

# 2017 年度安全报告——数据泄密

全球重大数据泄密事件回顾

全年泄密数据统计

41G 数据泄露和暗网

近年来, 全球各地无论是政府组织还是知名企业, 频繁被爆出大规模数据泄露事件, 尤以信息化程度发达的国家更为严重。2017 年全年有大量重大泄密的事件发生, 与之前的数据相比, 数据隐患并不令人乐观。

## 2017 年 6 月

IBM S 和 P I 两家研究机构针对 13 个国家和 419 家公司进行调研并形成“2017 年数据泄露成本调研: 全球概述”报告。通过调研显示数据泄露总成本达到 362 万美元。



## 2017 年 10 月

威瑞森电信公司 (Verizon) 又发布了一年一度的《2017 年的数据泄露调查报告》, 对以往的的安全事件和数据泄露进行了分析。这份最新报告总共分析了 42068 个安全事件以及来自 84 个国家的 1935 个漏洞。2017 年的数据泄露报告是一份“10 周年报”, 统计结果主要基于威瑞森公司在过去十年里从 65 家不同的组织获得的泄露数据。

在数据泄露原因方面, 62% 的数据泄露与黑客攻击有关; 81% 的数据泄露涉及到撞库或弱口令。

也就是说, 直到 2017 年, 人们使用密码的习惯依然不太好, 绝大部分人并没有养成定期修改密码的习惯。



2017 DataBreach Investigations Report



BREACH LEVEL INDEX  
DATA BREACHES

When many organizations are focused on preventing and stopping outside threats, the internal threats — malicious insiders, accidental loss, and other negligence — can be a forgotten risk.



2017 Poor Internal SecurityPractices  
Take a Toll



### 2017 年 12 月

2017 年 12 月,360CERT 通过大量数据调研和成本分析,对于含有敏感信息和机密信息的记录,发现数据泄露问题变的很严重,全年数据泄露事件的平均规模上升 2%,财产损失高达上亿。很多企业均遭遇过数据泄露,受损数据不等。

2017 年整体数据比 2016 年全年增加了 13%,其中,身份泄密很是堪忧,相比去年一年,增长了 49%。约 190 亿的数据泄密记录是在过去一年期间丢失和被盗,相比去年,增加了 164%。同时超过 5000 个数据泄密未知和未报告。在接下来的几年中,这很可能会开始改变,因为政府制定了相关的规章,提高数据泄密的透明度。



数据泄露指数是由泄密受损纪录数据、泄密数据类型以及风险评估指数构成。

泄密指数是通过以上三个因素(权重)计算而来。

### 重大数据泄露事件回顾

回顾整个 2017 年,产业信息化、数字化、网络化进程加速,互联网+已然成为一种不可逆的趋势,互联网、云计算、大数据带来更新式革命,然而新趋势下的数据安全状况变得越发严峻。

针对全年的数据泄露事件,360CERT 通过数据泄露指数来表明数据泄露事件的危害和影响力。

360CERT 梳理了 2017 年全球十大影响力的数据泄露事件,以此警示各企事业单位关注数据安全防护,保护其系统免受或降低泄密风险。

在 2017 年,有几个数据泄露评分指数达到 9.0 以上。下面是一些顶级数据泄露的总结:



### 事件一：全球最大管理咨询公司埃森哲大量敏感数据泄露

泄露纪录：4 台云存储服务器

泄露指数：9.2 分

事件时间：2017 年 10 月

事件回顾：2017 年 9 月 17 日，UpGuard 网络风险研究主管 Chris Vickery（克里斯·维克里）发现不安全的亚马逊 S3 存储桶，任何人将存储桶网页地址输入浏览器就能公开访问、下载。

9 月 18 日研究人员粗略分析后发现，4 个存储桶（acp-deployment、acpcollector、acp-software 和 acp-ssl）暴露了埃森哲的内部重要数据，包括云平台凭证和配置文件。

暴露的数据包括 API 数据、身份验证凭证、证书、加密密钥、客户信息，以及能被攻击者用来攻击埃森哲及其客户的其它更多数据。如果泄露的数据有效，攻击者可能会利用这些数据对客户发起攻击。CSTAR（UpGuard 的专有网络风险评估系统）对这起泄露事件的网络风险评分为 790。这起数据泄露表明，即使最先进、安全的企业也可能会将重要数据暴露在网上，造成严重后果。

这些数据一旦落入威胁攻击者之手，这些云服务器可能会将埃森哲及其数千个知名企业客户置于恶意攻击的风险之中，可能会造成不可估量的经济损失。



### 事件二：德勤 500 万数据泄漏，竟因员工将 G+ 公开平台当记事本 (28 日更新)

泄露纪录：500 万数据

泄露指数：9.2 分

事件时间：2017 年 9 月

事件回顾：2017 年 9 月 28 日德勤已成待宰鱼肉：关键系统 RDP、VPN 及代理登录细节泄露。

周一：跨国咨询公司德勤遭遇黑客攻击，公司称只是一次小事故

周二：德勤公司大量 VPN 泄露，其中包括用户名、密码以及操作细节，这些都被发布在一个 Github 仓库中（内容在不久之后被删除）。



后经查证，一位德勤员工在大约六个月前将公司代理登录凭证上传至他的 Google+ 上，这些信息直到刚刚才被删除。通过对泄露的登录信息分析可知，德勤将一些关键的系统公开在外，并且开启了远程桌面访问。然而安全起见这些都是应该设置在防火墙后并开启双因子认证的，事实上，德勤往往对他的客户推荐这种做法，虽然他自己并没有做到。

全球税务与审计公司 Deloitte( 德勤 ) 已经发表了官方公告称，公司遭受了一次网络攻击，在此次攻击中，攻击者成功窃取了大量数据，其中包括公司某些客户的私人邮件以及机密文档。

