2020 年全球数据泄露大事件盘点：数据“裸奔” 代价沉重

2020 年，新冠疫情肆虐全球，催化各行业加速数字化转型，数据的价值在进一步凸显，数据的泄露也在持续高频发生，企业面临资产与声誉的重大损失，公众深受隐私曝光与骚扰诈骗的困扰。

安全 419 联合华途信息梳理了 2020 年发生在全球各地的重大数据泄露事件，并针对当前形势给予实用的安全建议，以期对数据安全建设略尽绵薄之力。

【国内时间轴】

- **1 月 31 日丨中国电信超 2 亿条用户信息被卖**

新浪科技讯 1 月 3 日上午消息，日前，中国裁判文书网公布了《陈德武、陈亚华、姜福乾等侵犯公民个人信息罪二审刑事裁定书》。经法院二审审理查明：2013 年至 2016 年 9 月 27 日，被告人陈亚华从号百信息服务有限公司（为中国电信股份有限公司的全资子公司）数据库获取区分不同行业、地区的手机号码信息提供给陈德武，被告人陈德武以人民币 0.01 元/条至 0.2 元/条不等的价格在网络上出售，获利金额累计达人民币 2000 余万元，涉及公民个人信息 2 亿余条。

- **3 月 19 日丨微博 5.38 亿用户数据在暗网出售**

PingWest 品玩 3 月 19 日讯，近日，有用户发现 5.38 亿条微博用户信息在暗网出售，其中，1.72 亿条有账户基本信息，售价 0.177 比特币。涉及到的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。对此，微博安全总监罗诗尧回应表示：“泄漏的手机号是 19 年通过通讯录上传接口被暴力匹配的，其余公开信息都是网上抓来的。”同时，罗诗尧表示：“19 年被刷的部分数据，内部突发现异常后马上堵住了口子。我们第一时间报了警，取证后把相关信息递到了警方，同时一直也在追查网上售卖信息的黑灰产。用户的隐私至关重要，尤其还是涉及到手机号。”

- **4 月 16 日丨青岛胶州中心医院 6 千余人就诊名单泄露**

4 月 16 日 11 时 17 分，有当地市民在胶州政务网反应，微信朋友圈中流传着出入胶州中心医院的数千人名单，涉及相关人员个人信息，已严重影响个人生活，并被谣传感染了新冠肺

炎。网传文件显示，就诊人员被列入 12 个胶州市街道和乡镇，内容包括姓名、电话、身份证号码、个人详细居住地址、就诊类型，共涉及 6685 人。

- **4 月 22 日丨多地数千高校学生隐私遭泄露**

4 月，河南财经政法大学、西北工业大学明德学院、重庆大学城市科技学院等高校的数千名学生发现，自己的个人所得税 App 上有陌生公司的就职记录。税务人员称，很可能是学生信息被企业冒用，以达到偷税的目的。此外，有类似遭遇的还包括湖北武汉、山东青岛、安徽滁州等多地的高校学生。企业冒用大学生信息偷税俨然成为行业潜规则，而受害的大学生因无就业经验，往往对此难以察觉，维权更是困难重重。

- **4 月 24 日丨浙江一家银行泄露客户信息被罚 30 万**

4 月，有媒体报道，浙江岱山农商银行、浙江民泰商业银行有内部人员违规泄露客户信息。其中，浙江岱山农商银行被银保监会罚款 30 万，泄露信息的内部员工被禁业三年。南都记者注意到，类似泄露客户个人信息案件的“内鬼”多来自运营商、银行、物流等掌握大量个人信息的行业。在“净网 2018”、“净网 2019”、“净网 2020”专项行动中，公安机关在侵犯公民个人信息案件中抓获各行业“内鬼”3000 余名。

- **4 月 27 日丨 B 站知名 UP 主“党妹”数百 G 视频素材被盗**

4 月 27 日，哔哩哔哩视频网站拥有五百万粉丝的 UP 主“机智的党妹”发布消息称，自己被黑客勒索了，根据她的介绍是因为自己的视频素材被黑客盗取，对方要求支付“赎金”才愿意将素材还回来。

- **5 月 6 日丨中信银行违法泄露脱口秀艺人个人隐私**

5 月 6 日，脱口秀艺人池子微博发布长文，表示自己在处理与上海笑果文化传媒有限公司的合约纠纷时，收到来自对方的案件材料，里面包含自己在中信银行的个人账户交易明细，中信银行在未经本人允许的情况下，为“配合大客户的需要”，泄露了池子的个人信息，严重侵犯客户个人隐私。

- **5 月 7 日丨 5000 多万条个人信息在“暗网”倒卖**

5 月 7 日，江苏省南通市公安局公布，经过 4 个多月的缜密侦查，江苏南通、如东两级公安机关破获了一起特大“暗网”侵犯公民个人信息案，抓获犯罪嫌疑人 27 名，查获被售卖的公民个人信息数据 5000 多万条。这起案件也被公安部列为 2019 年以来全国公安机关侦破的 10 起侵犯公民个人信息违法犯罪典型案件之一。所谓“暗网”，是利用加密传输、P2P 对等网络等，为用户提供匿名互联网信息访问的一类技术手段。“暗网”的最大特点是经过加密处理，普通浏览器和搜索引擎无法进入，且使用比特币作为交易货币，很难追查到使用者的真实身份和所处位置，受到互联网犯罪分子青睐。

