3 月 22 日，国家互联网信息办公室公布《促进和规范数据跨境流动规定》（以下简称《规定》），自公布之日起施行。

国家互联网信息办公室有关负责人表示，数据跨境流动已经成为全球资金、信息、技术、人才、货物等资源要素交换、共享的基础。为了促进数据依法有序自由流动，激发数据要素价值，扩大高水平对外开放，《规定》对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度作出优化调整。

《规定》明确了重要数据出境安全评估申报标准，提出未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

《规定》规定了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件：一是国际贸易、跨境运输、学术合作、跨国

生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的；二是在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；三是为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息的；四是按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；五是紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；六是关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）的。

《规定》设立自由贸易试验区负面清单制度。提出自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内负面清单，经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

《规定》明确了应当申报数据出境安全评估的两类数据出境活动条件，一是关键信息基础设施运营者向境外提供个人信息或者重要数据；二是关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息。同时，明确了应当订立个人信息出境标准合同或者通过个人信息保护认证的数据出境活动条件，即关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。

《规定》同时对数据出境安全评估的有效期限和延期申请、数据安全保护义务和监督管理责任、与数据出境安全管理其他规定的衔接适用等作了规定。

来源：网信中国

网信办发布
《数据出境安全评估申报指南（第二版）和《个人信息出境标准合同备案指南（第二版）》

◉ **关键词：**数据安全；数据出境；个人信息保护

为了指导和帮助数据处理者规范有序申报数据出境安全评估、备案个人信息出境标准合同，国家互联网信息办公室编制了《数据出境安全评估申报指南（第二版）》、《个人信息出境标准合同备案指南（第二版）》，对申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求作出了说明，对数据处理者需要提交的相关材料进行了优化简化。

数据处理者因业务需要向境外提供重要数据和个人信息，应当遵守《数据出境安全评估办法》、《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》有关规定。符合数据出境安全评估适用情形的，按照申报指南申报数据出境安全评估；通过与境外接收方订立个人信息出境标准合同的方式向境外提供个人信息的，按照备案指南向所在地省级网信部门备案。

国家互联网信息办公室开通了“数据出境申报系统”，数据处理者可以通过该系统申报数据出境安全评估、备案个人信息出境标准合同，具体使用说明见系统首页《用户手册》。

来源：网信中国

《消费者权益保护法实施条例》发布
经营者应依法保护消费者个人信息

◉ **关键词：**个人信息保护；消费者权益；网络安全义务与责任

3 月 19 日，《中华人民共和国消费者权益保护法实施条例》（以下简称《条例》）公布，自 2024 年 7 月 1 日起施行。

《条例》共 7 章 53 条，其中，对消费者权益保护法规定的保障消费者人身财产安全、缺陷产品处理、禁止虚假宣传、明码标价、使用格式条款、履行质量担保责任、消费者个人信息保护等义务作了细化规定。补充了经营者关于老年人、未成年人消费者权益保护相关义务规定。

随着网络消费的增长，个人信息的过渡收集和管理问题，导致个人信息泄露事件频发。《条例》中规定，经营者应当依法保护消费者的个人信息。经营者在提供商品或者服务时，不得过度收集消费者个人信息，不得采用一次概括授权、默认授权等方式，强制或者变相强制消费者同意收集、使用与经营活动无直接关系的个人信息。经营者处理包含消费者的生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息以及不满十四周岁未成年人的个人信息等敏感个人信息的，应当符合有关法律、行政法规的规定。

