全球数据安全观察

总第 113 期 2022 年第 41 期

（2022.11.07-2022.11.13）

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、国务院新闻办发布《携手构建网络空间命运共同体》白皮书

11 月 7 日，国务院新闻办公室发布《携手构建网络空间命运共同体》白皮书。

白皮书中明确提出要“提高数据安全保障能力”、“提高数据安全和个人信息保护合作水平”以及“促进数据安全治理和开发利用”。

http://www.cac.gov.cn/2022-11/07/c_1669457523014880.htm

2、工信部发布《关于促进网络安全保险规范健康发展的意见（征求意见稿）》

11 月 7 日，工信部网站发布消息，公开征求对《关于促进网络安全保险规范健康发展的意见(征求意见稿)》的意见。

征求意见稿中提出了建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新、强化网络安全技术赋能保险发展、促进网络安全产业需求释放、培育网络安全保险发展生态等方面的指导意见。

https://wap.miit.gov.cn/gzcy/yjzj/art/2022/art_d7492c4755a74e87a07f626451d0f036.html

3、国家卫健委等三部门印发《“十四五”全民健康信息化规划》

11 月 7 日，国家卫生健康委、国家中医药局、国家疾控局印发了《“十四五”全民健康信息化规划》。

规划中提出要夯实网络与数据安全保障体系，包括全面落实网络安全和数据安全相关法规标准、完善网络安全和数据安全责任体系和管理制度、构建卫生健康行业网络可信体系。同时提出了数据安全能力提升行动，包括提升网络安全和数据安全保护能力、行业实战对抗能力、全行业人员网络安全和个人信息保护的意识和能力。

http://www.nhc.gov.cn/guihuaxxs/s3585u/202211/49eb570ca79a42f688f9efac42e3c0f1.shtml

4、国家标准《信息安全技术 关键信息基础设施安全保护要求》发布

近日，《信息安全技术 关键信息基础设施安全保护要求》国家标准发布，将于 2023 年 5 月 1 日正式实施。这项标准对于关键信息基础设施运营者提升保护能力、构建保障体系具有重要的基础性作用。

标准给出了关键信息基础设施安全的三项保护原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等 6 个方面提出了 111 条安全要求，为运营者开展关

键信息基础设施保护工作需求提供了强有力的标准保障。

http://www.gov.cn/xinwen/2022-11/07/content_5725199.htm

5、国家标准《信息安全技术 网络安全服务能力要求》公开征求意见

11 月 9 日，国家标准《信息安全技术 网络安全服务能力要求》公开征求意见。

征求意见稿中对网络安全服务能力提出了基本条件、组织管理、项目管理、供应链管理、技术能力、服务工具、远程服务、法律保障、数据保护、服务可持续性 10 项通用要求，从监测评估服务、安全运维服务、安全咨询服务、灾难恢复服务 4 种服务类型提出专项要求。

https://www.secrss.com/articles/48807

技术、产品与市场

1、BDS 国家工程研究中心启动 2022 年“数据安全优秀实践案例”的征集

2022 年 11 月 11 日，大数据协同安全技术国家工程研究中心（BDS 国家工程研究中心）向社会各界开展“2022 年数据安全优秀实践案例”征集活动。本次案例征集包括但不限于:

（1）行业数据安全解决方案：在政务、金融、电信、工业、交通、公安、医疗、能源和教育等行业中解决组织数据安全问题的整体或专项解决方案，案例在实践中取得良好效果，在本行业内具备可复制、可推广性。

（2）数据安全技术产品应用案例：涉及数据全生命周期安全保护、数据资产安全管理、数据分类分级、个人信息安全保护、数据安全风险发现和处置、数据安全评估、数据安全态势感知、数据流通共享安全、隐私计算、大数据安全监管、API 安全等方面的创新技术、优秀产品及其应用案例。

http://www.nelab-bdst.org.cn/index.php?g=&m=article&a=index&id=539&cid=68

2、2022 年暗网市场三大趋势

据《网络犯罪》预测，2023 年全球网络犯罪造成的损失将高达 8 万亿美元，网络犯罪市场将成为规模仅次于中国和美国的全球第三大“经济体”，其“GDP”增速更是高达 15%。

暗网市场的繁荣得益于（导致数据泄露的）网络攻击的快速增长。根据网络安全公司 SonicWall 最新公布的数据，2022 年网络攻击全面增长，各种技术和策略不断丰富，从入侵和恶意软件到较新的攻击媒介，如加密劫持和 NFT 犯罪。