- **5 月 20 日丨建设银行员工贩卖 5 万多条客户信息**

5 月 20 日，据媒体报道，江苏淮阴市淮安警方近期破获了一起特大贩卖公民个人信息案，共抓获 26 名嫌疑人，涉案金额 2000 多万元，涉及公民个人信息 5 万多条。建设银行员工将相关银行卡使用人的身份信息、电话号码、余额甚至交易记录售卖给下家，进行谋利。银行员工泄露个人账户信息，因涉及客户的资金安全，已不属于侵犯普通隐私的范畴，情节更加严重、恶劣。

- **6 月 5 日丨台湾 2000 万人个人信息在暗网泄露**

6 月 5 日，据媒体报道，研究人员近日在暗网上发现圈内知名卖家放出了一个“台湾全省房屋登记数据库”的数据库，大约 3.5GB，该数据库包含 2000 万条个人的姓名、邮件地址、电话号码、身份 ID、性别和出生日期记录，这意味着差不多全体台湾人民的个人数据都遭到了泄露。

- **6 月 8 日丨郑州某民办高校近两万名学生信息遭泄露**

6 月，郑州西亚斯学院近两万名学生信息遭到泄露，包括姓名、身份证号、专业、宿舍门牌

号等二十余项信息。事件发生后，多名学生反映收到骚扰电话。目前，学校称已报备公安机关，正在调查中。今年 4 月以来，多地的多所高校频繁发生个人信息泄露事件。有专家指出，上述如此大规模的数据泄露很可能是学校的某个环节出现过失导致的，学校需承担相应责任。

- **6 月 20 日丨蔡英文涉选举机密规划遭黑客攻击外泄**

据媒体报道，6 月蔡英文访美期间，包括民进党秘书长吴钊燮在内的多位干部邮寄地址、通讯软件遭骇，民进党云端硬盘也被入侵，包括蔡英文行程、内部沟通信件外流，连事涉选举机密的规划、重要文件，也全都外泄。

- **7 月 1 日丨四川某装修公司花 240 万买业主信息**

四川某装修公司为谋求快速发展，花费 240 余万元购买涉及川、渝、黔 3 省份近千楼盘 70 余万条公民个人信息。此案中，还有 4 人入侵四川 5 市房管系统，非法获取楼盘业主信息。7 月 30 日，记者从四川德昌警方获悉，截至今年 7 月 1 日，法院依法判决 27 人，还有多人被行政处罚，扣押、罚没涉案资金达 200 万元。目前，多家楼盘被行政处罚。针对所涉 5 市房管局，德昌警方已将相关线索通报 5 市网安部门。

- **8 月 13 日丨 6000 条多“珍爱网”账号信息被盗卖**

钱塘新区警方成功破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 2 名，扣押涉案电脑 1 台、电脑主机 2 台、硬盘 2 台、手机 11 部、手机卡 8 张、电话卡 40 余张，相关公民隐私信息资料 6000 余条。

- **9 月 7 日丨圆通“内鬼”泄露 40 万条客户信息**

今年 8 月，河北省邯郸市永年区某物流公司报案称：其公司员工账号被本公司物流风险控制系统监测出有违规异地查询非本网点运单号信息的行为，导致大量客户隐私信息有可能泄露。警方调查，涉案的“某物流公司内部员工”为五位圆通员工。9 月 7 日，警方将嫌疑人张某行、高某桥、马某杰抓获。该案涉案嫌疑人涉及河北、河南、山东等全国多个省市，涉案金额 120 余万元。

- **9 月 27 日丨广西医护人员倒卖 8 万条婴儿信息**

据南宁法院网消息，9 月 27 日下午，广西壮族自治区南宁市青秀区人民法院公开审理了一起 8 万多条新生儿、产妇信息被倒卖的案件，涉案人员包括一名医护人员。自 2018 年初开始，被告人李某某利用在广西壮族自治区妇幼保健院工作的便利，在为新生儿办理出生证时，非法下载新生儿和产妇的个人信息，总量达 89904 条。

- **10 月 15 日丨泰州警方破获一起侵犯公民个人信息案，涉及 800 余万条数据**

央视新闻 10 月 15 日消息，经过 6 个多月的缜密侦查，日前，江苏泰州警方破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 7 名，被售卖的公民个人信息达 800 多万条。

- **12 月 2 日丨泄露数据近 20 万条 团伙开发挂号软件获利被判刑**

北京青年报记者从北京西城法院得悉，该院审结了所有研发预定备案软件收获案件，该团伙经过备案软件获得病号信息，并不法供给应号市井，由号市井为病号备案赚取 200 至 700 元不等的效劳费。仅该案揭发的信息数据近 20 万条。

- **12 月 7 日丨男子泄露成都确诊女孩隐私信息被警方处罚**

2020 年 12 月 7 日 23 时许，王某(男，24 岁)将一张内容涉及“成都疫情及赵某某身份信息、活动轨迹”的图片在自己的微博转发，严重侵犯他人隐私，造成不良社会影响。经公安机关调查，王某对散布泄露赵某某个人隐私的行为供认不讳，并深刻认识到自己的错误。目前，王某因违反《中华人民共和国治安管理处罚法》相关规定已被我局依法予以行政处罚。

- **12 月 14 日丨央视曝光简历信息被贩卖 招聘平台成简历信息泄露源头**

12 月 14 日消息，央视记者调查发现，简历信息贩卖已经形成了一条灰色产业链。据报道，不少人在招聘平台上传建立后就会收到骚扰电话，自己的个人简历信息被招聘网站下载后转