来源：中国信息安全

《网络安全技术 生成式人工智能预训练和优化训练数据安全规范（征求意见稿）》等 4 项国家标准公开征求意见

◉ **关键词：**网络安全；数据安全；个人信息转移；人工智能

关于征求《数据安全技术 基于个人请求的个人信息转移要求（征求意见稿）》等 4 项国家标准意见的通知

网安秘字〔2024〕32 号

全国网络安全标准化技术委员会归口的《数据安全技术 基于个人请求的个人信息转移要求》等 4 项国家标准现已形成标准征求意见稿。

根据委员会标准制修订工作程序要求，现将该 4 项标准征求意见稿面向社会公开征求意见。如有意见或建议请于 2024 年 6 月 2 日 24:00 前反馈秘书处。

4 项国家标准征求意见稿清单：

《数据安全技术 基于个人请求的个人信息转移要求》

《数据安全技术 数字水印技术实现指南》

《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》

《网络安全技术 生成式人工智能数据标注安全规范》

全国网络安全标准化技术委员会秘书处

2024 年 4 月 3 日

划重点！
2024 年我国数据工作明确 8 大重点任务

◉ **关键词：**数字化；数据安全；数据要素 X

2024 年，国家数据局将从健全数据基础制度、提升数据资源开发利用水平、以数字化赋能高质量发展、促进数据科技创新发展、优化数据基础设施布局、强化数据安全保障能力、提升数据领域国际合作水平和发挥试点试验的引领作用等 8 方面推动数据工作。

4 月 1 日至 2 日召开的全国数据工作会议，是数据系统的首次全国性工作会议，为 2024 年我国数据工作领域“划重点”。

重点任务 1：健全数据基础制度。

建立健全数据产权制度。制定促进数据合规高效流通和交易的政策，围绕降低流通成本、提高流通效率，培育多层次数据流通交易体系。建立数据要素收益分配机制。健全数据流通利用安全治理机制。

重点任务 2：提升数据资源开发利用水平。

发挥公共数据资源开发利用的示范效应，推进公共数据资源管理和运营机制改革，对建立资源登记制度、授权运营披露机制等作出安排，同时明确公共数据授权运营的合规政策和管理要求，一体推进公共数据共享、开放和授权运营，平衡好公益性和市场化的关系。

持续探索企业数据、个人数据开发利用新路径，研究制定企业数据资源开发利用的政策，降低企业数据资源流通使用成本。全力推动“数据要素 ×”行动，联合地方搭建区域性、全国性竞赛平台，开展数据要素应用典型案例评选。着力繁荣数据开发利用生态，大力发展服务型、应用型、技术型数商。

重点任务 3：以数字化赋能高质量发展。

加快数字中国建设，抓好年度工作分解分工，建立指标体系，加强监测分析和督

促检查，办好第七届数字中国建设峰会。大力发展数字经济，制定支持数字经济高质量发展的政策，协同推进数字产业化和产业数字化。提升数字化公共服务水平，开展国家数字乡村试点工作，落实好数字经济促进共同富裕各项任务。

重点任务 4：促进数据科技创新发展。

围绕技术发展加快产业布局，形成数据科技与数据产业相互融合、相互促进的良性发展态势。

重点任务 5：优化数据基础设施布局。

加快全国一体化算力网和数据流通利用基础设施建设，围绕区域、行业和跨境等重点应用场景，储备一批着眼当前、有利长远的数据基础设施类项目，做到适度超前，为未来深度应用提供前期基础，加快研究制定数据基础设施建设指引，发挥好政府投资的放大效应。

重点任务 6：强化数据安全保障能力。

始终绷紧数据安全这根弦，加强对数据采集、储存、流通、使用的全过程安全管理，实现数据安全“可知、可视、可管、可控、可溯”。提升数据安全技术保障水平。

重点任务 7：提升数据领域国际合作水平。

统筹做好数字经济领域国际合作，积极推进“小而美”的数字合作项目，提升数字经济对外合作的时效性，助力企业“走出去”。完善国际数字治理“中国方案”，深入研究国际数字治理规则体系，积极参与世贸组织电子商务规则谈判。

持续优化数据跨境流动规则，强化数据跨境流动相关的基础设施建设和互联互通，鼓励自贸区因地制宜形成本地区数据跨境流动负面清单。

重点任务 8：发挥试点试验的引领作用。

鼓励有条件的地方先行先试，支持更多地方因地制宜加快发展，探索数据要素市场化配置改革的实现路径和方法，为政策制定提供经验。推广局部地区或特定领域的主要成果，以点带面推动发展。