以下是 2022 年值得关注的暗网市场三大新趋势:

（1）暗网市场爆发“价格战”：随着暗网上的产品供应在品种和数量方面都在快速增加（伴随一系列大规模数据泄露事件），以及加密货币市场的崩盘，2022 年暗网产品加个普遍下降。

（2）六大热门暗网市场：大量市场被关闭或关门，但同时又不断涌现新的市场取而代，2022 年规模最大的六个暗网市场为 Dark0de: 37%、ToRReZ: 30%、DarkFox: 21%、ASAP: 10%、Cannazon: 2%、G.Dreams: 不到 1%。

（3）240 亿用户账户“上市流通”：根据 DigitalShadows 发布的数据泄露报告“2022 年账户接管调查”，2022 年总计超过 240 亿用户账户凭证在暗网论坛和犯罪市场中流通，这个数字比两年前暴增了 65%。

https://www.secrss.com/articles/48824

3、研究：API 滥用和攻击给零售商带来了新的挑战

API 使应用程序能够共享数据和调用数字服务。Imperva Threat Research 的分析发现，来自 API 的流量占在线零售商网站和应用程序的所有流量的 41.6%。其中，12% 的流量流向端点，例如存储个人数据（例如凭证、身份证号等）的数据库。但更令人担忧的是，3-5% 的 API 流量被定向到未记录的 API 或影子 API，即安全团队不知道存在或不再保护的端点。

暴露或易受攻击的 API 对零售商来说是一个相当大的威胁，因为攻击者可以使用 API 作为窃取客户数据和支付信息的途径。API 滥用通常是通过自动攻击进行的，其中僵尸网络用不需要的流量淹没 API，寻找易受攻击的应用程序和未受保护的数据。

2021 年，API 攻击在 9 月至 10 月期间增加了 35%，在此基础上，11 月又飙升了 22%。这一发现表明，随着 API 和为电子商务服务提供支持的应用程序之间交换更多数据，不良行为者会在假日购物季期间扩大他们的努力。

https://www.helpnetsecurity.com/2022/11/11/retail-cybersecurity-threats/?web_view=true

4、《广东数据要素市场化配置改革白皮书》正式发布

11 月 8 日，广东省政务服务数据管理局召开《广东省数据要素市场化配置改革白皮书》新闻通气会，介绍近两年来广东数据要素市场化配置改革历程和实践探索。会上，广州数据交易所负责人许晶晶介绍，截至目前，**已有超 460 项数据产品、数据服务和数据能力等交易标的申请进场交易，累计会员数达到 190 多家，累计交易金额达到 2.09 亿元**。

《白皮书》从抢抓新机遇、构建市场治理体系、提升治理能力现代化水平、深化数据应用四方面阐述了广东的实践做法。其中，为率先构建数据要素市场治理体系，广东健全数据要素法规制度，相继施行《广东省数字经济促进条例》《广东省公共数据管理办法》等；培育一级数据要素市场，推进数据资源向资产转变；规范二级数据要素市场，促进数据要素高效流通，包括集中优势资源全力推进数据交易所发展，以及在国内首创“数据经纪人”。

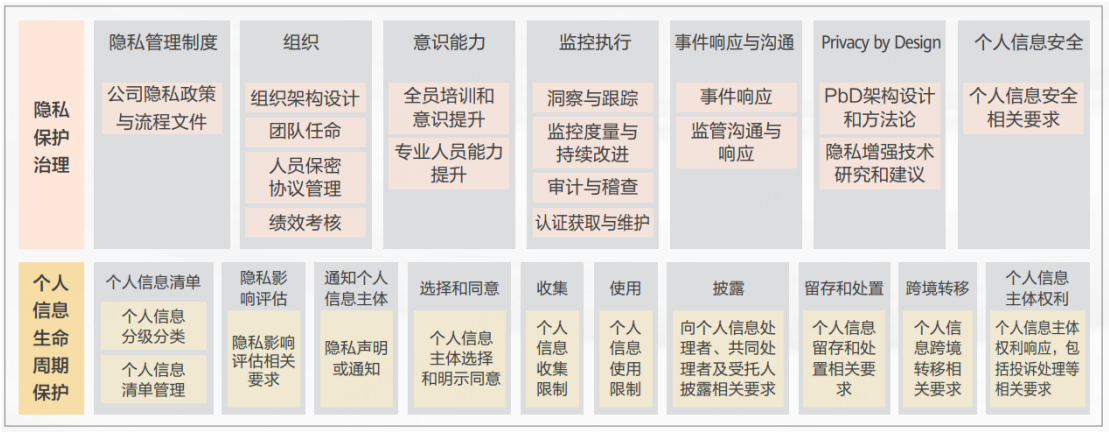
https://mp.weixin.qq.com/s/C7rBT8LaCg7HbGSPLYAsPA