手卖掉，QQ 等社交平台便是贩卖集中地。

- **12 月 21 日丨万名购买进口白虾的人员信息被泄露**

据重庆法院网消息，渝北法院受理并审结首例涉“新冠肺炎”疫情侵犯公民隐私权纠纷案。被告重庆某营销策划有限公司却将一份名为《重庆已购进口白虾顾客名单》的文章发布在其管理的公众号供下载，该名单包括原告赵某在内的重庆各区县一万多名购买进口白虾的人员的姓名、家庭住址、身份证号码、手机号码等详细个人信息。

【国外时间轴】

- **1 月 20 日丨近 50 万台服务器、路由器和 IoT 设备密码被泄露**

1 月 20 日，据外媒报道，某黑客组织在一个流行的黑客论坛上发布了一份涵盖 515000 多台服务器、家庭路由器和物联网智能设备的远程登录 Telnet 凭据列表，内容包含每台设备的 IP 地址、以及 Telnet 服务的用户名和密码。Telnet 是一种远程访问协议，可用于在互联网上控制设备，允许用户登录进入远程主机系统。据了解，该列表是通过扫描整个 Internet 来查找暴露其 Telnet 端口的设备而编制的。研究人员表示，此次事件是迄今为止已知的最大 Telnet 密码泄漏事件。

- **1 月 30 日丨化妆品巨头雅诗兰黛泄露 4.4 亿条邮箱记录**

安全研究人员 Jeremiah Fowler 于 1 月 30 日发现了暴露的数据库，他在数据库中的找到了用户电子邮件地址，在确定了来源后，立即试图与雅诗兰黛取得联系。此次泄露总共涉及 440,336,852 条记录，其中包含大量的审计日志和电子邮件地址。Fowler 表示，暴露的数据包括以纯文本形式存在的电子邮件地址，来自@estee.com 域的内部电子邮件地址也出现在数据库中。

- **2 月 11 日丨以色列 640 万选民数据遭泄露**

2 月 11 日，据外媒报道，近日由以色列总理内塔尼亚胡领导的利库德集团(Likud)开发的选举应用程序配置中的错误可能潜在地暴露并损害了近 650 万以色列公民的个人资料。据了解，此次泄漏是由 Verizon Media 以色列的前端开发人员 Ran Bar-Zik 发现并详细描述了这次泄露。目前 Haaretz，Calcalist 和 Ynet 等以色列当地媒体证实了 Bar-Zik 的发现，但是还不清楚在 Bar-Zik 发现和公开披露之前，暴露的服务器和数据是否被未经授权的人获取。

- **2 月 21 日丨米高梅酒店数据转储 1060 万旅客信息被泄露**

据外媒报道，2 月 21 日，超 1060 万名住在米高梅国际度假(MGM Resorts)酒店的客人的个人详细信息被公布在了一个黑客论坛上。除了普通游客之外，遭新曝光的信息还包括了一些名人、科技公司老总、记者、政府官员以及来自全球最大科技公司的职工。根据外媒 ZDNet 的分析，今天被曝光的 MGM 数据转储包含了 10,683,188 名曾在 MGM 酒店住过的客人的个人详细信息。泄露的文件中包含了个人详细信息，诸如全名、家庭住址、电话号码、电子邮件和生日等。

- **2 月底丨万豪国际再曝 520 万用户数据泄露**

连锁酒店万豪国际 4 月宣布，它已受到第二次数据泄露的打击，该数据泄露暴露了“多达 520 万名客人”的个人详细信息。该漏洞始于 2020 年 1 月中旬，并于 2020 年 2 月底被发现，其中包含了详细的联系方式，包括姓名、地址、出生日期、性别、电子邮件地址和电话号码。还披露了雇主名称、性别、住宿偏好和会员卡帐号。

- **3 月 4 日丨国泰航空泄露 940 万乘客资料，被罚款 500 万港币**

航空圈讯 英国资讯委员会办公室（ICO）当地时间 3 月 4 日公布消息说，对国泰航空有限 公司（Cathay Pacific Airways Limited）罚款 50 万英镑（约 450 万元人民币或者 500 万元港币），原因是该公司未能保护客户个人数据的安全。 ICO 称，2014 年 10 月至 2018 年 5 月期间，

国泰航空的计算机系统缺乏适当的安全措施，导致客户的个人信息被泄露，其中 111578 人来自英国，而全球约 940 万人。

- **3 月 23 日丨某英国安全公司云泄露 50 亿条安全记录**

据外媒报道，3 月，安全专家 Bob Diachenko 发现了一个疑似属于英国安全公司的一个不安全的 Elasticsearch 实例，其中包括在 2012 年到 2019 年之间和安全事件有关的 50 亿条记录。根据 Bob Diachenko 的说法，在 3 月 16 日，他在公网发现了一个缺乏保护的 Elasticsearch 实例，根据 SSL 证书和反向 DNS 记录，发现这个 Elasticsearch 似乎是由一家英国安全公司所管理。而且特别讽刺的是，其中包括一个“数据泄露数据库”，收集了 2012 年至 2019 年期间大量被报道（或许还有未报道）的安全事件中的数据。这个巨大的 Elasticsearch 由两个集合组成，一个包含了 5,088,635,374 条记录，另一个正实时更新，包含 1500 万条记录。被泄露的数据包括：哈希类型（显示密码的方式：MD5/哈希/纯文本等）、泄漏日期（年）、密码（哈希值或纯文本）、电子邮件、电子邮件域、泄漏源（某些显眼的泄漏源：Adobe，Last.fm，Twitter，LinkedIn，Tumblr，VK 等）。

