

全球数据安全观察

总第 98 期 2022 年第 26 期

(2022.07.18-2022.07.24)

大数据协同安全技术国家工程研究中心



目录

政策形势	1
1、市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》	1
2、上海发布关于促进“五型经济”发展的若干意见：探索跨境数据流动分类监管模式，打造国际数据港	1
3、贵州省发布加快推进“东数西算”工程建设全国一体化算力网络国家（贵州）枢纽节点的实施意见	2
4、安徽省通管局启动网络和数据安全检查，推进个人信息保护专项治理.....	2
5、工信部“一证通查 2.0”来了！	3
技术、产品与市场	4
1、隐私计算开源创新 数据市场有望提速	4
2、隐私浏览器 Brave 推出隐私保护数据收集系统 STAR	5
3、《数字中国发展报告（2021 年）》正式发布	5
4、广东将建设省级隐私计算和数据资产管理运营平台	7
5、福建大数据交易所揭牌 百亿市场合作清单发布	7
业界观点	9
1、陈凯华、康瑾：加快构建数据要素国家治理体系	9
2、侯玲林：将网络安全工作的“根基”和“底座”功能进一步夯实，为数字经济发展提供坚强防护	10
3、数据安全进入强监管时代，运营商安全能力优势如何发挥？	11
4、人民网评：维护网络安全、保护个人信息，滴滴须牢记！	12
5、数据监管观察：深圳数据领域综合性立法的探索与创新	13

数据安全事件	15
1、国家网信办对滴滴作出网络安全审查相关行政处罚	15
2、由于数据安全问题，荷兰学校的 Chrome 使用受到限制	15
3、因传送居民 IP 地址等数据到美国，欧委会被诉违反 GDPR	16
4、数字安全巨头 Entrust 遭遇勒索攻击.....	17
5、德国建材巨头可耐福遭到 Black Basta 勒索软件团伙的袭击.....	17
6、韩国出租车呼叫系统遭勒索攻击后中断，已支付赎金.	18
7、推特被黑客入侵：540 万账户信息泄露，卖价 3 万美元	18
8、Neopets 数据泄露暴露了 6900 万会员的个人数据.....	19
9、印度航班预订网站 Cleartrip 宣布数据泄露.....	19
10、新的“CloudMensis”Mac 恶意软件使用云存储窃取数据	20
11、Feelyou 心理健康应用程序披露 78,000 封用户电子邮件泄露事件.....	21
12、黑客从美国 300 家餐厅窃取 50,000 张信用卡信息..	22

政策形势

1、市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》

7月21日，市场监管总局公布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》。《实施意见》提出，将确定并适时调整网络安全服务认证目录，组建网络安全服务认证技术委员会，从事网络安全服务认证活动的认证机构应当依法设立，具备从事网络安全服务认证活动的专业能力，并经市场监管总局征求中央网信办、公安部意见后批准取得资质等9项意见。

<https://mp.weixin.qq.com/s/FBMqypMCBRMrorXkR1eVaQ>

2、上海发布关于促进“五型经济”发展的若干意见：探索跨境数据流动分类监管模式，打造国际数据港

7月15日，为做强做优“五型经济”，增创上海经济发展新优势，上海就促进创新型经济、服务型经济、总部型经济、开放型经济、流量型经济发展提出相关意见，其中包括：

（十八）打通人才、资金、数据等要素境内境外流通堵点。推进上海数据交易所建设，开展“正面清单+安全评估”数据跨境试点，在自贸试验区临港新片区探索跨境数据流动分

类监管模式，打造国际数据港。

（十九）促进流量线上线下融合。更好发挥数据流赋能作用，支持国内外流量巨头在沪集聚资金流、货物流、技术流、人才流，在线上线下融合中促进数字产业化和产业数字化。

https://mp.weixin.qq.com/s/bI6J_mUMB_JmVspGHLPWTQ

3、贵州省发布加快推进“东数西算”工程建设全国一体化算力网络国家（贵州）枢纽节点的实施意见

7月22日，贵州省人民政府发布了《加快推进“东数西算”工程建设全国一体化算力网络国家（贵州）枢纽节点的实施意见》，《意见》提出了关于实施算力集群攻坚行动、关于实施算力产业生态培育行动、关于实施算力应用创新行动。

