

全球数据安全观察

总第 26 期 2021 年第 2 期

(2020.01.04-2021.01.10)

摘要

本期全球数据安全观察搜集到的重要事件的主要类型为[数据泄露](#)和[数据合规问题](#)。

1. [支付处理公司 Juspay 发生 1 亿用户数据被泄露](#)
2. [超 2 亿国内用户信息在暗网销售](#)
3. [意大利的 Ho-Mobile 数据库中 250 万账户被盗](#)
4. [TOP25 游戏公司将近 100 万个账号被窃取](#)
5. [日产公司源代码泄露，由于 Git 服务器配置错误](#)
6. [万余运通客户信息被泄露并免费发布到黑客论坛](#)
7. [新西兰储备银行因合作伙伴被黑遭受数据泄露](#)
8. [2020 年企业违反 GDPR 被罚款超 1.7 亿欧元](#)

此外，在数据安全技术与观点方面主要讨论了：

1. [机密计算（TEE）](#)
2. [2020 年全球国防网络空间战略情况总数](#)
3. [大数据技术在公共信息安全领域的应用与发展趋势](#)
4. [区块链技术在政务数据资源共享场景的应用](#)
5. [民法典如何保护你的数据、网络虚拟财产](#)
6. [2021 年数据安全的三大趋势](#)

全球动态

1. 支付处理公司 Juspay 发生数据泄漏: 1 亿用户信息在暗网出售

2021 年 1 月 6 日, 援引外媒 ZDNet 报道, 印度支付处理公司 Juspay 超过 1 亿用户的借记卡、信用卡信息在暗网上销售。Juspay 主要为亚马逊、Swiggy、MakeMyTrip 等公司处理支付业务。

<http://hackernews.cc/archives/34570>

2. 疑似超 2 亿国内已泄漏用户信息在国外暗网论坛兜售

2021 年 1 月 4 日报道, 国外安全研究团队 Cyble 在一次日常安全监控中发现了多个帖子正在出售与中国公民有关的个人数据。经分析, 这些数据很可能来自微博、QQ 等多个社交媒体, 其中还发现了大量湖北省“公安县”公民的户口登记样本数据。威胁者还表示, 共有 730 万中国公民的数据可供出售, 包括身份证, 性别, 姓名, 出生日期, 手机号, 地址和邮编等记录。

<https://www.secrss.com/articles/28465>

3. 意大利的 Ho-Mobile 数据库中有 250 万个帐户被盗

2021 年 1 月 5 日，超过 250 万名 Ho-Mobile 客户的个人数据正在一个黑暗的网络黑客论坛上出售。数据包括个人身份信息，例如出生日期、电话号码、财务代码的物理地址和电子邮件地址。

<https://www.bleepingcomputer.com/news/security/vodafones-ho-mobile-admits-data-breach-25m-users-impacted/>

4. TOP25 游戏公司将近 100 万个与邮箱相关的账号被窃取销售

2021 年 1 月 5 日，威胁情报公司 KELA 的一份报告显示，已经发现有超过 500,000 个与 25 个领先游戏发行商的员工相关联的登录凭证在暗网集市上出售。该公司发现了将近 100 万个属于游戏客户和主要游戏公司员工的被盗帐户，其中一半在过去一年中最终在黑网上出售。

<https://www.welivesecurity.com/2021/01/05/breached-employee-credentials-gaming-companies/>

5. 日产公司因 Git 服务器配置错误，源代码泄露

2021 年 1 月 8 日，日产北美公司开发和使用的移动应用和内部工具的源代码在网上泄露，原因是该公司错误配置了

其中一台 Git 服务器。整个源代码集合大约有 20 GB，其中包含移动应用程序的源代码以及 Nissan 内部用于诊断，客户获取，市场研究或 NissanConnect 服务的各种工具。

<https://www.bleepingcomputer.com/news/security/nissan-na-source-code-leaked-due-to-default-admin-admin-credentials/>

6. 万余运通客户信息被免费发布到黑客论坛

2021 年 1 月 5 日，黑客已在黑客论坛上免费发布了 10000 个美国运通信用卡持有人的数据。泄漏的样本数据集会暴露完整的美国运通帐户（信用卡）号和客户的个人信息（PII），包括姓名，完整地址，电话号码，出生日期，性别等。

<https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/>

7. 新西兰储备银行因合作伙伴被黑遭受数据泄露

2021 年 1 月 10 日，据外媒报道，新西兰储备银行在攻击者非法访问第三方托管服务提供商存储的数据之后，遭受了数据泄露。储备银行是新西兰的中央银行，负责制定货币政策以稳定新西兰的价格，该行行长指出，违规行为已得到遏制，但可能已经暴露了商业和个人敏感信息。

<https://www.bleepingcomputer.com/news/security/new-zealand-reserve-bank-suffers-data-breach-via-hacked-storage-partner/>