- **4 月 11 日丨麦哲伦健康遭勒索软件攻击和数据泄露**

麦哲伦健康公司是《财富》 500 强公司之一，于 2020 年 4 月遭到勒索软件攻击和数据泄露袭击。这家医疗保健巨头证实说，大约 365,000 名患者受到了复杂的网络攻击。 根据调查，该攻击是通过全面计划的过程发起的，黑客首先安装了恶意软件以窃取员工的登录凭据。然后，他们在发送网络钓鱼电子邮件并假冒其客户端之前，利用网络钓鱼方案来访问麦哲伦的系统，然后再部署勒索软件攻击。数据窃贼能够窃取员工的登录凭据、个人信息、员工 ID 号、敏感的患者详细信息（例如 W-2 信息、社会保险号或纳税人 ID 号）。

- **4 月 14 日丨 50 万个 ZOOM 用户凭证信息外泄**

在 2020 年 4 月初，“暗网犯罪论坛上有 500,000 个被盗的 Zoom 密码可供出售”的消息震惊了应用程序用户。 据报道，超过半百万的 Zoom 帐户登录凭证已被出售，其中一些帐户凭证是免费赠送的。实际上，一些登录凭证每个售价不到美分！除帐户登录凭据外，受害者的个人会议 URL 和 HostKey 也可用。泄漏的帐户的详细信息属于金融机构、银行、学院和各种组织。

- **4 月 23 日丨 2.67 亿个 Facebook 帐户信息在暗网出售**

据外媒报道，4 月，网络安全公司 Cyble 发现，有 2.67 亿 Facebook 用户信息被盗，包括姓名、邮箱地址、电话、社会身份、性别等，这些信息在暗网上以仅 600 美元的价格出售。目前，尚未清楚这些信息是如何在第一时间被泄露的，不过根据 Cyble 工作人员的说法，很可能是第三方 API 泄露或报废导致的。虽然这次针对 Facebook 的攻击并不像此前 Zoom 一样对密码等敏感信息进行了窃取，但由于这些信息包含了用户的敏感资料，不法分子很有可能将其用于网络钓鱼诈骗或者发送垃圾邮件。

- **5 月 6 日丨成人网站泄露超百亿条用户敏感记录**

据外媒报道，5 月，一家主营成人直播服务的公司便遭遇了有史以来最大规模的用户敏感数据。泄露数据包含用户姓名、性取向、支付记录、聊天记录、电子邮件信息、IP 地址和密码哈希等，总计多达 108.8 亿条记录。在泄露高达 7TB 用户敏感数据之前，CAM4 还没来得及关闭它的服务器。这些敏感数据是由于一个不受保护的数据库集群而泄漏。CAM4 错误地配置了 Elasticsearch 集群，从而使一系列生产数据库不受在线保护，任何使用 Web 浏览器的人都可以访问。

- **5 月 8 日丨印尼电商巨头 Tokopedia9000 万账号信息在暗网售卖**

据外媒报道，5 月，数据泄露和网络安全情报公司 Under the Breach 发现有黑客在黑客论坛出售超过 1500 万 Tokopedia 用户信息。要访问该数据，论坛用户需要支付 8 个网站积分，相当于€2.13（约合 16 元人民币）。黑客称这是 2020 年 3 月 Tokopedia 泄露的 9100 万数据

的一部分。同时，该黑客也在出售完整的 9100 万用户数据集，售价 5000 美元。Tokopedia 是印度尼西亚最大的电商平台，也是访问量最大的印尼网站，有 4700 个雇员和 9000 万的活跃用户。Under the Breach 称泄露的数据是一个 PostgreSQL 数据库，包含个人用户数据等信息。泄露的数据中最重要的是用户的邮箱地址、全名、生日、哈希的用户口令，一些账户中还含有 MSISDN 信息。

- **5 月 8 日丨 4400 万巴基斯坦移动用户的详细信息在线泄漏**

据外媒报道，有 4400 万巴基斯坦移动订户的详细信息在线泄漏，并于上月底，一名黑客试图以折合 210 万美元的比特币的价格出售一个包含 1.15 亿巴基斯坦移动用户记录的软件包。

- **5 月 19 日丨英国廉价航空公司 easyJet 数据泄露面临 180 亿英镑巨额诉讼**

easyJet 于 5 月 19 日公开表示，属于 900 万客户的信息可能已经受到网络攻击遭泄露，其中还包括超过 2200 条信用卡记录。 此次事件归咎于“高度复杂”的攻击形式，攻击者设法访问系统的财务信息以及电子邮件地址和旅行详细信息。

- **5 月 26 日丨泰国移动运营商 AIS 云泄露 83 亿条互联网记录**

据外媒报道，5 月，研究人员发现了泰国移动运营商 Advanced Info Service (AIS)子公司控制的一个 ElasticSearch 数据库可公开访问，数据库包含大约 83 亿记录，容量约为 4.7 TB，每 24 小时增加 2 亿记录。AIS 是泰国最大的 GSM 移动运营商，用户约有 4000 万。可公开访问的数据库由其子公司 Advanced Wireless Network (AWN)控制，包括了 DNS 查询日志和 NetFlow 日志，这些数据可用于绘制一个用户的网络活动图。

- **6 月 8 日丨 WordPress 数百万网站数据库遭到窃取**

据外媒报道，6 月，黑客组织试图利用主题和插件中的已知漏洞从数百万个 WordPress 网站窃取数据库凭据。WordPress 是使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设属于自己的网站，同时，用户也可以把 WordPress 当作一个内容管理系统（CMS）来使用。WordPress 有许多第三方开发的免费模板，安装方式简单易用。