来源：新华网

信息安全在身边

警惕网络风险，共建人力防火墙

新型网络钓鱼攻击
伪装银行通知传播键盘记录器

◉ **关键词：**网络钓鱼；钓鱼邮件；诱饵文件

研究员发现了一场新型网络钓鱼活动，主要是使用新型加载程序恶意软件，搭载名为 Agent Tesla 的信息窃取程序和键盘记录器。

不久前就有一封带有此攻击链的钓鱼邮件。此邮件伪装成银行付款通知，以诱导用户点击并打开其附带的存档文件。然而这个存档文件隐藏了一个恶意加载程序，该加载程序激活了在受感染主机上部署 Agent Tesla 的过程。

在看似良性的文件中嵌入恶意软件的策略是攻击者反复采用的策略，以诱骗毫无戒心的受害者触发感染序列。

此次披露之际，还发现了一个名为 TA544 的网络犯罪组织进行的另一项网络钓鱼活动，该活动利用伪装成合法发票的 PDF 文件来传播 WikiLoader（又名 WailingCrab）并与命令和控制（C2）服务器建立连接，该服务器几乎完全包含被黑客入侵的 WordPress 网站。

安全小贴士

科技在不断发展，攻击者的手段也在不断进步，但万变不离其宗，只要做到“不明邮件不点击，陌生文件不打开，使用正版软件并定期更新和杀毒”，就能将绝大部分潜在的网络安全风险抵御在外。

日产大洋洲数据泄露影响约 10 万人

◉ **关键词：**网络攻击；勒索攻击；数据泄露；客户信息保护

日产大洋洲公司（Nissan Oceania）于近日发布官方声明，证实其在 2023 年 12 月遭遇了来自 Akira 勒索软件的网络攻击事件，导致大约 10 万人的数据泄露。

事件脉络

2023 年 12 月初，日产汽车在澳大利亚及新西兰地区的部门发布声明，指出公司正在对其内部网络系统遭受的网络攻击进行调查。尽管后续并未证实发生数据泄露事件，但日产公司依然提醒广大客户对其个人账户保持高度警惕，以防范潜在的诈骗威胁。

两周后，Akira 勒索软件团伙公开宣称对此次网络攻击事件负责，并声称已窃取日产汽车约 100GB 的数据信息，涉及员工个人信息、保密协议、项目数据以及合作伙伴和客户信息等敏感内容。

直到近期，日产汽车承认 Akira 勒索软件团伙窃取了一些现任和前任员工的数据，以及该地区日产、三菱、雷诺、Skyline、英菲尼迪、LDV 和 RAM 经销商的客户数据。

最新声明

日产汽车在最新声明中透露，预计在未来几周内，将正式向约十万名受影响的用户通报近期发生的信息泄露事件。

据日产方面所述，此次事件中，被盗的个人信息类型各异，其中约 10% 的受影响者遭受了政府身份信息的泄露，具体包括医疗保险卡、驾照、护照以及税务档案号等敏感信息。具体而言，数据集涵盖了大约 4000 张医疗保险卡信息、7500 份驾照数据、220 本护照资料以及 1300 个税务档案号。其余 90% 的大都是贷款相关文件、就业详情和出生日期等信息。

日产承诺将单独通知受影响的客户，告知他们暴露了哪些信息，他们可以做什么，

以及可以提供哪些形式的支持。但不幸的是，Akira 勒索软件团伙已经通过其在暗网上的勒索页面泄露了被盗数据。

（图片来自网络）

为了弥补受影响的用户，日产提供免费使用 IDCARE 的服务，通过澳大利亚的 Equifax 和新西兰的 Centrix 提供免费信用监控服务，并为更换受损的政府身份证提供报销。