正如其他信息安全专家发现的那样，除此之外还有很多信息在传播，这些信息可以通过 Shodan 搜索到。利用这些信息，黑客们可以黑入德勤的内部网络。Google+ 页面上的信息是所有人都能看到的，所以黑客可以通过 Google 搜索到非常多的信息，这些信息足以让他对德勤发起一次攻击。

当然了，此次的 Deloitte( 德勤 ) 数据泄露事件并不是第一次，而且肯定也不是最后一次，希望其他公司要提高警惕，千万不要“事不关己高高挂起”！

### 事件三、搞事情！影子经纪人响应团队正在为 NSA 泄露工具进行公开众筹

泄密类型：黑客组织

泄密指数：9.2 分

事件时间：2013 年（2017 年 10 月更新数据）

事件回顾：近期影子经纪人正式对外宣布称他们将会提供一个“月度漏洞披露计划”服务，而这项服务的订阅费为 100 个 ZCASH 币。这也就意味着，如果我们支付了影子经纪人所要求的月服务费，我们就能够第一时间拿到最新泄漏的漏洞信息。因此在这个众筹活动中，我们希望能够集中整个安全社区的可用资源，这样不仅能够尽量避免类似 WannaCry 这样的事件再次发生，而且这对于那些资金不够的白帽社区来说也是一次订阅最新月度披露数据的机会。

简而言之，我们的目标就是从利益相关的第三方筹到足够的资金来订阅影子经纪人每个月披露的漏洞信息。我们希望通过自己的努力完成以下几个任务：

1. 筹到足够的资金以购买 100 个 ZCASH 币；
2. 从正规合法的虚拟货币交易所购买 100 个 ZCASH 币；
3. 通过电子邮件地址将 100 个 ZCASH 币转账给影子经纪人；
4. 访问影子经纪人每个月公布的泄漏数据，并将其与所有资助者分享；
5. 对泄漏数据进行分析，确定披露数据的影响程度；



根据影子经纪人所提供的月度披露服务条款，每个月他们给出的漏洞内容可能与下列几种项目有关：

1. Web 浏览器、路由器和手机漏洞，以及相应的漏洞利用工具；
2. NSA Ops Disk 中的最新资料，包括 Windows 10 的漏洞以及相应的漏洞利用技术；
3. 被入侵网络中的数据，包括 SWIFT（环球同业银行金融电讯协会）或核武器计划；

影子经纪人手中可能没有太多额外的数据了，他们很有可能是在虚张声势，这也可能是一次明目张胆的欺诈活动。但是我们可以从公告 MS17-010 中看到，他们不仅很有可能拥有更多强大的攻击工具，而且还有可能拥有最新版 iOS 的越狱技术以及先进的 Android 端恶意软件。但这一切都只是我们的猜测，事实到底如何现在我们也无从得知。我们之前对影子经纪人泄漏的所有数据进行了分析，而结论就是这个黑客组织绝对是一个可信的威胁，因此我们认为他们这项月度披露服务的可信度非常高。



### 事件四、Equifax 美国征信机构数据泄露

泄密记录：1.5 亿用户

泄密指数：9.6

事件时间：2013 年（2017 年 10 月更新数据）

事件回顾：美国征信机构 Equifax 称它们的数据库遭到了攻击，将近 1.43 亿美国人的个人信息可能被泄露，这几乎是全美人口的一半。



报道称，网络犯罪者已经接触到了包括姓名、社会安全号码、出生日期、地址和驾照编号等在内的敏感信息。还有约 20.9 万美国客户的信用卡卡号泄露。此外，居住在英国和加拿大的人也受到影响。Equifax 称，这次信息泄露可能发生在 5 月中旬到 7 月之间。公司称它们于 7 月 29 日制止了此次攻击。

美国有线电视台 (CNN) 称，从被泄露信息的广度和类型来看，此次数据泄露可能是有史以来“最糟糕的”。将近 1.43 亿美国人的数据库详情的的确确掌握在黑客手中。这些数据可能导致不同层面的身份欺诈。一旦黑客将这些数据公布出去，就是一场大灾难。如今指责黑客似乎也无济于事，毕竟还是 Equifax 自己安保工作不到位才导致这次泄露。

那么黑客到底是通过什么方式获取到数据库的密码的呢？这些控制面板的确安全性很差，但其他部分是否安全？事实上，这些控制面板中还储存了一些加密数据，但密钥却放在面板内部。一旦面板被入侵，加密数据也不再安全。截图表明，这些密钥以及所有 Equifax 子公司的信息都保存妥善，但最后他们还是都被黑了。

Equifax 与执法部门配合展开了调查，并表示将在明年为其客户提供免费的身份盗窃保护和信用监控。



### 事件五、Uber 为 5700 万份数据向黑客买账

泄密纪录：5700 用户

泄密指数：9.3 分

事件时间：2017 年 9 月

事件回顾：去年 Uber 遭遇了大规模的数据泄露，泄露数据包括 5700 万司机与乘客的信息，而这件事则被当时的 CSO 以向黑客付款 10 万美元破财消灾的方式压制了下去。Uber 的 CSO（首席安全官）和他的助理因他们的恶劣行为被解雇。



数据泄露发生在去年十月份，包括 5000 万 Uber 用户的姓名、邮箱、电话号码和 700 万 Uber 司机的个人信息以及 60 万份美国司机驾驶证号码。不过 Uber 声称社会保障号、信用卡信息、交通地理信息等其他数据并未泄露。

黑客攻击过程如下：两个攻击者访问了 Uber 软件工程师的私有 Github 仓库并用从中拿到的登录凭证登录到了公司用来处理计算任务的亚马逊 Web 服务账户上，并在这个账户的数据中发现了乘客和司机的信息。接下来就是已知的勒索过程了。

Uber 此次大规模泄露事件相比 Yahoo、MySpace、Target、Anthem、Equifax 等黑客入侵事件来说并不算严重，但值得我们注意的是他们极端的问题处理方式：隐藏消息，而不是公之于众。这是 Khosrowshahi 从前辈 Travis Kalanick 手中继承 Uber 后最近的一次丑闻。