- **6 月 10 日丨印度 BellTroX 为客户提供黑客服务 7 年入侵 1 万多电邮账户**

6 月 10 日，据外媒报道，一家不知名印度 IT 公司 BellTroX 为客户提供黑客服务，7 年入侵全球超过 1 万个电子邮件账户。这家印度 IT 公司专门瞄准欧洲政府官员、巴哈马博彩大亨和以及美国私募股权巨头 KKR 等进行黑客活动。知情人士表示，BellTroX 的黑客行动正面临美国执法部门的调查。

- **6 月 19 日丨谷歌浏览器大规模用户安全信息泄露**

6 月 19 日，Awake Security 的研究人员表示，他们在谷歌浏览器的扩展程序中发现了一个间谍软件，并且已经被下载了 3200 多万次。如果有普通用户在家用电脑上使用扩展程序中带有恶意软件的浏览器，它会联系多个网站，然后传输用户信息，造成信息泄露。

- **6 月 22 日丨甲骨文公司泄露数十亿条网络数据记录**

6 月 22 日，据外媒报道，科技巨头甲骨文公司的数据管理平台 BlueKai 因为在服务器上不加密码从而泄露了全球数十亿人的数据记录。BlueKai 是一个基于云的大数据平台，其利用 Cookie 等跟踪技术能获取个人网络信息、阅读习惯、浏览内容等，并据此推断分析出收入水平、受教育水平、兴趣爱好等个人标签，进而精准推送广告。

- **7 月 16 日丨美国多位名人政要推特账号遭黑客入侵**

7 月 16 日电据美国有线电视新闻网报道，当地时间周三（15 日），多位美国名人政要的推特账户遭黑客入侵，发布比特币诈骗链接。账号遭黑客入侵的人士包括美国前总统奥巴马、民主党总统候选人拜登、微软公司创始人比尔·盖茨、亚马逊公司创始人杰夫·贝佐斯、金融大亨沃伦·巴菲特、特斯拉 CEO 埃隆·马斯克、纽约市前市长迈克尔·布隆伯格、歌手坎耶·韦斯特、美国社交名媛金·卡戴珊等。此次受到影响的名人政要账号数量众多，可以说是推特

历史上最大的安全事件。推特官方表示正在对此事进行调查，推特的部分功能将受限，推特认证账号将无法发布推文或者重置密码。

- **7 月 25 日丨任天堂泄露大量内部游戏与设备资料**

在线游戏先锋任天堂(Nintendo)今年早些时候遭遇重大数据泄露，超过 16 万用户账户在一次攻击中被攻破。黑客们利用这些在线账户通过任天堂网络购买数字产品，在此之前，黑客们对凭证填料发起了攻击。不过这并不是结束，在 7 月 25 日任天堂又再次遭遇了大规模的数据泄露，包括大量游戏例如《宝可梦》、《马里奥》、《塞尔达传说》等游戏以及 GB 系列 ROM 在内的大量开发源代码与相关资料。

- **8 月 8 日丨英特尔 20GB 内部数据泄漏**

英特尔正在调查安全漏洞，该公司在文件共享网站 MEGA 上在线上传了 20 GB 内部文件，其中包括 “机密”或“限制机密”标志的文件。

- **8 月 18 日丨美国酒业巨头百富门被窃取超 1TB 数据**

8 月 18 日，Sodinokibi（REvil）勒索软件运营商宣布，他们已经破坏了 Brown-Forman（百富门）的网络系统，该公司是美国烈酒和葡萄酒行业最大公司之一。事件发生后，此勒索软件团伙声称已窃取 1TB 的机密数据，并计划将最敏感的信息用于拍卖。据统计，该团伙窃取的数据包括员工的信息、公司协议、合同、财务报表等。

- **8 月 19 日丨游戏硬件厂商 Razer（雷蛇）在线商店泄露大量用户数据**

8 月 19 日左右，安全研究员 Bob Diachenko 发现了一个不安全的 Elasticsearch 数据库，该数据库暴露了大约 10 万个从 Razer 在线商店购买商品的用户信息。暴露的信息包括客户的姓名、电子邮件地址、电话号码、订单号、订单明细以及账单和送货地址。

- **8 月 20 日丨益百利（南非）2400 万客户数据泄露**

消费者信用报告机构 Experian 的南非分公司披露了数据泄露事件，该信贷机构承认已将其南非客户的个人详细资料移交给冒充客户的欺诈者。虽然 Experian 没有透露受影响用户的数量，但来自反欺诈和银行业非营利性机构南非银行风险中心（SABRIC）的一份报告称，该违规行为影响了 2400 万南非人和 793749 家本地企业。

- **8 月 20 日丨美国 AI 公司被曝泄露近 260 万医疗数据**

安全研究人员耶利米·福勒（Jeremiah Fowler）在 Secure Thoughts 上发表文章称，他发现近 260 万条包含姓名、医疗诊断记录、保险记录和支付记录在内的个人病历数据被泄露了。福勒写道，他早在 7 月 7 日发现了两个含有医疗数据记录的文件夹，里面总计有 2594261 条数据，而且任何人都可以通过互联网查看这些数据。

- **8 月 25 日丨网站 Freepik 用户数据泄露，影响 830 万用户**

Freepik 是一个致力于提供高质量免费照片和设计图形的网站，也是互联网上最受欢迎的网站之一。8 月 25 日，Freepik 披露了一起重大安全漏洞，一名黑客利用 SQL 注入漏洞访问其存储用户数据的数据库，并获得了其 Freepik 和 Flaticon 网站上 830 万注册用户的用户名和密码。

- **9 月 10 日丨 SK 海力士和 LG 电子机密资料大量外泄**

据韩国《东亚日报》9 月 10 日消息，SK 海力士和 LG 电子 9 日遭到一个黑客团体的网络软件攻击，内部机密资料大量外泄。被黑客入侵的文件中相当一部分包含客户交易信息等机密资料，因此有可能产生进一步的损失。

