2018 政企机构数据泄露形势分析报告

(2019.1)

发布机构：奇安信威胁情报中心

支持单位：补天漏洞响应平台、奇安信安服团队、奇安信安全监测与响应中心、奇安信行业安全研究中心

主要观点

- ✧ 数据泄露已经成为安全问题的风险源头，数据泄露事件逐年增多、危害范围不断增大。
- ✧ 网络攻击、内鬼窃取、内部人员操作失误，已经成为当前政企机构数据泄露的三大主要原因。
- ✧ 由于网站漏洞、弱口令等问题的存在，导致黑客使用社工或技术手段攻破企业的安全技术防线窃取数据。
- ✧ 在高额利益的趋势下，越来越多的内部人员利用职务之便非法获取公司数据进行贩卖。
- ✧ 由于内部人员缺乏安全和风险评估能力，导致一些无意识的错误操作引发公司数据泄露。
- ✧ 信息安全的投入与需要被保护目标的商业价值和社会价值严重不匹配，是一个全球性网络安全问题，也是造成大量数据信息泄露的根本原因。信息系统的建设、运维和管理人员网络安全意识薄弱，安全认知水平和风险评估能力均严重落后于信息网络技术及其应用的爆发式增长。
- ✧ 数据泄露事件造成的影响，已经逐渐超出了网络安全问题本身，越来越多的数据泄露事件与政治、经济、道德等因素交织在一起，折射出更多的社会问题，引起了社会更加广泛的关注与热议。

摘 要

网站漏洞泄露数据风险分析

- ✧ 2018 年 1-10 月，补天平台共收录可导致百万条以上数据泄露的网站漏洞 280 个，约占补天平台全年漏洞收录总数（18200 个）的 1.5%，涉及网站 129 个，共可造成 86.5 亿条数据泄露。
- ✧ 2018 年可造成数据泄露的这 280 个网站漏洞，较 2017 年（251 个）上升了 11.6%，且全部为高危漏洞。
- ✧ 2018 年的 280 个可导致数据泄露的网站漏洞，总计可能泄露信息为 86.5 亿条，比 2017 年的 51.1 亿条上升了 69.2%；比 2016 年的 60.5 亿条上升了 43.0%；比 2015 年的 55.3 亿条上升了 56.4%。网站漏洞导致数据泄露的规模正在逐年增加。
- ✧ 2018 年，平均每个漏洞可导致 3089.2 万条个人数据泄露，单个漏洞的危害大大增加。
- ✧ 从可导致数据泄露的网站漏洞技术类型来看，2018 年可能数据数据的网站漏洞中，命令执行（占比为 81.1%）、代码执行（7.9%）和弱口令（7.1%）占比最高，三者之和占全部数据泄露漏洞的 96.1%。
- ✧ 2018 年 1 至 10 月，补天平台收录的可导致数据泄露的 280 个网站漏洞中，共涉及到 86.5 亿条数据泄露。其中，1 月份曝出的可能泄露数据的漏洞个数最多，为 60 个网站漏洞；10 月份曝出的可能泄露的数据规模达到最高峰，为 14.0 亿条信息。
- ✧ 在 280 个可导致数据泄露的网站漏洞中，共有 30 个网站漏洞可泄露的数据规模在 5000 万条以上，其中还有 11 个漏洞可泄露的数据规模在 1 亿条以上。

应急响应处置的数据泄露事件

- ✧ 2018 年 1-11 月，安服团队共为全国各地多家大中型政企机构，提供了网络安全应急响应服务，参与和协助处置各类网络安全应急响应事件 717 次。其中，涉及到数据泄露事件共 130 起，占应急响应处置事件总数的 18.1%。
- ✧ 在涉及到数据泄露的政企机构中，政府部门是应急响应处置的数据泄露事件最多的行业，为 25 次，其次是事业单位，为 10 次；制造业，为 6 次。
- ✧ 95.5%的数据泄露事件是企业自行发现的，但是，仍有 4.5%的数据泄露事件，企业实际上是不自知的，他们是在得到了监管机构的通报或看到了媒体的公开报道后，才得知企业的内部数据已经被泄露的。
- ✧ 进一步对企业发现的网络攻击进行分析，54%的网络攻击事件是由于服务器病毒进行了告警；11.5%是由于 PC 病毒告警；6.2%是由于 webshell 告警；4.4%是由于网页被篡改。
- ✧ 从大中型政企机构数据泄露事件中的失陷区域来看，27.0%为内部服务器、数据库；23.6%为网站；18.0%为业务专网；16.9%为办公终端，12.4%为业务系统。
- ✧ 在安服团队 2018 年参与处置的 130 起数据泄露事件中，弱口令问题最为显著，约有 52.2%

的数据泄露事件是由于弱口令问题导致的。其次，25.7%的事件与未及时修复漏洞有关，包括：17.7%的服务器漏洞、6.2%的 Web 漏洞、1.8%设备漏洞。

全球政企机构数据泄露分析

- 2018 年，全球政企机构均发生了大量的重大数据泄露事件，本报告通过对国内外媒体公开报道的事件进行了整理，共抽样收集了 206 起重大数据泄露事件。
- 2018 年，全球政企机构重大数据泄漏事件中，13.1%为生活服务行业，12.1%为 IT 信息技术，11.7%为互联网行业。
- 从 2018 年政企机构重大数据泄露事件泄露数据的原因来看，约一半的事件是由于外部攻击导致的；但是也有 16%的事件是由于内部人员违规操作，主动泄露的数据，10.2%的事件是由于合作伙伴泄露。
- 从 2018 年全球重大数据泄露事件泄露数据的主要类型来看，59.2%的事件泄露的是实名信息；13.1%的事件泄露的是账号密码；7.8%的事件泄露的是保单信息。
- 206 起全球重大数据泄露事件中，约 74%的事件我们大概标记出了数据泄露的规模。这 153 起事件，泄露了约 13 亿条信息。
- 从 2018 年全球重大数据泄露事件泄露的数据规模分布来看，47.1%的事件泄露的数据规模在 100 万条以上。值的注意的是，7.1%的事件泄露规模在 1 亿条以上。

暗网上非法数据的交易情况

- 本文收集的 1000 条数据交易中，分别是由 368 个人发布的，约为每个人发布三条信息。具体来看，发布信息在 5 条以下的人数占 88.8%，发布信息在 5-10 条的人数占 6.3%，发布信息在 50 条以上仅有 1 人，占比为 0.3%。
- 从暗网上数据交易所涉及的行业来看，金融行业占比为 23.1%；互联网行业占比为 16.3%；生活服务行业占比为 6.1%。还有一部分并未明显说明的行业属性，遂归属于个人信息。个人数据占比为 8.5%。
- 从暗网上数据交易的类型来看，实名信息是被贩卖最多的一类信息，占比为 45.2%，其次为账号密码、数据库、用户信息、电话号码、行为记录等。
- 从暗网上数据交易的规模来看，10 万条以上的数据占到了 46.0%；10 万至 100 万条的数据占到了 23.4%；100 万至 500 万条的数据占到了 11.0%；1 亿条以上的数据，占比为 5.8%。
- 信息购买者购买数据的一般用途：精准营销、精准诈骗、在其他渠道贩卖。

关键词：补天平台、网站漏洞、应急响应、数据泄露

目 录

研究背景.....1

第一章 网站漏洞泄露数据风险分析.....2

一、 可泄露数据的网络漏洞数量.....2

二、 网站漏洞可泄露的数据规模.....4

第二章 应急响应处置的数据泄露事件.....5

一、 数据泄露事件的应急次数.....5

二、 数据泄露事件的行业分布.....5

三、 数据泄露事件的发现方式.....6

四、 数据泄露事件的失陷区域.....7

五、 数据泄露事件的自身弱点.....7

第三章 全球政企机构数据泄露分析.....9

一、 全球数据泄露事件的行业.....9

二、 全球数据泄露的原因.....9

三、 数据泄露的类型.....10

四、 数据泄露的规模.....11

第四章 暗网上非法数据的交易情况.....12

一、 活跃的数据发布者.....12

二、 数据交易所涉及的行业.....13

三、 数据交易的类型及规模.....13

四、 获取数据后的一般用途.....15

第五章 政企机构数据泄露的原因.....17

一、 弱口令是黑客攻击成功的关键因素.....17

二、 内鬼威胁成为数据泄露的重要源头.....17

三、 配置错误或操作不当事件频繁发生.....17

四、 安全投入与保护目标的价值不匹配.....17

第六章 政企机构数据泄露的趋势.....19

一、 数据泄露的数量和规模正在大幅度上升.....19

二、 对重要数据进行定向化攻击并实施勒索.....19

三、 外部力量督促企业加强安全建设.....19

四、 数据泄露事件折射更多社会问题.....19

五、 数字化转型的企业将面临更大的数据泄露风险.....20

第七章 防范数据泄露的建议.....21

一、 使用强密码并定期修改.....21

二、 加强网络安全意识.....21

三、 数据进行分类管理.....21

附录 1 国内机构重大数据泄露事件分析.....22

一、 内部威胁.....22

二、 外部威胁.....23

附录 2 国外机构重大数据泄露事件分析.....25

三、 IT 信息企业.....25

四、 政府机构.....27

五、 电信运营商.....29

六、 互联网.....32

七、 交通物流.....35

八、 教育.....38

九、 金融.....40

十、 军事.....44

十一、 生活服务.....45

十二、 医疗卫生.....50

十三、 制造业.....53

十四、 物联网.....54

十五、 其他 55

附录 3 暗网上重大数据交易事件 59

一、 军政及事业单位在暗网的重大数据交易事件 59

一、 IT 互联网企业在暗网的重大信息交易事件 60

二、 出行、酒店及餐饮行业在暗网的重大信息交易事件 61

三、 快递行业在暗网的重大数据交易事件 62

四、 医疗卫生机构在暗网的重大数据交易事件 63

五、 金融行业重大数据泄露事件交易事件 63

研究背景

自 2013 年斯诺登事件以来，全球数据泄露规模连年加剧。根据 Gemalto 发布的《数据泄露水平指数（BreachLevelIndex）》显示，仅 2018 年上半年，全球就发生了 945 起较大型的数据泄露事件，共计导致 45 亿条数据泄露，与 2017 年相比数量增加了 133%。

数据泄露已经成为：安全问题的风险源头、当前网络安全的最主要威胁和政企机构面临的重要安全风险之一，数据泄露事件逐年增多、危害范围不断增大。

造成政企机构数据泄露的原因主要有两类，一是外部攻击、二是内部威胁，内部威胁主要是指内鬼窃取和内部人员误操作。而从机构泄露的信息类型来看，主要也分为两类，个人信息和机密数据，后者是指政企机构内部除个人信息之外的商业机密、技术机密及其他机密信息。

在大数据产业迅猛发展的浪潮中，我国个人信息安全和隐私保护面临着严峻形势。个人信息作为数据信息的核心内容，面临着采集、存储、加工、各环节的使用规范化问题，与个人隐私息息相关。目前，一些行业个人数据泄露事件频发，不法分子甚至还会利用已经泄露的海量数据进行关联分析，甚至做出客户画像，实施精准营销和诈骗。

其他类型的数据泄露事件也十分让人担忧。例如，谷歌 Firebase 平台 2271 个数据库可公开访问，这些数据库中包括了 1 亿多条敏感数据，约为 113GB；Google+出现 API 漏洞，在 11 月的 6 天时间里，5250 万用户的姓名、电子邮箱、职业和年龄以及其他详细信息被访问。

为加强数据泄露管理、切实维护企业利益、及时制止数据泄露的损害扩大。本报告将从网站漏洞的数据泄露风险，安服应急响应处置的数据泄露事件，全球重大数据泄露事件以及暗网上的数据交易事件这四个方面，来系统性的分析政企机构数据泄露的风险及形势。

第一章 网站漏洞泄露数据风险分析

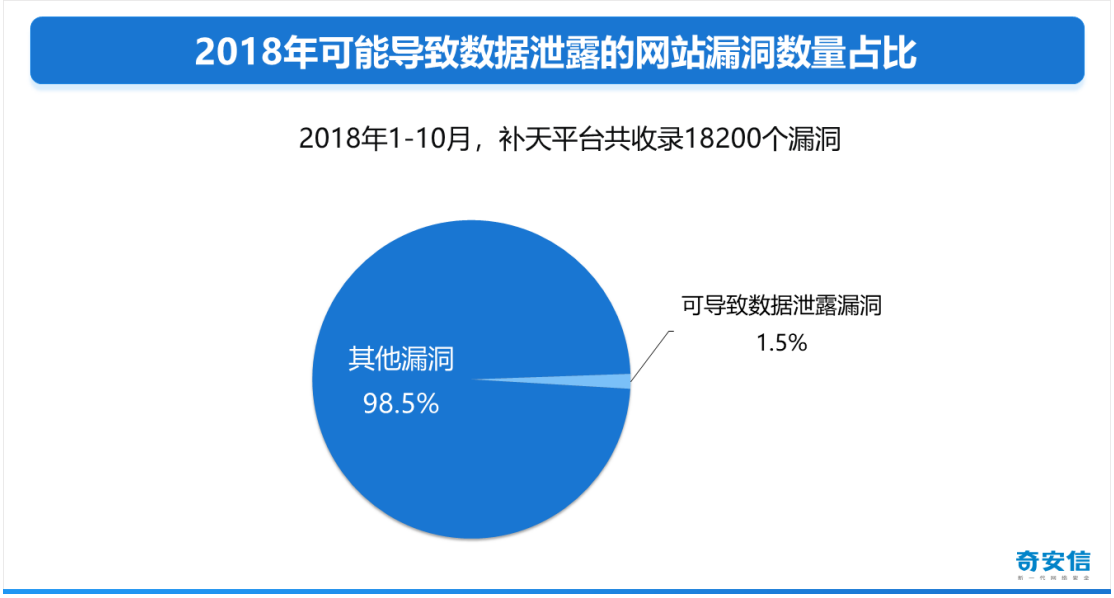
网站漏洞是当前的网络安全威胁之一，已对政企机构造成诸多危害，比如：数据库数据泄露、网页篡改、网页被挂马、服务器被恶意操作等。由于网站存在安全漏洞所导致得出的数据泄露，既是政企机构数据泄露的原因之一，也是数据安全的主要挑战之一。

本章将以补天平台 2018 年 1 月至 10 月，收录的可导致数据泄露的漏洞为基础，对 2018 年网站漏洞泄露数据的严峻形势进行简单分析。

一、 可泄露数据的网络漏洞数量

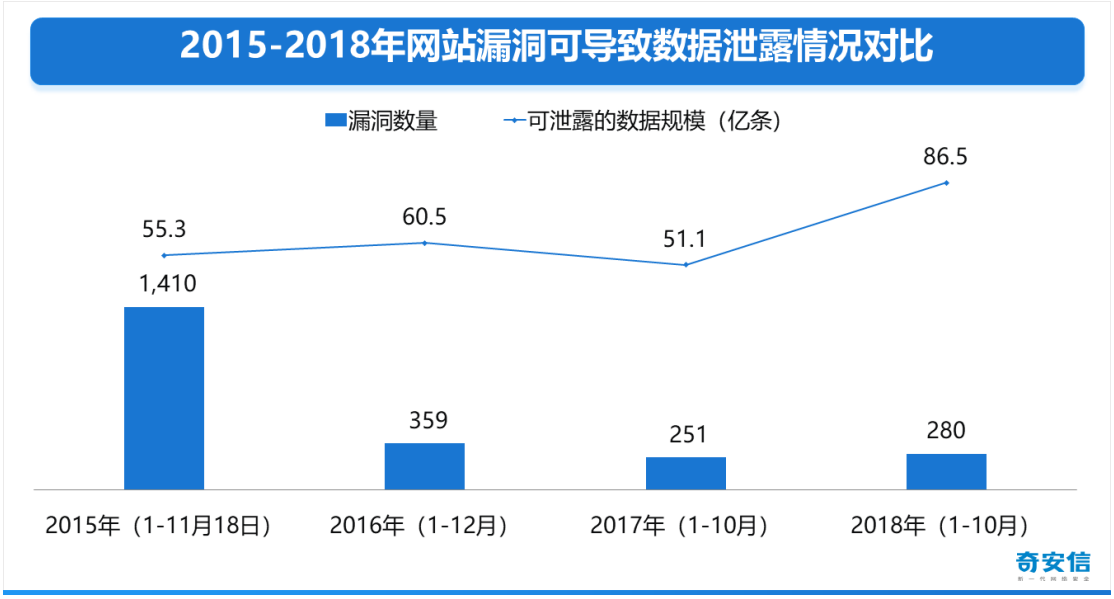
2018 年 1-10 月，补天平台共收录可导致百万条以上数据泄露的网站漏洞 280 个，约占补天平台全年漏洞收录总数（18200 个）的 1.5%，涉及网站 129 个，共可造成 86.5 亿条数据泄露。

2018 年可造成数据泄露的这 280 个网站漏洞，较 2017 年（251 个）上升了 11.6%，且全部为高危漏洞。

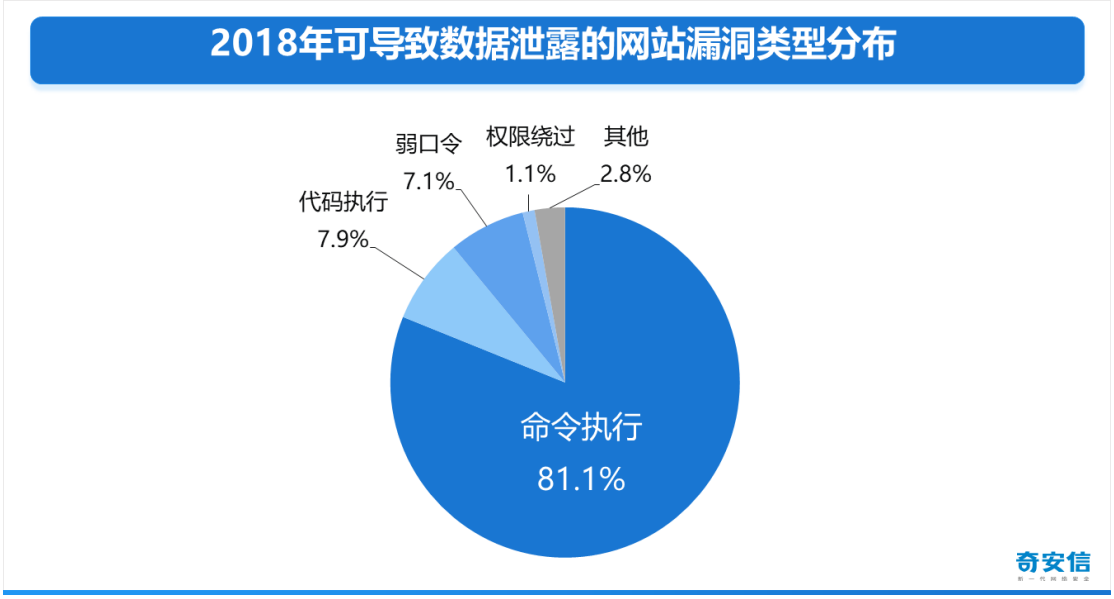


从 2015 年至 2018 年网站漏洞可导致数据泄露的规模对比来看，2018 年的 280 个可导致数据泄露的网站漏洞，总计可能泄露信息为 86.5 亿条，比 2017 年的 51.1 亿条上升了 69.2%；比 2016 年的 60.5 亿条上升了 43.0%；比 2015 年的 55.3 亿条上升了 56.4%。网站漏洞导致数据泄露的规模正在逐年增加。

2018 年，平均每个漏洞可导致 3089.2 万条个人数据泄露，单个漏洞的危害大大增加。



从可导致数据泄露的网站漏洞技术类型来看，2018 年可能泄露数据的网站漏洞中，命令执行占比最高，为 81.1%。主要是因为命令执行漏洞相比其他类型漏洞，产生的危害更高，白帽子为了不断提高自我的技术，所以更偏好“命令执行漏洞”。其次为代码执行和弱口令，占比分别为 7.9%和 7.1%。