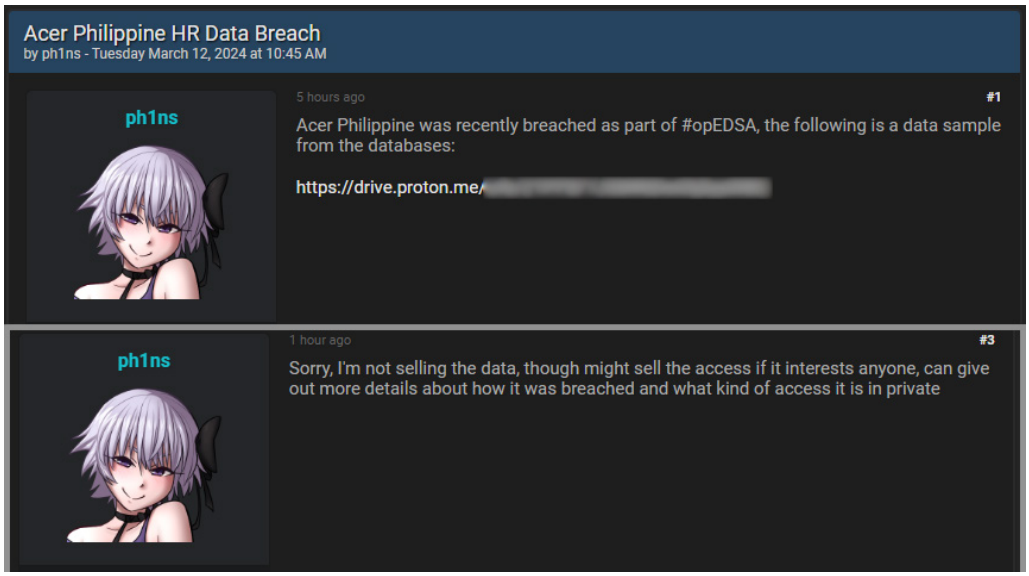
安全小贴士

勒索攻击是攻击者最常用的攻击手段之一，企业应定期备份企业重要数据，防患未然；在遭遇勒索攻击时，及时切断网络，报告专业安全部门进行处理，拒绝支付赎金，不给犯罪分子进行二次勒索或进行其它网络攻击活动提供资金。

宏碁菲律宾公司第三方供应商遭黑客攻击致数据泄露

◉ 关键词：网络安全；数据泄露；第三方供应商安全

宏碁（Acer），中国台湾地区的知名计算机硬件与电子产品制造商，素以其卓越的电脑产品性价比受到广泛赞誉。然而近日宏碁菲律宾分公司方面证实，其用于管理员工考勤数据的第三方服务供应商遭受了网络攻击，导致部分员工数据被非法窃取。



威胁攻击者发布的帖子（Bleeping Computer）

据可靠消息，一名自称为“ph1ns”的威胁攻击者在某黑客论坛上发布了一个链接，声称可以免费下载包含宏碁电脑员工数据的数据库。值得注意的是，该攻击者明确表示，此次网络攻击行为并未涉及勒索软件或数据加密，而是一次纯粹的数据盗窃行为，并未试图对宏碁电脑公司进行勒索。

安全事件发生后，媒体迅速与宏碁取得联系，以核实相关情况。宏碁发言人确认数据被盗，但并非来自公司内部系统。经调查，泄露源于菲律宾的一家外部供应商，导致部分员工数据外泄。目前，宏碁已经与供应商、网络安全专家和执法部门进行合作，

调查网络安全事件。

此外，宏碁方面始终坚称，目前尚未有客户数据遭受影响，亦无任何迹象显示宏碁的网络系统遭受任何形式的侵害。宏碁菲律宾公司亦发布了一份公开声明，对客户数据的安全性提供了类似的保证，并确认其系统不会受到损害。

安全小贴士

在网络安全领域，企业自身的安全固然重要，但同样不能忽视与第三方供应商的安全问题。为确保网络安全和数据安全，我们需要对第三方供应商进行仔细的挑选，明确对方网络安全层面的稳定性，与其建立紧密的合作机制，并制定全面的应急响应计划，以便在发生安全事件时能够及时、有效地应对。

苏格兰健康局遭网络攻击面临数据泄露风险

关键词：网络安全；数据泄露；勒索软件

苏格兰国家医疗服务系统（NHS）的一家信托机构在遭受潜在破坏者的威胁后，已出现服务中断以及可能的数据泄露风险。NHS 邓弗里斯和加洛韦在周五发布的正式声明中明确指出，该机构“持续受到集中且不断升级的网络攻击”。

医疗保健提供者正协同国家网络安全中心（NCSC）、苏格兰警察局及苏格兰政府深入调查此次事件。

“在黑客入侵系统的过程中，有可能获取了大量的数据，”警报严肃指出，“目前正与网络安全机构紧密合作，追查可能被访问的数据内容。尽管仍在调查中，但我们有理由相信这可能包括患者的身份信息及员工的身份信息。”