- **9 月 21 日丨美国金融犯罪执法网络局 FinCEN 机密文件泄露**

据英国广播公司 21 日报道，9 月 20 日，美国金融犯罪执法网络局（FinCEN）2500 多个机密文件又遭泄露，涉及约 2 万亿美元的交易。这些文件揭露了一些国际性银行让犯罪分子在世界各地转移赃款的行为。FinCEN 文件的泄露是过去五年来发生的一系列泄密事件中最新的一次，其文件内容揭露了秘密交易、洗钱和金融犯罪。

- **10 月 15 日丨在线书店 Barnes & Noble 被黑，消费者邮箱和购买记录泄露**

据外媒报道，虽然 Nook 在很大程度上已经被亚马逊的 Kindle 抛在脑后，但 Barnes & Noble 仍是一个拥有相当数量忠实客户的知名品牌。然而这些顾客现在可能有些担心，这家书商的报告显示，B&N 公司系统遭到了网络安全攻击，黑客可能已经获得了 B&N 客户的一些重要信息，其中可能包括他们的住址。

- **10 月 16 日丨希腊电信巨头用户信息泄露**

据希腊《中希时报》16 日报道，日前，希腊最大的电信网络公司 Cosmote 发生了一起重大数据泄露事件。大量希腊人的个人信息遭泄露，可能会对“国家安全问题”产生重大影响。据报道，此次信息泄露是不明身份“黑客”攻击网络造成的，他们窃取了 2020 年 9 月 1 日至 5 日期间的电话等数据。

- **10 月 30 日丨 美国安泰人寿用户信息泄露**

美国安泰人寿保险公司（Aetna）向美国卫生与公众服务部（HHS）支付 100 万美金并采取整改措施，以补救其此前违反《健康保险可携性和责任法案（HIPAA）》导致的损害后果。根据 HHS 的通讯稿，安泰曾三次违反 HIPAA 的相关义务：2017 年 4 月，安泰网站某页面的文件无需登录即可访问，造成超 5000 人的信息泄露；2017 年 8 月，安泰用窗信封给用户寄送通知，"HIV Medication"的字样出现在了信封窗中，导致逾 1 万人的信息泄露；2017 年 11 月，安泰寄送的研究报告信封上印有收件人所参加的房产项目的名称及标志，导致 1600 人的信息泄露。

- **10 月 31 日丨阿里旗下电商平台 Lazada 110 万账户信息被黑客入侵**

据报道，阿里巴巴旗下电商平台、新加坡电子商务公司 Lazada 今日宣布，其 110 万账号信息被黑客入侵。在这个拥有 570 万人口的国家（新加坡），这显然是一次重大的黑客入侵事件。这些账号信息包括用户的家庭住址、部分信用卡号码等。

- **11 月 4 日丨瑞典保险巨头 Folksam 数据泄露将 100 万瑞典人的信息泄露给谷歌、Facebook**

据 Folksam 市场和销售主管延斯·威克斯特伦(Jens Wikstrom)称，保险公司在进行内部审计后发现了数据泄露，并向瑞典数据保护局(Datainspektionen)报告了这一事件。Folksam 共享的敏感个人数据包括各种类型的信息，例如社会保险号或个人购买的工会或怀孕保险。科技巨头利用共享数据的分析结果，通过 Folksam 和其他公司的沟通渠道向客户提供定制服务。

- **11 月 10 日丨西班牙 Prestige 软件泄漏泄露了酒店住客的个人数据**

西班牙公司 Prestige Software 发生数据泄露，包括全球数百万酒店客人的姓名、身份证号等高度敏感数据。Booking.com 等多家在线预订平台的用户都是此次数据泄露的受害者。据了解，泄露的数据为 24.4GB，总计超过 1000 万个文件，包含 10 万多人的信用卡信息，最早可以追溯到 2013 年。

- **11 月 25 日丨基督教信仰应用程式 Pray.com 泄漏使用者的个人资料**

研究人员声称，总部位于圣莫尼卡的公司配置错误的云基础设施导致大约 1000 万人的个人数据暴露。据报道，该应用程序的开发人员没有适当地保护从该应用程序收集的大量数据储备。

- **12 月 4 日丨巴西卫生部官网存严重漏洞 2.43 亿巴西人个人信息被泄露**

早在 11 月就报道过 1600 万巴西 COVID-19 患者个人数据被曝光之后，巴西当地媒体 Estadao 12 月 4 日再次放出重料--包括在世和已故的在内，有超过 2.43 亿巴西人的个人信息已经在网络上曝光。这些数据来自于巴西卫生部官方网站的源代码，开发者在其中发现了重要政府数据库。该数据库包含巴西人提供给政府的所有个人信息，从全名到家庭住址，从电话号码到医疗详细信息。现在已经从站点的源代码中删除了凭据，但是尚不清楚是否有人访问过该系统并窃取了巴西公民的数据。

- **12 月 8 日丨意大利国防巨头 Leonardo S.p.A10GB 机密数据泄露**

近日，意大利警方逮捕了莱昂纳多(Leonardo SpA)的一名前雇员和另一名涉嫌盗窃公司敏感信息和军事信息的人。那不勒斯检察官办公室 11 月 5 日也曾表示，全球最大的国防承包商之一列莱昂纳多公司(Leonardo SpA)的航空结构和飞机部门仍在遭受网络攻击。该公司总部位于意大利罗马，拥有超过 49000 名员工，其在英国、美国和波兰的航空航天、军事和安全部门都有分支机构。