<https://mp.weixin.qq.com/s/VXMH0XgxDXqbCDcutcUWSQ>

4、安徽省通管局启动网络和数据安全检查，推进个人信息保护专项治理

7月18日，安徽省通信管理局发布关于开展2022年电信和互联网行业网络和数据安全检查的通知。检查内容包括通信网络单元定级备案情况、存在的漏洞等风险隐患、数据安全保护情况、个人信息保护工作情况、工业互联网企业网

络安全防护情况。

<https://mp.weixin.qq.com/s/OLY0EpZUsTH56fb-G5a1EQ>

5、工信部“一证通查 2.0”来了！

7月21日，为了防范用户不知情注册互联网账号等带来的涉诈风险，切实为群众排忧解难，工业和信息化部今日正式推出“一证通查 2.0”服务——全国互联网账号“一证通查”，用户凭借手机号码和身份证号码后六位，便可查询本人名下手机号码关联的互联网账号数量。

https://mp.weixin.qq.com/s/hn_nShxDjChaY9D2e2f7Fw

技术、产品与市场

1、隐私计算开源创新 数据市场有望提速

随着数据要素市场培育提速，隐私计算作为数据安全流通的关键技术，如何加快其技术开发以及商业化的速度成为市场关切。市场共识在于，在隐私计算“商业化大网”中，算法迭代、开源生态和场景普及缺一不可。据悉，蚂蚁集团已正式开源其隐私计算框架。

IDC 数据显示，2021 年中国隐私计算市场规模已突破 8.6 亿元，未来有望实现 110% 以上的市场增速。艾瑞咨询预计，到 2025 年，中国隐私计算市场规模将达到 145.1 亿元。中国信通院调研统计显示，55% 的国内隐私计算产品基于或参考了开源项目。中国信通院云大所大数据与区块链部副主任闫树表示，去年以来，隐私计算行业出现几个明显趋势：第一是如何加速性能；第二是如何提升产品稳定性；第三是真正从操作、算法二次开发、方便部署、说明文档等方面降低使用者门槛。整体看，适配不同场景，不同规模的数据，在安全和性能之间再平衡的产品越来越多。

<https://finance.sina.com.cn/tech/internet/2022-07-16/doc-imizmscv1782778.shtml>

2、隐私浏览器 Brave 推出隐私保护数据收集系统 STAR

7月20日消息，隐私浏览器 Brave 宣布推出隐私保护数据收集系统 STAR，该系统使用 k-anonymity 匿名算法，可在用户贡献数据且共享的情况下保护用户隐私。

STAR 可提供与现有系统相似或更高的隐私，使用现有的加密工具而非加密原语因此可更易理解，部署不需特殊硬件因此降低了成本，可提供小用户群的准确结果。

STAR 系统将在洛杉矶举行的 2022 年 ACM 计算机和通信安全会议上推出，并正在讨论 IETF（国际互联网工程任务组）可能的标准化。

<https://www.qianba.com/newsflash/p-434566.html>

3、《数字中国发展报告（2021 年）》正式发布

7月23日，第五届数字中国建设峰会在福州开幕。开幕式上发布了《数字中国发展报告（2021 年）》，介绍数字中国建设取得的显著成就，作出 2022 年数字中国建设展望。

一是建成全球规模最大、技术领先的网络基础设施。截至 2021 年底，我国已建成 142.5 万个 5G 基站，总量占全球 60% 以上。算力规模全球排名第二，近 5 年算力年均增速超过 30%。

二是数据资源价值加快释放。2017 年到 2021 年，我国

数据产量从 2.3ZB 增长至 6.6ZB，全球占比 9.9%，位居世界第二。大数据产业规模快速增长，从 2017 年的 4700 亿元增长至 2021 年的 1.3 万亿元。公共数据开放取得积极进展，2017 年到 2021 年，全国省级公共数据开放平台由 5 个增至 24 个，开放的有效数据集由 8398 个增至近 25 万个。各地积极探索数据治理规则，培育数据要素市场，促进数据流通交易和开发利用。