目前尚不清楚关于威胁行为者的最终意图以及违规的具体规模，然而根据现有情况，勒索软件成为了一个显著的潜在嫌疑。鉴于医疗保健提供商掌握大量个人及医疗数据，且对服务中断的忍受度相对较低，这使得其成为了基于经济利益的勒索集团的主要攻击目标。

Comparitech 去年发布报告称，过去七年中，勒索软件攻击已给美国经济带来高达 780 亿美元的损失。此外，2021 年爱尔兰卫生服务执行局（HSE）遭受的重大勒索软件攻击，已经导致了数千万英镑的经济损失。

NHS 邓弗里斯和加洛韦强调，泄露机密数据是一项极其严重的事项。因此，他们呼吁所有相关人员，包括工作人员和公众，应保持高度警惕，对任何声称拥有与他们有关的数据并试图访问其系统的行为，应立即采取措施进行防范。

安全小贴士

防范勒索攻击做到以下几点：

1）做好数据分类分级，并设置合理的访问权限；

2）定期备份重要数据，设置 8 位以上强密码并定期更新；

3）定期进行安全风险评估，并制定应急响应预案，防患未然；

4）不明邮件不打开，不明链接不点击；

5）只浏览安全可靠的网站，不下载来源不明的软件。

麦当劳全球系统中断
影响数千家门店运营

◉ **关键词：**网络安全；系统中断；第三方安全；配置错误

近日，麦当劳全球技术系统突发故障，波及美国、澳大利亚、加拿大、中国、德国、意大利、荷兰、韩国、瑞典等多个国家和地区的门店。为确保顾客体验和服务质量，部分门店不得不采取手工下单或暂时停业措施。

经过数小时的努力，麦当劳恢复系统并发表声明，明确指出此次故障并非网络安全事件，而是第三方供应商在配置更改时出现的错误。尽管声明已作出解释，但公众对于单一故障如何影响全球范围内众多麦当劳餐厅及 POS 系统仍存疑虑。部分网友对此事件发表观点，表达了对故障波及多个国家的不满和惊讶，并对麦当劳的全球技术系统提出质疑。

事后，麦当劳执行副总裁兼全球首席信息官布莱恩·赖斯签署并更新声明，并发送给麦当劳的所有全球员工、特许经营商和 DL 合作伙伴。赖斯代表公司对餐厅团队和顾客造成的任何不便表示歉意。但麦当劳方面并没有确定对大规模系统中断负责的第三方 IT 提供商的名称。

安全小贴士

在企业的运营和发展过程中，无论是利用云服务还是与其他合作伙伴进行合作，都不应过度依赖某一特定系统或第三方供应商。这种过度依赖可能会导致供应链中的某一环节出现问题时，对整个供应链产生重大的负面影响。为了确保企业的稳定运营和持续发展，建议企业采取多元化的策略和措施，降低对单一系统或供应商的依赖程度，从而确保供应链的稳定性和可靠性。

首个公开针对 AI 工作负载的大规模攻击：数千台服务器被黑

◉ **关键词：**网络安全；系统漏洞；生成式 AI；数据泄露

3 月 29 日，OpenAI、优步和亚马逊所使用的 AI 计算框架 Ray 发现了一个已被报告的漏洞，该漏洞遭到持续攻击，导致数千台存储 AI 工作负载和网络凭证的服务器被黑。据了解，这些攻击已经持续了 7 个月。