- **12 月 9 日丨富士康约 1200 台服务器常规业务文档和报告数据面临泄露**

据 BleepingComputer 追踪，电子巨头富士康一家在墨西哥的工厂遭受了勒索软件攻击，DoppelPaymer 勒索软件在其勒索软件数据泄漏站点上发布了富士康部分文件，泄漏的信息包括常规业务文档和报告，威胁索要 1804.0955 比特币赎金，按今天的比特币汇率计算，约为 3400 万美元。此次攻击事件使工厂日常业务的开展受到了不同程度的干扰。最直接的就是被加密文件无法访问，加密文件涉及到的相关业务被迫中断，业务连续性受到影响。

- **12 月 16 日丨全球 4500 万医学影像照片在线暴露**

根据 CybelAngel 最新发布的为期六个月的调查报告，由于存储、发送和接收医疗数据的技术存在安全问题，全球已经发现超过 4500 万张医学图像以及与之相关的个人身份信息（PII）和个人医疗保健信息（PHI）在线暴露。报告称，CybelAngel 分析团队使用工具扫描了大约 43 亿个 IP 地址，在全球医院和医疗中心的联网存储设备中发现了超过 4500 个医学影像及相关隐私数据暴露，这些图像被存储在 67 个国家（包括美国、英国、法国和德国）的 2140 台未受保护的（NAS）服务器上。

- **12 月 22 日丨英国能源公司数据遭泄露 整个客户数据库受损**

英国能源供应商 People's Energy 的联合创始人卡琳·索德（Karin Sode）告诉 BBC 新闻，其客户的敏感个人信息，包括姓名，地址，出生日期，电话号码，电费和电表 ID 被黑客窃取。在发现该违规行为之后，它已与所有 270,000 名当前客户联系，以告知他们该违规行为。

【数据防泄漏 刻不容缓】——华途信息产品总监 陈彬

- **全球疫情下的安全管理松懈及攻击激增**

2020 年几乎对所有企业来说都是充满挑战的一年，COVID-19 的肆虐流行引发了健康危机，导致全球经济遭到破坏，许多恶意行为者利用混乱的局面，对网络安全进行攻击并通过贩卖各类隐私数据从而获利。因此相较于以往年份，今年的数据泄露和监管罚款事件发生的频率及严重程度更高。随着社会对数据安全重视程度的提高，对于企业来说，如何保证数据安全将成为其重要工作之一。

- **内部滥用及泄露的情况显著增多，内部管理起到关键作用**

根据 IBM 和 Ponemon Institute 的 2020 年数据泄露成本报告显示，52%的数据泄露是由恶意外部人员造成的，另外 25%是由系统故障和攻击造成的，23%的人为错误，客户的个人身份信息（PII）占所有数据泄露的 80%，是最经常丢失或被盗的记录类型。鉴于 PII 因其敏感性而成为最有价值的数据类型，所以它也是数据保护法规最经常保护的数据类型。

- **医疗、金融等关键信息基础设施单位为重要保护对象**

近年来，数据泄露事件频繁爆出在**医疗、酒店、公共部门、零售、金融**等行业，造成了相关企业严重的声誉损失和经济损失，作为企业应着重保护自身机密数据以及用户的隐私数据。事实证明，在某些行业，员工疏忽是造成数据泄露的一大原因。例如排在榜首的是娱乐业，其中 34%的数据泄露是由粗心的员工造成的，其次是公共和消费产品部门，其中人为错误占数据泄露的 28%。在医疗保健领域，尽管有严格的法规，但员工疏忽是造成所有数

据泄露的 27%。另一方面，在交通运输中，只有 13%的数据泄露是由人为错误引起的，而在零售和科技行业，则占 17%。

➢ **泄露违法成本太低，个人、企业、国家监管部门都应重视**

由于面临着 COVID-19 大流行带来的困难，恶意行为者一直在寻找获利的机会，因此必须重视网络安全。同时，尽管数据保护机构由于当前的情况而表现出宽容，但当他们发现完全忽视了数据保护要求时，他们并没有施加令人垂涎的惩罚。现象表明，许多企业仍将数据安全视为一项事后考虑。如今，数据安全已成为业务运营的关键部分，并且不再有可以忽略的时间了。不管是国外还是国内，都相继出台了法律法规以保障数据安全。特别是 2020 年，国内**《数据安全法（草案）》《个人信息保护法（草案）》**两部重磅法律的相继出台，为我们的信息保护注入强心针，提高安全管理，让企业和个人远离数据泄露带来的巨额代价。

当国家监管趋严，用法律夯实保护公民个人信息的安全防线；当数据泄露频发，数据安全态势面临内忧外患、防护低效等多重挑战，建议采取相关有效的措施防止数据泄露：

①从安全需求角度

伴随社会高速发展，数据的安全越来越受到重视，而不法分子的攻击手段也层出不穷，传统权限类、枷锁类数据防护产品性能逐渐无法满足企业需要。此外，数据防护体系建设前，需开展数据治理工作，对数据进行分类分级，完整梳理企业数据资产，并针对重要数据和敏感数据采取适当、合理的管理和安全防护措施，对数据资产进行规范化管理和保护，确保数据安全，促进数据共享。基于上述数据安全需求，具备智能化内容识别能力的 DLP 产品应运而生。

②从法律监管角度

《网络安全法》中规定未经被搜集者同意，不得向他人提供个人信息。《数据安全管理办法》中也对数据的使用、保存、发送等层面进行防泄漏方面的规定，因此 DLP 产品除满足企业自身的数据安全需求外，可为行业合规管理和审计的时候提供内控相关的证据，提供基于合规审计的资料，帮助企业轻松应对审查及行业规范、数据安全监管要求。

