[公开]360BEST-DST-0-012-20200928

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 12 期 2020 年第 12 期

（2020.9.21-2020.9.27）

大数据协同安全技术国家工程实验室

全球动态

1. 印度 Covid-19 监视工具泄露其北邦政府下辖的人口数据，百万数据

2020 年 9 月 22 日报道，由于缺乏数据安全协议，印度一个用于追踪 COVID-19 患者的监测平台的安全已受到威胁，这无意中使该平台的访问完全开放，并暴露了印度各地数百万人的数据。这款名为“北方邦 Covid-19 监测平台”的软件似乎是由印度北方邦地方政府开发的。然而，平台内部的漏洞使其很容易暴露在恶意黑客和攻击之下，这可能破坏北方邦对新冠病毒大流行的反应。

https://www.vpnmentor.com/blog/report-india-covid-leak/

2. 即时通讯应用，让数十亿用户面临隐私攻击

近日，安全研究人员发现一些主流的，甚至以隐私保护为卖点的即时通讯应用，包括 Whatsapp、Signal 和 Telegram 都存在重大的隐私泄露问题。根源在于，这些应用的“联系人发现服务”使用户可以根据通讯录中的电话号码查找联系人，同时也为隐私泄露敞开了大门。

https://zhuanlan.51cto.com/art/202009/626545.htm

3. 微软 Bing 爆出罕见数据泄露事件，涉及 6.5 TB 文件，包含 130 亿条搜索记录

2020 年 9 月 24 日报道，Bing 爆出汉奸的网络安全漏洞，公司员工使后端服务器暴漏在网上，有超过 6.5TB 的日志文件被曝光，其中包括来自 Bing 搜索引擎的 130 亿条记录。泄露的服务器被标识为 Elasticsearch 系统，是高级系统，公司在该系统中聚集大量数据，轻松搜索和过滤数十亿条记录。

https://segmentfault.com/a/1190000024569075

4. 美国网络安全与基础设施安全局 CISA 网站遭黑客入侵

2020 年 9 月 25 日，据彭博社报道，美国当局周四表示，在黑客使用有效的访问凭据后，一家未具名的美国联邦机构遭到了网络攻击。据美国网络安全与基础设施安全局(CISA)称，虽然未透露有关黑客的许多细节，但联邦当局确实泄露了黑客能够浏览目录，复制至少一个文件并泄露数据信息。

https://mp.weixin.qq.com/s?__biz=MzAxMjE3ODU3MQ==&mid=2650484526&idx=2&sn=60787087715c6f3c2c85229cc20d32ac

5. 加密货币交易所 KuCoin 遭攻击，1.5 亿美元货币被盗

2020 年 9 月 26 日，据报道，总部位于新加坡的加密货

币交易所 KuCoin 披露其遭到了网络攻击，价值 1.5 亿美元的货币被盗。该公司在声明中证实，一黑客入侵了其系统，并盗取了其热钱包中的所有资产，包括比特币、erc -20 代币以及其他类型的代币。根据用户追踪被盗资金的 Etherium 地址，目前估计损失最小为 1.5 亿美元。

https://www.zdnet.com/article/kucoin-cryptocurrency-exchange-hacked-for-150-million/

6. 攻击者窃取 54 万体育注册会员的数据备份

2020 年 9 月 20 日，2020 国家网络安全宣传周 App 个人信息保护主题发布活动在京召开。中央网信办、工信部、公安部、市场监管总局四部委以及 App 专项治理工作组在会上公布了今年以来 App 专项治理工作的有关进程。

https://www.zdnet.com/article/details-of-540000-sports-referees-taken-in-failed-ransomware-attack/

7. 美国健身连锁店 Town Sports 60 万用户数据泄漏

2020 年 9 月 23 日，美国健身连锁店 Town Sports 遭受数据泄露，该公司所属数据库中包含超过 60 万人的个人信息已在 Internet 上公开。公开的信息包括姓名、地址、电话号码、电子邮件地址、信用卡的后四位数字、信用卡的有效期