5、华为首次发布《华为隐私保护治理白皮书》

11 月 7 日下午，2022 华为网络安全与隐私保护合规治理论坛在华为全联接大会(HUAWEI CONNECT)期间举办，并首次发布《华为隐私保护治理白皮书》，与业界分享华为的

隐私保护治理方法和实践经验。

华为的隐私保护治理方法即隐私合规 17/27 框架，该框架是在全球具有代表性的法律、法规与标准要求的基础上抽象出来的一套隐私合规治理方法，包含 17 个工作域、27 个工作项。华为在落地 17/27 框架的过程中，自建了自动化的 IT 工具，引入 AI 相关技术，完善对个人信息全生命周期的管理，并自动化地形成合规记录。华为的 IT 落地工具自设计之初，就按照支持全球各地的个人信息保护进行设计，支持按照国家和地区来定制数据清单模板，设置不同的流程角色、满足不同的业务场景，以支撑全球复杂的个人信息保护业务需要。



https://www.huawei.com/cn/news/2022/11/huawei-privacy-protection-whitepaper

业界观点

1、黄澄清：构建世界数据跨境流动的政策体系

11 月 10 日，在 2022 年世界互联网大会乌镇峰会数据治理论坛上，中国网络空间安全协会副理事长黄澄清结合主题“构建世界数据跨境流动的政策体系”进行发言。他谈到:

为数字经济高质量发展提供有力支撑,可以从以下方面入手:

一是要坚守法律底线，依法依规促进数据的有序流动。要处理好数据的开发利用，与个人隐私保护及数据安全的平衡关系。

二是加大政策宣传力度。大数据时代数据跨境涉及到政府、平台企业、社会网民等各个方面，行业社会组织应当引导企业专业人士，及广大网民积极参与有关政策法规制定，实施效果反馈的全过程。

三是推动数据安全技术的创新。数据安全有序流动的基础是技术创新成果的应用，当前要加强联邦发展，多方安全计算等数据安全前沿技术的研发，运用技术手段构建数据跨境流动安全风险的防控体系。

四是深化国际交流合作，形成更多数据安全有序跨境流动的国际共识。

https://www.esensoft.com/industry-news/dx-20016.html

2、张滨：技管结合保障数据跨境流动安全有序

11 月 10 日，2022 年世界互联网大会数据治理论坛在乌镇举行，论坛围绕数据跨境流动等主题进行了圆桌对话。中国移动信安中心总经理张滨结合工作实践，分享了对于数据跨境安全的思考与做法。

张滨介绍，近年来，我国不断完善数据跨境流动相关规范，治理工作呈现出系统化、精细化等特点。与此同时，数据跨境流动仍缺乏统一的国际规则，各国已出台的规定也不尽相同。张滨认为，数据跨境流动涉及的国家、专业机构、社会组织等企业等多类主体应坚持共建共赢，协同合作推进，在数据跨境流动领域形成科学有效的系统性方案。

张滨建议，国家政府画好“设计图”，建立健全法律法规、加强监督管理、完善工作机制，做好顶层设计。研究机构当好“先锋队”，瞄准重点技术项目，率先开展研究创新，积极推动技术突破。行业组织做好“协调人”，推动跨部门协作，健全标准规范，促进沟通交流。企业把好“执行关”，严格落实要求，创新应用场景，做好总结优化。

http://news.yesky.com/hotnews/439/2147428939.shtml

3、刘博：数据跨境流动，安全体系建设至关重要

11 月 10 日上午，2022 世界互联网大会数据治理论坛顺利召开。我国数据跨境规则初步形成，企业应如何着手数据跨境流动的安全体系建设。

安恒信息首席科学家、高级副总裁刘博表示，首先，企业应该对个人信息和重要数据的处理活动开展风险评估和管理工作，系统化开展数据安全体系建设；其次，对于数据出境活动进行日常的监控，从合法必要、范围可控等角度控制数据出境带来的风险；再次，加强境外数据接收方的合规管理；最后，通过开展 DSMM、DSM 等数据安全贯标活动验证数据安全体系的建设成果，证明数据保护的有效性。

http://news.yesky.com/hotnews/361/2147429361.shtml

4、数据安全左移成为数据保护策略演进的核心方向

数字化转型时期，数据的开发利用、数据价值的再创造让数据成为了新时代关注的焦点。数据开发利用的新场景、新兴技术的应用引入了全新的威胁风险，数据安全技术发展正面临着前所未有的挑战。