命令执行漏洞：当应用需要调用一些外部程序去处理内容的情况下，就会用到一些执行系统命令的函数。如 PHP 中的 system，exec，shell_exec 等，当用户可以控制命令执行函数中的参数时，将可注入恶意系统命令到正常命令中，造成命令执行攻击。简单来说，是指代码调用系统命令的时候，过滤不严格，从而导致攻击者可以执行任意系统命令。

利用条件：

1） 应用调用执行系统命令的函数；

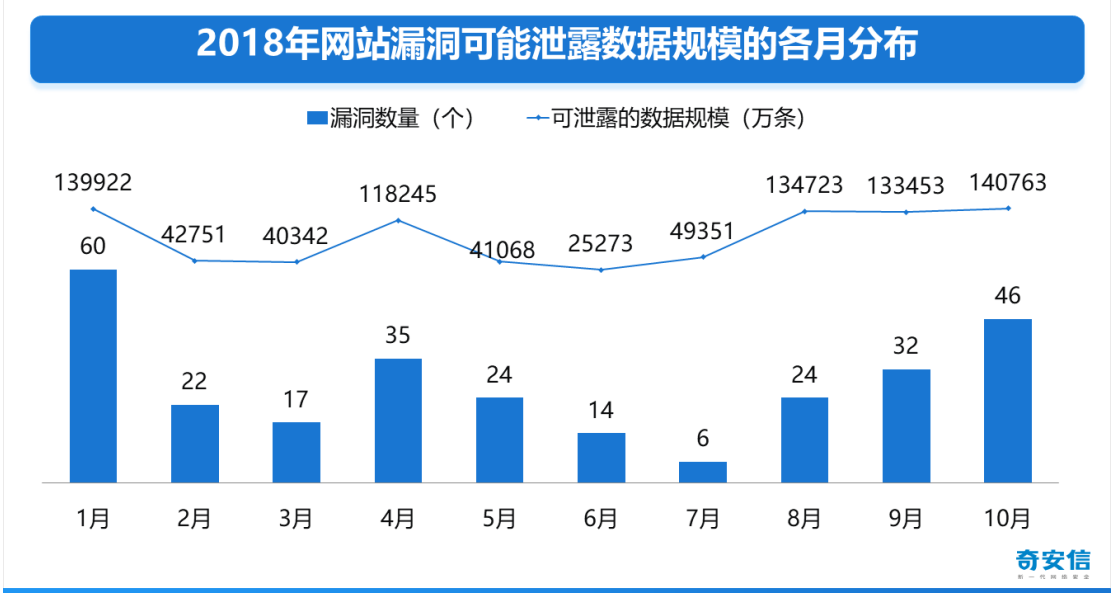
2） 将用户输入作为系统命令的参数拼接到了命令行中；

3） 没有对用户输入进行过滤或过滤不严。

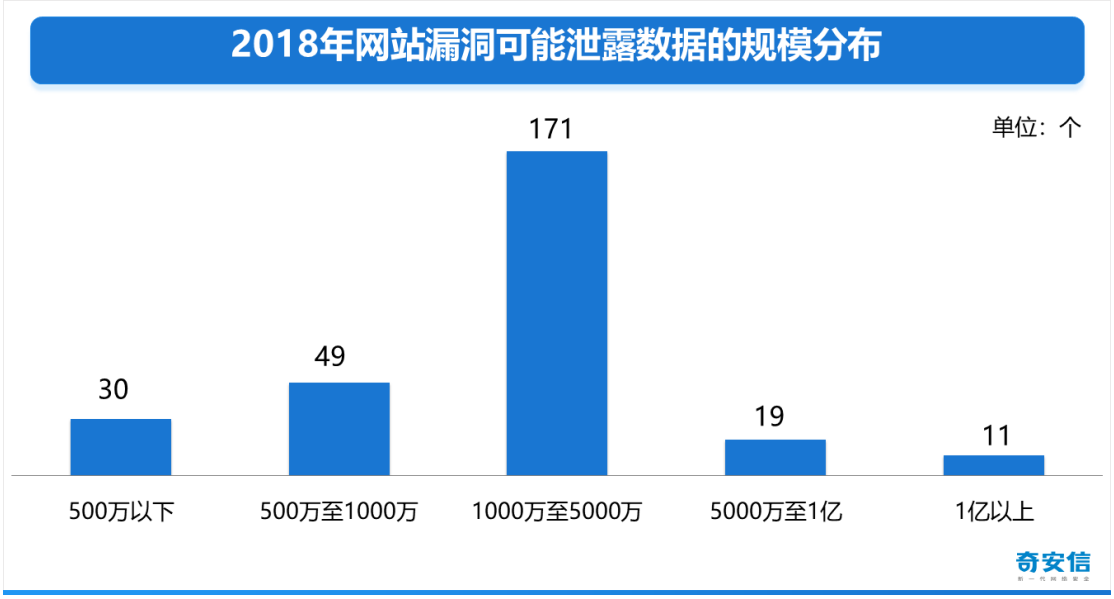
二、 网站漏洞可泄露的数据规模

2018 年 1 至 10 月，补天平台收录的可导致数据泄露的 280 个网站漏洞中，共涉及到 86.5 亿条数据泄露。其中，1 月份曝出的可能泄露数据的网站漏洞个数最多，为 60 个；10 月份曝出的可能泄露的数据规模达到最高峰，为 14.0 亿条信息。

下图给出 2018 年网站漏洞可能泄露数据规模的各月分布。



从网站漏洞可能泄露的数据规模来看，在 280 个可导致数据泄露的网站漏洞中，共有 30 个网站漏洞可泄露的数据规模在 5000 万条以上，其中还有 11 个漏洞可泄露的数据规模在 1 亿条以上。下图给出了 2018 年网站漏洞可能泄露数据的规模分布析。



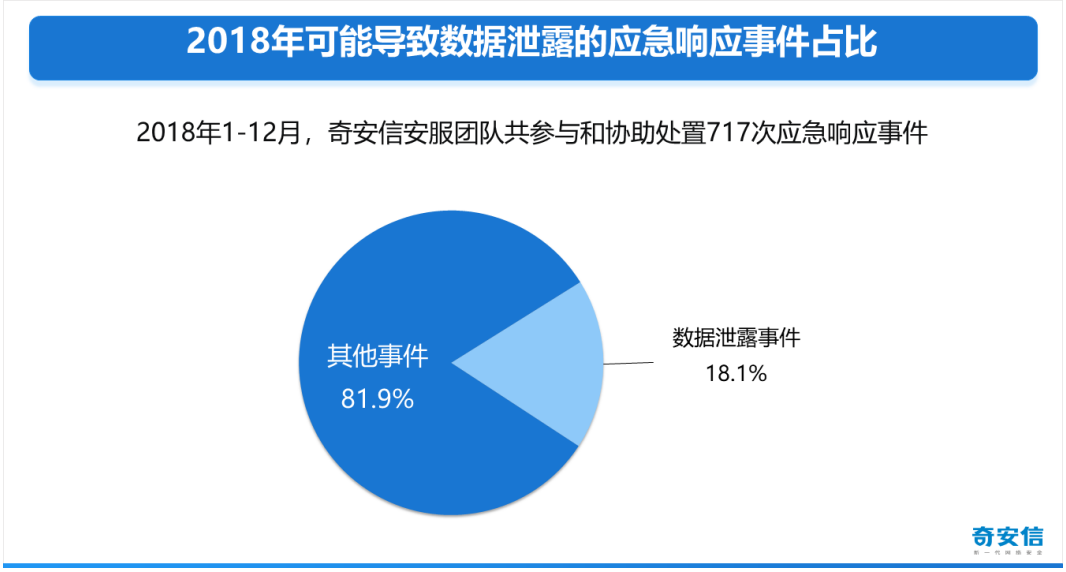
第二章 应急响应处置的数据泄露事件

通常来说，应急响应泛指安全技术人员在遇到突发事件后所采取的措施和行为。而突发事件则是指影响一个系统正常工作的情况。这里的系统即包括主机范畴内的问题，也包括网络范畴内的问题，例如：黑客入侵、信息窃取、拒绝服务攻击、网络流量异常等。

本章主要根据安服团队应急响应现场处置时，涉及到的政企机构数据丢失和敏感数据泄露的事件（下文统称为数据泄露事件）进行分析。

一、 数据泄露事件的应急次数

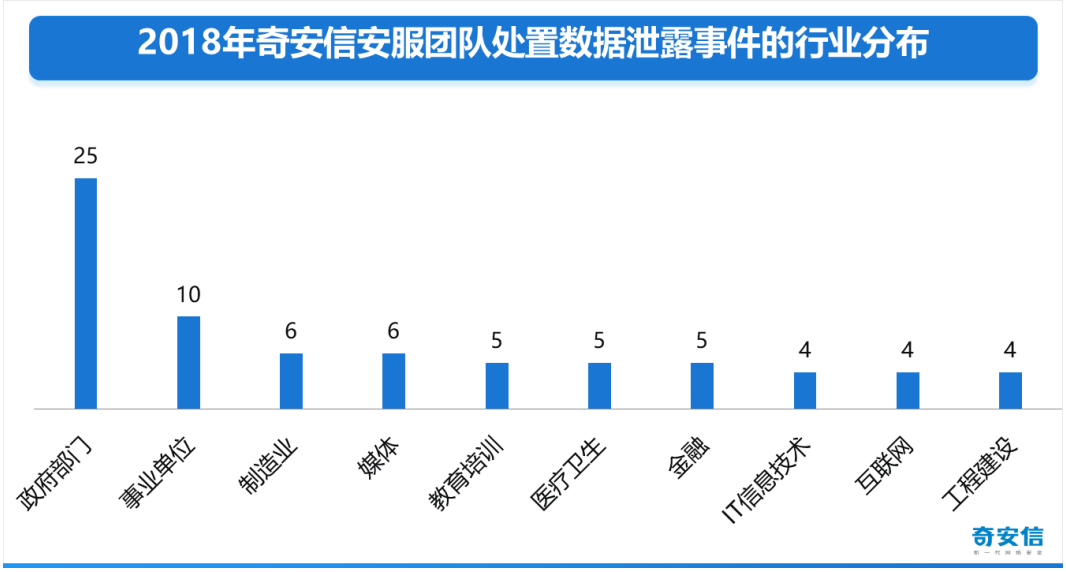
2018 年 1-11 月，安服团队共为全国各地多家大中型政企机构，提供了网络安全应急响应服务，参与和协助处置各类网络安全应急响应事件 717 次。其中，涉及到数据泄露事件共 130 次，占应急响应处置事件总数的 18.1%。



二、 数据泄露事件的行业分布

在涉及到数据泄露的政企机构中，政府部门是应急响应处置的数据泄露事件最多的行业，为 25 次，其次是事业单位，为 10 次；制造业，为 6 次。

下图给出了部分关键行业应急响应数据泄露事件的情况。

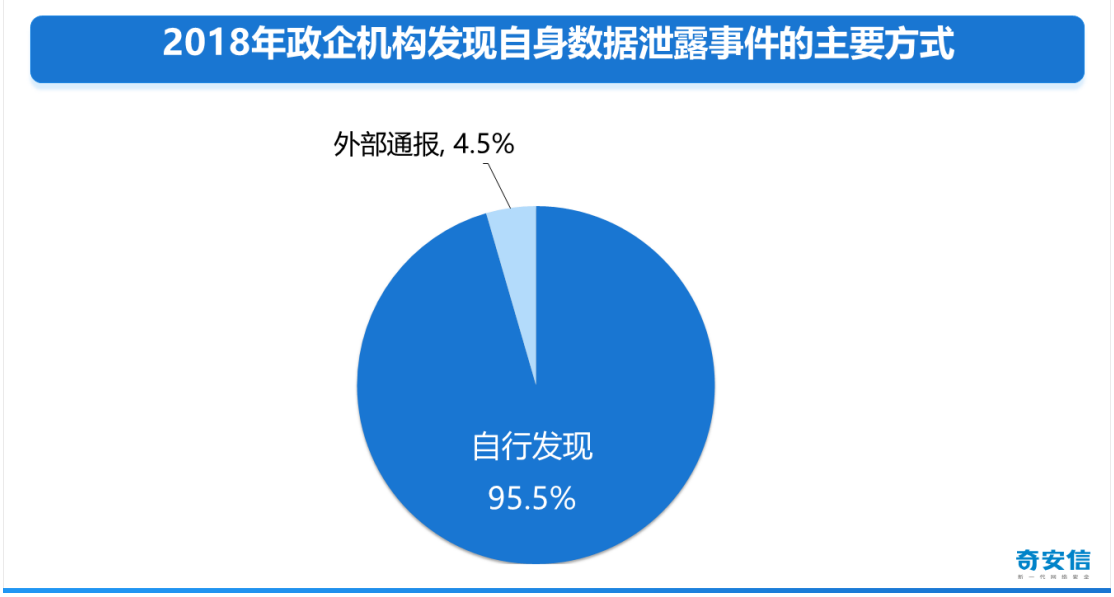


需要说明的是，应急响应次数多，并不意味着这个行业的整体安全状况差。这与机构本身的数量和性质有关，与奇安信的客户覆盖也有关。

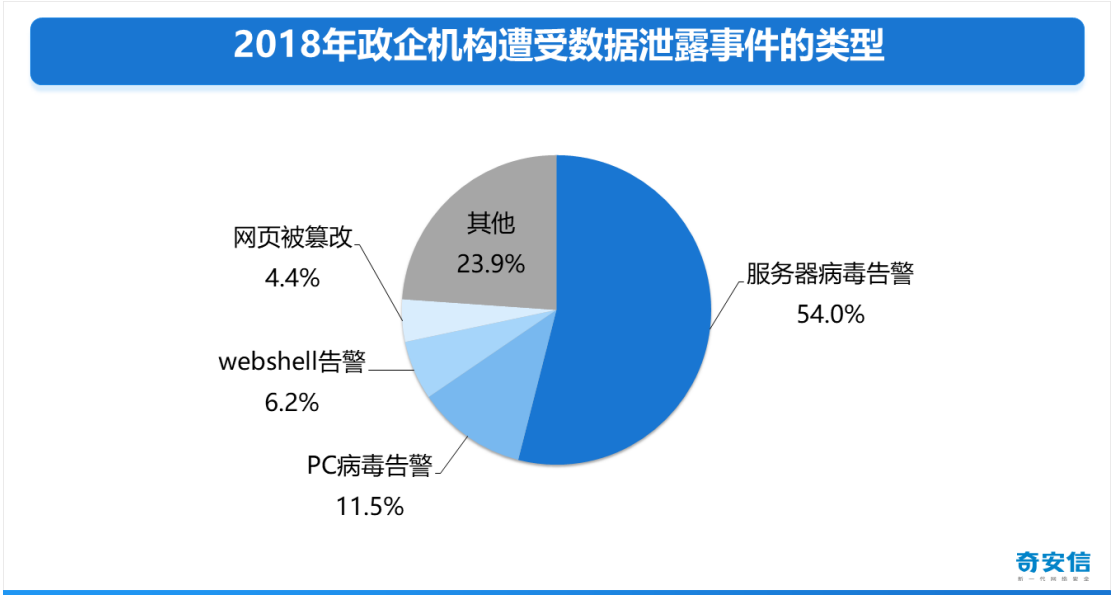
三、 数据泄露事件的发现方式

政企机构对网络攻击的重视程度、发现能力和主动响应的能力正在显著上升。95.5%的数据泄露事件是企业自行发现的，分析认为，这可能主要是由于 2017 年 6 月《网络安全法》的实施，大中型政企机构对安全事件的应急响应重视程度大幅提高，提早发现，尽早处置，自行响应渐成主流。

但是，仍有 4.5%的数据泄露事件，企业实际上是不自知的，他们是在得到了监管机构的通报或看到了媒体的公开报道后，才得知企业的内部数据已经被泄露的。

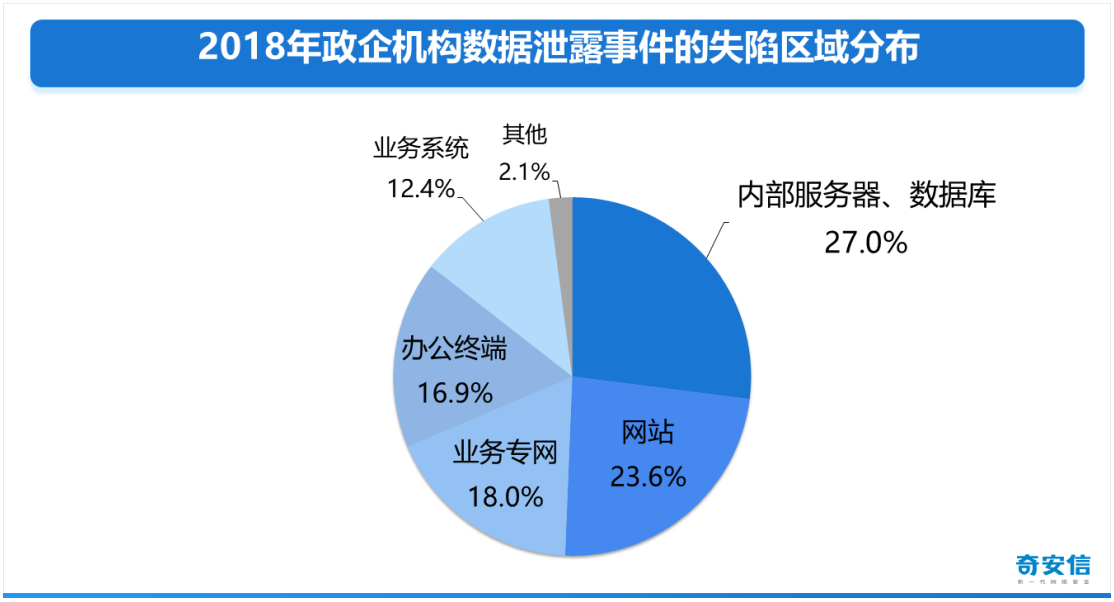


进一步对企业发现的网络攻击进行分析，54%的网络攻击事件是由于服务器病毒进行了告警；11.5%是由于 PC 病毒告警；6.2%是由于 webshell 告警；4.4%是由于网页被篡改。



四、 数据泄露事件的失陷区域

从大中型政企机构数据泄露事件中的失陷区域来看，27.0%为内部服务器、数据库；23.6%为网站；18.0%为业务专网；16.9%为办公终端，12.4%为业务系统。