三是数字技术创新能力快速提升。人工智能、云计算、大数据、区块链、量子信息等新兴技术跻身全球第一梯队。

四是数字经济发展规模全球领先。2017 年到 2021 年，我国数字经济规模从 27.2 万亿增至 45.5 万亿元，总量稳居世界第二，年均复合增长率达 13.6%，占国内生产总值比重从 32.9% 提升至 39.8%，成为推动经济增长的主要引擎之一。

五是数字政府治理服务效能显著增强。疫情加速了数字化进程，数字化有力支撑了疫情下经济社会发展和政府公共服务。

六是数字社会服务更加普惠便捷。2017 年到 2021 年，我国网民规模从 7.72 亿增长至 10.32 亿，互联网普及率提升至 73%。

七是数字化发展治理取得明显成效。法律法规体系加快健全完善，推动平台经济规范健康发展，有效维护市场主体

和人民群众合法权益。

八是数字领域国际合作稳步拓展。我国积极参与多边多方数字经济治理机制活动，为网络空间国际规则和技术标准制定贡献中国智慧和方案。

<https://mp.weixin.qq.com/s/bWj6P5DOS1KXjDjGfnz24A>

4、广东将建设省级隐私计算和数据资产管理运营平台

2022年7月24日，在第五届数字中国峰会的数字福建分论坛上，广东省政务服务数据管理局局长杨鹏飞表示，广东积极推进数据要素市场化配置改革，将强化数据要素流动的平台支撑。完善数据资源“一网共享”平台和公共数据开放超市，让各地各部门用数更加便捷。同时，建设省级隐私计算和数据资产管理运营平台，实现“数据不出域、可用不可见”，搭建数据资产凭证闭环体系。

<https://mp.weixin.qq.com/s/1P8mK7mj5uOXmp-63Gu7Tg>

5、福建大数据交易所揭牌 百亿市场合作清单发布

7月21日，以“放飞数字梦想”为主题的福建省数据要素与数字生态大会在福州数字中国会展中心举行，大会聚焦数据要素与数字生态培育，围绕促进大数据产业发展，推进数据资源化、价值化打造的一批合作平台在会上正式亮相，

并促成了一批大数据产业优质项目落地。

会上，福建大数据交易所正式揭牌，这是福建省推进数据要素市场化流通的一个新的里程碑。福建大数据交易所揭牌当日，完成挂牌的数据产品近 100 个，涉及能源类、金融类、通信类、征信类等类别，并完成了首批交易。

当天，福建省大数据集团发布“百亿市场合作清单”，聚焦上百项数字福建建设领域重大发展项目，与数字经济全链条生态企业共同分享数字建设新机遇，创造市场机会供给途径，激发全行业赋能数字经济高质量发展的积极性、主动性、创造性，充分释放数字化发展的放大、叠加、倍增效应。

<https://mp.weixin.qq.com/s/xQgPJB2cwxIN5nY4gsk7XQ>

业界观点

1、陈凯华、康瑾：加快构建数据要素国家治理体系

习近平总书记在主持召开中央全面深化改革委员会第二十六次会议时强调，数据基础制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

中国科学院科技战略咨询研究院研究员陈凯华、中国工业互联网研究院工程师康瑾认为构建数据要素国家治理体系是数字化高质量发展的迫切需要：**国家数据要素高效治理迫切需要构建数据要素国家治理体系，释放数据要素价值迫切需要构建数据要素国家治理体系，占据数字竞争制高点迫切需要构建数据要素国家治理体系。**

对此，两位专家提出了打造协同高效的数据要素国家治理体系的方向与思路：**构建兼顾效率、公平与安全的数据要素国家治理体系，打造面向数据应用全链条的数据要素国家治理体系，打造面向数据管理全链条的数据要素国家治理体系，坚持技术创新与制度创新双轮驱动，推动数据要素治理手段与机制变革，发挥政府与市场作用，打造多元主体协同**

