[公开]360NELab-DST-0-028-20210125

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 28 期 2021 年第 4 期

（2020.01.18-2021.01.24）

大数据协同安全技术国家工程实验室

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**泄露数据买卖、数据泄露**和**勒索软件问题**。

1. 卖公民数据的犯罪团伙，涉 6 亿条信息赚取 800 万
2. 美国位置数据公司通过亚马逊平台进行数据售卖
3. 黑客在论坛上免费发布 190 万个 Pixlr 用户记录
4. OpenWRT 论坛遭黑客攻击并出现数据泄露
5. 黑客窃走敏感财务信息 英特尔被迫提前发财报
6. Bonobos 服装店 70GB 数据库遭黑客泄露
7. 7700 万 Nitro PDF 用户数据泄露
8. 苏格兰环境保护署拒绝支付勒索软件赎金

此外，在数据安全技术与观点方面主要讨论了：

1. GDPR 生效后已执行 2.725 亿欧元的罚款
2. 新型勒索软件对制造业网络造成严重影响
3. 2020 年全球公开漏洞披露，超过 220 亿记录泄露
4. 中国地方政府数据开放报告（2020 下半年）发布
5. 构建政务信息系统密码应用管理体系的建议
6. 区块链技术视野下的数据权属问题
7. 供应链安全管理

全球动态

1. Telegram 卖公民数据的犯罪团伙被抓，涉 6 亿条信息赚取 800 万

2021 年 1 月 24 日报道，丹阳市公安局称，在“净网 2020”专项行动，丹阳市公安局网安大队会同丹阳荆林、导墅、开发区等 10 多个派出所，经过半年多时间的缜密侦查，成功侦破一起公安部督办的侵犯公民个人信息案。经查，这一“灰色产业链”涉及湖北、重庆、河北等 10 多个省市，警方抓获犯罪嫌疑人 30 名，查扣涉案资金 130 余万元，查获各类公民个人信息 6 亿余条。

https://mp.weixin.qq.com/s?__biz=MzU5NTA3MTk5Ng==&mid=2247488820&idx=1&sn=05f93cdccbe871ab1ca523449c21d731

2. 美国位置数据公司通过亚马逊平台进行数据售卖

X-Mode Social 是一家成立于 2013 年的美国公司，总部位于维珍尼亚雷斯顿，专门从事位置数据的研究。主要通过让 APP 内置其 SDK，从而进行位置数据收集和分析，并将其售卖给其他客户，客户包括美国军事承包商。根据研究人员最新发现，X-Mode 公司居然在亚马逊平台上，公然售卖

位置数据，并且涉及 Covid-19 位置数据。

https://www.secrss.com/articles/28817

3. 黑客在论坛上免费发布 190 万个 Pixlr 用户记录

2021 年 1 月 20 日，一名黑客泄露了 190 万个 Pixlr 用户记录，其中包括电子邮件地址、登录名、SHA-512 哈希密码、用户所在的国家、是否注册了新闻通讯以及其他内部信息。Pixlr 是一个非常流行且免费的在线照片编辑应用程序，具有许多与专业桌面照片编辑器（Photoshop）相同的功能。

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

4. OpenWRT 论坛遭黑客攻击并出现数据泄露

2021 年 1 月 18 日，OpenWRT 论坛宣布发生数据泄露，它是一个由路由器替代开源操作系统组成的爱好者团体。未经授权的第三方获得了 OpenWRT 论坛管理员访问权限，并复制了包含论坛用户详细信息和相关统计信息的列表。

https://www.bleepingcomputer.com/news/security/openwrt-forum-user-data-stolen-in-weekend-data-breach/

5. 黑客窃走敏感财务信息 英特尔被迫提前发财报

2021 年 1 月 28 日报道，美国芯片制造商英特尔证实，由于该公司的敏感财务信息周四被黑客从其公司网站窃走，迫使其提前发布 2020 年第四季度和全年财报。该公司认为，一名黑客已经获得了有关该公司定于收盘后发布的财报的全部细节。英特尔股价当天上涨逾 6%，仅在收盘最后 15 分钟交易中就上涨近 2%。

https://view.inews.qq.com/k/20210122A01DGL00?uid=&shareto=

6. Bonobos 服装店 70GB 数据库遭黑客泄露

2021 年 1 月 22 日，Bonobos 男装商店遭受了大规模的数据泄露，暴露了数百万客户的个人信息。泄漏的数据库是一个巨大的 70 GB SQL 文件，其中包含 Bonobos 网站使用的各种内部表。该数据库还包含各种威胁者更感兴趣的数据，例如客户的地址、电话号码、部分信用卡号（后四位数字）、订单信息、密码历史记录。

https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/

7. 7700 万 Nitro PDF 用户数据泄露

2021 年 1 月 20 日，包含 Nitro PDF 服务用户超过 7700 万条记录的电子邮件地址，名称和密码的数据库被盗，14GB 的泄漏数据库包含 7700 万条记录，其中包含用户的电子邮件地址、全名、bcrypt 哈希密码、标题、公司名称、P 地址以及其他与系统相关的信息。Nitro 是一款可帮助创建，编辑和签署 PDF 和数字文档的应用程序。

https://www.bleepingcomputer.com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/

8. 苏格兰环境保护署拒绝支付赎金，黑客泄露数千个文件

2021 年 1 月 22 日，据外媒报道，苏格兰环境保护局（SEPA）在平安夜遭到勒索软件攻击，网络罪犯在此过程中窃取了 1.2 GB 数据。攻击发生将近一个月后，SEPA 服务仍受到干扰。在该组织拒绝支付赎金之后，黑客已经发布了数千个被盗文件。

https://www.zdnet.com/article/hackers-publish-thousands-of-files-after-government-agency-refuses-to-pay-ransom/?&web_view=true