8. 2020 年企业违反 GDPR 被罚款超 1.7 亿欧元

财务分析网站 Finbold 使用 enforcementtracker.com 的数据计算得出，2020 年的罚款总额为 1.713 亿欧元。根据这些数据，意大利缴纳的罚款额最高，达 5800 万欧元，其次是英国，分别为 4400 万欧元和德国 3700 万。就 2020 年的罚单数量而言，西班牙以 128 次位居首位，其次是意大利（34），罗马尼亚（26），瑞典（15），比利时（13）和挪威（11）。服装零售商 H&M 去年的罚款最高（3500 万欧元），其次是意大利电信（2800 万欧元），英国航空公司（2200 万欧元），万豪酒店（2000 万欧元）和意大利电信运营商 Wind Tre（1700 万欧元）和沃达丰意大利（1200 万欧元）。

<https://www.secrss.com/articles/28501>

业界观点

1. 机密计算（TEE）简介

机密计算通过基于硬件的可信执行环境（TEE）保护使用中的数据，是近几个月来俘获大量关注的数据安全子领域，发展势头极为迅猛。

随着传输中数据和静态数据防护措施的发展，针对网络和存储设备的网络威胁越来越不容易得手，攻击者将目光转向了使用中数据。常见攻击方法包括内存刮取、CPU 边信道攻击和恶意软件注入。机密计算通过基于硬件的可信执行环境（TEE）保护使用中的数据，TEE 可提供一定水平的数据完整性、数据机密性和代码完整性保障。

https://mp.weixin.qq.com/s?__biz=MzkxNzA3MTgyNg==&mid=2247487496&idx=1&sn=5cf94f8ddb285ac4fef4cbf1d532de3

2. 2020 年全球国防网络空间情况综述

2020 年以来，世界各国持续发布网络空间军事战略、政策、法案和条令，着力加强网络军事能力建设顶层规划，完善网络空间作战机制，明确网络国防建设目标，加大网络能力投资力度，着力提升网络空间攻防能力，谋求在激烈的全

球网络空间竞争格局中占据主动权。

聚焦联合全域作战，以网络为核心融合全域作战能力。

聚焦国防网络发展，为发展下一代军事能力奠定基础。

聚焦作战能力提升，促进更具杀伤力军队现代化建设。

聚焦网络行为塑造，基于整体威慑提升国家网络安全。

聚焦网络安全防御，推动国家网络威胁防御体系构建。

<http://www.hackdig.com/01/hack-250302.htm>

3. 浅析大数据技术在公共信息安全领域的应用与发展趋势

随着社会信息的快速发展，公共信息安全问题备受社会公众关注，利用大数据技术提升公共信息安全防护水平、助力企业增值增效成为必然趋势。因此，以公共信息安全的全生命周期管理为视角，构建适应于公共信息安全防护的“四级”信息安全监测管理体系，围绕大数据在信息安全风险精确感知、风险主动防御、态势智能监测和风险信息回溯升级四个方面的应用技术，力求将大数据在信息安全领域的应用演化为 IT 商业智能发展趋势中的重要组成部分。

<https://mp.weixin.qq.com/s/Vr-fHcflAiRajAlWPuXVyA>

4. 政务数据资源共享是区块链技术自主创新的主战场

数字政府建设的重点和难点在于推进跨层级、跨地域、

跨系统、跨部门、跨业务的政务数据有序共享和协同服务。以数字政府建设为契机，推动政务服务领域区块链应用，有效解决数据有序共享、安全交互、可信协同、依法监管等问题；同时，政务服务领域可为区块链技术自主创新提供初始市场和先验机会。政务服务领域不能一个应用建一条链，防止形成新的“区块链信息孤岛”。

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

5. 专家解读：看民法典如何保护你的数据、网络虚拟财产

民法典明确，法律对数据、网络虚拟财产的保护有规定的，依照其规定。针对条文不够细的问题，专家表示，立法的时候进行了讨论，结果大家很难达成一致的意见，所以就把手里的问题留到将来的法律规定。而虚拟财产的情况更复杂，中间有一部分可能是财产，但是有一部分可能不是财产，因此期待着未来立法对这些问题做进一步的发展。民法典只是解决个人信息被侵害以后在法律上救济的问题，针对更多个人信息的保护，还是要等待个人信息保护法的出台。

https://mp.weixin.qq.com/s/ajl0m_ryJAmjEO65mG4aug

6. 2021 年数据安全三大趋势

首先，数字化转型仍是企业生存发展的必然选择，而数

据安全则是支撑数字化转型大厦的基石保障，合规需求和内生需求双重驱动，将会激发数据安全市场的活力。其次，网络边界不断消失，数据流动属性释放，使数据面临安全威胁呈现动态变化的特征，这将持续推动以零信任架构为代表的新理念、新技术的发展与落地。最后，数据安全保护的是高价值对象，关系着企业数字化转型成败，企业需要采用体系化的防护思路，进行以数据为中心的安全体系建设，覆盖各个场景，实现数据在哪里，安全就在哪里，安全跟着数据走。

<https://mp.weixin.qq.com/s/wuaCl-bdbQRVScENdje19g>