[公开]360NELab-DST-0-017-20201109

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 17 期 2020 年第 17 期

（2020.11.02-2020.11.08）

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**数据泄露、勒索软件**以及**政府对数据安全采取的措施**。

Github 的源代码在 Github 上泄露

酒店预订平台泄露数百万用户数据

数百万瑞典公民信息被泄露给 Google、Facebook 等巨头

黑客泄露价值 5.22GB 的 Mashable.com 数据库

560GB 的育碧《看门狗：军团》源代码泄露

2000 万个 Bigbasket 用户数据在暗网泄露

2020 年数据泄露数量突破 360 亿条

意大利酒商 Campari Group 遭勒索 1500 万美元

巴西最高法院遭勒索攻击，备份文件被加密

新加坡重新修订数据保护法

此外，在数据安全技术与观点方面主要讨论了：

美国大选与数据安全立法；《个人信息保护法（草案）》解读；安全防护体系建设；政府数字化转型；零信任架构；新基建与数据安全；量子计算与隐私；数据安全理念的“分、放、管、服”。

全球动态

1. 意大利酒商 Campari Group 遭勒索，被要挟 1500 万美元

2020 年 11 月 8 日报道，知名的意大利酒商 Campari Group（金巴利）本周对外公告，该公司在 11 月 1 日遭到黑客攻击，Campari 并未说明攻击细节，但 BleepingComputer 与 ZDNet 相继引用资安研究人员 Pancak3 所提供的证据，指称 Campari 感染了 Ragnar Locker 勒索软件，而且黑客提出高达 1,500 万美元的赎金请求。

http://www.safebase.cn/article-261827-1.html

2. Github 的源代码在 Github 上泄露

2020 年 11 月 5 日报道，开发人员和隐私权主义者 Resynth1943 宣布 GitHub 本身的 GitHub 源代码泄漏到 GitHub 自己的 DMCA 存储库中。

https://www.de24.news/2020/11/githubs-source-code-leaked-on-github-last-night-kind-of.html

3. 酒店预订平台泄露了数百万的用户数据

2020年11月9日报道，西班牙巴塞罗那一家名为 Prestige Software 的软件公司被发现暴露了全球数百万客户的敏感、

隐私和财务数据。尤其是来自 Booking.com、Expedia、Agoda、Amadeus、Hotels.com、Hotelbeds、Omnibees、Sabre 等几家公司的客户都是此次数据泄露事件的意外受害者。

https://www.hackread.com/hotel-reservation-platform-data-leak-online-booking-sites/

4. 巴西最高法院遭勒索软件攻击，文件备份被加密

2020 年 11 月 6 日报道，巴西高等法院（STJ）的网络基础设施遭受了大规模的勒索软件攻击，结果，其包括官方网站在内的服务被迫下线。勒索软件攻击发生在本周的星期一至星期二之间，但其细节仅在今天早些时候才披露。勒索软件运营商声称，整个 STJ 数据库已被加密，任何还原文件的尝试都是徒劳的。

https://www.hackread.com/ransomware-attack-brazil-top-court-encrypts-backups/

5. Folksam 证实百万瑞典公民信息泄露给 Google、Facebook 等巨头

根据知情人士透露的最新消息，当地时间 2020 年 11 月 03 日，瑞典最大的保险公司 Folksam 经证实，已将其大约一百万瑞典公民的客户个人信息泄露给了 Google 和 Facebook

等多家社交媒体以及技术巨头。众所周知，Folksam 是瑞典地区最大的保险公司之一，但是它们在跟多家技术巨头共享了旗下客户的个人信息之后，便引发了此次影响一百多万瑞典公民个人信息安全的数据泄露事件。

https://www.anquanke.com/post/id/221732

6. ShinyHunters 黑客泄露了价值 5.22GB 的 Mashable.com 数据库

2020 年 11 月 5 日报道，这次，臭名昭著的黑客通过 ShinyHunter 的在线手柄进行攻击，泄露了属于 Mashable.com（一家全球媒体和娱乐公司）的数据库。该价值 5.22GB 的数据库今天在一个著名的黑客论坛上被泄露。可以确认，该数据库现在包括俄语在内的其他多个论坛上都可用。

https://www.hackread.com/shinyhunters-hacker-leaks-mashable-database/

7. 2020 年数据泄露数量突破 360 亿条

2020 年 11 月 3 日，据外媒报道，根据风险基础安全（Risk Based Security）的数据，2020 年第三季度公开报告的数据泄露事件的数量有所下降，但全球另有数十亿条记录被暴露，使得今年的总数达到 360 亿。这些数据不仅包括窃取的数据，