各州和联邦的法律都有要求公司在敏感数据泄露发生时要通知用户和政府部门。Uber 表示它有义务通知驾驶证信息被泄露的司机用户，但可惜当时并没有做到。

Kalanick 在六月时因投资者压力被迫辞掉 CEO 职位，投资者认为他把公司置于严重的风险中。Uber 同时招聘了国家安全机构的前法律总顾问 Matt Olsen，希望他能帮助公司重建安全队伍，还请隶属于 FireEye 公司的 Mandiant 来协助调查这起事件。

Uber 最终声明并没有证据表示此次事件的泄露数据被黑客利用，并将为信息被泄露的司机提供免费的信息保护监控服务。

### 事件六、绝密文件！100G！泄露！NSA！ Amazon S3!

泄密纪录：100G 数据

泄密指数：9.9 分

事件时间：2017 年 9 月

事件回顾：近日，据外媒报道称，属于美国国家安全局（NSA）的一个高度敏感的硬盘驱动器的内容已经公开在了 Amazon Web Services 存储服务器上。

该虚拟磁盘镜像中包含了来自代号为“红色磁盘（Red Disk）”的陆军情报项目的超过 100GB 数据。分析显示，该磁盘镜像属于美国陆军的情报和安全司令部——被称为 INSCOM，它是隶属美国陆军和国家安全局的一个部门。

据悉，该磁盘镜像保留在非公开的 Amazon Web Services 存储服务器上，但却没有设置密码，这意味着任何发现它的人，都可以通过政府秘密文件挖掘信息。本次数据泄露事件是由安全公司 UpGuard 的网络风险研究主管 Chris Vickery 于今年 10 月份率先发现，并随即通报了相关政府机构这一违规行为的存在。随后，该存储服务器已经得到了保护。

此次泄漏事件是政府机密数据的又一次大曝光。自 2013 年爱德华·斯诺登（Edward Snowden）披露“棱镜门”以来，美国国家安全局已经成为头条新闻的常客。今年年初，前 NSA 合同工 Harold Martin 就曾因在 Booz Allen Hamilton 任职期间盗取国家文件及数据遭到 20 项刑事指控；6 月份，另一名 NSA 合同工 Reality Winner，又因涉嫌泄露 NSA 关于“俄罗斯试图干扰美国总统选举”的绝密级别（Top Secret level）文件而遭到逮捕。



### 事件七、五角大楼 AWS S3 配置错误，意外暴露 18 亿公民信息

泄密纪录：18 亿用户数据

泄密指数：9.2 分

事件时间：2017 年 11 月

事件回顾：11 月 22 日，据外媒报道称，美国五角大楼意外暴露了美国国防部的分类数据库，其中包含美国当局在全球社交媒体平台中收集到的 18 亿用户的个人信息。

此次泄露的数据为架在亚马逊 S3 云存储上的数据库。由于配置错误导致三台 S3 服务器“可公开下载”，其中一台服务器数据库中包含了近 18 亿条来自社交媒体和论坛的帖子，据猜测，这些信息很有可能是国防部从 2009 年到 2017 年 8 月时间内收集的。

美国网络安全公司 UpGuard 的安全研究人员 Chris Vickery 率先发现了这三个可以公开访问和下载的数据库，并分别将其命名为“centcom-backup”、“centcom-archive”以及“pacom-archive”。

美国中央司令部发言人 Josh Jacques 近期证实：“此次泄露事件由 AWS S3 配置错误导致，其用户可绕过安全协议访问数据。不过，我们现在已对其进行了保护与监控。一旦发现未经授权访问，我们将采取额外措施，以防网络犯罪分子非法访问。此外，我们搜集用户社交信息并无他意，仅仅用于政府公共网站的在线课程策划。



### 事件八、雅虎 30 亿帐号或已全部泄露，政监机构参与调查

泄密纪录：30 亿账号

泄密指数：9.2 分

事件时间：2013 年（2017 年 10 月更新数据）

事件回顾：早在 2013 年 8 月，雅虎曾发生过一起严重的数据泄露事件，有超过 10 亿用户的信息遭到外泄。



但在今年 10 月，雅虎对这一事件进行了新的披露：称通过与威瑞森通信公司（Verizon Communications）的业务合并过程中获得的新情报证实，此次网络攻击的影响范围远超过此前的估计，“所有帐户都有可能受到了影响。”

其实，早在 2014 年发生的数据泄露事件导致了至少 5 亿用户数据泄露。但雅虎在 2016 年 9 月才对外披露了那次泄露事件。对此，就雅虎公司的两起大规模数据泄露是否应该尽早报告给投资者一事，美国政府监管机构还进行了调查。

### 事件九、南非 3000 多万份个人信息遭公布或包括总统和部长

泄密纪录：3000 万用户信息

泄密指数：9.2 分

事件时间：2017 年 10 月

事件回顾：据称，该事件为南非史上规模最大的数据泄露事件，共有 3160 万份用户的个人资料被公之于众，其中包括姓名、身份证号、年龄、收入、地址、职业以及电话号码等。这些数据来自“拼图控股”集团旗下的艾达、ER 和房地产-1 等子公司。南非《时报》19 日披露称，祖马总统和财政部长吉加巴、警察部长姆巴鲁拉的个人信息可能也在其中。

南非的互联网安全专家表示，这些个人信息可能会被人拿到互联网上兜售。约堡大学互联网安全中心主任索尔姆斯表示，“有这些信息就够了，互联网犯罪分子可以冒充开办信用卡或进行网上订购等。”此次被黑客公布的数据来源于 Dracore Data Sciences 企业的 GoVault 平台，其公司客户包括南非最大的金融信贷机构——TransUnion。

事件发生后，安全研究人员立即进行搜索调查，发现 GoVault 平台将用户数据发布到了一台完全未经保护的 Web 服务器上，允许任意用户进行访问。



“涂鸦”项目即“斯诺登阻止器”是一款用于声称将“web beacon（网络信标）”标签嵌入机密文档中的软件，以便监控机构追踪泄密者和外国间谍。自3月份开始，维基解密已公布 Vault 7 系列中的数千份文档和其它声称来自 CIA 的机密信息。