共治的数据要素治理模式。

<https://mp.weixin.qq.com/s/uFKwasbi-9tLPzxKrSxm9w>

2、侯玲林：将网络安全工作的“根基”和“底座”功能进一步夯实，为数字经济发展提供坚强防护

7月13日，“2022（第七届）中国网络信息安全峰会”在京隆重召开。中国信息协会副会长侯玲林为峰会致辞。

侯玲林副会长讲到，我国网络市场正呈现出多元化发展势头，未来我国网络安全产品将更具创新性并且更加多元化，网络安全市场竞争也将更加激烈。此外，涉及网络安全问题的范围也正从传统领域向政治、经济、文化、社会、国防等诸多领域不断拓展，也使得网络安全发展边界不断延展，风险点位不断增多。

面临新的风险和挑战，侯玲林副会长提出五点看法：

第一，充实网络安全的发展内涵。数字经济时代，“网络安全”正逐渐向“数字安全”升级，随着技术发展亟需不断拓展“网络安全”的内涵和外延，构建新的数字安全体系刻不容缓。

第二，关键信息基础设施防护是网络安全的重中之重。关键信息基础设施防护应覆盖数据全生命周期各个环节，涵盖保密性、完整性、可用性、可靠性、弹性和隐私等多个维度，确保关键信息基础设施安全稳定运行。

第三，平衡兼顾“数据共享”与“数据安全”。数据已成为经济发展重要资源之一，“数据安全”正成为网络安全的中中之重。

第四，强化跨地区、跨行业、跨领域的协作联动，全力巩固网络安全。建立网络安全协同联动机制，第一时间解决安全数据输出和威胁情报的查询共享问题，实现协同联动、联防联控。

第五，加强网络安全人才队伍建设。要高度重视网络安全行业人才供需失衡问题。

<http://www.ciia.org.cn/news/18655.cshtml>

3、数据安全进入强监管时代，运营商安全能力优势如何发挥？

当前随着“新基建”的不断加码，信息安全产业迎来全新的发展浪潮，同时亦给运营商网络安全建设带来多重挑战。一是“新基建”融合架构加大了存储、计算、网络虚拟化等数据安全边界泛化的程度与风险。二是“新基建”场景下人工智能、大数据、区块链等新技术对安全防御智能化程度提出更高要求。三是多元化应用场景带来从“通用安全”向“按需安全”的挑战。四是新业务模式加快重塑网络安全生态的需求。

在此背景下，电信运营商作为建设数字中国、维护国家网信安全的主力军，应充分发挥运营商数据资源、网络技术

等方面优势与作用，推动自身安全能力对外输出，为各垂直行业提供安全保障，打造运营商自身新的价值增长点。

首先，运营商应**创新安全思路，从被动跟随到主动求变**。以往网络安全螺旋跟随式发展，转变为以新安全思路和技术应对新生技术和业务威胁。运营商需寻求网络安全内源式创新模式，由“跟随式”转为“引领式”发展，形成主动优势。其次，运营商应**寻求安全合力，从“松耦合”到“紧耦合”、从“后置松耦合”到“前置紧耦合”**推动云边协同，构筑从核心到边缘的安全防线。再者，**打造网络安全能力验证、评价、示范、认证平台全新的网络架构和应用场景**，呼唤整体化的解决场景融合，从孤立外挂到一体化共生，实现安全策略与场景深度交互。

<https://mp.weixin.qq.com/s/Xf5zp0XpseghJOGy9h912g>

4、人民网评：维护网络安全、保护个人信息，滴滴须牢记！

7月21日，国家网信办依据相关法律法规，对滴滴全球股份有限公司处人民币80.26亿元罚款，对滴滴全球股份有限公司董事长兼CEO程维、总裁柳青各处人民币100万元罚款。

