案例 | 网络安全应急响应典型案例（数据泄漏类）

来源：由数据安全域综合整理

数据泄露是一种安全违规行为，其中敏感、受保护或机密数据被未经授权的个人复制、传输、查看、窃取或使用。ISO/IEC 27040 将数据泄露定义为：导致意外或非法破坏、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的受保护数据的安全妥协。数据泄漏类型包括内部泄漏与外部泄漏两种。

一、内部泄漏 **1、内部人员窃密(主动泄密)**企业内部人员非法窃密，并将数据售卖给他人牟利。如客服人员、内部研发运维人员、数据运营人员等，通过自身权限获取企业数据以转售。

2、终端木马窃取企业内部人员的办公终端被植入木马，造成数据被窃取。如员工在办公终端.上插入来历不明的 U 盘，使用非正规渠道下载的盗版软件，单击钓鱼邮件的诱导内容等，导致终端被控制，造成数据泄露。

3、基础支撑平台泄露部署在企业内部的基础支撑平台，如包含企业敏感数据的 ES 平台、Redis 缓存数据库、数据仓库等基础平台，因被攻击，而导致数据泄露。

4、内部应用系统泄露攻击者利用未授权访问、数据遍历、管理弱密码、SQL 注入等漏洞，攻击企业内部的业务应用系统，获取相关数据。

二、外部泄漏

1、供应链泄露

自身供应链泄露：自身供应链是指企业自身产品生产和流通过程中的采购部门、生产部门、仓储部门、销售部门门等组成的供需网络。如电商体系中的物流系统、仓储管理系统、支付系统等，往往包含企业大量敏感信息，该类系统被恶意攻击者入侵，可造成数据泄露。

第三方供应商泄露：企业由于业务需要，使用或者购买了第三方服务，如供应商代码仓库、供应商外包人员服务、供应商提供的 SaaS 服务等。恶意攻击者通过入侵相关系统，造成数据泄露，或是第三方供应商为了牟取利益泄露数据。

-

2、互联网敏感信息将敏感数据上传至公开的互联网网站，随后搜索引擎收录企业相关网站，导致数据通过搜索引擎泄露。

- 公开的代码仓库：企业相关研发运维人员违规将代码主动上传至公开的代码仓库，如 GitHub、Gitee 等， 导致数据泄露。
- 网盘：企业相关人员违规将未加密的敏感数据主动上传至公开网盘，并进行分享，导致数据泄露。
- 社交网络：企业相关人员通过社交网络违规或无意识地披露敏感数据，导致数据泄露。

3、互联网应用系统泄露企业相关的互联网系统存在缺陷，如商城系统、VPN 系统、邮件系统等，恶意攻击者利用未授权访问、数据遍历、管理弱密码、SQL 注入等漏洞，造成数据被动泄露。

PART1 案例分享

1、大型国际信托有限公司项目经理，非法登录银行个人征信系统保存他人征信报告 被告人沈某案发前系某大型国际信托有限公司项目经理，利用任职便利，采取“撞库”等方式获取某银行个人征信系统用户名和密码，通过其所属国际信托有限公司与该银行之间进行专线互联的终端机，数次非法登录该银行个人征信系统，查询并下载保存他人征信报告共计 100 份。经查，沈某此前曾采取同样的作案手段，查询并下载保存他人征信报告共计 1000 余份。西城区法院以侵犯公民个人信息罪判处沈某有期徒刑 1 年，并处罚金 4000 元。

2、航空公司被植入木马程序，窃取乘客数据

2020 年 1 月，**中国**某航空公司向国家安全机关报告，该公司信息系统出现异常，怀疑遭到网络攻击。国家安全机关立即进行技术检查，确认相关信息系统遭到网络武器攻击，**多台重要服务器和网络设备被植入特种木马程序，部分乘客出行记录等数据被窃取**。安全域盘点 | 全球航空数据信息泄漏重大事件

3、1400 部“老年机”被植入木马 ，涉案金额高达上亿元。民警在开展“网

络侦查”工作中突然发现，攀枝花市有 89 部手机存在 2G 网络流量消费，以及非机主本人订购额外增值业务消费的异常情况。网安民警发现，这些手机网络数据都链接到同一个域名的服务器，经远程勘验，确定该服务器即为犯罪分子实施犯罪行为使用的木马服务器。通过数据追踪，发现全国竟有 1400 余万部手机被该木马服务器控制。经查明，犯罪团伙在与多家手机主板生产商合作过程中，将木马程序植入手机主板内。装有上述主板的手机出售后，犯罪团伙通过之前植入的木马程序，控制手机回传数据，获取用户手机号码、短信内容等信息，利用手机木马程序，向手机用户发送开通增值订购业务确认的短信，同时控制受害人手机回复“Y”进行开通，一系列操作完成后再将此次收发的短信记录删除。利用这样隐蔽的犯罪手法，该案 4 个犯罪团伙 23 名犯罪嫌疑人，非法牟利上亿元。