数据安全保护诉求正在发生变化：从以网络和系统为中心到以数据为中心、从关注网络边界到跟踪数据流转路径、从单品各自为阵到一致性安全原则、从被动响应到持续风险

评估。

基于以上数据安全保护诉求的变化，需要新的防护理念和安全架构，使数据在全生命周期的处理活动中都能保证被安全地存储、使用、共享，既要满足合规要求又要做到风险可控，这需要将数据防护措施从边界延展到数据运营（DataOps）的全流程。数据安全左移是数字时代以数据为中心的安全发展的必然趋势，使安全能力前置，在数据处理的第一现场持续对数据处理和使用的过程进行追踪，横贯数据处理流转的整个环节，发掘数据风险的真正源头。

在数据安全左移之中，存在三个核心能力:

第一是全链路数据识别和追踪，即追踪数据的各种使用维度，包括端点侧、Server 侧、流量侧、API 侧、Docker 侧等，数据安全永远关注数据的使用与流转。

第二是轻量化自适应防护，当无法承受全链路识别追踪所带来的压力时，通过轻量化的方式，可以有效降低各维度的成本，包括最终使用侧的成本与维护侧的成本。通过自适应的方式，根据风险进行量化评估，便能实现对全流程进行监测和分析，以便对症下药。

第三是数据安全风险评估，脱离传统的技术为辅、人力为主的方式，更多地以工具及产品为主导，利用自动化的方式进行风险评估，提高业务落地过程中的可执行性。

https://www.secrss.com/articles/48783

5、如何保护自己的个人信息安全观点

如今，保护你的个人数据不仅仅是明智之举，还是必须之举。随着全世界的联网程度变得越来越高，你的个人信息也变得越来越有价值。无论是利用网站漏洞泄露的信息入侵你的其他帐户，还是控制你的个人电脑以勒索赎金，一旦不义之财到手，不法分子会毫不犹豫地毁掉你的生活。遵循几个基本的安全原则有助于保护你免受互联网上的大多数攻击。更棒的是，这五个简单的安全任务只需要很短的时间就能完成。

（1）使用密码管理器

这种工具可以为你创建随机的强密码，存储信息，并自动填写网站和软件上的登录信息。有些浏览器也开始提供基本的密码管理工具，它们在必要时派得上用场，但总体上还不够好。购买一款合适的密码管理器物有所值，特别是因为许多服务都提供免费套餐。

（2）启用双重身份验证

双重身份验证要求你在能够登录之前通过两种方式确认帐户：使用你知道的东西和你拥有的东西。"你知道的东西"就是你的用户名和密码。"你拥有的东西"则来自你所拥有的

授权工具。

（3）使用安全软件确保安全

即使在 2021 年，你仍应该运行反病毒软件和防火墙。不过好消息是：Windows 10 附带的微软防火墙现在可以出色地完成这项工作，而与该操作系统（包括防病毒软件）捆绑在一起的 Windows Security 工具现在提供了异常好的保护。更棒的是，如果你没有运行第三方替代方案，它们会在 Windows 10 中默认启用。

（4）不要使用 Windows 管理员帐户

以下是最不为人知的安全专业提示之一：不要每天使用 Windows 管理员帐户，而是要使用二级标准帐户。

许多恶意软件企图潜入你的系统。只有管理员帐户才能在 Windows 中安装软件。如果你使用标准帐户，就无法允许流氓程序无意中进入到你的 PC，至少不容易进入。

（5）备份你的数据

最后，备份数据是你的安全工具包中一个被低估的却至关重要的方面。如果病毒设法突破了计算机的防线，拥有全面的备份可以帮助你恢复任何丢失的数据，还有可能帮助你避免支付勒索软件赎金。

http://studyofnet.com/516178785.html

数据安全事件

1、医疗保险巨头 Medibank 拒绝向黑客支付赎金

11 月 8 日报道，The Hacker News 网站披露，澳大利亚最大的医疗保险公司 Medibank 明确表示，不会向对其发动网络攻击并窃取内部数据的犯罪分子支付赎金。