维护网络安全、保护个人信息，兹事体大，不能儿戏，更不能反其道而行之。法律明确规定，任何组织、个人不得

非法收集、使用、加工、传输他人个人信息。作为一家体量较大、掌握较多用户信息的企业，滴滴更有责任履行网络安全、数据安全、个人信息保护义务。这是底线问题，滴滴应牢记心间。

“查处一案、警示一片”，依法依规处理滴滴，给滴滴敲响了警钟，也给相关企业发出了警示：所有的互联网企业都要依法合规运营，都要守住底线、健康有序发展。如果价值观跑偏了，发展方向走歪了，把法律法规碾在脚下，不仅法律不答应，人民群众也不会答应。

https://www.ts.cn/xwzx/gnxw/202207/t20220721_8074545.shtml

5、数据监管观察：深圳数据领域综合性立法的探索与创新

2021年6月29日，深圳市人大常委会出台《深圳经济特区数据条例》（以下简称《条例》）。《条例》是国内数据领域首部综合性立法，内容涵盖个人数据、公共数据、数据要素市场、数据安全等方面，为强化个人数据保护、加强公共数据管理、培育数据要素市场提供了法治保障和制度环境，为我国《个人信息保护法》的出台作出有益探索，对促进数据治理体系和治理能力现代化具有先行示范意义。

深圳市人民代表大会常务委员会法制工作委员会办公

室雷伟珍撰写了文章《深圳数据领域综合性立法的探索与创新》，供关注数据监管的读者参考。文章主要要点如下：

（1）深圳有必要在数据治理法律制度构建方面先行先试，通过经济特区立法，着力平衡发展数字经济与保护个人数据、数据开发利用与数据安全之间的关系，力图在确保数据安全、保护个人数据的基础上，最大程度地激发、释放数据作为生产要素的经济价值，为深圳市数字产业、数字经济的发展提供良好的法治环境。

（2）为促进实现数据要素价值，《深圳经济特区数据条例》填补目前数据交易、公平竞争相关法律规范的空白，探索培育数据要素市场。

（3）深圳市人大常委会充分发挥经济特区立法的变通和创新优势，对个人数据保护、公共数据治理、数据要素市场培育作出一系列创设性规定，为国家相关立法作出积极探索，为数据立法做好先行示范。

<https://www.secrss.com/articles/45001>

数据安全事件

1、国家网信办对滴滴作出网络安全审查相关行政处罚

根据网络安全审查结论及发现的问题和线索，国家互联网信息办公室依法对滴滴全球股份有限公司涉嫌违法行为进行立案调查。经查实，滴滴全球股份有限公司违反《网络安全法》《数据安全法》《个人信息保护法》的违法违规事实清楚、证据确凿、情节严重、性质恶劣。

7月21日，国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对滴滴全球股份有限公司处人民币80.26亿元罚款，对滴滴全球股份有限公司董事长兼CEO程维、总裁柳青各处人民币100万元罚款。

<https://mp.weixin.qq.com/s/JvME41TaNixTLQXC2mYMqg>

2、由于数据安全问题，荷兰学校的 Chrome 使用受到限制

2022年7月23日，据报道，出于对数据隐私的担忧，荷兰教育部决定在2023年8月之前对Chrome操作系统和Chrome网络浏览器的使用实施一些限制。官员们担心谷歌服务会收集学生数据并将其提供给大型广告网络，这些网络将其用于帮助教育以外的目的。由于国家监管机构不知道学生个人数据的存储和处理位置或方式，因此存在违反欧盟

GDPR（通用数据保护条例）的担忧。

<https://www.bleepingcomputer.com/news/security/chrome-use-subject-to-restrictions-in-dutch-schools-over-data-security-concerns/>

3、因传送居民 IP 地址等数据到美国，欧委会被诉违反 GDPR

2022 年 7 月 19 日，据欧洲媒体 EURACTIV 报道，因 IP 地址等个人信息被转移到美国，一位德国公民起诉欧盟委员会违反《通用数据保护条例》（GDPR）。