4、3.14GB 数据被盗！索尼证实今年两次重大数据泄露索尼证实今年早些时候遭遇了两次重大数据泄露，可能导致大量个人信息泄露。据介绍，第一次数据泄露发生在今年 5 月 28 日，由 Clop 勒索软件集团通过 MOVE it Transfer 平台中的零日漏洞发起，该漏洞追踪编号为 CVE-2023-34362，是个高危的 SQL 注入漏洞，可以远程执行任意代码。第二次数据泄露发生在 9 月末，一个名为 RansomedVC 的勒索攻击组织声称入侵了索尼的在线服务器，并窃取了超过 3.14GB 包含大量用户详细信息的数据。3.14GB 数据被盗！索尼证实今年两次重大数据泄露

5、由于受损的第三方应用程序导致万豪数据泄露

2020 年 1 月，黑客滥用了万豪用来提供客人服务的第三方应用程序，最终获得了 520 万份万豪顾客的记录。这些记录包括护照数据、联系方式、性别、生日、忠诚账户详细信息和个人喜好等。万豪的安全团队注意到可疑活动，并于 2020 年 2 月底封锁了内部人员造成的安全漏洞。这次重大数据泄露可能影响了近 3.39 亿酒店顾客。万豪酒店及度假村最终因违反《通用数据保护条例（GDPR》的合规要求被处罚款 1840 万英镑。

6、AI 研究人员意外泄露 38TB 内部数据，包括私钥、密码！微软的 AI 研究团队在 GitHub 上发布了开源训练数据，但是一同意外暴露了 38TB 的其他内部数据，包括微软几名员工个人 PC 的磁盘备份。而在这个磁盘备份中，又包含了

机密、私人密钥、密码和数百名 Microsoft 员工超过 30000 条 Microsoft Teams 内部消息。微软特大泄漏事件！AI 研究人员意外泄露 38TB 内部数据，包括私钥、密码！

7、智慧停车数据泄露形势严峻　“寻车”黑产团伙作案猖獗 2022 年，威胁猎人风险情报平台捕获到一批“智慧停车平台”攻击工具，对多个“智慧停车平台”的 API 接口发起大规模攻击，非法盗取车辆的停车信息，包括车辆当前的停车位置、停车时长等，并借此掌握车主的行踪轨迹。犯罪团伙的作案过程涉及黑产工具攻击、数据盗取、安装 GPS、资金交易等环节，=形成了一条完整的“寻车”业务链。

PART2 企业如何防范

一、数据加密：对交换数据进行加密，避免他人窥视通过部署专业的数据加密软件来对企业内部员工电脑文件进行加密，实现对数据文件只允许在企业环境内合理使用，未经允许，任何私下拷贝或外发带离重要文件，都将无法打开使用，显示为乱码！当前，数据加密被公认的最有效的数据保护措施之一。

二、数据完整：保证数据交换的完整性数据加密传输，第三方无法通过技术等工具篡改已受保护的信息数据，确保数据准确和完整，避免欺诈、钓鱼等事件的发生。

三、权限管控：有效管控内部数据，不外泄内部泄密是企业数据泄露的根源之一，内部员工可能有意或无意的不当行为，是造成数据泄露的关键原因。研究发现，78%的数据泄露事件和内部员工（包括前雇员）有关。企业不能仅依靠制度约束，也要应用安全技术进行数据管理，如数据加密、数据防泄漏、数据溯源、数据分类分级、访问权限管控等策略，这样才能有效降低数据泄露的风险。

通过部署专业的数据加密软件来对企业内部员工电脑文件进行加密，实现对数据文件只允许在企业环境内合理使用，未经允许，任何私下拷贝或外发带离重要文件，都将无法打开使用，显示为乱码。

防止企业内部文件泄露事件的发生（如：内部文件私下通过 QQ、微信等聊天工具外发出去无法使用，加密后的文件在指定环境内正常使用，未获得允许脱离环

境，加密文件呈现乱码，任何通过非正规途径外发出去或者使用，都是加密状态），以保护电脑文件的安全。

内容参考：

https://blog.csdn.net/sycamorelg/article/details/123516930https://baijiahao.baidu.com/sid=1777001357452115171&wfr=spider&for=pc