和会员的帐单记录。

https://securityaffairs.co/wordpress/108674/data-breach/town-sports-data-leak.html

8. 动视发生严重个人资料泄漏事件：超 50 万账号被曝光

据外媒 Dexerto 报道，可能有超过 50 万个动视账号被入侵，包括密码在内的登录凭证信息被泄漏。动视账户主要用于追踪《使命召唤》游戏的进度，以及包括《只狼：影逝二度》等其他动视游戏，并邀请更多玩家加入。

http://hackernews.cc/archives/32267

9. 日本最大移动运营商电子支付用户遭盗刷，金额超 1000 万日元

2020 年 9 月 22 日，日本最大的移动运营商 “都科摩”的电子支付系统被曝出接连发生多起盗刷事件，受害者大多数是在手机等移动终端下载了 “都科摩”的支付软件，然后与自己的银行账户绑定，目前，涉及银行 10 余家，累计盗刷金额超过 1000 万日元，约合人民币 64 万元。

https://finance.sina.com.cn/tech/2020-09-22/doc-iivhvpwy8181973.shtml

10.欧盟 2024 年前将引入加密数字货币资产制度

两份欧盟文件显示，欧盟将在四年内引入新的规则，通过使用区块链和类似“稳定币”(Stablecoin)这样的加密数字货币资产，让跨境支付更快、更便宜。目前，欧元区支付交易中有 78%使用的是现金。

https://www.cnbeta.com/articles/tech/1031095.htm

11.Microsoft Windows XP 源代码在线泄漏

2020 年 9 月 25 日报道，微软历史悠久的操作系统 Windows XP（据称仍可驱动全球所有笔记本电脑和台式机的 1%以上）其源代码与 Windows Server 2003 版本源代码被在线泄漏。几份报告表明，这些洪流文件的集合重达 43GB，据说还包含 Windows Server 2000 和一些 Microsoft 较旧的操作系统的源代码。泄漏者声称在过去几个月中已经编译了泄漏的 Microsoft 源代码的集合，还表示许多微软操作系统源代码文件已经在黑客之间私下传递了多年。

https://thehackernews.com/2020/09/windows-xp-source-code.html

业界观点

1. NIST 发布针对勒索软件的《数据完整性恢复指南》

近日，美国国家标准技术研究院（NIST）发布了主要针对勒索软件的《数据完整性恢复指南（SP）1800-11》，企业可利用该指南从勒索软件等破坏性恶意软件、内部攻击、员工错误中恢复数据完整性（包括电子邮件、员工记录、财务记录和客户的数据）。勒索软件是目前企业面对的最具破坏性的威胁之一。NIST（SP）1800-11 可以帮助组织制定从影响数据完整性的攻击中恢复的策略，恢复并维持运营并管理企业风险。

https://www.secrss.com/articles/25900

2. 大数据防“疫”实战，数据安全要“动静结合”

新冠疫情发生以来，我国利用各种信息手段收集患者、感染者、密切接触者乃至几乎每个人的信息，以追踪技术定位传染源并加以切断，从而有效地控制、减缓了病毒的传播。但是，这些“尽可能”被收集的数据也成为大家忧虑的问题。因此，在满足新冠肺炎疫情防控信息化的同时，要实现网络安全和个人隐私保护，必然离不开数据脱敏技术。

https://www.4hou.com/posts/2OZP

3. 福布斯：2021 年十大数字化转型趋势

9 月 21 日，福布斯网站发文分析 2021 年十大数字化转型趋势：5G、客户数据平台、混合云、网络安全、机密计算、无头科技、居家办公、人工智能、设备外形、量子计算。