业界观点

1. GDPR 生效后已执行 2.725 亿欧元的罚款

近日，跨国律师事务所 DLA Piper 公布了一份《通用数据保护条例》（GDPR）罚款和数据违规报告。在罚款数额方面，报告显示，2018 年 5 月 25 日 GDPR 实施后，数据保护当局已经执行了 2.725 亿欧元的罚款，涉及欧盟 27 个成员国以及英国、挪威、冰岛和列支敦士登。其中，2020 年 1 月 28 日以来执行的罚款数额为 1.585 亿欧元。意大利监管机构累计罚款超过 6930 万欧元，位居榜首。德国和法国分列第二和第三，罚款总额分别为 6910 万欧元和 5440 万欧元。此外，在数据泄露事件数量上，报告显示，数据泄露事件共计 28.1 万起，其中德国(77747 起)、荷兰(66527 起)和英国(30536 起)向监管机构通报的数据泄露数量最多。

https://mp.weixin.qq.com/s/sZkOLciKdV71nGLpaL9i6w

2. 新型勒索软件对制造业网络造成严重影响

新型勒索软件在 2020 年严重扰乱了制造业，今年第三季度出现了一种令人不安的趋势，攻击者似乎在其勒索软件运营中把制造企业作为攻击目标。在过去几年里，**勒索软件**

的攻击者对他们的目标变得更加有选择性。他们已经开始摆脱大规模传播勒索软件垃圾广告的做法，开始采用一种被称为“大猎物搜寻”(big game hunting)的精准方法。勒索软件攻击者现在对大中型企业的攻击，每次都会获得很大的赔偿。对大中型企业的攻击更加复杂，需要更多的时间来观察、追踪和行动。这就是为什么大多数影响大型行业(如制造业)的勒索软件家族被称为“侵入后勒索软件（post-intrusion ransomware）”。简而言之，**攻击者在安装勒索软件之前就已经通过其他途径进入了网络**。

https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

3. 2020 年全球公开漏洞披露 730 起，超过 220 亿记录泄露

根据 Tenable 公司安全反应小组（SRT）的一份新报告，从 2020 年 1 月到 10 月，全球共有 730 起公开漏洞披露事件，导致超过 220 亿份记录被曝光。据分析，35%的入侵与勒索软件攻击有关，造成了重大的财务损失，而 14%的入侵是由于电子邮件泄露造成的。攻击者主要依赖未修补的漏洞，并将多个漏洞链接在一起。从 2015 年到 2020 年，报告的通用漏洞披露（cve）数量以 36.6%的平均年增长率增长。

https://www.cnbeta.com/articles/tech/1078495.htm

4. 中国地方政府数据开放报告（2020 下半年）发布

近日，由复旦大学数字与移动治理实验室出品的“2020 下半年中国开放数林指数”和《2020 下半年中国地方政府数据开放报告》正式发布。《中国地方政府数据开放报告》和“中国开放数林指数”是我国首个专注于评估政府数据开放水平的专业指数和报告，由复旦大学数字与移动治理实验室制作，复旦大学和国家信息中心数字中国研究院联合发布。

https://mp.weixin.qq.com/s/9z4FL4ROsr1a1suz2o7-Fw

5. 有关构建政务信息系统密码应用管理体系的建议

随着《中华人民共和国密码法》的出台，我国对密码应用从顶层做出了战略部署和高度要求。各政务部门在开展密码应用工作过程中，普遍存在密码管理职能分工不明确的问题。为研究解决此问题，梳理汇总当前国家法律法规和标准规范明确的密码政策要求，分析政务密码体系架构，总结电子政务典型密码应用，围绕业务应用部门、安全管理部门、认证服务方、密码管理部门四个角色，提出一套基于**需求分析、设施建设、电子认证、密码管理和监督**的政务密码应用管理体系。

https://mp.weixin.qq.com/s/IEDxw9r-2BeHSZzYtx8A2A

6. 区块链技术视野下的数据权属问题

区块链中的数据权属问题仅指用户上链别数据即事务数据、实体数据和合约数据的归属。应区分公有链、联盟链和私有链，分别研究各自的数据权属。公有链中，因不存在中心式数据控制者，也无收集处理数据的行为，任何节点或用户对于共有链上记载的非自己上传的数据均不享有民事权益。联盟链和私有链中，参与成员可对数据的权属与利用进行约定。区块链上的政务数据归国家所有。

https://mp.weixin.qq.com/s/d_rdKGjGsZpo9SMwDFcXmA

7. 供应链安全管理

供应链就是以合适的价格、地点和时间为顾客提供他们需要的资源。对正在交付的产品或服务的完整性、正在交换的数据的隐私性以及相关交易的完整性的任何中断和风险都可能造成破坏性的运营、财务和品牌影响。来自内部人员或攻击者的数据泄露、勒索软件攻击和恶意活动可能发生在供应链的任意环节。即使是本地化到单个供应商或第三方供应商的安全事件，也可能严重扰乱计划、制定和交付过程。供应链的强大程度取决于其最脆弱的实体。**供应链安全管理**

主要涉及五个方面：数据保护、数据本地化、数据可见性及治理、欺诈预防、第三方风险。

https://mp.weixin.qq.com/s?__biz=MjM5NjA0NjgyMA==&mid=2651112340&idx=1&sn=135edcfb07db65068b81a111c31ba9c7