[公开]360NELab-DST-0-036-20210329

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 36 期 2021 年第 12 期

（2020.03.22-2021.03.28）

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**数据丢失泄露**和**勒索软件**问题。

1. Zoom 的屏幕共享功能泄露用户敏感信息
2. 能源巨头 Shell 披露由 Accelion 造成的数据泄露
3. 在线交易经纪商 FBS 泄露 20TB 数据 160 亿条记录
4. 以色列最严重数据泄露事件：650 万选民信息曝光
5. 3000 万美国人受到 Astoria 公司数据泄露的影响
6. 大数据黑市交易：平均每人至少有 4 条信息泄露
7. 迈阿密大学科罗拉多州的数据被勒索团队泄露
8. 加拿大无线通信设备制造商遭勒索攻击

此外，在数据安全技术与观点方面主要讨论了：

1. 国家网信办等四部门规定 App 必要个人信息范围
2. 实现全密文计算的主流技术与现实挑战
3. 全球主要国家和地区数字政策及其战略考量
4. 大数据黑市调查：寄生的千亿“产业链”
5. 央视 3·15 晚会，“个人隐私”合规引发行业思考
6. 智能汽车如何保障数据安全
7. 数字人民币的可控匿名及交易安全
8. 美国拜登政府网络政策前瞻

全球动态

1. Zoom 的屏幕共享功能泄露用户敏感信息

2021 年 3 月 22 日，据外媒报道，Zoom 的屏幕共享功能中的一个漏洞暴露了演示者屏幕中他们不希望共享的部分，这可能会泄漏电子邮件或密码。

https://threatpost.com/zoom-glitch-leaks-data/164876/

2. 能源巨头 Shell 披露由 Accelion 造成的数据泄露

2021 年 3 月 22 日，据外媒报道，攻击者入侵了该公司由 Accellion 文件传输设备（FTA）提供支持的安全文件共享系统后，能源巨头 Shell 公司披露了数据泄露事件。据该公司称，在攻击过程中访问的某些数据属于利益相关者和 Shell 子公司。

https://www.bleepingcomputer.com/news/security/energy-giant-shell-discloses-data-breach-after-accellion-hack/

3. 在线交易经纪商 FBS 泄露 20TB 数据 160 亿条记录

2021 年 3 月 25 日，据外媒报道，安全研究人员团队发现了著名的在线交易经纪商 FBS 公开的近 20TB 大量数据，其中包括超过 160 亿条记录。泄漏的数据还包括未编辑的信

用卡和全球数百万用户的护照。

https://www.hackread.com/online-trading-broker-fbs-exposes-data/

4. 以色列最严重数据泄露事件：650 万选民信息全部曝光

2021 年 3 月 25 日报道，距离总统大选不到 24 小时，超过 650 万以色列选民的个人身份与登记信息却遭到黑客公开泄露。根据目前的情况看，问题出在软件厂商 Elector Software 为以色列利库德党开发的投票应用 Elector 身上。此次外泄的数据包括登记选民的住址、电话号码和出生日期。

https://www.secrss.com/articles/30070

5. 3000 万美国人受到 Astoria 公司数据泄露的影响

2021 年 3 月 25 日，研究人员发现在 DarK Web 中有 3000 万记录受 Astoria 公司数据泄露影响的美国人的记录。Astoria 是一家领先的公司，它利用网站网络来收集有关可能正在寻找折扣汽车贷款，其他医疗保险甚至发薪日贷款人的信息。

https://securityaffairs.co/wordpress/115934/breaking-news/astoria-company-data-leak.html

6. 大数据黑市交易触目惊心：平均每人至少有 4 条个人信息泄露

2021 年 3 月 24 日，据不完全统计，国内个人信息泄露数达 55.3 亿条左右。平均算下来，每个人就有 4 条相关的个人信息泄露，车辆、房产、地址、职业、年龄、电话号码、身份证信息等在黑市上频繁流动。

https://www.cnbeta.com/articles/tech/1105601.htm

7. 勒索软件团伙泄露从迈阿密大学科罗拉多州窃取的数据

2021 年 3 月 23 日报道，Clop 勒索软件团伙在网上发布了科罗拉多大学和迈阿密大学窃取的文件的屏幕截图，包括大学财务文件，学生成绩，学业成绩，入学信息和学生传记信息。据称，威胁参与者是通过 Accellion FTA 漏洞窃取了数据。

https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-colorado-miami-universities/

8. 加拿大无线通信设备制造商 Sierra Wireless 遭勒索攻击，工厂中断生产

2021 年 3 月 23 日消息，加拿大无线通信设备制造商 Sierra Wireless 今天披露了遭受勒索软件攻击，勒索软件对

Sierra 的内部 IT 网络进行了加密，从而阻止员工访问与制造和计划相关的内部文档和系统，迫使其停止了所有生产基地的生产。

https://www.bleepingcomputer.com/news/security/ransomware-attack-shuts-down-sierra-wireless-iot-maker/

业界观点

1. 国家网信办等四部门发文规定 App 必要个人信息范围

近日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《规定》），旨在落实《中华人民共和国网络安全法》关于个人信息收集合法、正当、必要的原则，规范移动互联网应用程序（App）个人信息收集行为，保障公民个人信息安全。