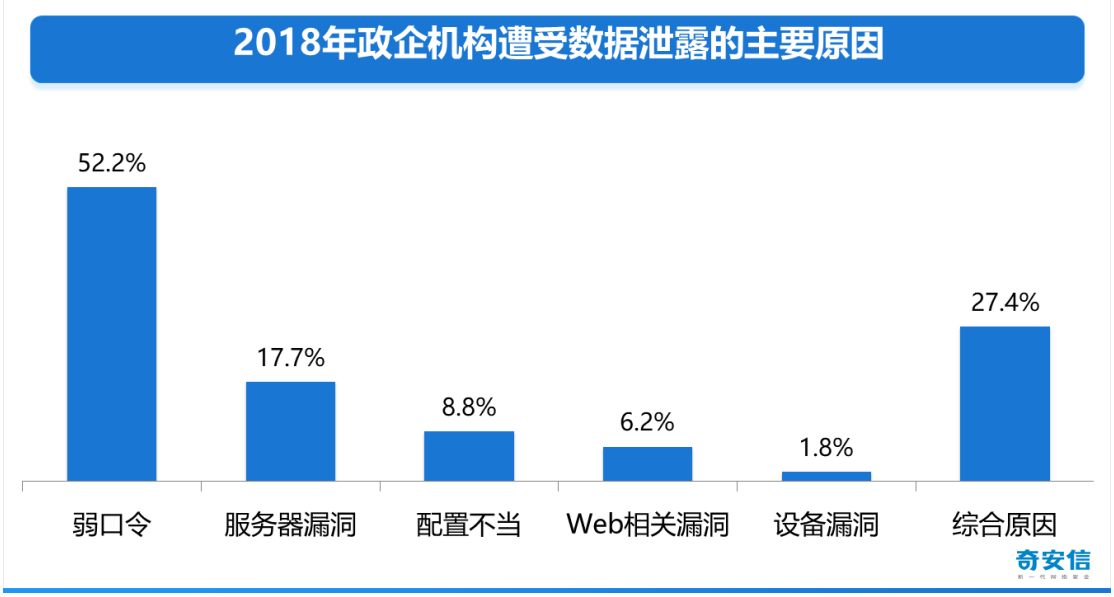


五、 数据泄露事件的自身弱点

数据泄露事件的发生，往往会暴露出相关政企机构内部存在的安全运营和管理问题。在安服团队 2018 年参与处置的 130 起数据泄露事件中，弱口令问题最为显著，约有 52.2%的数据泄露事件是由于弱口令问题导致的。

其次，25.7%的事件与未及时修复漏洞有关（业界已知，但相关机构可能不知道），包括：17.7%的服务器漏洞、6.2%的 Web 漏洞、1.8%设备漏洞。

整体呈现出数据泄露渠道多样，如黑客攻击、系统漏洞以及内部管理人员的不法操作等，难以从源头上消除。下图为 2018 年政企机构遭受数据泄露的主要原因分布。



我们这里所说的弱口令，并不单单指的是使用较短的字符组合，下面列举了常见的弱口令组合：

1） 较短的字符组合，如：111111、123456、abc123

2） 常见的破解字典中的短语，如：iloveyou、password、admin

3） 多个系统使用同一个口令去访问，长时间的使用同一个口令

4） 基于某种通用规则或使用习惯，如：360@1234、taobao@1234

需要特别说明的是，由于政企机构的内部网络安全建设错综复杂，可能由于多种原因致使其遭受网络攻击，本文只对我们处置的数据泄露事件中常见的问题进行分析。

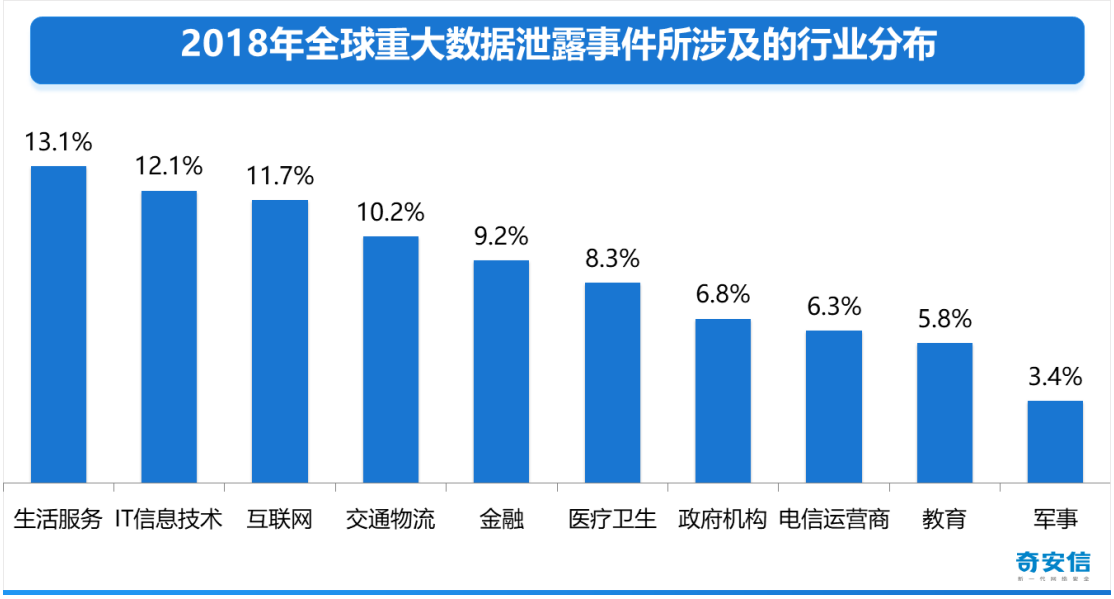
第三章 全球政企机构数据泄露分析

2018 年，全球政企机构均发生了大量的重大数据泄露事件，本报告对国内外媒体公开报道的事件进行了整理，共抽样收集了 206 起重大数据泄露事件。本章将基于这 206 起事件，对全球的数据泄露安全风险及由此引发的其他安全问题进行总结和简要分析。

一、 全球数据泄露事件的行业

2018 年，全球政企机构重大数据泄漏事件中，13.1%为生活服务行业（生活服务主要是指酒店、商场、食品、餐饮、服装及其他日用消费品与服务等与日常生活密切相关的企业），12.1%为 IT 信息技术，11.7%为互联网行业。

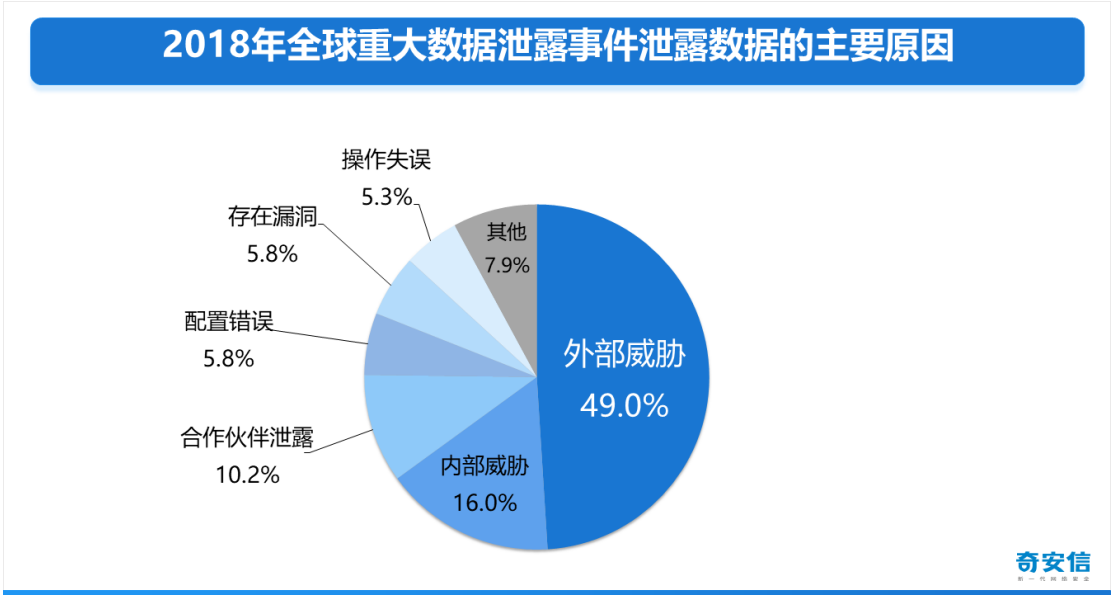
下图给出了 2018 年全球政企机构重大数据泄露事件所涉及到的十大行业分布。



二、 全球数据泄露的原因

从 2018 年政企机构重大数据泄露事件泄露数据的原因来看，约一半的事件是由于外部攻击导致的；但是也有 16%的事件是由于内部人员违规操作，主动泄露的数据，10.2%的事件是由于合作伙伴泄露（主要是指供应商和服务商）。

内鬼作案是数据泄露的一个重要途径。我们不仅要防外也要防内，做好数据操作的审计，防止非授权信息读取，防止越权的敏感信息读取，包括一些过度的数据读取其实也是一种泄露，比如：在办一些业务的时候本来只用知道该用户的姓名、性别及年龄，但是在相关资料上还能看到其联系方式、工作单位等信息，这样的过度读取或者暴露个人信息的行为也不合适。



三、 数据泄露的类型

根据数据的敏感度，我们把政企机构泄露的信息划分为以下几个类型：

1）实名信息：如姓名、电话、身份证、银行卡、家庭住址等信息。

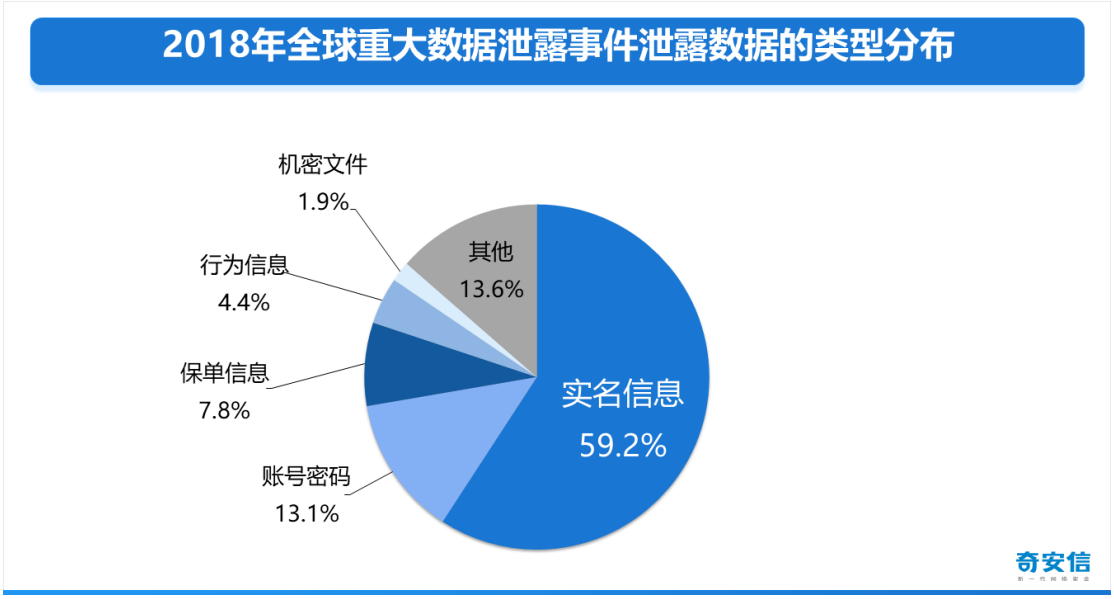
2）帐号密码：如各类网站登录帐号密码、游戏帐号密码、电子邮箱帐号密码等。

3）保单信息：如保单号、保险信息、车险信息等。

4）行为记录：如聊天记录，购物记录、差旅信息等。

5）机密文件：如财务信息、合同信息、风险投资信息等。

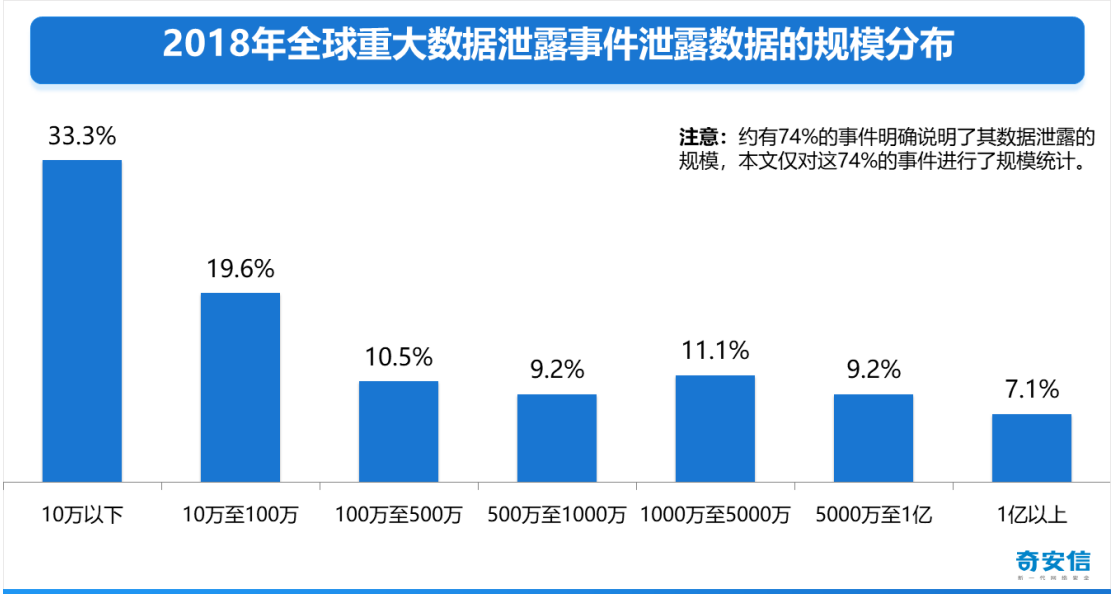
从 2018 年全球重大数据泄露事件泄露数据的主要类型来看，59.2%的事件泄露的是实名信息；13.1%的事件泄露的是账号密码；7.8%的事件泄露的是保单信息；4.4%为行为信息，1.9%为机密文件。



四、 数据泄露的规模

我们收录的 206 起全球重大数据泄露事件中，约 74%的事件我们大概标记出了数据泄露的规模。这 153 起事件，泄露了约 13 亿条信息。

从 2018 年全球重大数据泄露事件泄露的数据规模分布来看，47.1%的事件泄露的数据规模在 100 万条以上。值的注意的是，7.1%的事件泄露规模在 1 亿条以上。下图显示了 2018 年全球重大数据泄露事件泄露数据的规模分布。



第四章 暗网上非法数据的交易情况

“暗网”（Darknet 或 DarkWeb）指只能通过特殊软件、授权或对电脑作特别设置才能访问，在流行的搜索引擎上无法查到的特殊网络。这种特殊网络的服务器地址和数据传输通常都是“隐身”的，难以通过常规技术手段查找检索，“暗网”成员的相互联络具有极端私密性，一般技术手段很难拦截，即便拦截也难以破译。

暗网由于自带“隐身”属性，成为了大多数犯罪份子的主要集中地。很多被黑客窃取或者公司内鬼泄漏的数据一般都会在暗网出售。总体来讲，暗网虽然在网络规模上，跟明网相比要小得多，但大多数非法信息交易都集中在暗网。

从某暗网交易平台上，我们抽样收录了 2018 年 9-12 月以来不法分子发布的 1000 条数据交易情况，本章将对暗网上非法数据的交易情况进行总结和简要分析。

一、 活跃的数据发布者

暗网不同于明网，需要安装特定的浏览器和部署，才能登录。登录暗网的人群常常是带着特殊目的和属性，以非法交易为目的的暗网使用者，主要分为以下几类：

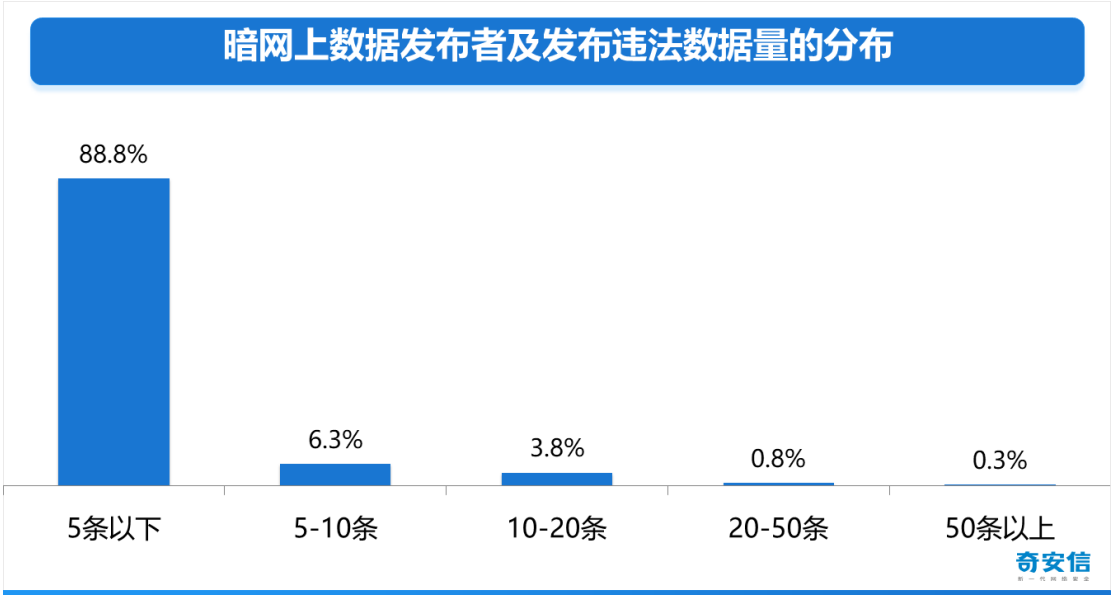
1） 违法、违禁物品、服务、数据、资料等的提供者；

2） 违法、违禁物品、服务、数据、资料等的购买者；

3） 网络诈骗犯罪团伙；

4） 非法中介、黄牛；

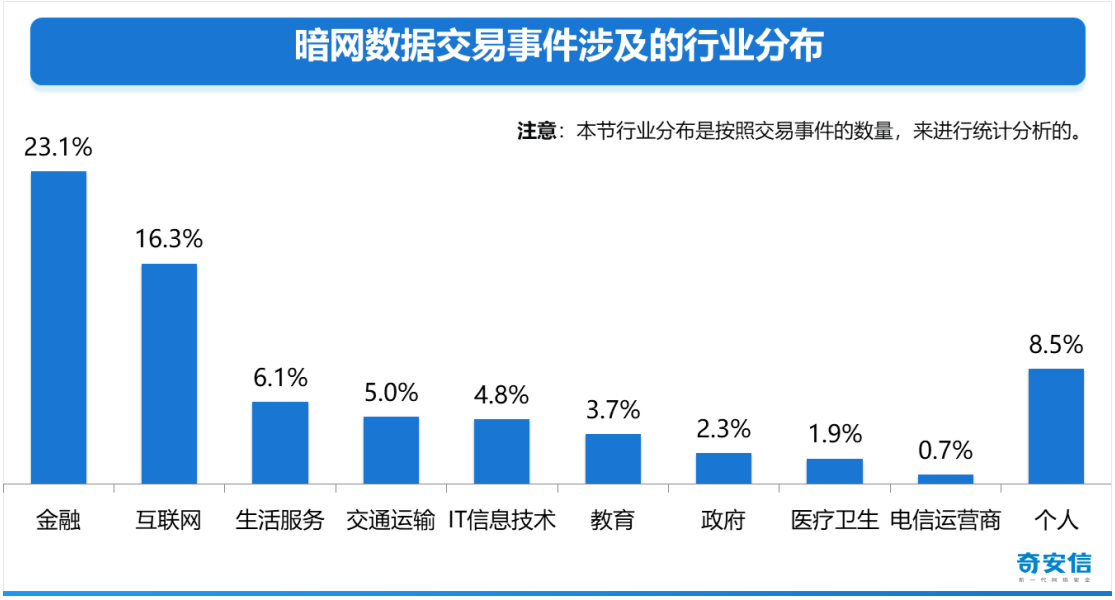
从暗网上数据发布者的活跃人数来看，本文收集这的 1000 条数据交易中，分别由 368 个人发布的，平均每个发布者发布约三条信息。具体来看，发布信息在 5 条以下的人数占 88.8%，发布信息在 5-10 条的人数占 6.3%，发布信息在 10-20 条的人数占 3.8%，发布信息在 20-50 条的人数占 0.8%，发布信息在 50 条以上仅有 1 人，占比为 0.3%。



二、 数据交易所涉及的行业

从暗网上数据交易所涉及的行业来看，金融行业占比为 23.1%；互联网行业占比为 16.3%；生活服务行业占比为 6.1%。还有一部分并未明显说明的行业属性，遂归属于个人信息。个人数据占比为 8.5%。