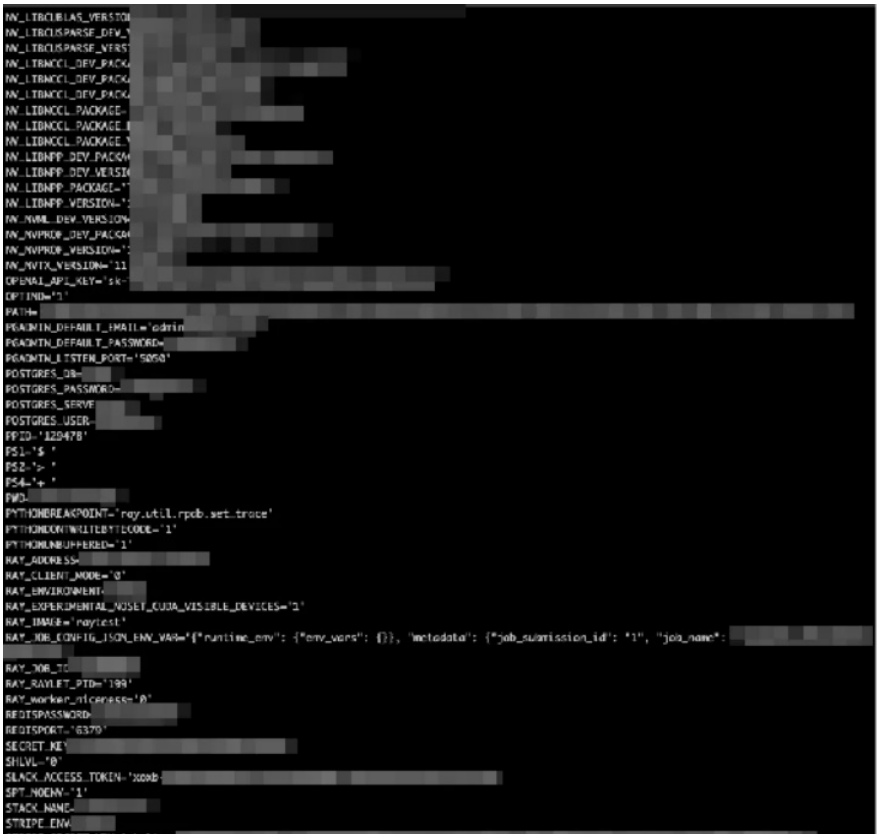
攻击者不仅篡改了 AI 模型，还泄露了访问内部网络和数据库的网络凭证，并获取了 OpenAI、Hugging Face、Stripe 和 Azure 等平台帐号的访问令牌。除了破坏模型和窃取凭证，攻击者还在能够提供大量算力的被侵入基础设施上安装了加密货币挖矿软件，并设置了反向 shell，通过这种基于文本的界面实现对服务器的远程控制。

发现这些攻击的安全公司 Oligo 的研究人员在一篇文章中指出：“一旦攻击者掌控 Ray 生产集群，等于中了大奖。有价值的公司数据加上远程代码执行，攻击者很容易就能获得现金收益，而且可以完全隐匿在暗处，做到神不知鬼不觉（使用静态安全工具不可能检测到这种攻击）。”

被窃取的敏感信息包括 AI 生产工作负载。利用这些信息，攻击者可以在训练阶段控制或篡改模型，从而破坏模型的完整性。易受攻击的集群中，中央仪表板通常暴露在互联网上，这使得任何有意的人都可以查看迄今为止输入的所有命令。利用这些历史数据，入侵者可以快速了解模型的工作方式，并推测可以访问哪些敏感数据。

Oligo 获取的屏幕截图显示，敏感私人数据和集群已经遭到了大规模的黑客攻击。被窃取的资源包括内部数据库以及 OpenAI、Stripe 和 Slack 帐号的加密密码哈希值和访问凭证。

Ray 是一个用于扩展 AI 应用程序的开源框架，允许大量应用程序同时高效地运行。通常，这些应用程序在大规模服务器集群上运行。框架正常运行主要依赖于提供接口显示和控制运行任务和应用程序的中央仪表板。这个仪表板提供了名为“任务 API”（Jobs API）编程接口，允许用户通过简单的 HTTP 请求向集群发送一系列命令，无需身份验证。



（图：OpenAI、Stripe、Slack 的 token 和数据库令牌凭据）

去年，安全公司 Bishop Fox 的研究人员将这种行为标记为高严重性的代码执行漏洞，其跟踪编号为 CVE-2023-48022。然而 Ray 的开发者和维护者 Anyscale 回应称该漏洞不存在。对于被报告的“任务 API”的内部行为，Anyscale 表示并非漏洞，并且不会在短期内得到解决。但 Anyscale 的回应招致了一些批评，批评者指出，由于 Anyscale 声称被报告行为不是漏洞，这导致了很多安全工具未能标记攻击。