CIA 称“涂鸦”是“一款批量处理工具，用于处理预生成水印并将这些水印插入由外国情报官员窃取的文档中”。

### 事件十、维基解密公布 CIA 用于追踪泄密者的源代码

泄密纪录：3 万用户

泄密指数：9.1 分

事件时间：2017 年 7 月

涂鸦工具如何运作？

涂鸦的编程语言是 C#，它为每个文档都生成随机水印，并将水印插入文档、将所有经处理的文档保存在导出目录中，并创建一个日志文件识别插入每个文档中的水印。



这种技术跟“追踪像素”的运作方式一致，后者就是将微小的像素图像内嵌到邮件中，这样影响人员和活动人员就能追踪有多说明用户查看了广告。而 CIA 通过将微小的唯一生成的文件插入“可能被盗”的机密文档中，而文件托管在由 CIA 控制的服务器上。这样，每次有人查看水印文档时包括泄密者，它都会秘密在后台加载一个嵌入式文件，在 CIA 服务器上创建一个条目包括访问这些文件的人员信息如时间戳及其 IP 地址。

仅在微软 Office 产品中起作用

用户手册还指出这款工具旨在针对 Office 离线文档，因此如果打水印的文档在 OpenOffice 或者 LibreOffice 中打开的话，水印和 URL 会被暴露给用户。它在微软 Office 2013（Windows 8.1×64）文档，Office 97 至 2016（Windows 95 上不起作用）文档，以及表单未被锁定、未加密或不受密码保护的文档中起作用。

然而，由于隐藏的水印是从远程服务器加载的，因此这种技术应该只有在访问水印文档的用户联网的情况下才起作用。

维基解密指出，最新的涂鸦版本（v1.0 RC1）是在 2016 年 3 月 1 日发布，这说明至少在去年还在使用而且本来应该在 2066 年才解密。更多技术详情可访问《用户手册》。

截至目前，维基解密发布了 CIA 针对流行硬件和软件的人侵利用代码“Year Zero”文档、针对 iPhone 和 Mac 的利用代码“Dark Matter”、“Marble”文档、以及披露了能入侵微软 Windows 并绕过杀毒保护措施的能轻易创建自定义恶意软件的一个框架即“Grasshopper”文档。

### 事件十一、韩最大加密货币交易所被黑客攻击：3 万客户数据泄露

泄密纪录：3 万用户

泄密指数：9.2 分

事件时间：2017 年 7 月

事件回顾：正当韩国正被对比特币和以太币等加密货币进行监管立法的时候，却有报道称该国最大的加密货币交易所 Bithumb 遭到了黑客入侵。据 BBC 报道，3 万名客户数据被泄露，黑客利用欺骗来的数据窃取用户账户里的资金。BraveNewCoin 则解释了 Bithumb 用户是“语音钓鱼”的受害者，因为有自称该交易所工作人员的骗子打电话来忽悠他们。

交易所声称受本次事件影响的客户约占总数的 3%。

据悉，本次泄露发生于 2 月份，原因是一名员工的家用 PC 涉入其中（而不是公司总部的计算机服务器出现了问题）。Bithumb 表示在 6 月 29 日发现了此事，并于次日向当局进行了汇报。

作为全球五大比特币交易所之一，Bithumb 去年的比特币交易量达到了 2 万亿韩元左右（约合 118 亿 RMB），日交易量也超过了 1.3 万比特币（占全球交易量 10%）。

Bithumb 已承诺初步向每位客户赔偿 10 万韩元（约 86 美元 / 590 元 RMB），剩余部分将在验证后补足。

### 事件十二、趣店数百万学生数据泄露，称或遭内部员工报复

泄密纪录：100 万用户

泄密指数：9.1 分

事件时间：2017 年 11 月

事件回顾：11 月 20 日，有关媒体发布消息称，趣店数据疑似外泄，十万可买百万学生信息，离职员工称“内鬼”所为。此次泄露的数据维度极为细致，除学生借款金额、滞纳金等金融数据外，甚至还包括学生父母电话、学信网账号密码等隐私信息。趣店以校园贷起家，之后退出校园，转向白领市场，提供“现金贷”和消费分期贷款。2017 年 10 月 19 日，趣店正式登陆美国纳斯达克。

有媒体采访内部员工得知，趣店曾因 9 月的大规模裁员事件未能合理安排离职员工的抚恤问题，造成此次数据泄露事件有可能是内鬼所为。此外，多位趣店离职员工表示，早期趣店数据管理存在巨大安全隐患。



### 综述：

随着网络攻击日趋复杂、日益频发，国内外各行各业的公司和机构对数据泄漏问题越发担忧。事实上，CDW 的研究显示，在过去的两年里，每四家机构当中就有一家遭遇过数据泄漏。许多公司称，这类事故严重威胁了公司邮件、网络和敏感信息的安全。并且随着远程办公和移动计算的普及，防止数据泄漏也变得愈加复杂和困难。

#### 针对企业：

第一步就是承认数据泄漏的风险确实存在。认识到这点之后才能建立有效的防止数据泄漏的计划。

第二步，定义机构的所有数据。这项工作看似艰巨繁杂，但为防止数据泄漏而做的数据定义并非那么困难。关键在于将机密信息（如社保号）和机密文档（如含有社保账号的文件）明确区分开来。同时也要明白，任何机构都有自己的关键业务数据，这部分数据必须加以保护。