近期，Medibank 遭到了一次严重的网络攻击，从公司内部调查结果来看，约有 970 万名现客户或前客户的姓名、出生日期、地址、电话号码和电子邮件地址，以及 ahm 客户的医疗保险号码、国际客户的护照号码和签证详细信息等个人信息泄露。

泄露的主要人群包括大约 510 万 Medibank 客户、约 280 万 ahm 客户和约 180 万国际客户。

此外，Medibank 进一步表示，除了客户姓名、出生日期等详细个人信息外，此次网络攻击事件也导致约 16 万名 Medibank 客户、约 30 万名 ahm 客户和约 2 万名国际客户的健康索赔数据被盗。这些数据主要包括服务提供商名称、客户接受某些医疗服务的地点，以及与所实施的诊断和程序相关的代码。

https://www.freebuf.com/news/349114.html

2、新的勒索骗局可能会损害网站的声誉，泄露数据

11 月 12 日，据外媒报道，一个针对全球的网站所有者和管理员的活跃勒索骗局，声称攻击了他们的服务器并要求 2,500 美元不泄露数据。

攻击者（自称为蒙特萨诺团队）发送了主题为“您的网站、数据库和电子邮件已被黑客入侵”的电子邮件。这些电子邮件似乎没有针对性，来自所有垂直领域的赎金要求收件人，包括个人博主、政府机构和大公司。

该垃圾邮件消息警告说，如果目标不支付 2,500 美元，黑客将泄露被盗数据，损害他们的声誉，并将网站列入垃圾邮件黑名单。他们正在通过大量电子邮件发送给许多人，只是试图吓唬人们付款。

https://www.bleepingcomputer.com/news/security/new-extortion-scam-threatens-to-damage-sites-reputation-leak-data/

3、Lockbit 团伙泄露了从全球高科技巨头 Thales 窃取的数据

11 月 13 日报道，Lockbit 3.0 勒索软件团伙开始泄露据称从法国国防和科技集团 Thales 窃取的信息。本月初，法国国防和技术组织证实，勒索软件组织 LockBit 3.0 声称窃取了其部分数据。

Thales 于 10 月 31 日被添加到 Lockbit 3.0 组织的受害者名单中，该团伙威胁要在 2022 年 11 月 7 日之前公布被盗数据，如果该公司在截止日期前不支付赎金。

截止日期已到，勒索软件团伙信守诺言并实施了威胁。上周五，该组织开始发布从公司窃取的机密数据。

https://securityaffairs.co/wordpress/138471/data-breach/lockbit-leaked-thales-files.html

4、LockBit 称已窃取咨询公司 Kearney & Company 的数据

据 11 月 6 日报道，勒索团伙 LockBit 声称已窃取咨询和 IT 服务提供商 Kearney & Company 的数据。LockBit 于 11 月 5 日将该公司添加到被攻击名单中，并威胁如果不付赎金，他们将在 2022 年 11 月 26 日之前公布窃取的数据。目前，勒索团伙已经公开了一份被盗数据的样本，其中包括财务文件、合同、审计报告和账单文件等。勒索团伙要求支付 200 万美元以销毁数据，并要求 1 万美元将计时延长 24 小时。

https://securityaffairs.co/wordpress/138136/cyber-crime/lockbit-ransomware-kearney-company.html

5、乌克兰“网军”入侵俄罗斯央行，公布大量敏感数据

11 月 9 日消息，乌克兰黑客分子称已成功入侵俄罗斯中

央银行，并窃取到数千份内部文件。

外媒 The Record 审查了上周四（11 月 3 日）公开发布的部分“被盗”文件，总计 2.6 GB，包含 27000 个文件。从内容上看，这些文件主要涉及银行运营、安全政策以及部分前任/现任员工的个人数据。

黑客分子们在 Telegram 上写道，“如果俄罗斯央行无法保护自己的数据，又怎么保证卢布的稳定？”这起入侵事件出自乌克兰 IT 军成员之手，该组织在俄乌战争爆发后建立，有超 20 万名网络志愿者，各成员协同对俄罗斯网站开展分布式拒绝服务攻击。