下图给出了暗网上数据交易所涉及的前九大行业及个人数据的情况。



三、 数据交易的类型及规模

根据数据的敏感度，我们把暗网上交易的数据分为以下几个类型：

1）实名信息：如姓名、电话、身份证、银行卡、家庭住址等包含实名的信息。

2）帐号密码：如各类网站登录帐号密码、游戏帐号密码、电子邮箱帐号密码等。

3）保单信息：如保单号、保险信息、车险信息等。

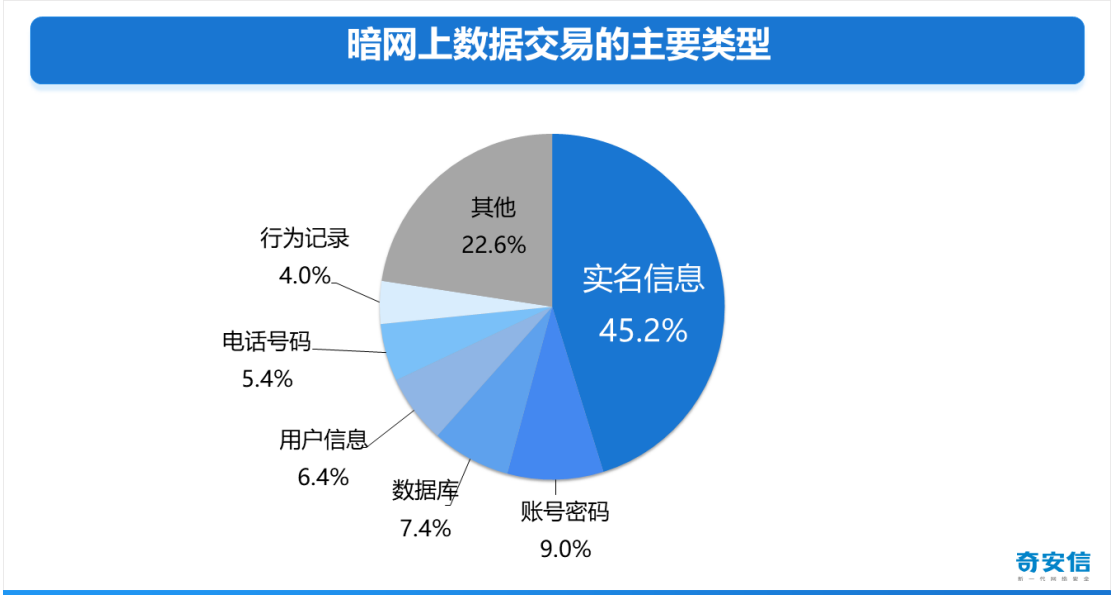
4）行为记录：如聊天记录，购物记录、差旅信息等。

5）机密文件：如财务信息、合同信息、风险投资信息等。

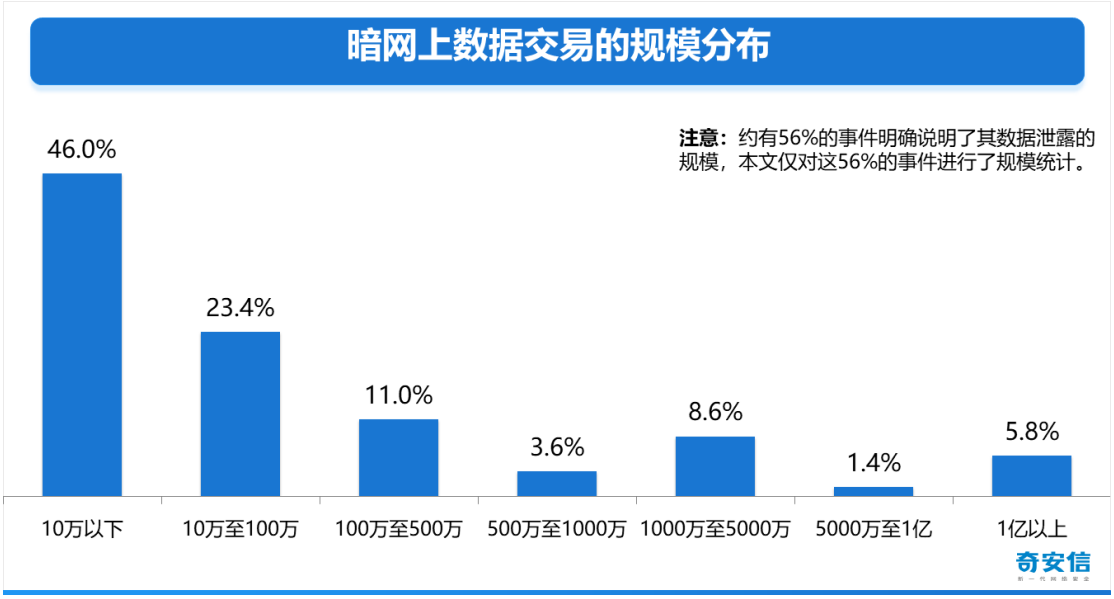
6）用户信息：如邮箱号码、账户列表、QQ 号码、会员列表等不包含真实姓名的信息。

7）电话号码：属于用户信息，如账户名及手机号码、注册号码。

从暗网上数据交易的类型来看，实名信息是被贩卖最多的一类信息，占比为 45.2%，其次为账号密码、数据库、用户信息、电话号码、行为记录等。下图列出了暗网上数据交易的主要类型及占比。



从暗网上数据交易的规模来看，10 万条以上的数据占到了 46.0%；10 万至 100 万条的数据占到了 23.4%；100 万至 500 万条的数据占到了 11.0%；500 万至 1000 万条的数据占到了 3.6%；1000 万至 5000 万条的数据占到了 8.6%；5000 万到 1 亿条的数据占比为 1.4%；1 亿条以上的数据，占比为 5.8%。具体分布如下图所示。



四、 获取数据后的一般用途

实名信息既是政企机构泄露最多的信息类型，也是暗网上信息贩卖最多的类型。本文的实名信息主要是指姓名、电话、身份证、银行卡、家庭住址等包含实名的信息。下面介绍了几种，信息购买者购买数据的一般用途。

1） 精准营销

通过对人群基本属性、行为习惯、商业价值等多种维度信息数据综合分析，精准的进行目标受众的画像和定位，实现基于大数据的精准营销。例如，拥有用户流量入口的社交软件和媒体公司，纷纷通过整合自有和外部的媒介资源，在用户画像的基础上针对行业客户提供广告精准投放服务。

保健品、保险、理财、房地产中介等行业是数据的主要购买者。在众多公民个人信息中，老人和学生的信息相对来说更受欢迎。老人的信息经常会被相关公司用来推销保健品,而学生的信息则被一些教育机构用来招生宣传。

信息购买者根据购买的数据，对人群进行定向的营销推广，常见的形势有：推销电话、短信骚扰、垃圾邮件和广告弹窗等。

2） 精准诈骗

信息被泄露后，一些上门推销、诈骗电话短信、垃圾邮件、神秘包裹等不请自来。调查显示，其中最困扰网友的是诈骗电话和短信。根据中新网报道，PC 端与微信端均有超过 70%的网友表示诈骗电话、短信是自己信息被泄露后，最困扰自己的事情。而此前中国银联就曾利用大数据分析向社会发布安全提醒，电信诈骗案、盗窃银行卡、非法套现、冒用他人银行卡、网络消费诈骗等，其中超过 90%是由于个人数据泄露引致，已成为犯罪主要源头。

3） 在其他渠道贩卖

信息倒卖者以低价购买公民个人信息、随后以高价卖出，非法获益。

根据中研网报道，在齐齐哈尔农垦区人民法院 2017 年的一起判决中，被告人崔文虎便是一名从上线低价购买公民个人信息、随后以高价卖出的倒卖信息者。从 2015 年 5 月开始，崔文虎在一年半的时间里先后倒卖 6 次公民个人信息，累计获利近 10000 元。

第五章 政企机构数据泄露的原因

网络攻击、内鬼窃取、内部人员操作失误，已经成为当前政企机构数据泄露的三大主要原因。黑客使用社工或技术手段攻破企业的安全技术防线窃取数据；内部人员利用职务之便非法获取公司数据进行贩卖；内部人员无意识的错误操作引发公司数据泄露。

一、 弱口令是黑客攻击成功的关键因素

口令是网络系统的第一道防线，当前的网络系统都是通过口令来验证用户身份、实施访问控制的。口令攻击是指黑客以口令为攻击目标，破解合法用户的口令，或避开口令验证过程，然后冒充合法用户嵌入目标网络系统，夺取目标系统控制权的过程。

而现实生活中，人们常会不经意之间使用了弱口令去防护自己或企业的资产。根据安服团队应急响应的数据显示，52.2%的事件是由于使用弱口令导致其所在机构被攻击的，弱口令问题依然是黑客能够攻击成功的关键因素。

黑客破解或绕过我们设置的口令，进入了目标网络系统后，他就能够随心所欲的窃取、破坏和篡改被侵入方的信息，直至完全控制被侵入方。

二、 内鬼威胁成为数据泄露的重要源头

内部人员在高额利益的驱使下铤而走险，利用职务之便非法获取大量公民个人信息出卖，已经成为数据泄露的重要源头。

2018 年全球重大数据泄露事件统计分析显示，16%的政企机构数据泄露事件是由于内部威胁导致的，内部威胁已经成为数据泄露的第二大源头。比如：社区卫生服务中心的徐某，多次从系统中导出新生婴儿及预产信息进行贩卖；机关单位的朱某，利用职务便利越权下载了公民个人信息，造成大量个人信息外泄；知名酒企的蔡某，多次通过拍照或直接用 U 盘拷贝的方式，窃取防伪溯源数据，从中非法获益。

内部人员进行违规操作、出卖公司利益已经成为公司的一大威胁。

三、 配置错误或操作不当事件频繁发生

误发送邮件、权限设置错误和服务器配置不当等误操作，导致的数据泄露事件正在显著上升，这也从中反应了内部人员缺乏一定的安全意识或风险评估能力。

2018 年全球重大数据泄露事件统计分析显示，11.1%的事件是由于配置错误或操作不当导致的政企机构数据泄露。比如：某健康应用的服务器没有设置密码，导致任何人都能够查看登录者和发送的消息内容；某公司程序员将数据库连接方式上传至 GitHub 导致其泄露；某服务器管理员没有关闭 Django 应用程序的调试模式，导致 API 密钥、数据库密码或 AWS 访问密钥之类的敏感信息暴露。

四、 安全投入与保护目标的价值不匹配

IDC2016 年数据显示，中国的网络安全建设已经处于落后的地步，2016 年全球信息安全建设的投入占整体信息建设投入的比例中，美国占比达到了 4.78%，全球平均水平为 3.7%，而中国仅为 1.8%，尚未达到全球平均水平的二分之一。

信息安全的投入、与需要被保护目标的商业价值、社会价值不匹配，不能满足安全运维的需要。比如：马来西亚教育部推出的学校考试分析系统，由于存在漏洞的情况上线、明文存储密码、无视读者的警告等原因，导致上线第一天就被被迫下线。

安全投入不足与保护目标价值不匹配，一方面反映出很多企业在技术和管理层面目前仍未达到国家安全标准；另一方面也反映出网络安全保障的意识、认知和能力均落后于信息网络技术及其应用的爆发式增长。

第六章 政企机构数据泄露的趋势

一、 数据泄露的数量和规模正在大幅度上升

各行业、领域、国家在 2018 年都出现了大规模的数据泄露事件，根据补天平台数据显示，2018 年比 2017 年的数据泄露规模上升了 69.2%，数据泄露事件的数量在上升的同时也更加常态化。

数据泄露的数量和规模都在不断上涨，表明我们所面临的风险正在超过企业采取安全措施的保护能力。随着全球信息化程度的提高，全社会对网络和数字化技术的依赖，这一情况很有可能还将加剧。

二、 对重要数据进行定向化攻击并实施勒索

针对重点行业、重要数据，黑客也会进行盯梢，反复研究并实行攻击。针对这类机密数据，黑客在窃取成功后，不是进行贩卖，而是反其道而行，对受害者进行勒索。

比如：黑客在加拿大银行的蒙特利尔银行窃取数据后，向银行勒索并声称：已经访问了客户的账户以及相关数据，若不支付 100 万赎金就将公开被盗客户数据。

比如：黑客 DarkOverlord 在从一家为保险公司提供咨询服务的律师事务所窃取到 911 文件后，竟然向该律师事务所实施勒索，索要赎金。

三、 外部力量督促企业加强安全建设

数据泄露事件往往具有很强的隐蔽性，其发现过程具有一定的潜伏期。暗网上数据交易被披露、受害者受到骚扰后的举报、媒体的监督报道，这三大现象已经成为企业发现自身数据被泄露的新原因，同时也反逼企业不断加强网络安全建设和数据保护措施。

比如：张女士刚生完孩子不久，夫妻两个人频繁接到母婴拍照、奶粉购买、新生儿保险等推销电话，张女士报警后，警方通过查处才发现是某地卫生系统出现内鬼，向外贩卖数据，由于张女士及时举报，警方及时查处并揭露了内鬼，避免了更多的新生儿信息被暴露。

普通民众一旦发现自己的信息被泄露后，及时向警方举报，有助于揭露数据泄露的源头，更有助于企业发现自身的数据泄露，加强安全建设。

四、 数据泄露事件折射更多社会问题

我们往往认为数据泄露会导致社会诈骗泛滥，但是，现在数据泄露已经造成更加广泛的影响，与更多的政治、经济、道德等事件交织在一起，引起社会更多的热议。

比如：2019 年 1 月，澎湃新闻报道“深圳父母虐童事件，爆料者被罚”，王某和钟某二人利用非法获得的刘某为监管子女状况在家中安装的网络监控摄像头账号及密码，多次登录摄像头偷窥，并下载编辑后发布。该事件引起社会热议后，警方迅速采取行动：女童父母被采取刑事强制措施，视频发布者遭到行政处罚。但是，此次事件除了引起社会人士对儿童的

关注外，还引发了对“爆料者”非法手段曝光行为的讨论，是否可以用非法手段揭示正义行为等问题。

又如：黑客 DarkOverlord 曾声称，已经从一家为保险公司提供咨询服务的律师事务所窃取到 911 文件，事后该律师事务所违反之前达成的赎回协议，向执法部门进行了报告。黑客组织们因无法忍受律师事务所的欺骗，向外公布了部分 911 数据。该事件又一次引起了人们对 911 恐怖袭击事件的关注。

五、 数字化转型的企业将面临更大的数据泄露风险

数据泄露问题是政企机构数字化转型过程中普遍存在的安全问题。数字化转型较早，信息系统网络化程度相对较高的行业和领域，被暴露出来的问题也相对较多。如金融、通信、新兴互联网等领域。但随着数字化转型的逐渐深入以及网络安全建设水平的不断提高，这些行业或领域在度过数据泄露的高峰期后，安全问题会逐渐缓和。

相比之下，某些数字化转型相对较晚的行业或领域，如某些大型政府机构、制造业，以及某些传统实体经济，现在暴露出来的问题就相对较少，但在未来不可避免的数字化转型过程中，也必然会逐渐暴露出越来越多的安全问题，面临越来越大的数据泄露风险。

从另一个角度来看，在消费互联网时代，聚集大量个人服务的信息系统，往往容易成为数据泄露的高发点。而在未来，随着智慧城市的建设，产业互联网的出现，传统的实体经济的互联网化，政务云和互联网+的普及，政府机构和实体经济将有可能面临更大的数据泄露风险，成为数据泄露新的高发领域。

第七章 防范数据泄露的建议

我们面临很多问题：信息系统无法杜绝漏洞，机构本身的防护机制不健全，对数据的重要程度不敏感，以及对安全配置的疏忽大意等。但是，我们还是可以通过以下措施来最大化的减少数据泄露。

一、 使用强密码并定期修改

设置密码尽量复杂，并且不同的网站设置不同的密码。面对密码复杂繁多不容易记忆的情况下，我们可以制定不同的规则，比如：密码=网站名称+物品+大写+数据+标志等。既有一定的规则容易记忆，又能保证每个网站密码的不一样。

此方法有效的防范了黑客拖库、撞库等常用手段。

二、 加强网络安全意识

每个员工，甚至是不使用计算机的人，都有可能成为攻击者的目标。而公司新近雇用的员工则是社会工程师最容易突破的薄弱环节，企业的安全培训和安全策略务必要加强这方面的注意，正确的教育和培训，将会极大的提升员工正确处理企业内部信息的意识。

定期举行安全意识培训，加强员工的安全意识，使每个员工都认识到，不仅是上司或管理人员拥有攻击者想追寻的信息。当一个知道公司办事程序、专用术语和内部标识的人打来电话时，并不意味着他或她就可以知道所查询的信息，对方可能是公司以前的员工或是知道公司内部一般情况的合同工。

三、 数据进行分类管理

应仔细检查信息的分类并制定资料分类策略，注意哪些正式员工可以到的看似无害也可能会导致敏感数据泄露的信息。

企业的安全策略应遍布企业的各个地方，而无所谓职位的高低。资料数据的分类策略将帮助企业，实施对信息使用的正确控制，如果没有分类策略，所有的内部信息都应被视为保密，除非另做指定。

附录 1 国内机构重大数据泄露事件分析

一、 内部威胁

（一） 某地方卫生系统出“内鬼”泄露 50 多万条新生婴儿和预产孕妇信息

2018 年 1 月，某警方侦破了一起新生婴儿信息倒卖链条。从新学婴儿数据泄露的源头来看：某社区卫生服务中心工作人员徐某，掌握了某市“妇幼信息某管理系统”市级权限账号密码，利用职务之便，多次将 2016 年至 2017 年的某市新生婴儿信息及预产信息导出。被抓获前，他累计非法下载新生婴儿数据 50 余万条，贩卖新生婴儿信息数万余条。

值得注意的是，在该案中，徐某仅是某市某社区卫生服务中心工作人员，却掌握了某市“妇幼信息某管理系统”市级权限账号密码。

从卫生系统“内鬼”徐某到公开出售信息的黄某，多名犯罪嫌疑人层层转手，组成了一条长长的新生婴儿信息倒卖链条。

（二） 某员工私自转让公司权限给朋友，致使 30 余万条医生数据泄露

2018 年 2 月，某警方侦破了一起医生信息窃取案件。从医生数据泄露的源头来看：武某任职某企业管理咨询（上海）有限公司广州分公司移动医疗顾问一职，拥有公司某应用系统的工作权限，通过其手机二维码可进入系统，内有大量医生信息。出于朋友情面和同情心理，遂把上述权限给了卢谋。

获得权限后，卢某找来“计算机技术很好”的大学舍友温某，卢某指使温某利用该权限通过计算机技术进入应用系统后台，盗取系统内的医生信息。

截至 2016 年 10 月 11 日，被告人卢某、温某等人共窃取系统内的信息共计 352962 条。一条完整的医生信息包括姓名、手机号码、医院名称、职务及属地等。

庆幸的是，被抓获时，温某尚未把爬取到的医生信息交给卢某。

（三） 合作公司员工泄露防伪数据 700 万条，某知名酒企损失超百万

2018 年 2 月，某警方侦破了知名酒被仿造的案件。从防伪数据泄露的源头来看：蔡某拿任职于某公司的“国酒 XX 防伪溯源系统”项目专项经理，在 2014 年 4 月至 2016 年 9 月期间，曾多次利用职务之便通过拍照、直接用 U 盘拷贝的方式窃取某知名酒企股份有限公司防伪溯源数据，并将窃取出来的数据泄露给蔡某刚。