第三步，中小企业需要制定移动设备的安全使用政策，考虑现有的安全保护措施，以及完善移动设备的管理机制。

第四步：把数据保护政策传达给员工。政策要简明实用，明确哪些数据是机密的，机密数据应如何使用，以及员工应如何使用移动设备。

#### 针对个人用户：

谨防钓鱼网站、慎连 wifi、不在社交平台中随意透露个人信息、慎重参加网络调查、抽奖活动、妥善处理快递单、车票等、及时清除旧手机的数据信息。大数据时代，挖掘个人隐私的方法数不胜数，即使很简单的信息，多维度凑到一起也能发现你不可告人的秘密。目前还有没有保护隐私很好的方法，除非你回归原始社会。

#### 针对第三方数据平台：

第三方系统的安全问题是最近一些数据泄露事件的原因，包括 Target，JP Morgan 的数据泄露事件，都或多或少与第三方系统有关。比如黑客对 Target 的攻击就是从 Target 的空调服务商入手的，而 JP Morgan 则是通过第三方网站进行的渗透。

与往常一样，2017 年全年的数据泄密事件有各种来源。但是在一个大数据统计以及记录数据表明，数据泄密的最大来源是意外丢失和因疏忽而使信息暴露的数据。

## 数据泄密重要数据统计

### 数据泄密的流程

数据资源在整个互联网中起着相关重要的作用，这些数据资源关乎着每个人的财产安全。数据资源隐藏着庞大的经济效益，真因为这许多黑客痛过定点渗透、外挂木马、钓鱼、伪基站等方式方法来获取这些数据资源。由于受利益的驱使，除了黑客之外，还有一部分公司内部人员恶意出售接触到的数据，从中获取很大的现金。也有部分公司员工缺乏安全意识把数据存放在不安全的地方，导致数据被泄露。

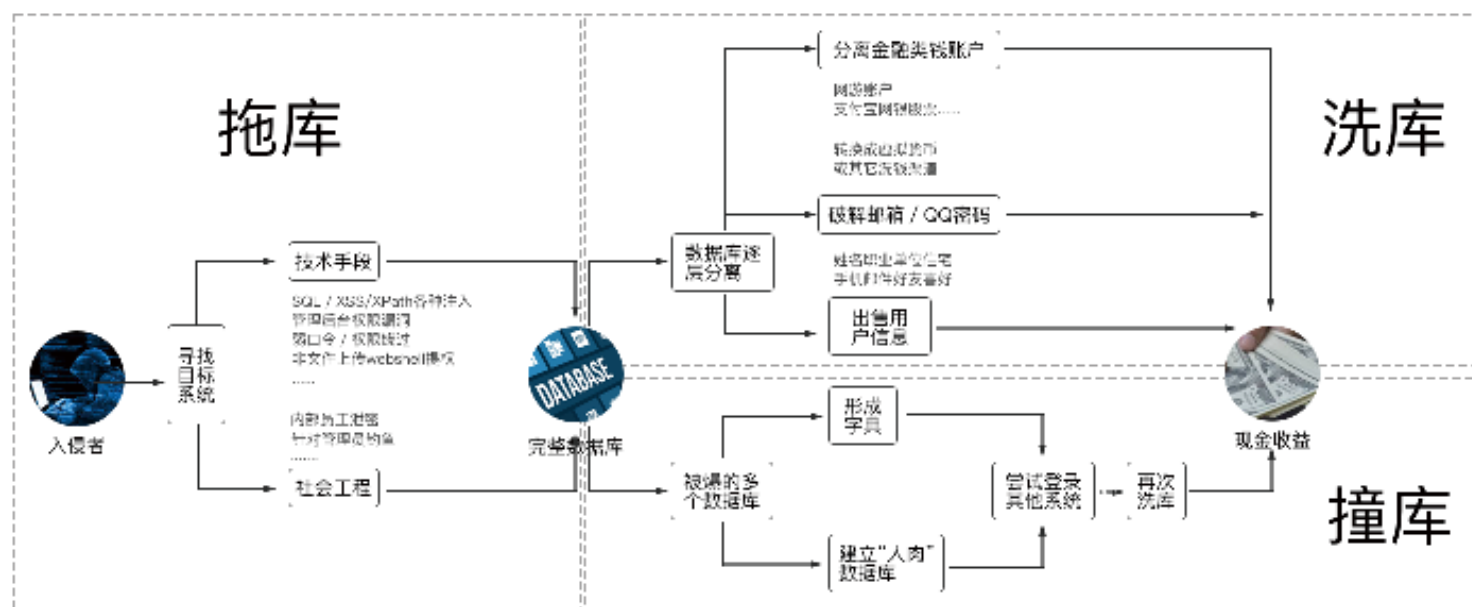
数据一旦被泄露，那么就会产生一系列的危害，很多用户由于缺乏安全意识，不能及时的发现自己的数据泄露，只有当自己的财产受到损失才能被感知，所以用户感知是越来越慢的。

	如何泄密？	数据利用？	数据信封
数据资源	黑客攻击	金融类——直接提现 虚拟物品，如游戏装备——洗号 涉及个人信息——诈骗、隐私泄密 公司业务数据——商业竞争	撞库
	木马		
	内部人员		
	自身		
资源价值	由大—————小（越来越小）		
用户感知	由小—————大（越来越大）		



数据泄露的流程整个流程可以分为：拖库、洗库、撞库。入侵者通过不法手段来入侵有价值的数据系统，然后对数据进行逐层分离，找到一些金融类的帐户，然后通过入侵支付宝、网银、网游账号获取高额的现金收益。