来源：安全内参

安全小贴士

随着 AI 大模型的不断开发和运营，各大企业都积极参与这场 AI 变革之中，然而对于用于训练的数据安全性却并不能够得到很好的保障，在此建议企业对训练数据做好分类分级管理，做到脱敏处理，并严格设置员工访问权限，严禁员工上传企业重要数据至任何 AI 工具中。

某房产中介卖了 4 万条业主信息！物业、快递都是“帮凶

◉ **关键词：**数据安全；信息泄露；个人信息保护

近日，某检察院以侵犯公民个人信息罪对廖某提起公诉，并同时提起刑事附带民事公益诉讼。

廖某从事房产中介工作，2023 年 6 月至 7 月间，廖某利用工作便利，获得了大量的顾客个人信息，包括姓名、联系方式、房产地址、车位、房屋状况等。并在未获得当事人授权的情况下，通过微信将上述信息出售给同行，获利人民币 5000 元。

被告人廖某说：“这些信息是公司提供的，号码不全的话需要去小区里面，跟保安、物业，包括一些快递小哥进行购买。”经鉴定，廖某通过微信共发送带有个人信息、电话号码等信息的数据共 39204 条。

近期，法院当庭对本案做出一审宣判，被告人廖某犯侵犯公民个人信息罪，判处有期徒刑十一个月，缓刑二年，并处罚金五千元；禁止其在缓刑考验期内从事房地产经纪活动。

来源：人民网

安全小贴士

《中华人民共和国个人信息保护法》明确规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。本案中不仅是廖某个人进行了违法行为，保安、物业等也同流合污，没有做到对公民个人信息保护的责任和义务。

安全警钟长鸣

网络安全，意识为先
警钟长鸣，常抓不懈

4·15 国家安全教育日

新时代，新考验 国家安全，你我共筑

◉ **关键词：**国家安全；网络安全；数据安全；个人信息保护

2024 年是习近平总书记提出总体国家安全观 10 周年，4 月 15 日也迎来了第 9 个全民国家安全教育日。为深入贯彻落实总体国家安全观，今年的全民国家安全教育日宣传教育活动特别确立了“总体国家安全观·创新引领 10 周年”的主题，进一步推动全社会形成维护国家安全的强大合力，共同构筑起坚不可摧的国家安全屏障。

了解国家安全知识，共筑国家安全长城

“全民国家安全教育日”设立背景

全民国家安全教育日是为了增强全民国家安全意识，维护国家安全而设立的节日。2015 年 7 月 1 日，第十二届全国人民代表大会常务委员会第十五次会议通过《中华人民共和国国家安全法》，其中规定每年 4 月 15 日为全民国家安全教育日。

什么是国家安全?

2015 年 7 月 1 日施行的《中华人民共和国国家安全法》明确指出：国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

国家安全包括哪些领域?

国家安全涉及以下这些重点领域：政治安全、军事安全、国土安全、经济安全、金融安全、文化安全、社会安全、科技安全、网络安全、粮食安全、生态安全、资源安全、

核安全、海外利益安全、太空安全、深海安全、极地安全、生物安全、人工智能安全、数据安全等。

国家安全教育案例

案例一：注意！网上求“薪”，落入陷阱！

小王是军工企业的一名技术人员，由于家庭经济紧张，决定在网络上兼职，便在招聘网站上发布求职信息。为提高简历的“含金量”，小王特意在个人信息中强调了自己在军工企业工作。不久后，某“境外咨询公司”向小王发送邮件，高薪聘其为公司顾问。小王被对方提出的“丰厚报酬”所俘获，逐渐迷失自我，丧失了底线。他抱着“狠捞一票就收手”的心态，向对方出卖我军事秘密，被国家安全机关及时抓获。

案例解析：

不少境外团伙以“兼职”、“招聘”的名义，专门寻找我国高精尖人才，以高额利益引诱其吐露涉密内容，遇到此类信息，需保持警惕，不落入陷阱。

案例二：警惕！加入群聊，聊到“红线”！

小张是航空制造行业的工作人员，因专业领域和兴趣爱好，在多个社交软件中加入了数个“航模同好群”。在群聊中，小张无意中透露了自己从事航空制造的信息。一名网友马上联系小张，频繁互动，对方向小张索要航展大会上新型飞机照片后，进一步索要单位内部照片。事后小张幡然醒悟，向国家安全机关进行举报，但已造成一定程度的失泄密，给单位造成一定的损失，自己也受到党纪政务处分。经查，该网友的真实身份是境外间谍情报机关人员，其加入多个军事、航空领域聊天群，就是伺机通过业内人员非法获取涉密信息。