https://www.secrss.com/articles/25833

4. 移动 App 在个人信息保护上需重点解决哪些问题

(1) 完整规范的隐私政策，让用户充分享有知情权

(2) 收集个人信息应遵循最小必要原则，并征得用户授权同意

(3) 规范个人信息的使用、委托处理、共享、转让和公开披露行为，与隐私政策的声明保持一致，能够让用户放心

(4) 用户具有对个人信息进行查询、更正、删除、注销账号等主体权利

https://mp.weixin.qq.com/s/-RX7ldKu7-BwAPNQVW8NnQ

5. 跨境电商中的数据安全问题

跨境电商领域的数据安全问题体现在以下几方面：

(1) **跨境电商平台环节的数据安全问题：**跨境电商平台企业在注册、购买和支付等环节掌握着大量的用户数据，而

平台的系统漏洞和数据保护权责不清晰，是造成电商平台信息泄露的重要原因；

(2) **跨境电商物流环节的数据安全问题：**主要风险体现在物流系统漏洞和物流单据的交易。物流单据的交易风险往往集中在那些管理松散的物流代理点；

(3)**跨境电商用户环节的数据安全问题：**在用户环节容易出现的数据安全的问题是木马病毒、钓鱼和账号被盗等。

https://www.secrss.com/articles/25825

6. 企业构建应对国际合作的数据安全治理原则建议

中国企业在推动数据安全治理方面开始发挥着重要作用。企业在数据安全治理方面可以努力做到以下四个方面的工作：

(1) 区分数据的不同属性是构建数据保护国际治理规范的核心问题；

(2) 建立“用技术解决技术带来的问题”的原则；

(3) 不同的企业必须针对自己的情况塑造合适的“技术中性”伦理观；

(4) 企业要多参与数据安全的国际讨论。

https://www.secrss.com/articles/25824

7. CNCERT 发布《2020 年上半年我国互联网网络安全监测数据分析报告》

本报告全面反映 2020 年上半年我国互联网在恶意程序传播、漏洞风险、DDoS 攻击、网站安全等方面的情况。

(1) 恶意程序

上半年，**发现智能设备恶意程序样本约 126 万余个**，其中大部分属于 Mirai 家族和 Gafgyt 家族，**占比超过 96.0%**。服务端传播源 IP 地址 5 万余个，我国境内疑似受感染智能设备 IP 地址数量约 92 万个。

(2) 漏洞风险

国家信息安全漏洞共享平台（CNVD）收录通用型安全漏洞 11,073 个，同比大幅增长 89.0%。其中，高危漏洞收录数量为 4,280 个（占 38.7%），同比大幅增长 108.3%，“零日”漏洞收录数量为 4,582 个（占 41.4%），同比大幅增长 80.7%。**2020 年上半年，CNVD 处置涉及政府机构、重要信息系统等网络安全漏洞事件近 1.5 万起。**

(3) DDoS 攻击

DDoS 攻击仍是互联网用户面临的最常见、影响较大的网络安全威胁之一。抽样监测发现，我国每日峰值流量超过 10Gbps 的大流量 DDoS 攻击事件数量约 220 起。

(4) 网站安全

监测发现针对我国境内网站仿冒页面约 1.9 万个。境内外约 1.8 万个 IP 地址对我国境内约 3.59 万个网站植入后门，我国境内被植入后门的网站数量较 2019 年上半年增长 36.9%。**我国境内遭篡改的网站有约 7.4 万个，其中被篡改的政府网站有 318 个。**

(5) 云平台安全

我国云平台网络安全威胁形势依然较为严峻。首先，发生在我国主流云平台上的各类网络安全事件数量占比仍然较高。其中**云平台上遭受 DDoS 攻击次数占境内目标被攻击次数的 76.1%、被植入后门链接数量占境内全部被植入后门链接数量的 90.3%、被篡改网页数量占境内被篡改网页数量的 93.2%。**其次，攻击者经常利用我国云平台发起网络攻击.

(6) 工控系统安全

监测发现暴露在互联网上的工业设备达 4,630 台，**境内工业控制系统的网络资产持续遭受来自境外的扫描嗅探，**日均超过 2 万次。经分析，嗅探行为源自于美国、英国、德国等境外 90 个国家，**目标涉及境内能源、制造、通信等重点行业的联网工业控制设备和系统。**CNVD、CVE、NVD 及 CNNVD 四大漏洞平台新增收录工业控制系统产品漏洞共计 323 个，其中高中危漏洞占比达 94.7%。

https://www.secrss.com/articles/25892