据法院审理查明，被蔡某拿披露数据量共计 700 余万条（可制作成 700 万瓶能够通过防伪溯源验证的假冒酒）。

但随着泄密事件发生，某知名酒企只得向其他公司重新采购防伪密管系统，并将原有防伪标签升级为安全芯片防伪标签，同时废弃前期采购的 4.3 万余枚防伪标签。据计算，防伪数据库的泄露直接导致某知名酒企经济损失约 105.7 万元。

（四） 某地方公务员利用职务之便，泄露 82 万条公民信息

2018 年 3 月，某法院审理了某地方公务员窃取信息案件。从公民个人数据泄露的源头

来看：朱某任职于某机关单位。从 2010 年起，朱某利用职务便利，应朋友刘某、王某的要求，超越职权下载了一些公民个人信息，并将这些信息分别提供给他们使用，造成大量的公民个人数据泄露。

经统计，2010 年 4 月至 2016 年 9 月，朱某向刘某提供公民个人信息 70 余万条，2011 年 11 月至 2016 年 7 月，朱某向王某提供公民个人信息 12 余万条。

（五） 某科技公司内鬼窃取 500 余万条个人信息，并在网上售卖

2018 年 4 月，某警方侦破了一起个人信息兜售案。从数据泄露的源头来看：北京某高校博士毕业马某，利用在科技公司工作的机会，以黑客技术破解公司数据库，非法盗取海量公民个人信息，包括：淘宝信息、金融信息、医疗信息、社保信息、车辆信息等，其中包括居民身份证号、家庭住址、电话号码等隐私。

此后，8 人团伙在网上贩卖出售公民信息，数量达 500 余万条，容量达 60G。目前，8 名犯罪嫌疑人全部归案。

二、 外部威胁

（一） 某手机厂商称：4 万消费者的信用卡数据泄露

2018 年 1 月，某手机厂商发布声明称，4 万名消费者的信用卡信息在 2017 年 11 月至 2018 年 1 月 11 日期间遭不明黑客盗取。

该手机厂商证实：网上支付系统遭入侵。攻击者针对其中一个系统发动攻击并将恶意脚本注入支付页面代码中窃取用户付款时输入的信用卡信息，该恶意脚本能直接从消费者浏览器窗口中捕获完整的信用卡信息，包括信用卡号、到期日期和安全代码。

然而，该手机厂商认为通过所保存的信用卡、PayPal 账户或者“经由 PayPal 通过信用卡”方法购买手机的消费者并未受影响。

（二） 北京某教育网站遭入侵，攻击者窃取 7 万余元

2018 年 4 月，朱某从一个 QQ 群中得知可以利用网站漏洞进入服务器后台，从而得到管理员权限，修改余额并提现的方法。而且 QQ 群给出了具体的链接，几乎不需要多少专业知识，一学就会。

所以，朱某在网上注册成为北京某教育科技公司网上商城的会员，利用网站漏洞进入服务器后台，对余额进行修改，打开提现功能。从 2016 年 11 月至 2017 年 3 月这几个月间，他多次从商城提现，共窃取 7 万余元。

（三） 多家美容医院的客户信息被窃取

2018 年 7 月，某警方侦破了一起盗窃、贩卖美容整形医院客户信息的案件，在美容整形医院网站上植入木马，侵入服务器，盗取客户信息，层层转手后贩卖给其他美容整形医院。

从美容整形医院客户数据泄露的源头来看：苏某与蒋某制作木马病毒后，假扮美容客户向医院客服咨询，将病毒链接藏匿在整形需求图片上，发送给工作人员。工作打开图片时，服务器被植入木马，客户隐私资料即被盗取。

潘在网上发出求购美容整形客户资料广告，苏某看到后一拍即合，将其发展为下线。“黑

中介”杨某某作为批量信息买主，将信息加价后再转让给末端的市场人员，由他们通过电话、网络等方式对客户直接“引流”到愿意给他们提成的医院。为了规避法律风险，他们还安排专门的中间人负责收付款，以防止黑色资金被监控。

（四） 某知名酒店集团 5 亿条数据泄露

2018 年 8 月，有网民发帖称售卖某知名酒店集团旗下所有酒店数据，该网友在帖子中称，所有数据脱库时间是 8 月 14 日，每部分数据都提供 10000 条测试数据。所有数据打包售卖 8 比特币，按照当天汇率约合 37 万人民币，随后又称，要减价至 1 比特币出售。

事故原因疑似该公司程序员将数据库连接方式上传至 github 导致其泄露，目前还无法完全得知到细节。

售卖的数据分为三个部分：

1） 官网注册资料，包括姓名、手机号、邮箱、身份证号、登录密码等，共 53G，大约 1.23 亿条记录；

2） 酒店入住登记身份信息，包括姓名、身份证号、家庭住址、生日、内部 ID 号，共 22.3G，约 1.3 亿人身份证信息；

3） 酒店开房记录，包括内部 id 号，同房间关联号、姓名、卡号、手机号、邮箱、入住时间、离开时间、酒店 id 号、房间号、消费金额等，共 66.2G，约 2.4 亿条记录。

8 月底，暗网上出现了某知名集团旗下多个连锁酒店客户信息数据的交易行为，数据标价 8 个比特币，约等于人民币 35 万人民币，数据泄露涉及到 1.3 亿人的个人信息及开房记录。9 月 19 日消息，窃取旗下酒店数据信息嫌疑人已经被上海警方抓获。

（五） “XX 驿站”一千万条快递数据被非法窃取

2018 年 9 月，某省公安厅获悉破获 1 个非法获取公民信息团伙，抓获犯罪嫌疑人 21 名。而被非法窃取的信息，经警方查实均系快递数据，来源于各大高校的大学生的快递信息。这些信息包含有单号、姓名、手机号、快递公司名称等。这类信息较为敏感，且数据的准确率极高。

警方通报，该案中，犯罪团伙并非采取以往的直接网络攻击盗取模式，而是对安装在物流网点手持终端（俗称巴枪）中的“XX 驿站”APP 进行破解后，植入控件程序。通过相关省份“XX 驿站”服务商进行推广安装后，直接通过数据回传获得数据。

截至破案，遭非法窃取的快递数据超过 1000 万条

（六） 某知名酒店数据库遭入侵，5 亿顾客信息或泄露

2018 年 11 月 30 日，某国际酒店集团（MarriottInternational）宣布，旗下某酒店（StarwoodHotel）的一个顾客预订数据库被黑客入侵，可能有约 5 亿顾客的数据泄露。这些可能被泄露的信息包括顾客的姓名、通信地址、电话号码、电子邮箱、护照号码、喜达屋 VIP 客户信息、出生日期、性别和其他一些个人信息。对于部分客户，可能被泄露的信息还包括支付卡号码和有效日期，但这些数据是加密的。

某知名酒店表示，调查结果显示，有一未授权方复制并加密了这些数据。而且，自 2014 年就开始了对其网络进行未授权访问。

附录 2 国外机构重大数据泄露事件分析

三、 IT 信息企业

（一） 问题综述

2018 年信息泄露事件叠出，传统行业的数据或者网络被入侵、被窃取，状况堪忧，然而为之提供先进的 IT 基础设施与信息化服务，或者托管服务的专业 IT 技术公司，尤其应该为之警醒。因为客户一旦把自家的数据放在了 IT 厂商的云计算设施、大型数据库软件中，这些 IT 技术厂商自身的计算系统与存储系统的安全至关重要。2018 年，IT 技术厂商发生的数据安全事件，多半因为云系统或者数据库配置疏忽或存在潜在隐患，而导致大量数据变的“毫无遮拦”。

（二） 数千台 Etcd 服务器可任意权限访问，暴露 750MB 密码和密钥

2018 年 3 月，据外媒报道，安全研究人员 GiovanniCollazo 通过 Shodan 搜索引擎发现近 2300 台安装了“etcd”组件的服务器暴露在互联网上，利用一些简单脚本即可从中获取登录凭证。目前 Collazo 经过测试已经成功地从这些服务器上检索到了来自 1485 个 IP、约 750MB 的数据，其中包括 8781 个密码、650AWS 访问密钥、23 个密钥和 8 个私钥。

虽然 Collazo 并没有测试这些凭证，但其中一些被推测是有效的，有可能会被攻击者用来侵入系统。此外，根据 Collazo 的说法，任何人只需几分钟时间就可以获得数百个可用于窃取数据或执行勒索软件攻击的数据库证书列表。

（三） 芬兰某公共服务网站数据泄露，超过 13 万芬兰公民受影响

2018 年 4 月，据芬兰媒体 SvenskaYle 的报道，芬兰通信管理局（FICORA）于 2018 年 4 月 6 日通过自己的网站向所有芬兰公民发出警告称，一个由赫尔辛基新企业中心（“HelsinginUusyrityskeskus”）负责维护的网站（liiketoimintasuunnitelma[.]com）在本周二遭遇了匿名黑客的攻击，大约有 13 万用户的账户用户名和密码被窃取，同时被窃取的还包括其他一些机密信息。从受害者数量来看，这将是该国有史以来发生的第三大数据泄露事件。

FICORA 表示，该网站并没有对存储的任何信息进行加密，无论是用户名还是密码都采用明文形式进行储存，这使得网络犯罪分子更容易利用它们。由于用户名和密码是以明文形式泄露的，因此赫尔辛基新企业中心董事会主席 JarmoHyökyvaara 建议，如果有用户在其他信息系统或网络服务使用了相同用户名和密码，应该立即对这些密码进行修改。而一旦 Liiketoimintasuunnitelma 网站重新恢复上线，还应该立即对该网站的账户密码进行修改。

（四） 美国软件公司 AgentRun 意外泄露众多保险公司客户个人敏感信息

2018 年 5 月，据外媒 ZDNet 报道，美国软件公司 AgentRun 在最近意外暴露了成千上万保单持有人的个人敏感信息，而究其原因是因为一个未加密的 AmazonS3 存储桶。

ZDNet 指出，不安全的存储桶没有使用密码保护，任何人都可以对其进行访问。该 AmazonS3 存储桶包含了大量的缓存数据，涉及数千名不同保险公司客户的个人敏感信息，包括类似 Cigna 和 SafeCoInsurance 这样的大型保险公司的客户，遭泄露的信息可能包括保险单文件、健康和医疗信息、各种证件的扫描件以及一些财务数据。

在整个数据泄露持续的一小时中，可被公众访问的数据包括：保单文件包含详细的保单持有人个人信息，如姓名、电子邮箱地址、出生日期和电话号码。在某些情况下，一些文件还显示了收入范围、种族和婚姻状况，甚至还附上了空白的银行支票。对于扫描件而言，涉及到各种证件，如社会安全卡片、医疗卡、驾驶执照、选民证和军人证件；医疗记录文件则包含了可以确定保单持有人医疗状况的各种信息，包括个人的处方、剂量和费用。

（五） 德国托管服务商 DomainFactory 大量客户数据遭外泄

2018 年 7 月，DomainFactory 公司在公告中指出，一名匿名黑客在 DomainFactory 的技术支持论坛上发帖称，他已经成功侵入了 DomainFactory 的客户数据库，并分享了几名 DomainFactory 客户的内部数据作为证据。发现这篇贴子后，该公司立即对其论坛进行了离线处理并展开了调查。调查结果显示，黑客的说法并非虚构。

DomainFactory 最终确认了这一泄露事件，并公布了能够被黑客所访问的数据类型，同时向客户发出了更改密码建议。泄露的数据包括：客户名称、公司名称、客户账户 ID、实际住址、电子邮件地址、电话号码、DomainFactory 手机密码、出生日期、银行名称及账号等。

（六） 销售背锅！AWS 官方人员导致 GoDaddy 数据泄漏

2018 年 8 月，UpGuard 网络风险小组近日发现了重大的数据泄露，涉及的文件似乎描述了在亚马逊 AWS 云上运行的 GoDaddy 基础设施，并采取了保护措施，防止将来有人利用该信息。泄露的这些文件放在公众可访问的亚马逊 S3 存储桶中，包括成千上万个系统的基本配置信息以及在亚马逊 AWS 上运行那些系统的定价选项，包括不同情况下给予的折扣。泄露的配置信息包括主机名、操作系统、“工作负载”（系统干什么用的）、AWS 区域、内存和 CPU 规格等更多信息。实际上，这些数据直接泄露了一个规模非常大的 AWS 云基础设施部署环境，各个系统有 41 个列以及汇总和建模数据，分成总计、平均值及其他计算字段。还似乎包括 GoDaddy 从亚马逊 AWS 获得的折扣。

（七） 澳大利亚 16 岁高中生数次入侵苹果服务器，下载 90G 文件

2018 年 8 月，澳大利亚一名 16 岁高中生曾通过家中电脑成功入侵苹果服务器，在随后的一年时间里，他又数次入侵，下载了约 90GB 的重要文件，并访问过用户账号。

据悉，该少年在黑客界颇为有名。在发动攻击时，他使用了 VPN 和其他工具来避免被追踪。但百密一疏，该少年使用的 MacBook 笔记本电脑的序列号被苹果服务器所记录。

（八） Adapt.io123GB 数据可公开访问

2018 年 11 月，Hacken 公司的安全专家发现了一个可公开访问且没有设置密码的 MongoDB 数据库，其大小为 123GB，包含 9,376,173 条个人信息记录。泄露的信息包括：公司名、公司介绍、姓名、头衔/级别/职位、行业、公司规模、公司收入、电话号码、公司吸纳有联系人、电子邮件等。

经过仔细审查之后，Hacken 公司的安全专家得出结论，这个数据库来自一个名为“Adapt.io”的商业服务网站。根据其网站的描述：“Adapt 提供了数以百万计的商业联系方式。Adapt 的免费工具可帮助您通过电子邮件、电话和众多联系人来丰富您在任何网站上的商业信息。”

（九） FIESP 近两亿条记录泄露

2018 年 11 月，Hacken 公司的安全专家在使用 Binaryedge.io 平台审核可公开访问的 Elasticsearch 数据库的搜索结果时，发现了似乎是由巴西圣保罗州工业联合会（FIESP）编制的个人信息记录。FIESP 隶属于巴西国家产业联合会，包括 133 个商业协会，涵盖 13 万个行业，这些行业占巴西国内生产总值（GDP）的 42%。

存储在可公开访问的 Elasticsearch 数据库中的记录，总计数为 180,104,892 条，其中至少有 3 个数据集（FIESP、celurares 和 externo）包含巴西公民的姓名、个人身份证号码、纳税人登记证明、性别、出生日期、完整地址、电子邮箱地址、电话号码等个人信息。

Hacken 公司的安全专家表示，他们在向 FIESP 发出通知后并没有收到任何回复。该数据库最终是在该公司的巴西粉丝 PauloBrito 通过电话与 FIESP 取得联系之后，才得到离线处理的。

（十） “不设防”的 MongoDB 暴露 6600 万条数据

2018 年 12 月，安全研究人员发现，超过 6600 万数据在一个没有保护的数据库中，只要知道网址任何人都可以访问，而这些数据似乎来自 LinkedIn 个人资料。数据缓存包括可识别用户的个人详细信息，可帮助攻击者创建难以识别的网络钓鱼攻击。

根据 Hacken 网络风险研究总监 BobDiachenko 的说法，这些数据通过 MongoDB 公开了这个问题，无需身份验证即可进行访问。这 66,147,856 条特别的记录包含全名，个人或企业电子邮件地址，用户的位置详细信息技能，电话号码和工作经历，甚至还有个人 LinkedIn 个人资料的链接。

目前研究人员无法确定该数据库的所有者，但该数据库现在已不再在线，但并不排除它再次出现在网络上的可能性。

（十一） 联想的一台笔记本失窃了：它拥有成千上万名员工的姓名、月薪、银行账号

2018 年 12 月，联想公司通知亚太区员工：一台存储有众多员工未加密数据的办公笔记本失窃！里面有成千上万名员工的工资单信息，包括亚太区员工的姓名、月薪和银行账号。

根据外媒披露，新加坡一名联想员工由公司发放的一台笔记本电脑失窃；要命的是，里面有亚太区成千上万员工的一大堆未经加密的工资单数据。

关于这次重大事故的细节是联想工作人员告诉称，他们对这个严重的错误感到困惑不解。联想已向员工发去了道歉信，承认这个重大的安全问题。

四、 政府机构

（一） 问题综述

2018 年，拥有全体国民个人信息的政府机构，也频现信息泄露事件，不仅是欠发达的南亚地区，还包括发达的欧美地区，都出现关乎民生的重要个人信息系统数据泄露的报道。泄露的数据重要性且不说，一些政府对相关机构或人士反馈数据窃密风险的状况，反应措施不力甚至漠然，这将使国民的数据及隐私处于更加危险的境地。相比之下，欠发达地区对待泄露风险的反应，不应是消极辩解，而应该是担起责任。

（二） 印度全民个人信息遭泄漏，售价不足 6 英镑

2018 年 1 月，根据印度《论坛报》(Tribune)进行的调查显示，超过 10 亿印度公民的个人资料（包括指纹和虹膜等生物识别信息）正在在线出售，售价不足 6 英镑。

这些数据是存储在世界上最大的国营生物识别数据库——Aadhaar 中。同时在线出售的还有可用于生成虚假 Aadhaar 卡的软件。此前，印度政府认为，Aadhaar 项目将帮助把大量的印度公民纳入数字经济之中，会对印度的社会发展产生广泛的意义，下令强制该国公民必须在 2017 年 12 月 31 日之前将 Aadhaar 号码与自己的银行账户、手机号码、保险账户、永久性账号卡（PANCard）以及其他服务绑定起来。但有批评者认为，该系统的好处被夸大了，并正在面临不断增长的安全风险。

（三） 印度国家生物特征库 Aadhaar 疑似数据泄漏

2018 年 3 月据相关媒体报道，法国一名安全研究员 BaptisteRobert 通过推文宣称，他在印度政府和非政府机构网站上共找到了 2 万张 Aadhaar 卡的电子图片（PDF 或 jpeg 格式），而整个过程只花了约 3 个小时的时间。

Aadhaar 目前拥有着世界上最大的生物识别数据库，已经收集了超过十亿印度公民的虹膜扫描和指纹。随后，印度唯一身份认证管理局（UniqueIdentificationAuthorityofIndia，UIDAI）却重申 Aadhaar“依然安全可靠”，并将安全漏洞的报告驳回，称其为“不负责任”和“远离真相”。

（四） 印度某政府网站意外泄露大量公民敏感信息，目前仍未修复

2018 年 4 月，安全研究员 SrinivasKodali 报告了一起数据泄露事件，受影响的是一个隶属印度安得拉邦的政府网站。根据 Kodali 的描述，遭泄露的数据包括 Aadhaar 号码、银行分行、IFSC 代码和帐号、姓名、地址、身份证号码、手机号码、配给卡号码、职业、宗教信仰和种姓信息。

虽然印度政府和 UIDAI（印度唯一身份认证中心）曾辩称仅是 Aadhaar 卡号，并不包含印度公民的所有个人信息。但在印度，Aadhaar 号码与其他的个人信息相关联是一个不争的事实。Kodali 强调，不法黑客具备生成这种关联列表的能力，这些信息完全可以被用来锁定某个单一的个人。另外，这个数据库是公开可用的，并且允许任何人在未经授权的情况下访问。

（五） 美国监狱电话监控供应商 Securus 被黑，大量数据遭窃取

2018 年 5 月，一位匿名黑客从 Securus 窃取了大量数据，Securus 是一家为监狱囚犯提供电话服务的公司，并且为执法部门提供追踪电话使用服务。窃取的数据包括电子表格，上面的标志显示文档属于警方，里面有 2800 个用户名，还有邮件地址、手机号、密码、安全提示问题，数据最早可以追溯到 2011 年。

（六） 美国政府网站 HealthCare.gov 被黑，7.5 万人敏感信息泄露

2018 年 10 月，负责 HealthCare.gov 网站的机构称他们在一个与 HealthCare.gov 交互的政府计算机系统中发现了一起黑客攻击行为，导致大约 7.5 万人的敏感个人数据遭到泄露。