案例解析：

社区、群聊不要乱加，内部成员鱼龙混杂，难保存在不法分子，引诱你透露个人敏感信息、企业重要信息、国家机密信息，一旦不慎落入陷阱，将给自己、企业和国家带来极大影响。

案例三：谨记！网络识别信息，存在泄密风险！

某办公室干部小赵，为图便利，利用某款图文识别小程序转换一份机密级文件，文件随即被该小程序运营公司工作人员从服务器中获取并公开发布，造成恶劣影响。案件发生后，小赵被给予党内警告、政务警告处分。

案例解析：

通过图文识别的方式处理文件，使图像形式的文件能够转为文字档，在此过程中，被拍摄的文件实际上已经被上传到了应用程序的服务器上，对于涉密文件而言，相当于是将涉密文件上传至了网络，对国家秘密安全造成危害。

来源：国家安全部

准确识别危害国家安全的行为活动 时刻警惕，及时举报

破坏国家安全的行为有哪些？

《中华人民共和国国家安全法》规定：本法所称危害国家安全的行为，是指境外机构、组织、个人实施或者指使、资助他人实施的，或者境内组织、个人与境外机构、组织、个人相勾结实施的下列危害中华人民共和国国家安全的行为：

（一）阴谋颠覆政府，分裂国家，推翻社会主义制度的；

（二）参加间谍组织或者接受间谍组织及其代理人的任务的；

（三）窃取、刺探、收买、非法提供国家秘密的；

（四）策动、勾引、收买国家工作人员叛变的；

（五）进行危害国家安全的其他破坏活动的。

日常生活中应警惕哪些危害国家安全的活动？

（1）一些可疑人员未经批准到内部做调查，进行科技、经济、企业等情况搜集。发现这种情况不能随意提供，并向当地公安机关或国家安全机关报告。

（2）警惕境外电台、电视、网络等传媒的煽动、造谣。

（3）一些境外组织和人员经常出现在我军事、保密单位周边，乘机盗取秘密情报和信息。如遇有可疑人员要立即报告。

（4）一些有境外背景的组织和个人，利用一些群众不满情绪，煽动与政府对抗。遇到这些情况，应立即报告。

维护国家安全的义务有哪些？

《中华人民共和国国家安全法》第七十七条明确规定：

（一）遵守宪法、法律法规关于国家安全的有关规定；

（二）及时报告危害国家安全活动的线索；

（三）如实提供所知悉的涉及危害国家安全活动的证据；

（四）为国家安全工作提供便利条件或者其他协助；

（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；

（六）保守所知悉的国家秘密；

（七）法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

《宪法》规定：

第五十一条 中华人民共和国公民在行使自由和权利的时候，不得损害国家的、社会的、集体的利益和其他公民的合法的自由和权利。

第五十二条 中华人民共和国公民有维护国家统一和全国各民族团结的义务。

第五十三条 中华人民共和国公民必须遵守宪法和法律，保守国家秘密，爱护公共财产，遵守劳动纪律，遵守公共秩序，尊重社会公德。

第五十四条 中华人民共和国公民有维护祖国的安全、荣誉和利益的义务，不得有危害祖国的安全、荣誉和利益的行为。

第五十五条 保卫祖国、抵抗侵略是中华人民共和国每一个公民的神圣职责。

依照法律服兵役和参加民兵组织是中华人民共和国公民的光荣义务。

第五十六条 中华人民共和国公民有依照法律纳税的义务。

发现侵害国家安全行为如何举报？

国家安全机关受理公民和组织举报的电话是 12339，这条热线是由国家安全部设立的，以方便公民和组织向国家安全机关举报间谍行为或线索。

国家安全，重于泰山
坚守爱国之心，共筑安全防线


成都理工大学
CHENGDU UNIVERSITY OF TECHNOLOGY
1956