支持原告方的欧洲数据协会（EuGD）指出，该诉讼涉及欧洲未来会议(Conference of The Future of Europe)网站。该网站为欧盟委员会牵头成立，旨在让欧盟公民参与决定欧盟及其成员国的未来。亚马逊网络服务(Amazon Web Services)托管此网站，这也意味着，用户在此网站进行注册时，IP 地址等个人数据都将被转移到位于美国的亚马逊服务器。

根据 GDPR 规定，在欧盟委员会未作出充分性认定的情况下，控制者或处理者只有在提供了适当的保障措施，并为数据主体提供了可执行的权利和有效的法律救济措施的前提下，才可将个人数据转移到第三国。

<https://www.secrss.com/articles/44917>

4、数字安全巨头 **Entrust** 遭遇勒索攻击

2022 年 7 月 25 日，据 Bleeping Computer 消息，数字安全巨头 **Entrust** 已经承认，自己遭受了网络攻击，攻击者破坏了其内部网络，并窃取了一定规模的数据。**Entrust** 是一家专注于在线信任和身份管理的安全公司，为政企用户提供广泛的服务，包括加密通信、安全数字支付和身份证明等解决方案。此次攻击造成内部数据泄露，很有可能会影响到大量使用 **Entrust** 进行身份管理和身份验证的关键和敏感组织。

<https://hackernews.cc/archives/40277>

5、德国建材巨头可耐福遭到 **Black Basta** 勒索软件团伙的袭击

2022 年 7 月 19 日，可耐福集团 (**Knauf**) 宣布，它已成为网络攻击的目标，该攻击扰乱了其业务运营，迫使其全球 IT 团队关闭所有 IT 系统以隔离事件。可耐福 (**Knauf**) 是一家总部位于德国的跨国建筑和建筑材料生产商，拥有全球约 81% 的墙板市场。实际的网络攻击发生在 2022 年 6 月 29 日晚。名为 **Black Basta** 的勒索软件团伙已通过在其勒索网站上发布公告，于 2022 年 7 月 16 日将可耐福列为受害者，从而对此次攻击负责。**Black Basta** 勒索软件团伙公布了在可耐福攻击期间泄露的 20% 的文件，超过 350 名访问

者访问了这些文件。这些文件包括电子邮件通信、用户凭据、员工联系信息、生产文档和 ID 扫描的样本。

<https://www.bleepingcomputer.com/news/security/building-materials-giant-knauf-hit-by-black-basta-ransomware-gang/>

6、韩国出租车呼叫系统遭勒索攻击后中断，已支付赎金

据媒体 7 月 18 日透露，韩国一家运营出租车呼叫系统的公司遭到勒索攻击。据韩联社报道，截至 18 日下午 5 点，江原道春川、东海、阳区、旌善、仁济、高城、襄阳等地的出租车呼叫系统仍无法正常运行。系统开发商表示，其在 17 日凌晨 2 点左右遭到海外黑客的勒索攻击，所有服务中心和备份服务器都已被感染。目前，该公司已支付赎金并获得解密密钥，正在对系统进行紧急恢复，预计恢复时间为两到三天。

<https://www.databreaches.net/south-korean-call-taxi-system-paralyzed-by-ransomware-attack-company-pays-ransom-to-get-decryptor/>

7、推特被黑客入侵：540 万账户信息泄露，卖价 3 万美元

2022 年 7 月 24 日，据报道，推特因安全漏洞被黑客入侵，共计 540 万个账户的联系方式泄露，推特官方已确认存在该安全漏洞。泄露的 540 万个账户包括推特 ID 与其关联

的电话号码和电子邮件信息，已在一个黑客论坛上出售，价格为 3 万美元(约 20.28 万元人民币)。

<https://securityaffairs.co/wordpress/133593/data-breach/twitter-leaked-data.html>

8、Neopets 数据泄露暴露了 6900 万会员的个人数据

2022 年 7 月 20 日，虚拟宠物网站 Neopets 遭受了数据泄露，导致源代码和包含超过 6900 万会员个人信息的数据库被盗。7 月 19 日，一个名为“TarTarX”的黑客开始以四个比特币的价格出售 Neopets.com 网站的源代码和数据库，按今天的价格计算价值约 94000 美元。TarTarX 表示他们窃取了数据库和 neopets.com 网站的大约 460MB(压缩)源代码。卖家声称，该数据库包含超过 6900 万会员的帐户信息，包括会员的用户名，姓名，电子邮件地址，邮政编码，出生日期，性别，国家/地区，初始注册电子邮件以及其他与网站/游戏相关的信息。