《规定》明确了地图导航、网络约车、即时通信、网络购物等 39 类常见类型移动应用程序必要个人信息范围，要求其运营者不得因用户不同意提供非必要个人信息，而拒绝用户使用 App 基本功能服务。

https://mp.weixin.qq.com/s/_7WPqPwVhUufitQWPSgceQ

2. 实现全密文计算的主流技术与现实挑战

在数据即黄金的时代，从数据里挖掘价值实现价值共享，是时代和科技发展赋予的新使命。然而，价值共享是以不侵犯数据隐私的数据分析为前提的，而计算是数据分析的主要手段。

世界上没有绝对安全的系统，安全在攻防博弈中进展。

随着效率提升的安全多方计算、全同态加密等密码协议的深入研究，泄露减少的可信硬件方案的持续推进，全密文计算时代早晚会到来。

https://www.secrss.com/articles/29077

3. 全球主要国家和地区数字政策及其战略考量

新科技革命促使数字技术、数字经济领域产生大量规则空白。传统国际机制在回应数字经济治理需求中遇到阻力，新规则新秩序处于建构期。世界主要国家和地区为应对数字全球化的机遇与挑战，积极出台数字政策，并深深打上本国政治经济的烙印。未来全球数字治理将更加直面开放与保守、多边与孤立、发展与安全的权衡与博弈，对数字经济政策、进程和影响产生深刻影响。

https://mp.weixin.qq.com/s/JRzXgjv_xvt1rI4cYnokfw

4. 大数据黑市调查：内鬼、黑客、清洗者、料商、买家等寄生的千亿“产业链”

黑市数据交易利益链已经可以清晰的划分为四级，第一级黑客或内鬼、高精深网络软件盗取公民个人信息；第二级盗取的公民个人信息进入料商手中，料商建立自己的信息数据库；第三级，是料商不断发展代理商，将数据进行倒卖；

第四级就是信息使用者，也就是数据终极流向买家手中，他们拿到信息后，进行电话营销或实施电信诈骗。

https://mp.weixin.qq.com/s/6qcv1yk88RSktpkvpD2m6w

5. 央视 3·15 晚会上曝光网络安全问题，“个人隐私”合规引发行业思考

今年央视3.15晚会上曝出多起涉及“个人隐私”问题的网络安全事件，一改往日将关注重点**转向了网络安全问题的“个人隐私”问题**。特别是随着信息技术的高速发展，人类的生活也发生了颠覆式的变化。5G 技术、AI 技术则加速了各行各业智能化发展，推动了全球智慧城市建设的步伐。然而科学技术是一把双刃剑，本次“315 晚会”就是科技对各行业健康发展发起的“警钟”。当然，随着法律法规的完善，安全技术的升级，相关部门也必须及时亮剑，打破其侥幸心理，让互联网信息受到真正保护，保障数字经济行稳致远。

今年是“十四五”开局之年，构建“双循环”新发展格局将迈出第一步。**构建新发展格局，网络安全中的“个人隐私”保护同样是重要环节，只有让老百姓安心放心消费，市场循环才可能真正畅通起来。**

https://mp.weixin.qq.com/s/EDrQJeBKXJOJks0G_40YSw

6. 从特斯拉上海工厂摄像头被入侵，谈智能汽车如何保障数据安全

3 月 10 日，针对特斯拉上海工厂摄像头被黑客入侵，特斯拉回应称，目前已经停止了这些摄像头的联网，并进一步提升各环节的安全把控。在汽车智能化时代，可从以下几点做好数据安全：**第一：提升信息安全意识；第二：系统与软件开发不能完全交给第三方；第三：要采用国家级的工业云服务器作为备份。**

https://www.163.com/dy/article/G4QCN7GR0527L1KT.html

7. 数字人民币的可控匿名及交易安全

数字人民币是数字形式的法定货币，可控匿名是数字人民币的重要特征。可控匿名的第一层含义，是匿名，就是要满足合理的匿名支付和隐私保护的需求；第二层含义，是可控，在保护合理匿名需求同时，也要保持对犯罪行为的打击能力。数字人民币将采取“小额匿名、大额可溯”的设计，一方面体现了其 M0（流通中的货币）的定位，保障公众合理的匿名交易和个人信息保护的需求；另一方面，也是防控和打击洗钱、恐怖融资、逃税等违法犯罪行为，维护金融安全的客观需要。同时数字人民币钱包采用了分级分类的设计，根据 KYC（认识你的客户）程度的不同开立不同级别的数字

钱包，满足公众不同的支付需求。钱包余额和支付限额会随着 KYC 强度的增强而提高。这样可满足公众合理的隐私保护需求，有效防范大额可疑交易风险。

https://mp.weixin.qq.com/s/-f9DoY0l1Vfr3IbHDolyfg

8. 美国拜登政府网络政策前瞻

拜登政府出台网络战略和政策文件，可能尚需时日。现在，可从其既往的发言和声明中大体上管窥其网络政策的要点。**加大对网络基础设施和人才的投资**。这是加强网络能力建设的务实举措，具有实质性意义。目前来看，拜登有意加大在网络基础设施建设和人才培养方面的投入，将是夯实美国网络实力的务实举措。**加强与私营部门、学术界和公民社会的伙伴关系**。美国往届政府都强调在网络安全领域建立公私伙伴关系（PPP），注重发挥“多利益攸关方”的作用。**继续致力于网络空间国际规则的制定**。2020 年初，拜登在《外交》杂志发表了题为《为何美国必须再次发挥领导作用——拯救特朗普之后的美国外交政策》的文章，阐述了其外交政策的基本思路。可见，在网络空间国际规则制定方面的大国博弈仍将继续。

https://www.secrss.com/articles/30131