另一方面也可以将用户的个人信息批量出售获取现金。当数据一旦被利用，在进行建立人肉数据库，进行撞库。

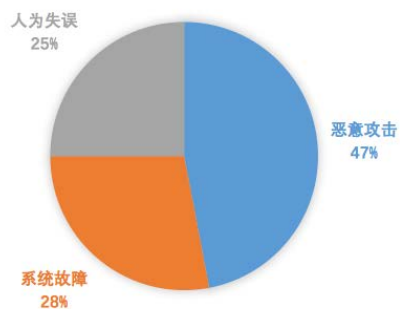


### 数据泄露的来源

与往常一样，2017 年全年的数据泄密事件有各种来源。但是在一个大数据统计以及记录数据表明，数据泄密的最大来源是意外丢失和因疏忽而使信息暴露的数据。

2017 年全年数据泄露最大的来源是恶意攻击，占总比重的 47%。这导致很大的数据都是被盗的。

2017年全年数据泄露来源比例



在这些事件中，有 47% 涉及恶意攻击或犯罪攻击，25% 因员工或承包商疏忽所致（人为因素），28% 与系统故障相关，包括 IT 故障、业务流程故障等等。

### 数据泄露的影响因素

#### A：成本因素。

据悉《2017 年数据泄露成本调研全球概述》统计有大约 20 个因素对数据泄露成本会有影响。有些因素可以使数据泄露成本下降，有些因素是会让成本增加。

影响成本下降：如图所示，事件响应团队、广泛使用加密技术、员工培训、BCM 参与、参与威胁共享计划及使用安全 分析工具等因素使得单条受损记录产生的数据泄露单条成本下降了。

影响成本上升：第三方参与、广泛迁移至云端、合规缺陷、广泛使用移动平台、设备丢失或被盗、急于通知等因素使得数据泄露的单条成本（以负数显示）上升了。

#### B：丢失的记录数量。

丢失纪录条数越多，数据泄露的成本越高。事件规模越大，相对应的成本就越高。

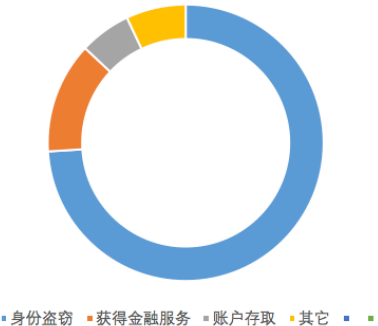
#### C：行业客户流失。

客户流失的越多，数据泄密的成本越高。通告数据表明，影响客户流失的因素有两方面，一方面是所处的国家，不同国家流失程度不一样，日本流失最大；另一方面是行业因素，行业更容易出现客户流失的情况。

数据泄露的类型

由于一直如此，在过去的几年里，身份盗窃是攻击在 2017 年这个战术是全年的数据泄露事件中最常用的模式，占期间所有事件的大约四分之三 (74%)。事实上，和 2016 年相比较身份盗窃破坏的数量继续保持高位，并且导致多条纪录被窃取显示，安全机构和相关机构没有充分应对这一威胁。

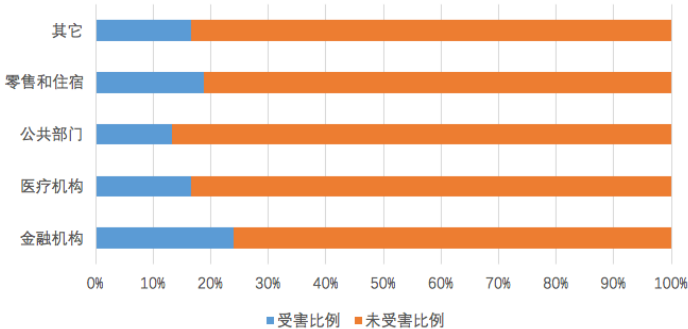
2017年全年数据泄露类型比重



数据泄露涉及行业比重

在行业分布上，金融行业依然首当其冲，24% 的数据泄露事件和金融机构有关；其次是医疗保健行业 15%；再往后是销售行业 15% 以及公共部门 12%。其中医疗行业是勒索的重灾区，真可谓“不给钱就撕票”

2017年全年行业数据泄露比重

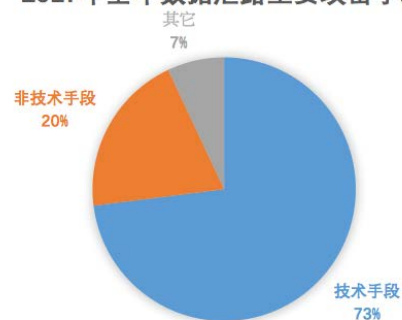


这里需要注意，学术界正逐渐“崛起”成为黑客攻击的目标，比如高校的高新科研部门。犯罪分子已经意识到很多知识产权和商业机密都是起源于高等院校的学术研究，而且，和入侵政府系统以及成熟的商业系统相比，入侵大学的系统和窃取研究机密更加简单。

## 数据泄露的主要采取的手段

导致数据泄露的主要手段分为技术手段(黑客入侵、软件漏洞、恶意木马)、非技术手段(内部人员泄密、非有意识泄密)。

2017年全年数据泄露主要攻击手段



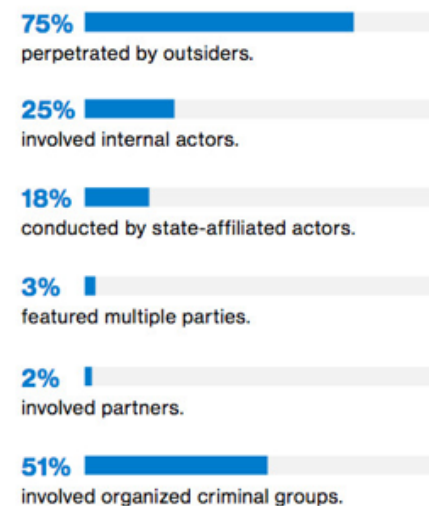
## 组织出现其他数据泄露事件的可能性

360CERT 对以往的的安全事件和数据泄露进行了分析, 分析指出在调查的几万个安全事件中, 内部威胁占 25%, 75% 是外部攻击导致。

在外部攻击中, 51% 的网络攻击涉及到有组织有计划的犯罪集团。18% 的外部攻击涉及国家背景。



### Who's behind the breaches?





## 41G 密码泄露和暗网

2017 年 12 月 5 日，一位名为 tomasvanagas 的用户在 reddit 论坛上公开了一份高达 41GB 的数据泄密文件（“社工库”），文件包含了 14 亿条明文性质的互联网用户密码记录。近几年大大小小的数据泄密事件频发，而这可能是迄今为止被公开的最大的一次数据泄密文件，而且从这份数据的完整性来看，数据整理者做得较为完整和专业。在万物互联的大安全时代里，需要互联网用户，信息安全行业和相关受影响的公司实体对数据泄密事件有足够清醒的认识和作为。