其设计由美国联邦医疗保险暨补助服务中心（CMS）监督，并由多个联邦承包商建立。该网站投资高达 8 亿美金。CMS 的管理在声明中说，“我们正努力尽快查明可能受到影响的个人，以便我们能够通知他们，并提供信贷保护等资源。”

（七） S3 存储桶配置错误，暴露 52.7 万美国选民个人信息

2018 年 10 月，UpGuard 网络风险团队透露，一个归属于美国茶党爱国者公民基金（TeaPartyPatriotsCitizensFund，TPPCF）的亚马逊 S3 存储桶因为一个配置错误，意外暴露了包括全名和电话号码在内的 52.7 万选民的个人敏感数据。暴露的数据中还包括战略文件、呼叫源文件、营销资产和其他一些文件，这些文件揭示了 TPPCF 将美国选民在政治上动员起来的集中努力，这一努力最终帮助唐纳德•特朗普（DonaldTrump）赢得了美国总统大选。

（八） 法国外交部称紧急联络人信息数据库遭黑客入侵

2018 年 12 月，法国外交和欧洲事务部发表了一份声明，宣称其计算机系统遭黑客入侵，访问并保存了紧急联络人信息的数据库，导致众多个人信息被泄露。据悉，大概 54 万份个人档案信息在事件中被窃，其中包含姓名、电话号码和电子邮件地址等信息。

目前，这一安全漏洞已得到修复。该部还在事件发生 72 小时内联系了法国数据监管机构 CNIL。

2010 年，法国外交和欧洲事务部就创建了一项名为“阿丽亚娜”（Ariane）的紧急服务——如果你打算前往不安全的国家时，可以在“阿丽亚娜”平台上进行登记，将这一信息告诉外交和欧洲事务部。这样一来，你就会收到安全简报，如果当地有危机发生，法国外交和欧洲事务部将会联系你，而且会保存紧急联络人信息，以防你在出境时遇到了意外情况。

此次被泄露就是“阿丽亚娜”平台，保存紧急联络人信息的数据库。

五、 电信运营商

（一） 问题综述

电信运营商也是 IT 信息化领域的领先代表，但其本身业务特点决定了天然拥有广大用户的手机号码、通话记录等更具隐私特点的数据，因此成为不法分子“偏好”寻找系统漏洞和持续攻击的对象。如果电信运营商的日常持续的安全管理与监测工作不到位，数据泄露的隐患就非常严重，2018 年很多老牌的电信巨头都吃过这类亏。

（二） 电信巨头加拿大贝尔公司数据又被泄，近 10 万用户受影响

2018 年 1 月，加拿大最大的电信公司加拿大贝尔公司(BellCanada)开始通知 10 万名消

费者称他们的个人数据已遭攻陷。贝尔公司指出，消费者的姓名和邮件地址遭“非法访问”，但加拿大多家新闻报告称黑客可能也获得了电话号码、用户名和账户号。然而，贝尔公司表示尚未有证据表明信用卡或银行信息遭攻陷。

这是贝尔公司第二次遭遇数据泄露事件。2016 年 5 月，该公司证实称约 190 万个活跃邮件地址和约 1700 个姓名和活跃电话号码遭黑客访问。目前尚不清楚这两起事件之间是否存在关联。

（三） 俄罗斯电信公司意外暴露数千名富豪客户个人信息

2018 年 1 月，据路透社（Reuters）报道，数千名在一家区域互联网服务提供商完成注册的莫斯科富人可能已经暴露了他们的个人信息，这其中就包括他们的姓名、家庭住址和手机号码等。

报道称，这起备受关注的数据泄露事件的所有受害者全都是俄罗斯互联网提供商 AkadoTelecom 的客户，这是一家由亿万富翁维克托•维克塞尔伯格（ViktorVekselberg）拥有的大型电信网络。目前，该公司表示已对此次事件展开调查。

（四） 瑞士电信证实 80 万数据被盗，涉全国 1/10 公民信息

2018 年 2 月，一个身份不明的用户访问了 Swisscom 客户的姓名、地址、电话号码和出生日期等信息，目前 Swisscom 认为该用户是通过其销售合作伙伴获取数据的。

据 IBTimes 报道，瑞士电信（Swisscom）于 2 月 7 日承认其用户数据在去年年底遭到破坏，约 80 万名客户（占瑞士总人口的 10%）的个人信息遭到泄露。不过 Swisscom 承诺此次事件不会涉及用户任何敏感信息（比如密码、会话或支付数据）。此外，为了更好地保护第三方公司对个人数据的访问，Swisscom 做出了一些重要改变，其中包括：相关合作伙伴公司的访问权限已被立即封锁；在销售合作伙伴账户中引入双因素认证，同时削减运行大容量查询的能力；第三方账户上的任何异常活动都会触发警报并阻止访问。

（五） 印度国有运营商 BSNL 内网遭入侵，4.7 万员工个人信息随意浏览

2018 年 3 月，根据《印度经济时报(TheEconomicTimes,ET)》及多家国外媒体的报道，法国安全研究人 RobertBaptiste 声称已获得了印度国有电信运营商 BharatSancharNigamLimited（BSNL）内部网络数据库的访问权，该数据库包含超过 4.7 万名员工的详细信息。

早前，Baptiste 还与 ET 分享了一个包含 BSNL 离职和现任员工姓名、职称、密码、手机号码、出生日期、退休日期、电子邮件地址等详细信息的数据库样本。ET 随后从数据库中调取了六名员工的个人信息，并通过电话验证了他们的身份属实。

Baptiste 已通过 Twitter 与 BSNL 进行了接触，并通知了他们关于这个问题。该公司的 IT 团队与他进行了讨论，最终确认了问题的严重性。目前，大部分漏洞已经被修复，而一些网站也已经被删除。

据 Baptiste 反馈，这个问题最初是由印度安全研究员 SaiKrishnaKothapalli 在两年前报道的，但在当时并没有得到 BSNL 的答复。

（六） 泰国最大的 4G 移动运营商 TrueMoveH 遭遇数据泄露

2018 年 4 月，泰国最大的 4G 移动运营商 TrueMoveH 遭遇数据泄露，AWS 上 46000 人

的数据被直接曝光在网上，包括驾驶执照和护照，以及身份证件的扫描件等。

安全研究人员 NiallMerrigan 发现数据泄露问题之后，试图将此问题告知 TrueMoveH，但运营商没有回应。Merrigan 透露，该 AWS 存储桶包含总计 32GB 的 46,000 条记录。

在媒体曝光之后，TrueMoveH 发布了一份声明，澄清数据泄漏影响了其子公司 ITrueMart。一位法律专家表示，TrueMoveH 可能面临数据泄露的惩罚，而安全专家呼吁电信运营商开始引入更完善的数据保护措施。

（七） 西班牙电信 Telefónica 存漏洞，可暴露数百万用户的完整个人数据

2018 年 7 月，据 ElEspanol 报道，西班牙电信（Telefónica）在 16 日凌晨被西班牙消费者协会 FACUA 发现存在一个安全漏洞。透过这个漏洞能够访问数百万用户的完整个人数据。暴露给黑客的信息包括固定电话和移动电话用户的全名、国家身份证号码、家庭住址、银行记录和通话记录，而所有这些数据都可以以电子表格的形式下载。

Telefónica 表示，他们在接到这一通知后，立即对该漏洞进行了修复。另外，也向有关当局进行了报告。而 ElEspanol 称，因为该漏洞而可能遭到泄露的数据包括用户的个人身份信息和支付卡信息，并且漏洞极其易于利用，即使是不具备高技术水平的入侵者也能够访问对它们进行访问。

有专家表示，“Telefónica 作为全球十大电信公司之一，收入超过 530 亿美元。令人惊讶的是，Telefónica 用户的数据居然可以轻松下载为未加密的电子表格。”

（八） T-Mobile 又泄露超过 200 万客户数据

2018 年 8 月，T-Mobile 公司披露，在黑客获得对其系统的访问权后，窃取了“一小部分”客户的个人信息，可能包括：个人信息，如姓名，帐单邮政编码，电话号码，电子邮件地址，帐号和帐户类型。其代表表示，今次数据泄露违规行为影响其 7700 万客户中约 3%的客户，约占 230 万人。

其实，在 2016 年 6 月份时已经发生了一起数据泄露事件，T-Mobile 的一名员工在 T-Mobile 捷克共和国窃取了超过 150 万的客户记录，以便出售以获取利润，最终使得捷克共和国警方介入调查。但该公司表示，数据泄露是被其中一名员工窃取，该员工在尝试销售数据时被捕获。

（九） 美国电信巨头 Comcast 爆漏洞，暴露 2650 万用户个人信息

2018 年 8 月，研究员发现 ComcastXfinity 无意中暴露了超过 2650 万名用户的家庭住址和社会安全号码。隶属于这家全美第二大互联网服务提供商的在线客户门户网站上被发现存在两个此前未被报告的漏洞，这使得即使是不具备太多专业技能的黑客也可以很容易地访问这些敏感信息。

在 BuzzFeedNews 向 Comcast 报告了这项调查结果之后，该公司对漏洞进行了修复。Comcast 发言人 DavidMcGuire 告诉 BuzzFeedNews：“我们迅速对这些问题进行了调查，在几个小时内我们修复了这两个漏洞，消除了研究人员所描述的潜在威胁。我们非常重视用户的安全，目前没有证据表明漏洞曾被用来攻击 Comcast 的客户。”

（十） Voxox 短信数据库遭泄，暴露短信认证安全问题

一家位于加州圣地亚哥的通信公司 Voxox，由于服务器没有密码保护，导致任何知道该

去哪儿窥视的人都能看到近乎实时的短信数据流。驻柏林的安全研究员塞巴斯蒂安·考尔（SébastienKaul）发现，Voxox 的一个二级域名指向了这个无遮无拦的服务器。更糟糕的是，这个在亚马逊 Elasticsearch 上运行的数据库还配置了 Kibana 前端，使得其中的数据易于读取、浏览以及按照姓名、手机号码和短信内容进行检索。

此安全失误导致一个庞大的数据库遭到泄露，该数据库中的数千万条短信中包含了密码重置链接、双因素认证代码以及快递通知等等。

在 TechCrunch 发出问询后，Voxox 已将数据库脱机。在关闭时，该数据库上似乎拥有年初以来的逾 2600 万条短信。不过，我们可以从数据库的可视化前端查看到平台每分钟处理的短信数量，它表明实际的数字可能更高。

（十一） 黑进 TalkTalk 公司的两黑客分别被判 1 年、10 个月

2018 年 11 月，两名来自英格兰斯塔福德郡塔姆沃思的男子因参与 2015 年 TalkTalk 公司黑客攻击事件而被判入狱。据悉，21 岁的康纳·奥尔索普（ConnorAllsopp）与 23 岁的马修·汉利（MatthewHanley）两人已对黑客指控认罪。奥尔索普被判处 8 月的监禁，而汉利被判处 12 月的监禁。

2015 年 10 月，TalkTalk 电信集团公司公开披露，其服务器受“持续网络攻击”，而且，黑客窃取了该公司客户的姓名、住址、出生日期、电子邮箱地址及电话号码信息，且窃取了 1.5 万用户的财务数据。攻击者还曾试图勒索电信公司 TalkTalk 首席执行官狄多·哈丁（DidoHarding）。

六、 互联网

（一） 问题综述

2018 年数据泄露的“野火”烧到了互联网公司，曾经认为对数据和网络的保护非常有把握、技术和人才也非常领先的互联网，在今年数据泄露的严峻形势下，也难逃一劫！包括 Facebook、Google、Amazon、Quora 等大佬企业和新星互联网企业都没有幸免。让全世界看到数据的安全保护，绝不是一劳永逸的工作。

（二） Facebook 隐私泄露人数上升至 8700 万，用户主要集中在美国

2018 年 4 月，Facebook 首席技术官 MikeSchroepfer 发表的一则博客文章称，我们认为 Facebook 上约有 8700 万用户，大约 81.6%是美国用户，或许受到 CambridgeAnalytica 获取数据的影响。此前，受到此次事件影响的 Facebook 用户数预计在 5000 万左右，8700 万人的数字较之前的预估有了大幅提升。

由 CambridgeAnalytica 大数据分析公司所引发的 Facebook 用户数据大面积泄漏事件目前仍在发酵，尽管 Facebook 方面已经公布一系列措施已改善用户数据安全管理，但关于此事件的调查仍在进行中。

（三） Facebook 披露严重漏洞：黑客可控制 5000 万用户账号

2018 年 9 月，Facebook 周五宣布，该公司发现了一个安全漏洞，黑客可利用这个漏洞来获取信息，而这些信息原本可令黑客控制约 5000 万个用户账号。在披露这一消息之前，Facebook 股价已经下跌了 1.5%左右，消息传出后进一步走低，到收盘时下跌 2.59%报 164.46

美元，盘中一度触及 162.56 美元的低点。

Facebook 发布博文称，该公司的工程团队发现，黑客在 Facebook 的“ViewAs”功能中找到了一个代码漏洞。Facebook 之所以能发现这个漏洞，是因为该公司在 9 月 16 日注意到用户活动大增。Facebook 表示将暂时关闭 ViewAs 功能，将对其安全性进行审查。Facebook 表示已通知美国联邦调查局（FBI）和爱尔兰数据保护委员会（IrishDataProtectionCommission）等执法机关，目的是解决任何有关一般数据保护条例（GDPR）的问题。

（四） Facebook 严重漏洞调查：2900 万用户数据失窃，易受针对性钓鱼影响

2018 年 10 月，Facebook 周五宣布，网络攻击者利用一个自动程序窃取了 Facebook 约 2900 万个账户的数据。该公司表示，将在未来几天向受影响用户发送信息，告知他们在攻击中被访问了哪些类型的信息。

据介绍，攻击者从 1400 万用户中获取了个人资料的详细信息，如出生日期、雇主、教育历史、宗教信仰、使用的设备类型、跟踪的页面以及最近的搜索和位置登记。对于其他 1500 万用户，入侵仅限于姓名和联系方式。此外，攻击者还可以看到约 40 万用户的帖子和好友列表。

根据今年 5 月欧盟颁布的“通用数据保护条例”，Facebook 必须在得知妥协后 72 小时内发出通知。Facebook 的主要欧盟数据监管机构爱尔兰数据保护专员上周对这起泄密事件展开了调查。包括美国康涅狄格州和纽约州在内的其他司法管辖区的有关部门也在调查这起袭击事件。

（五） Facebook 又泄露 700 万用户个人照片，可能面临 16 亿美元罚款

2018 年 12 月，据外媒报道，社交网络巨头 Facebook 可能面临超过 16 亿美元的罚款，因为它刚刚在一次安全入侵事件中暴露了近 700 万用户的个人照片。爱尔兰数据保护委员会（IDPC）表示，它已对这个安全入侵事件是否遵守了一般数据保护法(GDPR)的相关规定展开了调查。其中有些被曝光的照片是用户从未在该社交网络上分享过的照片。

电子隐私信息中心（ElectronicPrivacyInformationCenter）执行董事马克-罗滕贝格（MarcRotenberg）称，这一安全入侵事件可能会让 Facebook 违反它在 2011 年与美国贸易监管机构签署的一项协议，该协议要求 Facebook 改善其隐私做法，否则将面临罚款。

（六） 谷歌关闭个人版 Google+：因 50 万用户数据遭到曝露

2018 年 10 月 9 日，据报道，谷歌周一在公司博客中宣布，公司将关闭旗下社交网站 Google+的消费者版本。此前该公司宣布，Google+在长达两年多时间里存在一个软件漏洞，导致最多 50 万名用户的数据可能曝露给了外部开发者。

谷歌称，公司今年 3 月就已发现这个漏洞并推出补丁加以修复，并表示没有证据表明用户数据被滥用，也并无证据表明任何开发者明知或利用了这个漏洞。

受此影响，谷歌母公司 Alphabet 股价下跌 1.02%，报收于 1155.92 美元。

（七） Google+再曝严重漏洞影响 5250 万用户，将被提前关闭

2018 年 12 月，谷歌表示，在 Google+PeopleAPI 中找到另外一个严重的安全漏洞，可导致开发者窃取 5250 万名用户的个人信息，包括姓名、邮件地址、职业和年龄。将导致谷歌将在 2019 年四月，即比计划时间提前四个月关闭该社交服务。

这个易受攻击的 API 被称为“People:get”，旨在让开发人员请求和用户资料相关的基本信息。然而，谷歌在 11 月发布的软件更新导致 Google+PeopleAPI 中出现 bug，导致即使在用户资料被设置为“非公开”的情况下，app 仍可查看用户信息。

（八） 亚马逊解雇擅自向第三方商家披露用户信息的员工

2018 年 10 月，亚马逊称公司解雇了一名擅自向网站上的第三方商家披露消费者电子邮件地址的员工，该员工的行为违反了亚马逊的政策。亚马逊发言人在声明中说：“须对此事负责的个人已被停职，我们支持执法部分采取诉讼。”

根据发送给消费者的通知，亚马逊已经提醒购物者但表示并不需要采取更改密码等措施。公司并没有披露受影响消费者数量。

（九） 亚马逊因“技术错误”泄漏部分客户信息，包含姓名、邮件地址

2018 年 11 月，据外媒报道，亚马逊向受影响客户发送的电子邮件显示，由于“技术错误”导致一些客户的姓名和电子邮件地址遭到泄漏。周三上午，数人在网上分享了这些电子邮件的截图。

亚马逊在一份声明中说，“我们已经解决了这个问题，并通知了可能受到影响的客户。”

亚马逊没有回答有关有多少客户受到这一错误的影响，也没有回答有关信息公开时间的问题。亚马逊一位发言人告诉 CNBC，亚马逊的网站和系统都没有被破坏。该公司没有透露客户信息的可见位置。

（十） 全球最大同性社交软件 Grindr 存漏洞，可泄露用户信息及位置

2018 年 3 月，美国 NBC 的一份报道称，一款名为 Grindr 的交友应用程序存在两个安全问题，它可以暴露超过 300 万用户的信息，包括那些选择不共享这些信息的人的位置数据。

此漏洞是 AtlasLane 公司的首席执行官 TreverFaden 在创建了一个名为 C*ckblocked 的网站后发现的，他的网站在输入 Grindr 用户名和密码后可查看谁屏蔽了他们。但用户登录成功后，Faden 就可以访问用户档案中没有公开的用户数据，包括未读消息、电子邮件地址、删除的照片以及用户的位置信息。

Grindr 为全球最大的同性社交网站，今年 1 月初被北京昆仑万维科技股份有限公司收购，其拥有的用户超过几百万遍布 234 个国家。

（十一） 实时聊天供应商被黑，致使西尔斯、达美航空、百思买用户信用卡泄漏

2018 年 4 月，美国百货连锁公司西尔斯(Sears)、达美航空(DeltaAirlines)以及百思买(BestBuy)因共用的软件提供商被黑而导致客户的支付卡详情遭暴露。

这家被黑的公司位于美国加州圣荷西，提供多种客户支持服务，包括实时聊天系统和人工智能聊天机器人等。

达美航空公司表示，攻击者设法窃取的信息包括持卡人姓名、地址、卡号、CVV 号码以及有效期。但该公司虽然并未说明受影响的乘客人数有多少，但表示攻击者并未获得访问护照或政府身份详情的权限，同时也未获得访问托管在 SkyMiles 计划中的数据的权限。

（十二） 供应商产品感染恶意软件，致使 Ticketmaster 英国网站客户信息泄

露

2018 年 6 月，票务销售公司 Ticketmaster 的英国网站宣布，他们在 Ticketmaster 网站相关产品中发现了恶意软件，部分客户的个人信息或付款信息或许已因此遭到泄露。