还包括基于云的错误配置，这些错误配置可能危及信息，但不会导致恶意行为者获取信息。

https://mp.weixin.qq.com/s/6Ae1sgOH5Dsfanpu0t61sw

8. 560GB 育碧《看门狗：军团》源码泄漏

2020 年 11 月 5 日报道，勒索软件组织 Egregor 对外声称成功入侵了育碧和 Crytek 两大游戏公司，获得了包括《看门狗：军团》源代码在内的诸多内部内容。今天，该组织正式发布了这款游戏的源代码，并在多个专用追踪器上放出了下载链接，源代码大小为 560 GB。。

https://hot.cnbeta.com/articles/game/1049469.htm

9. 新加坡重新修订数据保护法 出于合法目的的商业活动将无需用户同意

2020 年 11 月 2 日报道，新加坡已经更新了其《个人数据保护法》（Personal Data Protection Act，PDPA），允许本地企业在未经事先同意的情况下就出于某些目的（例如业务改进和研究）使用消费者数据。同时修正案还规定对数据泄露处以更严厉的罚款，最高罚款可以高于先前的 100 万新加坡元。

https://www.zdnet.com/article/singapore-updates-data-protectio

n-law-to-exclude-user-consent-for-legitimate-business-purposes/

10.2000 万个 Bigbasket 用户的数据在暗网上泄露

2020 年 11 月 7 日，据外媒报道，印度著名的在线杂货店 Bigbasket 遭到了数据泄露，其中有超过 2000 万人的数据在暗网上泄露，档案大小为 15 GB，售价超过 40,000 美元。BigBasket 由阿里巴巴集团，Mirae Asset-Naver 亚洲成长基金和 CDC 集团共同创立。

https://securityaffairs.co/wordpress/110543/data-breach/bigbasket-details-dark-web.html

业界观点

1. 美国大选将改变美国隐私与数据安全立法走向

与大多数国家不同的是，美国目前为止并没有一部广泛适用的数据隐私法。虽然两党都有制定数据隐私法的动机，但这些关键性的差异尚无法弥合，因而阻止了这项立法的通过——这是为何大选结果将决定美国隐私立法命运的原因。

如果白宫和参议院由不同政党控制：联邦隐私法案仍有可能通过，但会由于两党之争而进一步被推迟到 2023 年年初。此外，关键条款将经过更为激烈的谈判才能获得通过。

如果拜登获胜且民主党控制了参议院：联邦隐私法很可能会通过，不过需要等到 2022 年两年国会会议的后半程才能最终通过。

如果特朗普连任且共和党继续控制参议院：这项法案同样可能会在 2021 年 1 月开始的本届国会的后半段通过。

https://www.secrss.com/articles/26808

2. 《个人信息保护法（草案）》的立法思考

《个人信息保护法（草案）》更加侧重对个体个人信息权益的保障。与《数据安全法》《网络安全法》更加侧重国家安全与公共安全不同，《个人信息保护法（草案）更加侧

重对个体个人信息权益的保障。例如草案确立的以个人“知情—同意”为核心的数据处理规则。专章规定的个人权利，对应的个人信息处理义务章节也是以落实个人信息权益为导向。采用了民法典“个人信息处理”的概念，遵循了民法典确定的信息处理者管理思路。从这一角度看，可以说，《个人信息保护法（草案）》是以《民法典》所确立的个人信息民事权益为基础，从国家监管角度，用公权力细化、落实个人信息民事合法权益的保障法。