<https://hackernews.cc/archives/39883>

9、印度航班预订网站 Cleartrip 宣布数据泄露

2022 年 7 月 18 日，印度航班预订网站 Cleartrip 宣布了涉及未知数量受害者信息的数据泄露事件。“到目前为止的

调查表明，用户的姓名、电子邮件 ID 和电话号码等信息可能受到了影响，”公司发言人说。安全研究员 Sunny Nehra 在 Twitter 上分享了黑客在私人论坛上发布的被盗文件的截图，泄漏的文件包括客户和供应商的大量数据。

<https://therecord.media/indian-flight-booking-site-cleartrip-announces-data-breach/>

10、新的“CloudMensis”Mac 恶意软件使用云存储窃取数据

ESET 安全公司的研究人员发现了一种名为 CloudMensis 的新型恶意软件。它会利用 DropBox、pCloud 和 Yandex Disk 等公开可用的云存储提供商，来渗透 macOS 系统并窃取用户数据，包括文档、电子邮件附件等。该恶意软件还可用于捕获受害者设备上的屏幕截图。

由于 CloudMensis 可以绕过苹果的 macOS 隐私服务设置 (TCC)，因此它能够实时查看用户在其 macOS 设备上的活动并从云存储程序中提取数据。CloudMensis 的一长串监视命令还允许它在未经授权或不知情的情况下在给定受害者的设备上执行一系列操作。

这种绕过苹果的 macOS TCC 的能力表明 CloudMensis 绝不是一种基本类型的恶意软件。相反，它的复杂程度令人担忧。

<https://www.makeuseof.com/cloudmensis-mac-malware-steals-data/>

11、Feelyou 心理健康应用程序披露 78,000 封用户电子邮件泄露事件

2022 年 7 月 19 日，据外媒报道，流行的心理健康应用 Feelyou 宣布了一个平台漏洞，该漏洞暴露了近 78,000 名用户的电子邮件地址。

安全研究员在对其他几个心理健康追踪器和类似应用程序进行逆向工程时发现了这个问题。该漏洞导致任何人都可以看到 Feelyou 应用上 177 个国家/地区的 77,967 名用户的电子邮件地址，并将其与平台上发布的帖子联系起来。Feelyou 允许用户每天跟踪他们的情绪并分享他们的感受。

“我们通过调查确认，除了电子邮件地址之外没有其他影响。Feelyou 不会在应用程序中存储以下信息：姓名、地址、电话号码、密码、信用卡信息和识别个人的信息，”该公司补充道。

https://therecord.media/feelyou-mental-health-app-says-emails-of-78000-users-exposed-in-breach/?web_view=true

12、黑客从美国 300 家餐厅窃取 50,000 张信用卡信息

2022 年 7 月 19 日，据外媒报道，在针对三个在线订购平台的两次网络浏览活动中，超过 300 家餐厅客户的支付卡详细信息被盗。

Web-skimmers 或 Magecart 恶意软件通常是 JavaScript 代码，当在线购物者在结帐页面上键入信用卡数据时，它会收集信用卡数据。最近，安全研究人员发现已有两个 Magecart 活动将恶意代码注入 MenuDrive、Harbortouch 和 InTouchPOS 的在线订购门户。结果导致 50,000 张支付卡被盗，并已在暗网上的各个市场上出售。

Magecart 是网络犯罪分子的总称，他们使用刷卡技术从销售点(POS)或电子商务系统使用的支付卡中窃取凭证。他们通常最终在暗网上的黑客论坛上出售这些被盗的凭据。

https://www.bleepingcomputer.com/news/security/hackers-steal-50-000-credit-cards-from-300-us-restaurants/?&web_view=true