③从产品用户体验角度

传统的磁盘加密、文件加密类产品都采用从源头一刀切的方式防止数据泄漏，该方式固然安全性高，但在一定程度会改变用户原有操作习惯，影响业务效率，用户体验不太友好。而 DLP 产品通过内容深度识别，可在多种场景下进行智能化防护，对用户使用来说该防护的存在是无感知的，即丝毫不改变原有操作习惯，提高用户体验。

④从企业 IT 管理角度

大多数公司缺乏针对敏感、涉密数据的管控和审计能力，确保公司敏感、涉密数据遵循统一的策略，在共享和开放的过程中保障数据安全，需要部署数据安全防护措施，防止敏感数泄漏导致对公司产生的严重影响。DLP 产品可有效支撑企业的 IT 管理，帮助规范内部网络，减少 IT 管理人员工作量、工作复杂度，从而优化 IT 环境，同时结合企业的相关规章制度，把数据安全管理要求落地。

华途数据防泄漏系统 对敏感信息进行全方位防泄漏保护

华途数据防泄漏系统由 1 中心 6 模块组成，由统一管理平台控制，下面包含终端保护、数据发现、网络监控、网络保护、邮件保护、应用保护六大网络防护模块。它适用于掌握社会、行业、个人秘密、私密数据的金融、运营商、政府、医疗、能源等行业，网络运营者与关键信息基础设施运营者，对敏感信息进行全方位的防泄漏保护。

1 中心 6 模块：

统一管理平台是基于 B/S 架构的综合管理平台，可配置基于用户角色的访问控制和系统管理选项。用户通过管理平台可依据内置策略模板，统一制定数据防泄漏策略，并集中下发到各安全模块，从而对客户敏感数据进行全方位的保护。管理平台可视化地呈现敏感数据分布状况和安全态势，可生成泄漏事件日志和报表，帮助用户进行审计、补救以及追溯操作。

模块①丨网络监控：

监控所有 HTTP、SMTP、FTP 等非加密网络链接，分析应用协议内容，发现并记录可能违反数据安全策略的数据通信。

模块②丨网络保护：

在网络监控基础上增加 HTTPS 协议的网络数据流量内容恢复和扫描，进行实时审计和阻断。

模块③丨数据发现：

扫描邮件服务器、应用服务器、文件服务器以及数据库、大数据平台等，根据扫描结果生成用户敏感信息分布地图。

模块④丨终端保护：

扫描并发现电脑上的敏感信息分布和不当存储，监控对敏感信息的使用并进行实时保护。

模块⑤丨邮件保护：

监控并自动分析所有外发的电子邮件，对违反数据安全策略的邮件立即阻止或发起人工审批过程。

模块⑥丨应用保护：

对 OA、ERP、 Web 下载等应用系统的访问流量进行内容恢复和扫描，进行实时审计和阻断。

三大防护方向：

① 在线网络泄密防护

网络监控或网络保护模块可以对在线网络的泄密行为实时审计或阻断，可以监管采用 WEB 邮件外发、网盘/云盘上传、FTP 上传及网页上传等方式传输的数据内容。

② 个人终端泄密防护

终端保护针对在线或离线的个人终端的泄密行为实时审计并阻断。通过实时监控外设、本地文件和应用程序的使用情况，在外设拷贝敏感内容，或应用程序访问敏感内容时进行拦截扫描，包括 USB 拷贝、光驱刻录、SD 卡拷贝、邮件客户端软件外发、业务系统以及即时通讯软件外发等方式传输的数据内容。

③ 数据存储安全防护

采用周期性增量更新的方式帮助管理者掌握内网中，及时发现涉密数据文件违规存储行为。还能记录并统计每部门、每终端、每类型敏感数据的详细存储路径，自动绘制敏感信息分布地图。此外，可对各大主流数据库、大数据平台中的结构化数据进行挖掘并进行自动化数据识别、分析、分类。通过引入自然语言处理、统计模型、特征分析、机器学习等方法，形成可以快速查看的结果集及统计报表。

三大核心优势：

①全面覆盖结构化和非结构数据泄漏途径

随着数据时代到来，数据的爆炸式增长，华途 DLP 产品可对主流数据库及大数据平台中结构化数据进行分类分级，为企业开展数据资产管理、数据治理工作、敏感数据发现和数据安全治理场景等提供基础，此外可结合华途文档加密系统 DSM、华途文档权限管理系统 DRM 等优势产品，形成完整的非结构化数据防护方案，做到数据安全防护与业务效率的有效平衡，满足企业对于数据安全与业务高效的双重需求。

②内容识别核心技术，拥有行业标杆验证

通过数据字典、OCR 技术、数据库技术、指纹匹配、语义模型等方法，形成了非常完整的金融、运营商等行业标杆的相应防护策略模板，企业也可根据其特定需求定制相应的策略模板。

③较强的数据分类分级功能

可自动发现、梳理并识别存储设施内的非结构化敏感数据，并对所有发现的敏感数据计算其数据指纹，针对性制定不同密级、不同类型的敏感数据监管和保护策略，智能化防止敏感信息的外泄；针对数据库及大数据平台中结构化数据，可进一步识别表格之间的关联关系，自动化识别数据含义和数据关系，最终生成完整、可视化的分析报告，可帮助企业快速了解和认识数据，为企业开展数据资产管理、数据治理工作、敏感数据发现和数据安全治理场景等提供基础。