在 41G 的文件中，整理者提供了完整的数据和专业的操作说明，文件操作日期显示文档作者在 11 月 29 日作了最后一次更新。

文档主要信息如下：

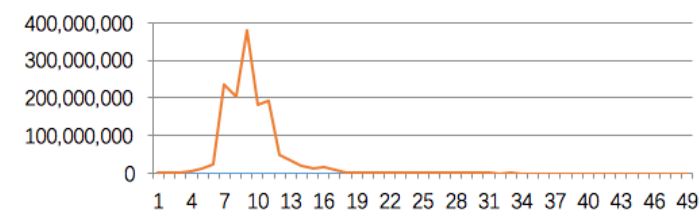
①、README 说明文件一方面对数据文件作了较为详细，专业的介绍，同时也提供了“比特币”和“Dogecoin”币捐赠地址（1NrNf6E3rTuDDGeUdU2CMpGNyrQAeB7dNT, DFqkJHnb5t5Y6e4mbXTiS9aEhspFkzxkPU），此举可能是为了保证“收钱”的匿名性。

②、数据文件包含了 14 亿条记录（1,400,553,869），全部是明文密码。

③、此次 14 亿条用户密码信息不全是未公开的数据泄露，而是包含了此前 252 起数据泄露事件的合集。数据导入日志显示，整理者从 2017 年 8 月 7 日开始到 2017 年 11 月 9 日分批进行了 252 次数据导入。大部分导入为数字编号，一部分导入有很清楚的数据源，其中疑似包括 Anti Public Combo List, Exploitin, MySpace, Linkedin, YouPorn, Last.FM 和部分国内公司实体等在内的的用户隐私数据。

排名	百分比	注解域名
1	19.49%	yahoo.com
2	13.47%	hotmail.com
3	8.38%	gmail.com
4	8.01%	mail.ru
5	3.94%	aol.com
6	3.14%	yandex.ru
7	2.06%	rambler.ru
8	1.71%	qq.com
9	1.18%	163.com
10	1.15%	hotmail.fr
11	1.07%	web.de
12	0.94%	live.com
13	0.90%	msn.com
14	0.90%	gmx.de
15	0.81%	bk.ru
16	0.72%	list.ru
17	0.70%	hotmail.co.uk
18	0.68%	inbox.ru
19	0.66%	yahoo.fr
20	0.63%	yahoo.co.uk

④、从密码长度分布图观察，密码长度为 9 的最多，数据量为 380304432，三亿 8 千万条。



## ⑤、最长用密码 top100

1	2	3	4	5	6	7	8	9	10
123456	123456789	qwerty	111111	password	12345678	abc123	1234567	homelesspa	password1
11	12	13	14	15	16	17	18	19	20
123123	000000	1234567890	12345	iloveyou	1q2w3e4r5t	qwertyuiop	1234	123321	123456a
21	22	23	24	25	26	27	28	29	30
monkey	dragon	123	666666	654321	1qaz2wsx	121212	123qwe	a123456	qwe123
31	32	33	34	35	36	37	38	39	40
tinkle	target123	gwertry	1q2w3e4r	gwertry123	zag12wsx	1q2w3e4r	7777777	zxcvbnm	123abc
41	42	43	44	45	46	47	48	49	50
qwerty123	987654321	222222	qwerty1	qazwsx	112233	555555	12345a	1q2w3e	123123123
51	52	53	54	55	56	57	58	59	60
asdfghjkl	fuckyou	FQRG7CS493	1234qwer	aaaaaaa	159753	computer	1111111	123654	888888
61	62	63	64	65	66	67	68	69	70
iloveyou1	789456123	michael	fuckyou1	princess	sunshine	football	777777	j38ifUbn	999999
71	72	73	74	75	76	77	78	79	80
asdfgh	1111	linkedin	789456	princess1	123456789a	88888888	a12345	abcd1234	football1
81	82	83	84	85	86	87	88	89	90
12qwaszx	jordan23	monkey1	qwer1234	asd123	gfghjkm	samsung	shadow	love123	Status
91	92	93	94	95	96	97	98	99	100
333333	azerty	superman	michael1	asdf	daniel	baseball	zxcvbn	111111	love

## 暗网中的隐私数据交易

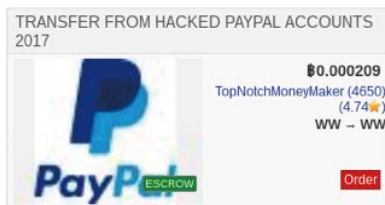
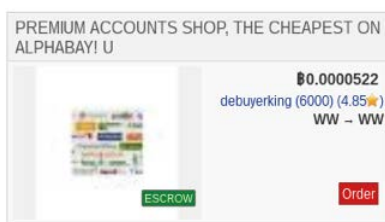
据悉，此次公开的数据文件源自于“暗网”（常规方式访问不到的网络）。在“暗网”中，提供了一系列包括毒品，武器，黑客户服务，恶意软件，隐私数据等形形色色的交易服务，因其具备匿名化的特点，吸引了来来往往的网络犯罪份子。近年尽管较为知名的 Hansa 和 AlphaBay 均被叫停，但“暗网”从未消失。

文件中的泄露数据很大一部分都可以关联到相应的黑客攻击导致的数据泄密事件，比如，雅虎在 17 年 10 月承认 30 亿密码泄露，但是密码泄露早在 13 年发生；AOL 在 2014 年发现邮箱密码泄密；2016 年国外安全网站披露疑似大量 Gmail，Yahoo mail 和 Hot mail 邮箱账号在“暗网”中交易。