个人信息保护法（草案）》的中国特色：第一，个人信息处理者监管思路。第二，数据本地化和跨境。

相关思考建议：第一，需要细化考虑与《网络安全法》《数据安全法》的衔接问题。第二，和民事立法的协调问题和民事规则的创新问题。

https://www.secrss.com/articles/26789

3. 实战化背景下的安全防护能力体系建设思路

结合常见的攻击方式，防守方应当具备如下防御能力，对现有的网络安全保障体系加以补充和完善，

(1) 防微杜渐：防范被踩点

(2) 收缩战线：收敛攻击面

(3) 纵深防御：立体防渗透

(4) 守护核心：找到关键点

(5) 洞若观火：全方位监控

https://www.secrss.com/articles/26786

4. 国外政府数字化转型战略研究及启示

国外政府数字化转型战略的提出表明数字政府建设进入“深水区”，在认知与战略、数据与服务、能力与保障等方面面临着新挑战；各国战略内容总体上“大同小异”；国外战略在数字化项目投资评估与采购改革，数字服务等关键基础标准与绩效指标建立，**隐私保护准则制定及嵌入服务与数据治理全过程，鼓励政府数据开放，提升公务员数字能力**等方面为我国提供了有益经验。

https://www.secrss.com/articles/26829

5. 亚太地区零信任采纳开始加速

全球新冠肺炎疫情加速云迁移和远程办公，同时，公司企业正努力应对快速更新的监管规定和消费者施加的数据隐私压力。各种趋势作用下，亚太地区的企业主管必须采取新的安全方法，加速零信任采纳。现在正是拥抱零信任的好时机，可以向全球同行和其他已踏上零信任旅途的人取经。

https://mp.weixin.qq.com/s/lXB8C7a2DCmu_95zEiCXNw

6. 新基建时代，数据安全是底线

新基建时代，云、5G、物联网、大数据、智慧城市等技术应用于各业务场景中，多元技术的融合将成为新基建下主要生产工具，数据作为主要的生产资料，对于用户来说是金矿，若没有利用好数据，它将变成手铐，所以说**数据安全是底线**。与传统的基建不同，新基建有几个特点：数据化、网格化、智能化，在新基建的建设过程中可能会带来一些安全挑战：包括数据的访问权限控制、数据的保密性、数据防篡改、数据全生命周期溯源等影响业务发展，所以在数据安全上要求有高品质的适配、灵活拓展性、高可靠性、先进的数据治理技术，保障数据全生命周期的安全。

https://mp.weixin.qq.com/s/qx6cSDZkN9vHVE3Z_qApWw

7. 量子计算对个人隐私和社会秘密的威胁

随着量子计算技术的发展，人们对传统加密措施在量子计算面前的安全性产生了疑虑。大型量子计算机可能迅速破解一定规模之下的 RSA 算法和其他基于大数分解和离散对数困难性的密码算法，同时所有基于攻击者计算复杂性假设而构造的密码算法的安全性也将大大降低。目前，秘密信息、个人隐私等重要数据都在传统密码技术的保护下进行传输

和保存。对有特定目的的攻击者来说，即便现在没有具体的攻击能力，但他们可以先窃取并保存此类加密信息，等量子计算机发展成熟后，再对其进行破译。故而，量子计算对网络安全的威胁是长远的。另一方面，量子密码为提升信息安全保障能力提供了新思路。已经出现将量子特性用于构造信息加密算法的技术，主要是量子密码和后量子密码。

https://mp.weixin.qq.com/s/Ck3nF9J0bhgKGVBh9tL_GA

8. 数据安全理念之“分•放•管•服”

数据安全需在对数据资产进行分类分级的基础上才能有效地开展数据保护工作。数据实现价值的流动过程中，需要根据相应的制度、合规要求，实现对人的权限、职责、访问对象等的划“分”。“放”的含义是指数据的流动与应用，而“管”则是指保障数据的安全。高效的数据应用给机构带来巨大的业务价值，但如果没有数据安全的保障，机构则时刻面临着巨大的运营风险，两者之间需要动态平衡。同时，安全能力的实现，不仅需要顶层的规划设计，还需要安全工具的合理运用，以及长期可持续的安全运营，而这一切都需要安全“服”务的保障。

https://mp.weixin.qq.com/s/Ck3nF9J0bhgKGVBh9tL_GA