[公开]360NELab-DST-0-018-20201116

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 18 期 2020 年第 18 期

（2020.11.09-2020.11.15）

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**（恶意攻击或操作不当倒是泄露等）和**勒索软件**。

1. 少年黑客（高中生）窃取上亿条公民信息
2. Vertafor 泄露了 2770 万德克萨斯州驾驶员的数据
3. 在线游乐场 Animal Jam 遭受了数据泄露
4. 123RF 数百万条数据在暗网销售
5. ShinyHunters 入侵 Pluto TV 服务，暴露 320 万帐户
6. 580 万条 RedDoorz 用户记录在暗网上出售
7. 疫情期间美国医院成为黑客攻击的重灾区
8. IoT 成为勒索软件攻击的新突破口
9. 黑客滥用脸书公开勒索攻击，迫使受害者支付赎金
10. 笔记本电脑制造商仁宝被勒索攻击，赎金$1700 万

此外，在数据安全技术与观点方面主要讨论了：

区块链金融；强密码规则的局限；欧盟与我国的数据跨境传输；针对加密流量的攻击；英国的网络安全态势；数据本地化。

全球动态

1. 高中生窃取上亿条公民个人信息，“少年黑客”赔偿并公开道歉

2020 年 11 月 14 日报道，在 2018 年 6 月到 7 月的短短一个月时间里，小文就通过自编软件非法获取了约 1 亿条公民个人信息，全部存储于数据库中。小文为了存储获取到的“海量”公民个人信息，专门在境外租用十多台服务器。为了不让其他人发现漏洞，在获取了海量公民个人信息后，小文向百度公司反馈，将网站存在的漏洞进行封堵。此后，小文在通过微信、QQ 群及境外聊天工具，向他人兜售获取到的公民个人信息，其中部分交易以比特币为交易货币，共计获利约人民币 2 万元。

今年 10 月，在法院的主持下，双方达成调解协议，“鉴于小文作案时还未成年，案发后充分认识到自己的过错，并且已经承担了相应的民事责任，以调解结案的方式可以节约司法资源，达到更好的社会效果。”该案承办检察官何浦说。

http://www.safebase.cn/article-261858-1.html

2. Vertafore 数据泄露暴露了 2770 万德克萨斯州驾驶员的数据

2020 年 11 月 13 日，Vertafore 宣布由于人为错误，意外暴露了 2770 万德克萨斯州驾驶员的信息。公开的数据包括得克萨斯州驾驶执照号码，姓名，出生日期，地址和车辆登记历史。

https://securityaffairs.co/wordpress/110848/data-breach/vertafore-data-breach.html

3. 在线游乐场 Animal Jam 遭受了数据泄露

2020 年 11 月 11 日，广受欢迎的儿童在线游乐场 Animal Jam 遭受了数据泄露，两个被盗数据库分别名为“game_accounts”和“users”，其中包含大约 4,600 万个被盗用户记录。

https://www.bleepingcomputer.com/news/security/animal-jam-kids-virtual-world-hit-by-data-breach-impacts-46m-accounts/

4. 123RF 数百万条数据在暗网销售

2020 年 11 月 12 日，在黑客开始在黑客论坛上出售包含 830 万用户记录的数据库之后，照片图片网站 123RF 遭受了数据泄露。从 BleepingComputer 看到的数据库样本中，窃取

的数据包括 123RF 成员的全名、电子邮件地址、MD5 哈希密码、公司名称、电话号码、地址、PayPal 电子邮件和 IP 地址。

https://www.bleepingcomputer.com/news/security/popular-stock-photo-service-hit-by-data-breach-83m-records-for-sale/

5. ShinyHunters 入侵 Pluto TV 服务，暴露了 320 万个用户帐户

2020 年 11 月 14 日，一名黑客在一个黑客论坛上免费共享了 320 万个 Pluto TV 用户帐户，并声称这些帐户被 ShinyHunters 威胁者偷走了。数据库样本包含成员的名称、电子邮件地址、bcrypt 哈希密码、生日、设备平台和 IP 地址。

https://securityaffairs.co/wordpress/110931/data-breach/pluto-tv-database-shinyhunters.html

6. 580 万条 RedDoorz 用户记录在暗网上出售

2020 年 11 月 10 日报道，在 9 月 RedDoorz 遭受了未授权访问导致的数据泄露之后，现在攻击者正在黑客论坛上出售其数据库，其中包含 580 万条用户记录。RedDoorz 是位于新加坡的酒店管理和预订平台，在整个东南亚拥有 1,000 多家酒店。

https://www.bleepingcomputer.com/news/security/58-million-reddoorz-user-records-for-sale-on-hacking-forum/