Ticketmaster 是一家大型票务销售公司，总部位于美国加利福尼亚州，运营点遍布全球，主营票务类型为娱乐、体育。根据其官方公告，6 月 23 日 TicketmasterUK 在由 Ticketmaster 的外部第三方供应商 InbentaTechnologies 托管的客户支持产品中发现了恶意软件。发现恶意软件后，他们禁用了所有 Ticketmaster 网站上的 Inbenta 产品。尽管如此，部分客户的个人信息已经因此泄露，可能暴露的个人信息包括：姓名，地址，电子邮件地址，电话号码，付款详情和 Ticketmaster 登录详细信息。

（十三） 社交新闻网站 Reddit 遭黑客攻击，2007 年之前的备份数据泄漏

2018 年 8 月，美国社交新闻网站 Reddit 周三宣布，该公司的几个系统遭到黑客入侵，导致一些用户数据被盗，其中包括用户目前使用的电子邮箱以及 2007 年的一份包含旧加密密码的数据库备份。

Reddit 称，黑客获取了旧数据库备份的一个副本，其中包含了早期 Reddit 用户数据，时间跨度从 2005 年该网站成立到 2007 年 5 月。Reddit 表示，此次攻击是通过拦截员工的短信实现的，该短信中包含了一次性登录码。该公司还补充道，他们已经将此事通知受影响的用户。

（十四） 黑客售 8 万个 Facebook 用户信息：每个账号售价 10 美分

2018 年 11 月，据 BBC 报道，黑客称其已经窃取和公布了至少 8.1 万个 Facebook 用户账号的私人信息，并以每个账号 10 美分的价格出售其所盗取的数据。

BBC 获悉，在个人细节信息被盗的用户中，很多都是乌克兰和俄罗斯用户，但也有一些来自英国、美国、巴西及其他国家。黑客以每个账号 10 美分的价格出售其所盗取的数据，但他们此前发布的广告现已下线。

此次黑客事件最早是在今年 9 月曝光的，当时一名昵称为“FBSaler”的用户在一个英语在线论坛上发布帖子称：“我们出售 Facebook 用户的个人信息。我们的数据库里有 1.2 亿个账号。”随后，网络安全公司 DigitalShadows 代表 BBC 进行了调查，并确认被在线发布的 8.1 万多个账号中包含了用户私人信息。

（十五） 美版“知乎”Quora 遭黑客入侵：1 亿用户数据裸奔

2018 年 12 月，据报道，美国社交问答 Quora 网站称，该公司已经聘请“顶尖数字法证和安全公司”，并且已经上报执法部门。他们上周五发现其用户数据遭到身份不明的第三方非法获取。亚当在博客中表示，大约 1 亿 Quora 用户可能有大量信息遭到泄露，包括：帐号信息、公开内容和活动，以及非公开内容和活动。

Quora 表示，匿名提交问题和答案的用户不会受此影响，因为 Quora 并没有存储任何与匿名用户有关的信息。

七、 交通物流

（一） 问题综述

2018 年交通出行数据泄露事件分布在民航、铁路、水运、城市出行、货运等各个领域，这说明交通领域的信息化建设已经越来越深入，而相关的安全建设则显出不足。尤其今年涉及航空公司的数据信息泄露事件频发，一方面反映了这个领域的个人信息更易引起黑客的注意，同时也提醒民航机构，未来改善旅客的出行体验以及强化企业品牌，网络安全的得力保障是必不可少一环。

（二） 澳洲最大汽车共享服务公司 GoGet 被黑客入侵，会员信息惨遭泄漏

2018 年 2 月，GoGet 公司向其客户发出警告，称他们的车辆预定系统在去年遭到了黑客的入侵，在去年 7 月 27 日之前注册的会员个人信息已经遭到泄露。

GoGet 是澳大利亚首家，也是规模最大的一家汽车共享服务公司，业务覆盖澳洲五大主要城市，这包括：悉尼、墨尔本、堪培拉、布里斯班和阿德莱德。

泄露信息的多少取决于 GoGet 用户在填写会员登录表时录入的具体个人资料内容，这可能包括：姓名、家庭住址、电子邮箱地址、电话号码、出生日期、驾驶执照详细信息、就业单位、紧急联系人的姓名和电话号码以及 GoGet 管理帐户详细信息。

（三） 航运巨头马士基旗下子公司近半员工个人信息泄漏

2018 年 3 月，根据《丹麦海军时报（MaritimeDanmark）》的报道，航运公司 SvizterAustralia 有大约 500 人受到了数据泄露事件的影响，而遭到泄露的个人信息可能包括税务档案号码、亲属详情以及退休金账户信息。

初步调查结果显示，在 2017 年 5 月该公司的三个关键电子邮箱账户遭到了匿名黑客的入侵，约 6 万封电子邮件被秘密地自动转发到了两个公司外部电子邮箱账户。

Svitzer 的通信主管 NicoleHolyer 表示，该公司在今年 3 月 1 日收到了警告后阻止了黑客的电子邮件盗窃行为。另根据 Holyer 的说法，该公司使用由第三方电子邮件服务提供商托管的服务，目前该公司已经向提供商送达了法院命令，以向调查人员提供访问权限。

（四） 中东打车巨头 Careem 被黑，1400 万乘客信息失窃

2018 年 4 月，一家位于迪拜的叫车公司 Careem 向媒体透露称该公司遭遇了网络攻击并造成了数据泄露。黑客盗取的数据包括用户的姓名、电子邮箱地址、手机号、和行程数据，所有在今年 1 月 14 之前注册过 Careem 的用户都受到了影响。据 Careem 称，目前无迹象表明黑客有获取到用户的密码和信用卡号。

该数据泄露事件涉及到的用户包括 55.8 万名司机和 1400 万乘客。Careem 目前在全球 13 个国家运营，覆盖 90 个城市。Careem 曾宣布其在土耳其和巴基斯坦等国处于市场领先地位。

（五） 南非再次遭遇数据泄露：近 100 万公民个人信息网上曝光

继 2017 年南非遭遇一起大规模的数据泄露事故，2018 年 5 月，这个国家又发生了一起数据泄露，导致 93.4 万人的个人记录在网络上被曝光。本次曝出的数据，涵盖了国民身份证号码、电子邮件地址、全名、以及明文密码。

Driving Licence Per Licence Code Population as at 28 February 2017

Category	A	A1	B	C	C1	EB	EC	EC1	Total
Gauteng	176 132	44 509	1 016 535	4 677	1 237 803	1 309 393	304 376	225 171	**4 318 596**
KwaZulu-Natal	60 501	13 022	450 450	4 893	606 910	576 524	172 239	69 856	**1 954 395**
Western Cape	111 884	28 338	568 541	4 633	200 597	801 556	120 868	50 496	**1 886 913**
Eastern Cape	34 168	9 190	226 252	1 101	195 993	311 478	71 417	46 206	**895 805**
Free State	26 222	9 006	139 440	511	152 631	175 718	79 770	35 329	**618 627**
Mpumalanga	22 806	6 602	118 470	2 613	407 156	159 641	108 173	52 226	**877 687**
North West	19 726	6 429	112 891	1 672	207 321	141 547	55 106	37 251	**581 943**
Limpopo	14 973	3 862	74 446	1 745	555 451	108 989	94 544	65 592	**919 602**
Northern Cape	9 405	2 437	50 326	434	65 514	65 465	25 207	11 421	**230 209**
Total	**475 817**	**123 395**	**2 757 351**	**22 279**	**3 629 376**	**3 650 311**	**1 031 700**	**593 548**	**12 283 777**

南非 eNATIS 驾照人数统计（2017 年 3 月）

在专家帮助下，外媒厘清了数据泄露与南非一家负责在线支付罚款的公司有关。被泄露的数据库，是在一个公共网络服务商上被发现的，系统属于一家处理南非电子交通罚款的公司。

（六） 欧洲铁路系统遭遇黑客攻击，大量旅客数据泄露

2018 年 5 月，旅行网站欧洲铁路（RailEurope）公司向客户发布通告表示，有黑客入侵了该公司的机票预定网站，或已窃取了大量敏感数据。欧洲铁路北美有限公司（RENA）表示，因此次黑客事件可能泄露客户的个人信息包括：

1） 姓名；

2） 性别；

3） 收件地址；

4） 发票地址；

5） 电话号码；

6） 电子邮件地址；

7） 信用卡/借记卡号码；

8） 支付卡到期日期与验证值。

除此之外，某些注册用户的用户名与密码也可能遭遇外泄。更令人担忧的是，黑客已经在 RENA 系统当中驻留近三个月之久。RENA 在 2018 年 2 月 16 日与银行联系时，开始意识到其欧洲铁路网站可能存在问题，直到 5 月才确认该泄露事件。

（七） 38 万笔用户支付信息失窃，英国航空公司道歉

2018 年 9 月，英国航空公司 7 日为乘客信息失窃道歉，承诺将赔偿遭受经济损失的用户。英国政府已知道这起“网络攻击”，正调查事件经过。

据英航的母公司国际航空集团 6 日透漏，8 月 21 日至 9 月 5 日，英航网站及手机应用程序遭受“黑客”攻击，涉及大约 38 万笔用户网上支付交易；用户姓名、住址、电子邮箱账号、信用卡卡号及有效期、安全码泄露，航班信息和护照信息没有失窃。

英航董事长克鲁斯告诉记者，黑客作案手法“极其复杂”，为英航在线运营 20 多年来所未见。黑客没有破坏英航加密系统，而是用“另一种非常复杂”的方式侵入英航系统并获取

用户信息。

（八） 英国航空承认最近发生的网络攻击比想象中还要糟糕

2018 年 10 月，据外媒报道，英国航空公司（BritishAirways）证实，发生于 9 月 6 日的网络攻击可能已经导致 8 月 21 日-9 月 5 日之间的乘客的数据被盗。

在与网络法医专家和英国国家犯罪署合作之后，这家公司还发现，此次攻击之前，受影响的数据包含了 7.7 万张带有 CVV 银行卡和 10.8 万张没有 CVV 银行卡的姓名、账单地址、电子邮箱地址、卡号、卡有效期。

虽然现在还没有证据表明黑客将银行卡信息用于不法活动，但这起事件还是突显出了即便像英国航空这样的大公司其网络安全状况同样也令人担忧。

（九） 美国邮政局修复 API 漏洞，6000 万用户个人信息或受影响

2018 年 11 月，据报道，美国邮政局（USPS）周三发布补丁修补了一个 API 漏洞。攻击者可在该 API 的“帮助”下，利用任何数量的“通配符”搜索参数获取其他用户的大量数据：从用户名、账号到实际地址和联系方式等等。该漏洞可允许任何拥有 USPS.com 账户的人查看其他用户账户，大约有 6000 万美国邮政用户受该安全漏洞影响。

根据 KerbsonSecurity 的报道，这个漏洞在一年前由一名独立的安全研究员首次发现，该研究员随后告知了美国邮政局，然而从未获得任何回复，直到上周 Krebs 以该研究员名义联系了美国邮政局。

（十） 尼日利亚最大航空公司 ArikAir 云泄露大量乘客数据

2018 年 11 月初，据尼日利亚当地媒体《优质时报（PremiumTimes）》报道，尼日利亚国内最大的航空公司 ArikAi 公布的数据显示，该航空公司的大量乘客数据因为一个没有得到保护的亚马逊 S3 存储桶暴露在了网上。

根据 Cloudflare 的安全主管 JustinPaine 的说法，日前他在日常扫描活动中发现了一个包含大量 CSV 文件的亚马逊 S3 存储桶，而这些敏感文件很可能归 ArikAir 航空公司所有。

JustinPaine 的分析显示，遭泄露的数据包含了乘客的姓名、电子邮箱地址、订购时的 IP 地址以及使用的信用卡哈希值。此外，还包括信用卡的信息、订购的日期、支付的金额、使用的货币类型、设备指纹以及出入境机场。

八、 教育

（一） 问题综述

2018 年教育领域的数据泄露虽然不多，但是涉及的是青少年和下一代少年学生群体的个人信息，因此非常触动民众的敏感神经。尤其是部分公共机构，手里拥有大量的学生信息，而保护措施乏善可陈，甚至没有承担应有的责任，令黑客轻易获取数据，无形之中放大了学生及家长遭遇网络诈骗及其他网络攻击的风险。

（二） 教育网站存漏洞，俄罗斯 1400 万大学毕业生个人信息泄漏

俄罗斯技术社区网站 Habrahabr 上，一名昵称为 NoraQ 的用户（黑客）2018 年 1 月 29 日发文称，1400 万名俄罗斯大学毕业生信息泄露。俄罗斯总人口数量约为 1.46 亿，即十分

之一俄罗斯人的信息泄露。泄漏信息包括姓名、出生日期、个人账户的保险号码、纳税人识别号码、电子邮件地址等，文件大小约为 5GB。

NoraQ 在俄罗斯联邦教育科学联督局服务网站上发现了一个 SQL 注入漏洞，通过这个漏洞他下载了上述 1400 万名毕业生信息。

（三） 全美最大公立网校 FLVS 遭遇数据泄露，近 37 万师生受影响

2018 年 3 月 14 日，佛罗里达虚拟学校（FloridaVirtualSchool，简称 FLVS），在一份声明中表示，近 37 万名师生的个人敏感信息可能已经遭到了外泄，以及 2000 多名教师可能会因此受到影响。可能泄漏数据包括学生的姓名、出生日期、学校帐户用户名和密码，以及其父母的姓名和电子邮件地址。

FLVS 成立于 1997 年，是全美第一所也是最大的一所公立虚拟学校。FLVS 表示，他们的 IT 人员在 2 月曾发现一台服务器存在严重的配置错误问题，这导致该服务器对于黑客来说是“完全开放”的。

目前，FLVS 已经将此事通报给了政府执法部门。除此之外，FLVS 还将会为受影响的师生提供为期一年的年度免费信用监控服务。

（四） 因员工发错邮件，普渡大学 2.6 万名学生详细信息暴露

2018 年 5 月，美国印第安纳州西拉法叶市的普渡大学（PurdueUniversity）发生了一起数据泄露事件，恰恰就只是因为一名工作人员一不小心犯下的一个低级错误导致的。据报道，在这起数据泄露事件中，所涉及的数据超过 2.6 万条。

在解释这一事件时，普渡大学助理法律顾问 TrentKlingerman 表示，该校的一名工作人员原本计划是要发送一份与财政援助计划有关的宣传手册，但无意中将包含学生个人信息的表格发送给了学生的家长。邮件附件是一个 Excel 文件，包含了超过 2.6 万名学生的数据。

（五） 数据泄露影响超过 1000 万公民，马来西亚教育部 SAPS 系统紧急下线

2018 年 6 月，据马来西亚媒体 MalayMail 报道，在发现存在一个可能暴露超过 1000 万公民个人信息的安全漏洞之后，由马来西亚教育部推出的学校考试分析系统（SitemAnalisisPeperiksaanSekolah，SAPS）被迫紧急下线。

报道指出，一位要求匿名的读者在上周五晚向 MalayMail 爆料称，教育部此前无视他的警告，迫使他不得不向媒体寻求帮助。之后，他向马来西亚计算机紧急响应小组（MyCERT）进行了通报。MyCERT 在周六中午对 MalayMail 出了回应，该系统之后也在同一天被下线。

“这是一个很好的系统，但是它的后端完全失败，他们存储了数以百万计学生的细节记录，但是他们从不隐藏这些信息。一些非常个人的细节可以未经允许被访问，他们只是忽略了它。”这位匿名读者报料说，“这个系统从上线第一天起就存在漏洞。”他还抱怨登录机制是“一个彻头彻尾的笑话”，因为密码存储在一个纯文本文档中，没有进行任何加密处理。

（六） 加拿大亚岗昆学院服务器感染恶意软件，超过 11 万条记录泄露

2018 年 7 月，位于加拿大安大略省的亚岗昆学院发布了一份声明，通报了一起影响到人数众多的大规模数据泄露事件。此次黑客入侵事件最初发生在 2018 年 5 月 16 日，亚岗昆学院的服务器被发现感染了恶意软件。

该学院已经确认了 4568 名个人，包括学生和校友，可能遭泄露的数据包括出生日期和家庭住址。另有 106931 名个人，包括学生、校友以及现任和前任员工，可能遭泄露的信息是一些公开的非敏感信息。学院已经就此事通知了安大略省信息和隐私专员以及渥太华警察局。

九、 金融

（一） 问题综述

2018 年金融企业由于其特殊的属性，一直是黑客们关注的攻击的焦点，并且一些不法分子不仅拿盗取的银行的大量数据贩卖获利，而且还有部分黑客竟然明目张胆勒索金融机构，显示了黑客的贪婪。另外，从原因上看，系统漏洞、内鬼、供应链厂商泄露等都是金融机构遭遇数据被窃的导火索。

（二） NAS 配置不当，保险公司大量敏感数据泄露

2018 年 1 月 19 日，UpGuard 网络风险研究主任 ChrisVickery 留意到了美国马里兰联合保险协会（MDJIA），因为他发现了属于该保险协会的一个联网存储（NAS）设备，该设备通过一个开放端口与互联网连接，而它内含与协会 IT 运营的重要敏感数据。因存储设备的错误配置，将数千客户的信息泄露到网上。

与被泄数据存储一起被曝光的是 JIA 客户文件和声明的备份，包括客户姓名，地址，电话号码，生日以及社保号，支票扫描件，银行账号和保险单号。除了这些重要的客户信息，

这次泄露还曝光了一个内部访问凭证数列，它原本用于管理和控制 MDJIA 协会的运营，包括远程桌面，邮件，第三方用户名和密码。

（三） AWS 存储桶泄露 50.4GB 数据，美国消费金融巨头受影响

2018 年 3 月，云安全厂商 UpGuard 公司网络风险小组发现一批由于 AmazonWebServices（简称 AWS）S3 存储桶未受保护而泄露的 50.4GB 数据。经证实，此 AWS 存储桶属于云商务智能（简称 BI）与分析厂商 Birst 公司。

这 50.4GB 数据涉及 Birst 公司主要客户 CapitalOne（一家位于弗吉尼亚州麦克莱恩市的金融服务巨头，亦为全美第八大商业银行），包含 CapitalOne 网络基础设施配置信息以及 Birst 公司的设备技术信息。

根据 UpGuard 公司发布的官方博文，这批数据当中包含密码、管理访问凭证以及私钥，且专供 Birst 公司内部云环境中的 CapitalOne 相关系统使用。攻击者利用这批遭到泄露的数据足以掌握 CapitalOne 对 Birst 设备的使用方式，进而入侵 IT 系统并深入挖掘该公司的内部资讯。

（四） 美国征信公司信息泄露事件升级，新增 240 万受害者

2018 年 3 月，据报道，美国征信公司伊奎法克斯(Equifax)表示，关于 2017 年 9 月曝出的 1.4 亿用户个人信息泄露事件，近日又发现另外 240 万名受害者。

伊奎法克斯称，之前未发现新的受害客户，是因为他们的社会安全号码并未与部分驾照资讯一同被窃取。而社会安全号码似乎是被黑客攻击的重点。该公司还表示，将会通知这些用户，并为他们提供防盗保护和信用报告监控服务。

（五） 离职员工窃取客户联系人名单，SunTrust 银行 150 万客户信息泄露

2018 年 4 月，美国 SunTrust 银行证实，在一名离职员工偷窃了该公司的客户联系人名单之后，超过 150 万名客户的个人信息可能已经因此遭到泄露。

SunTrust 银行的首席执行官 WilliamRogers 称，这属于团伙作案，这名离职的前员工通过与第三方合作成功对公司的客户联系人名单进行了盗窃。名单包含的客户个人信息包括客户的姓名、地址、电话号码以及某些账户余额。

Rogers 表示，SunTrust 银行正在积极配合第三方安全专家和执法部门进行事件调查。尽管调查工作仍在在进行中，但出于对客户负责，SunTrust 银行正在主动通知约 150 万名客户。