中央银行是俄罗斯最重要的金融机构之一，也是该国货币政策制定者和国家货币监管者。据俄罗斯媒体报道，央行方面否认其系统遭黑客入侵，并表示这些所谓外泄文件原本就存放在公开域内。

https://www.secrss.com/articles/48803

6、Aveanna 医疗保健数据泄露可能导致公司损失超过 100 万美元

11 月 7 日，据外媒报道，一家总部位于佐治亚州的家庭医疗保健和临终关怀提供商将向马萨诸塞州支付近 50 万美元，以结束与影响近 17 万名患者的数据泄露有关的州诉

讼。

马萨诸塞州总检察长的一份投诉称，超过 50 名员工遭受到了为期两个月的网络钓鱼攻击。集体诉讼投诉称，网络钓鱼者窃取了患者数据，包括社会安全号码、付款细节、护照和驾驶执照上的识别号码、诊断信息和治疗类型。这一事件影响了 166,077 名个人、患者和员工。

投诉还称，该公司的攻击后审查“承认其当前的网络安全态势缺乏”。除了指出缺乏多因素身份验证外，它还表示该公司的网络缺乏 SIEM 系统。

https://www.bankinfosecurity.com/aveanna-healthcare-data-breach-could-cost-firm-more-than-1m-a-20428?&web_view=true

7、将机密藏在三明治中，美国夫妇因出售核潜艇机密被判入狱

11 月 10 日，据美国司法部网站消息，一夫妇因试图窃取核潜艇设计机密并出售，于 11 月 9 日正式被判刑入狱。

据称，44 岁的被告乔纳森·托贝在任职海军核工程师期间，具备访问海军核推进装置机密信息，包括军事敏感的设计元素、性能特征以及核动力潜艇反应堆其他敏感数据的权限，他协同自己 46 岁的妻子戴安娜·托贝，试图将上述部分

信息出售给外国政府。

https://www.freebuf.com/news/349380.html

8、泰安：手机店主为“拉新”非法售卖公民个人信息

11 月 10 日消息，近日，泰安市公安局高新区分局徂徕派出所抓获 1 名涉嫌侵犯公民个人信息罪的网上在逃人员吴某（女，37 岁）。经查，吴某在自己经营的手机店里，利用售卖手机或是给客户实名办理手机卡之际，在客户不知情的情况下，手机号绑定注册多个 APP 软件，并从中获取佣金。因吴某经营移动通讯店，其经营范围及服务人群为不特定群体，利用提供服务的过程获得公民个人信息并出售、获利，已触犯刑法。

警方提醒，当前，产品推销、房子装修、金融贷款等各种骚扰短信、电话依然屡禁不止，严重侵害公民生活安宁。市场经营者法律意识淡薄，收集公民个人信息后，又转卖给他人用于市场经营活动。市场经营者未经被收集者同意而向他人提供公民个人信息的，有可能构成侵犯公民个人信息罪。因此，市场经营者在收集公民个人信息时要履行适当保管义务，约束自己行为，切莫贪图蝇头小利而触碰法律红线。

https://mp.weixin.qq.com/s/Aa3O3NMK74ihbMRuYf-6IA

9、黑客公布俄天然气公司 260 万用户的数据

据电报频道 Data1eaks 报道，亲乌克兰黑客入侵并在网络上发布了俄罗斯天然气工业股份公司媒体拥有的俄罗斯社交网络 Yappy 的 260 万用户的数据。

在合并的数据库中包含了姓名，姓氏，出生日期，电话号码，所用设备的型号以及附加到 Yappy 帐户的其他平台上的帐户。根据 Data1eaks 的数据，泄露的数据截至 2022 年 7 月 1 日。原子能机构确认该数据库载有真实数据。

https://cn-sec.com/archives/1402578.html

10、安全工具 urlscan.io 会无意中泄露敏感的 URL 和数据

11 月 7 日报道，Positive Security 发现网站扫描和分析引擎 urlscan.io 可泄露敏感的 URL 和数据。Urlscan.io 被描述为 Web 沙箱，通过其 API 集成到多个安全解决方案中。鉴于此 API 的集成类型以及数据库中的数据量，有大量的数据可被匿名用户搜索和检索。2 月份的初步调查发现了属于苹果域名的 url，其中一些还包括共享的 iCloud 文件和日历邀请回复链接。最重要的是，分析还发现配置错误的安全工具会将通过邮件收到的所有链接作为公共扫描提交给 urlscan.io。

https://thehackernews.com/2022/11/experts-find-urlscan-security-scanner.html

《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/