7. 疫情期间美国医院成为黑客攻击的重灾区

2020 年 11 月 12 日报道，今年秋季，美国医院在经受新冠疫情的严重考验之外还成为了网络攻击者重点针对的目标。目前已知的重大攻击事件中，包括由数百家医院组成的连锁机构 Universal Health Services 等等。此外还有一个自称是 UNC1878 的黑客组织发起的攻击威胁到了美国数百家个人医疗机构。

https://www.cnbeta.com/articles/tech/1052415.htm

8. IoT 成为勒索软件攻击的新突破口

2020 年 11 月 13 日报道，随着越来越多的企业依靠物联网设备来采集数据，物联网设备为黑客提供了进入企业网络的通道。根据 SonicWall 安全研究人员近日发布的 2020 年第三季度威胁情报，物联网攻击数量增加了 30%，勒索软件攻击数量激增了 40%，而恶意软件总量下降了 39%。企业在享受 IoT 设备带来的便利的同时，也应采取相应措施保护硬件设备及网络免受日益复杂的勒索软件攻击。

https://www.secrss.com/articles/27018

9. 黑客滥用脸书广告公开勒索软件攻击事件，迫使受害者支付赎金

2020 年 11 月 14 日报道，黑客为了能让勒索软件攻击的效益更好，这 2、3 年来不仅纷纷将目标转向企业，也要胁不付钱就公开被加密的机密资料，希望受害者会支付赎金，但近期却出现黑客为了要赎金，挟持他人的脸书账号来投放广告，要求遭到勒索软件攻击的企业限期付款的情况。

http://www.safebase.cn/article-261859-1.html

10.笔记本电脑制造商仁宝遭到勒索软件袭击，被索要 1700 万美元

2020 年 11 月 9 日，中国台湾省笔记本电脑制造商仁宝电脑遭受了 DoppelPaymer 勒索软件攻击，攻击者要求将近 1700 万美元的赎金。

https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/

业界观点

1. 区块链金融网络安全的风险与应对思路新探

区块链技术的应用未来将非常广泛，其大致可以分为三个阶段：

(1) 在加密数字货币及金融领域的集中应用，以比特币和各种通证经济的创生与支付为代表；

(2) 以智能合约为代表，在其它金融领域的运用，如跨境支付、期权凭证或数字资产通证化等；

(3) 区块链应用逐步拓展到非金融领域，即国家当前正大力推广的区块链＋产业融合，诸如区块链＋教育、养老、精准扶贫、医疗健康、社会保障等。

目前，区块链技术的应用正处于第二阶段与第三阶段的过渡时期，特别是在金融领域，一方面产生了许多运用，比如高效的跨境支付，数字资产及其衍生品交易等等，甚至为少部分投资者提供了暴富的机会，另一方面亦存在着诸多巨大的风险隐患，不容忽视。

https://www.secvery.com/3826.html

2. 卡内基梅隆大学研究人员发现强密码规则不起作用

当用户为一个新账户创建密码时，可能会被要求使用大

写字母，数字和特殊字符，让黑客更难以破解密码。然而，卡内基梅隆大学的研究人员表示，这些要求并不能让你的密码变得更强，创建和记忆安全密码的最佳方法是使用密码管理器。

https://www.cnbeta.com/articles/tech/1052695.htm

3. 欧盟国际数据传输新规挑战我国数据报送制度

在欧盟法院于 7 月作出 Schrems II 案件判决后，能否以及如何通过“标准合同条款”(SCCs)向欧盟以外国家传输个人数据，成为悬而未决但又亟待解决的问题。一旦上述草案生效，欧盟向我国基于“标准合同条款”(SCCs)的数据传输必将面临重大挑战，这是因为，我国企业向政府报送个人数据的实践恐难满足上述欧盟“重要保障”的要求。

在现有制度架构下，我国政府机关调取企业数据的措施与欧盟要求相去甚远。在《个人信息保护法》制定的关键时期，建议增加相应条款，确立报送数据的合法性原则、比例原则、保密性原则、正当程序原则以及相关法定程序，并通过统一的监管机构为个体提供充分、顺畅的救济渠道。这不但便于我国与欧盟之间的数据传输，更有助于提升我国个人信息保障水平，最终增进人民的福祉。

https://www.secrss.com/articles/27036

4. 未来五年对加密流量的攻击将增长 260%

根据 Zscaler 的新威胁研究报告，未来五年，针对绕过传统安全控制的加密流量（SSL）的攻击将增长 260%。他们表明，网络犯罪分子不会因全球健康危机而受到劝阻，因此他们将目标对准了医疗行业。继医疗保健之后，研究发现受到基于 SSL 的威胁攻击的行业主要是: 医疗: 16 亿(25.5%)、金融和保险: 12 亿（18.3%）、制造业: 11 亿（17.4%）、政府: 9.52 亿（14.3%）、服务: 7.3 亿（13.8%）。

https://www.secrss.com/articles/26973

5. 英政府 2020 网络安全年报: 1/3 攻击活动与新冠病毒有关

英国政府通讯部（GCHQ）下辖部门国家网络安全中心（NCSC）的 2020 年度报告显示，过去一年当中，NCSC 协助处理了涉及 1200 名受害者的共计 723 次网络攻击，其中 200 起与新冠病毒有关，几乎占上报事件总数的三分之一。随着网络攻击在强度与针对性方面的不断提升，NCSC 在今年处理的勒索软件攻击数量也达到去年的 3 倍。

https://www.secrss.com/articles/26875

6. 数据本地化：一种基于有限理性的数据防御主义

面对全球信息技术强弱不均的国家实力结构以及数据往往向强势国家流动的现状，一个国家会采取以守住对自有数据控制权的方式确保自身安全。但决策的有限理性让一个国家在数据跨境流动政策的选择上追求“满意”而不是“最优”目标，一个处于相对竞争劣势的国家更有可能采取防御型互联网治理政策，表现为强烈的网络主权立场，并诉诸数据主权的话语工具。中国未来需要结合国际形势的变化逐步去除消极防御主义色彩，积极建立一种**以效率发展为路径**的跨境数据有序自由流动秩序。

https://www.secrss.com/articles/27044