文件中还有部分数据源来源不明。今年还有 2 次大量数据泄露事件，Anti-public 的 4.5 亿条邮箱账号和密码泄密事件，和 Explotin 的 5.9 亿条密码数据泄密事件。从安全社区角度看，Anti-Public 和 Explotin 事件都有一定证据显示，相关的泄密数据在 2016 年底就可以在“暗网”上获取，但是直至 2017 年 5 月才向大众公开，这些数据来源目前都还处于未知状态。

目前相关安全公司和安全研究人员都会对“暗网”和“数字货币”的交易进行长期的跟踪和分析，从而获取更多的威胁情报来更好的维护互联网安全。

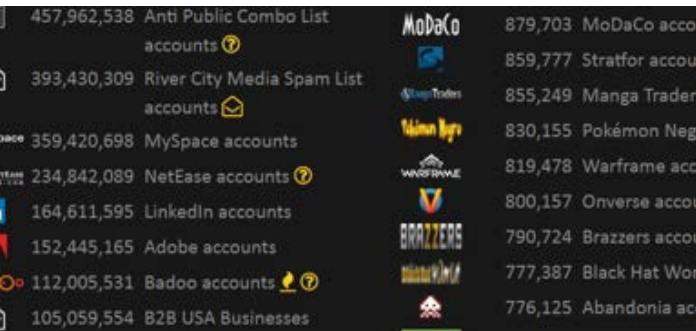




## 大安全时代下的反思

当下，是一个万物互联的大安全时代。

数据泄露问题对于个人和企业的影响都更加严峻。个人用户在访问更多的设备，社交平台，网站平台的同时，自身的网络帐号密码也面临着泄露风险。随着企业 IT 架构日益复杂以及员工数量日益庞大，企业现有的安全措施已经远远无法满足安全需求，从而将用户隐私数据置于危险境地。



457,962,538 Anti Public Combo List accounts	MoDaCo	879,703 MoDaCo accounts
393,430,309 River City Media Spam List accounts	Stratfor	859,777 Stratfor accounts
359,420,698 MySpace accounts	Manga Trader	855,249 Manga Trader accounts
234,842,089 NetEase accounts	Pokémon Neg	830,155 Pokémon Neg accounts
164,611,595 LinkedIn accounts	Warframe acc	819,478 Warframe accounts
152,445,165 Adobe accounts	Onverse acco	800,157 Onverse accounts
112,005,531 Badoo accounts	Brazzers acco	790,724 Brazzers accounts
105,059,554 82B USA Businesses	Black Hat Wor	777,387 Black Hat Wor
	Abandonia ac	776,125 Abandonia ac

数据泄露事件的背后往往与个人，企业息息相关。个人没有定期更改密码的习惯，在不同网站使用相同的密码且设置过于简单，如果不能及时的处理好泄露事件，name 利用泄露数据库对高价值网站（如金融行业）进行“密码撞库”，针对特定个人进行目标渗透等等一系列的黑客攻击将会变得愈发猖狂。

## 密码泄露事件

个人在面对数据泄露事件时，要提高自身的安全意识并采取合理的措施来避免问题的扩大化。个人用户要根据网站，设备重要等级分级使用多个独立高强度密码，定期变更密码，及时到数据泄露的公开网站进行自查。

企业在面对数据泄露事件时，应尽量做到“坚持两个原则，完成两个流程”。坚持对用户安全负责的原则；坚持专业的事要交给专业的人做的原则，联合和信任相关安全专业团队参与安全事件处理。同时，一方面要完成内外协同的完整事件应急处置流程，包括事件回溯和负责任的影响面评估等；另一方面要完成安全事件对外披露和受影响用户的通知流程（如引导用户修改密码等）。

大安全时代，41G 的数据泄露事件并不是单一厂商的密码泄露，而是一直以来或明或暗的安全事件的总体，个人，信息安全行业，公司实体都无法置身事外，需要建立一个协同联动的机制和体系。

### 总结

从上述总结的政企数据泄密事件来看，主要的泄密风险除了黑客攻击、木马病毒、钓鱼网站等外部因素，缺乏整套行之有效的安全管理系统、内部员工泄密以及内部管理等内部因素成为引发的数据泄密事件的主要诱因。泄密领域也进一步扩大，掌握大量民众个人信息的金融行业依旧是数据泄露的“重灾区”。

信息数据的爆炸式增长，推动信息化逐步进入数据技术 (DT) 时代，数据成为驱动业务发展的核心动力，基于数据驱动为核心重构信息系统已经逐步成为共识。在“互联网+”时代，企业面临的安全挑战会越来越严峻。随着大数据、云计算以及移动互联网的高度融合，对数据安全技术提出了更高的要求，泄密事件将呈高发势头。

没有网络安全就没有国家安全，大数据时代，机遇与挑战并存。面对新形势新问题，坚持安全与发展并重，筑牢我国大数据安全管理的防线，守卫好我国信息主权和用户隐私，才能防止大而无序、大而无安，真正实现大有所长、大有所用。



### 参考资料

<https://www.hackeye.net/securityevent/11530.aspx>

<http://www.aqniu.com/industry/30413.html>

[https://www6.gemalto.com/breach-level-index-2017-h1-report?utm\\_medium=press-release&utm\\_campaign=bli-lp-report](https://www6.gemalto.com/breach-level-index-2017-h1-report?utm_medium=press-release&utm_campaign=bli-lp-report)

[http://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2017\\_Report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf)

<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130CNZH>

<http://www.aqniu.com/industry/17871.html>

<http://blog.csdn.net/csdnnews/article/details/78620918>

<http://www.freebuf.com/articles/database/158465.html>

<https://www.anquanke.com/post/id/92302>

### 关于 360CERT

360CERT 全称“360 Computer Emergency Readiness Team”,我们致力于维护计算机网络空间安全,是 360 公司基于“协同联动, 主动发现, 快速响应”的指导原则,对重大网络安全事件进行快速预警、应急响应的安全协调团队。



微信公众号



新浪微博