（六） Delta、Sears 供应商遭网络攻击，数十万名客户信用卡信息可能曝光

2018 年 4 月，据外媒报道，Delta 和 Sears 发布声明称，相关曝光的数据泄露事件可能泄露了数十万客户的信用卡资料。上述数据泄露事件最先由路透社曝出，其发生的地点为一家同时为 Delta 和 Sears 在线聊天平台提供服务的公司。

目前，联邦执法部门、银行以及 IT 安全公司正在对这一安全事件进行调查。而 Sears 和 Delta 都分别开设了针对此事件的客户通道，前者开通了一个客户咨询热线，后者设立了一个专用解答网页 delta.com/response。

（七） 澳大利亚联邦银行遗失了 1200 万条用户银行数据

2018 年 5 月，外媒 BuzzFeed 报道，澳大利亚第一大商业银行澳大利亚联邦银行（CBA）证实，包含客户姓名、地址、账号和 2000 年至 2016 年的交易详情记录的两个存储磁带，在一次数据中心转运任务中被其分包商 Fuji-Xerox 丢失。其中至少包含 1200 万名用户的银行交易数据。

当银行意识到这起事件时，其委托三方统计公司毕马威（KPMG）进行过一次独立的剖析调查，以了解具体情况，并通知了澳大利亚信息专员办公室（OAIC）。毕马威（KPMG）在调查后发现存储带很有可能已被处置，很难寻回。

（八） 加拿大两家银行遭黑客勒索，9 万名客户信息被盗

2018 年 5 月，据加拿大《环球邮报》报道，两家加拿大银行——蒙特利尔银行（BankofMontreal）和网上银行 SimpliiFinancial——都对外表示遭到黑客袭击，并且发出警告称，袭击两家银行的黑客声称已经访问了客户的账户以及相关个人信息，并威胁将公开这些数据。约 9 万名客户信息被盗，这可能是加拿大金融机构遭受的首次重大攻击。

蒙特利尔银行的发言人表示，事件之后收到了攻击者的威胁，称若不支付 100 万赎金就将公开被盗客户数据。此次两家银行遭受的袭击事件似乎是相关联的。该行表示，目前正在进行彻底调查并且已经告知所有相关联的机构来评估潜在的损失。

（九） PayPal 旗下移动支付服务 Venmo 默认公开用户交易信息（已遭滥用）

2018 年 7 月，一名隐私提倡者 HangDoThiDuc 发布最新调查结果表示，多数 Venmo 交易被记录在任何人均可访问的一个公共 API 中，原因是 Venmoapp 的默认设置为所有用户设置为“公开”。他通过这一隐私策略查询 VenmoAPI 并下载了该公司所有 2017 年的公开交易记录，总计 207,984,218 条。

除非用户特别更改了这个值，否则他们通过 Venmo 转账 app 做出的所有交易都被记录且任何人均可通过 Venmo 公共 API 遭访问。通过这个 API 暴露的数据包括发送人和收款方的姓和名、Venmo 头像、交易日期、交易留言、交易类型等。据悉，Venmo 是一款仅在美国使用的移动支付应用，于 2009 年推出。2013 年，Venmo 成为 PayPal 子公司。

（十） 黑进上百家美国企业窃取 1500 万张信用卡记录，三名乌克兰黑客被捕

2018 年 8 月，据外媒报道，三名乌克兰公民近日因参与一项针对 100 多家美国企业的

长期网络攻击行动而被捕。根据起诉书了解到，该团伙在过去总共从 6500 多个销售点终端盗取了超 1500 万张信用卡记录。据安全研究人员介绍，这个叫做 Carbanak 的团伙利用社交工程和网络钓鱼攻击渗入到企业并从中盗取金融数据。

最初的感染主要通过恶意软件诸如电子邮件附件或有时候假装丢失酒店预订信息或 SEC（美证券交易委员会）投诉文件展开。

现在，DmytroFedorov、FedirHladyr、AndriiKolpakov 被控犯有阴谋罪、电信欺诈罪、计算机黑客罪、访问设备欺诈罪、严重身份盗窃罪等 26 项罪名。

（十一） 智利 1.4 万信用卡资料被黑客组织盗取

2018 年 7 月，根据智利政府公布的消息，黑客盗取了智利约 1.4 万张信用卡的资料，并将这些资料公布在社交媒体上。

据报道，在这起案件中，黑客公布了信用卡卡号、有效期限及安全码，受攻击影响的银行包括桑坦德银行（Santander）、伊塔乌银行（Itau）、丰业银行（Scotiabank）和智利银行（BancodeChile），这些银行已通知客户遭入侵一事。

智利政府的银行监管机构表示，这起袭击行动是黑客组织“影子经纪人”（ShadowBrokers）展开的，该组织因入侵美国国家安全局（NSA）而闻名。

（十二） 新蛋网用户信用卡数据泄漏：恶意代码已侵入约 1 个月

2018 年 9 月下旬，据报道，在过去约 1 个月的时间，购物网站新蛋（Newegg）的用户数据发生泄露事故，目前新蛋正在对网站进行整理改进。

有安全研究人员发现，黑客将 15 行恶意盗刷代码植入新蛋网支付页面，从 8 月 14 月-9 月 18 日，代码一直存在。这种恶意代码从用户手中窃取信用卡数据，传输到由黑客控制的服务器。黑客的代码同时影响桌面端和移动端用户，只是目前还不清楚移动端用户是否已经受到影响。安全研究人员指出，攻击新蛋网的方式十分巧妙，伪装极好，与英国航空公司（BritishAirways）信用卡泄露事件、以及之前发生的 Ticketmaster 泄露事件有些类似。

（十三） 超 2 万张银行卡数据在暗网兜售，几乎涵盖巴基斯坦国内所有银行

2018 年 11 月，据巴基斯坦 GEO 电视台报道，几乎所有巴基斯坦银行在最近都受到了黑客入侵的影响，而这一令人震惊的消息已经在上周得到了巴基斯坦联邦调查局（FIA）网络犯罪部门负责人的证实。

根据俄罗斯网络安全公司 Group-IB 最近发布的一份报告，其在暗网上发现一批数据，包含了超过 2 万张巴基斯坦银行卡的详细信息，而这些数据归属于在该国运营的“大多数银行”的客户。巴基斯坦 PakCERT 的专家认为，这些数据是通过银行客户的刷卡行为获得的。这些支付卡数据正在暗网出售，售价从 100 美元至 160 美元不等。

（十四） 汇丰银行美国分部发生非授权访问和数据泄露

2018 年 11 月，汇丰银行（美国）通知客户 10 月 4 日至 10 月 14 日期间发生了数据泄露，攻击者访问了访问该金融机构的在线账户。

泄露的信息包括：客户全名，邮寄地址，电话号码，电子邮件地址，出生日期，帐号，帐户类型，帐户余额，交易历史记录，收款人帐户信息以及可用的帐单历史记录。

为应对安全漏洞，汇丰银行的美国子公司暂停了在线账户访问以防止滥用。数据泄露后，汇丰银行加强了个人网上银行的认证流程，增加了额外的安全保障。

（十五） DarkOverlord 黑客发布了第一批“秘密”911 文件

据雷锋网报道，2018 年 12 月 31 日，黑客组织 DarkOverlord 在一篇发表于源代码分享网站 Pastebin 上的帖子中威胁称：

他们已经从一家为保险公司 HiscoxSyndicaresLtd.提供咨询服务的律师事务所窃取到文件。事后，律师事务所与黑客组织达成了赎回协议，并确定对方按协议缴纳赎金即可拿回全部数据。但是，该律师事务所并未履行诺言，向执法部门进行了报告。

2019 年 1 月初，DarkOverlord 竟然真的公布了大约 70M 的 911 恐怖袭击相关资料，同时第一批解密密钥被公之于众。

十、 军事

（一） 问题综述

军队的网络一般比较封闭，但也有大量连接到 Internet 的网络，而且存在诸多泄密渠道。从 2018 年和军事相关的数据泄露事件看，内部文件管控不当，系统漏洞，社会工程学攻击以及第三方服务方网络安全建设缺失，都是泄密的原因。

（二） 超过两万名美国海军陆战队队员个人资料遭意外泄露

2018 年 3 月，根据美国海军陆战队机关报《海军陆战队时报（MarineCorpsTimes）》的报道，约 21,426 名海军陆战队士兵、水手和其他相关工作人员的个人敏感信息被意外暴露给了外界。泄露信息包含大量高度敏感的信息，例如社会安全号码、银行电子资金转账记录和银行转账号码、信用卡信息、家庭住址以及紧急联系信息等。

报道称，事件原因已查明，在 2 月 26 日早上，美国国防部的自动监护旅游系统（DefenseTravelSystem，DTS）将一封未加密的电子邮件发送给了一份错误的电子邮箱地址列表。未加密的电子邮件不仅被无意中发送给了民用帐户，而且还被发送给了在未分类的海军官方域名“usmc.mil”上托管的帐户。目前，还不清楚有多少人收到这封电子邮件。

（三） 美空军“死神”无人机文件泄露

2018 年 7，威胁情报公司 RecordedFuture 发布报告指出，其 2018 年 6 月发现有黑客在暗网出售美国空军 MQ-9Reaper（“死神”）无人机的相关文件，这份文件包含与 MQ-9Reaper 相关空军人员名单、无人机维护和培训资料。经研究人员调查确认，这些文件是真实的。

研究人员调查发现，这名黑客通过先前披露的 FTP 漏洞访问了美国 Creech 空军基地一台 Netgear 路由器，从而获取了这些文件。而事件中，同样遭遇入侵的一名上尉，2018 年 2 月刚完成了网络安全培训，理应了解防止非授权访问的必要操作。

（四） 女童子军信息泄露事件中 2800 名成员个人信息外泄

2018 年 11 月，黑客入侵美国加利福尼亚州橙县女童子军分部，2800 名女童子军及其家庭成员个人信息可能遭泄露。据橙县女童子军称，某未知威胁者于 9 月 30 日至 10 月 1 日实施入侵，获取了该童子军分部运营的电子邮箱账户的访问权限，并用其发送邮件。

据女童子军分部（GSOC）称，该账户之前用于为女童子军成员安排出行，因此，黑客可通过访问该账户获取个人数据。经确认，黑客或已窃取部分成员姓名、出生日期、家庭住址、保险单号及健康病历。专家警告，外泄信息可能被用来进行基于社会工程学的网络攻击。

（五） 热门无人机交易网站数据库泄露，致使英国军方警方政府单位的购买记录曝光

2018 年 4 月，热门无人机交易网站 DronesForLess.co.uk 将未加密的整个交易数据库暴露在网上，导致数千名警方、军方、政府和私人客户的购买记录遭曝光。Secret-bases.co.uk 公司的 Alan 发现了这起事件，他指出，DronesForLess.co.uk 的运营人员未能保护 web 基础设施的关键部门免遭好奇之人的窥探。

约 1 万多份购买收据存储在该网站的 web 服务器中。收据详情包括购买人姓名、地址、电话号码、邮件地址、IP 地址、用于连接到该网站的设备、下单商品详情、发卡行以及付款用的信用卡的后四位数字。涉及的客户名称包括伦敦警察厅、英国陆军预备役少校、英国国防部采购部门某员工、英国国家犯罪局某员工、英国国防科技实验室、英国陆军步兵试验和开发部队（InfantryTrialsandDevelopmentUnit）。

（六） 英国空军遭遇黑客攻击，F-35 隐形战机数据疑泄露

英国《每日邮报》2018 年 8 月 6 日报道，英国皇家空军 F-35B 战机的部分信息已经泄露！英国计划从美国购买 138 架该型战机，皇家空军和海军航空兵都将装备。

然而，英国皇家空军一名女军人的手机约会应用软件 Tinder 账户被黑客入侵，黑客在获取她的信息后，开始以她的身份与一名男同事（空军）联系，聊起了两个月前刚抵达英国的 F-35A 隐身战机。

尽管这名女军人很快就发现自己的账号被盗用了，但还是晚了。从黑客与那名男同事的聊天记录来看，黑客非常得心应手用各种语言陷阱，从那名男同事那里套取了 F-35B 战机的部分信息，其中不乏机密信息。

（七） 中东地区政军企高层遭钓鱼间谍攻击，攻击者已收集逾 30GB 数据

2018 年 5 月，根据 Lookout 安全公司发布的报告，攻击者使用“StealMango”等监控软件工具成功地攻陷政府、军方、医疗等人员的移动设备，已经收集了超过 30G 的受攻陷数据，包括通话记录、音频记录、设备位置信息以及文本信息。某钓鱼攻击活动通过自定义监控软件感染安卓设备，从多个国家尤其是中东地区的高层提取数据。

Lookout 公司表示，约 100 台独立设备遭针对性监控活动的影响，包括政府官员、军方人员的设备，以及位于巴基斯坦、阿富汗、印度、伊拉克和阿联酋等地的活动家。其它国家如美国和德国的官员数据也遭收集。

十一、 生活服务

（一） 问题综述

生活服务类的企业机构涉及广泛，包括电商零售、服装贸易、旅行预订等，和民众的生活息息相关，其所拥有的数据也比较分散，由于网络安全建设层次不齐，因此曝光的隐患也比比皆是。当前，社会层面整体越来越重视网络安全，这些生活服务类企业也应提高保护能

力。

（二） 英国电子零售商 DixonsCarphone 公布严重数据泄露事件

2018 年 6 月，英国家喻户晓的手机零售商 DixonsCarphone 宣布，正在调查“对公司所持有的某些数据的越权访问”。该公司指出该越权访问“试图攻陷 CurrysPCWorld 和 DixonsTravel 商店中其中一个处理系统中的 590 万张卡”，“以及包含非金融个人数据的 120 万个记录，如姓名、地址或邮件地址”。

这可能是英国历史上发生的规模最大的数据泄露事件。

如果整个事件被按 GDPR 规定处理，那么 ICO 可能会对 DixonsCarphone 开出全球年收入总额的 4%的罚单。去年，该公司的年销售总额为 105 亿英镑（折合 140 亿美元）。根据 GDPR 开出的罚单可能达到数亿英镑。

（三） 阿迪达斯可能泄漏了数百万美国消费者信息，官方称正在调查

2018 年 6 月，德国运动品牌阿迪达斯在网站上发布通知称，未授权人员声称获得对消费者数据的访问权限，数百万名美国消费者或受影响。

未经授权人员可能已获得访问在阿迪达斯美国网站上购物的消费者用户名、密码哈希和通讯信息的权限，该公司将它们称之为“有限信息”。阿迪达斯向某些媒体机构表示事件可能影响“数百万”消费者，但它发布声明称并非所有位于美国的消费者均受影响。

（四） 法国眼镜连锁店 Opticalcenter 因泄露用户数据被罚 25 万欧元

2018 年 6 月，据《费加罗报》报道，法国眼镜连锁店 Opticalcenter 因泄露用户数据，被法国独立机构信息与自由委员会（Cnil）罚款 25 万欧元（约合人民币 188.66 万元），该金额创造了 Cnil 最高罚款记录。

法国当局表示，这是 Cnil 首次开出如此高金额的罚单。2017 年 7 月，Cnil 接到相关举报后查证，Opticalcenter 的用户可以通过其网站主页看到其他客户的购物发票。这些发票包含姓名、邮箱地址和视力矫正度数等一些私人信息，部分发票上还有用户的社保帐号。

据悉，法国 2016 年颁布的个人信息数据保护法使得 Cnil 的惩罚权限，由 15 万欧元上调至 300 万欧元；而 GDPR，让这一数字上调至 2000 万欧元和营业额的 4%。

（五） 健康应用 PumpUp 服务器未设密码，超过 600 万用户个人信息暴露

2018 年 6 月，据外媒 ZDnet 报道，位于加拿大安大略省的 PumpUp 公司发布声明称，旗下同名社交健康追踪应用无意中暴露了用户的隐私和敏感数据，包括用户之间发送的健康信息和私人消息。

PumpUp 公司在全球拥有超过 600 万用户。其数据都被存储在一个核心的后端服务器，并托管在亚马逊的云端。然而，安全研究员 OliverHough 发现，该服务器并没有设置密码，这使得任何人都能够查看都有谁在进行登录、谁在实时发送消息以及消息的内容。

ZDnet 指出，暴露的数据主要包括用户的电子邮箱地址、出生日期、性别和用户所在位置的地理信息，以及用户的生物特征、锻炼和活动目标、用户头像，还有用户是否已经被屏蔽、是否对应用进行了评分。此外，该应用还暴露了用户提交的健康信息，如身高、体重、咖啡因和酒精摄入量、吸烟频率、健康问题、药物和受伤处等。

（六） 酒店预订软件 FastBooking 被黑，数百家酒店旅客入住和支付信息泄露

2018 年 6 月，数百家酒店的旅客个人详情和支付卡数据被盗，而数据是从巴黎公司 FastBooking 被盗的。该公司向全球 100 个国家的 4000 多家酒店出售酒店预订软件。

FastBooking 公司称，事件发生在 6 月 14 日，当时攻击者利用托管在服务器上某个应用中的漏洞安装恶意工具（恶意软件）。该工具可导致黑客远程访问服务器以提取数据。6 月 19 日 FastBooking 员工发现数据遭泄露，并在不到 6 小时的时间里解决了该问题。

FastBooking 公司指出，黑客窃取的信息包括旅客的姓氏和名字、国籍、邮政地址、邮件地址以及和酒店预订相关的信息（酒店名称、入住和离店详情）。在某些情况下，某些支付卡详情也被盗，如打印在支付卡上的姓名、卡号及其有效期。

（七） 美国 Chili’s 连锁餐厅支付系统被黑，用户支付卡信息遭破坏

2018 年 5 月布林克国际公司发现其旗下 Chili's 连锁餐厅 1600 家门店的顾客支付卡信息受到破坏，这可能导致部分餐厅顾客的支付卡相关信息被非法访问或盗窃。经初步调查，这一恶性事件发生的时间范围为 2018 年 3 月——4 月。

Chili's 考察后确定这是由于有人将恶意软件放置在餐厅销售点的机器内，使得同伙可以从他们的相关支付系统中删除在餐厅消费顾客的支付卡信息（包括信用卡、借记卡、卡号及持卡人姓名）。

Chili's 当前正与一个外部取证技术团队合作，以尽快确定信息缺口的性质及全部范围。与此同时，以最快速度向顾客发布了通知，承诺尽可能提供欺诈解决和信用监控服务，还给出了详细具体的参考安全建议。

（八） 美国连锁餐厅 Applebee 被黑，160 多家门店 POS 系统支付信息泄漏

2018 年 3 月，根据 RMH 特许经营控股（RMHFranchiseHoldings）在其网站上发布的公告来看，部分由 RMH 拥有和经营的 Applebee 餐厅的销售点（POS）系统被匿名黑客安装了恶意软件，旨在窃取消费者的支付卡信息。这意味着消费者的姓名、支付卡号码、以及在限定时间内处理的卡片验证码可能因此遭到了泄露。

RMH 透露，这起事件是在 2 月 13 日被发现的。在得知潜在事件后，RMH 立即展开了调查并获得了网络安全取证公司的帮助。根据公告显示，事件影响了位于阿拉巴马州、亚利桑那州、佛罗里达州等 14 州的 160 多家 Applebee 餐厅，这几乎代表了 RMH 拥有和经营的所有餐馆。

（九） 美国奢侈品巨头 SaksFifthAvenue 遭黑客攻击，500 万张银行卡信息被盗

2018 年 4 月，根据安全公司 GeminiAdvisory 披露，奢侈品百货连锁 SaksFifthAvenue（萨克斯第五大道精品百货店）已证实遭受攻陷，500 万购物者的银行卡信息遭泄露。初步分析表明犯罪分子窃取数据的时间实在 2017 年 5 月至今。从目前对可用数据的分析来看，除了 SaksFifthAvenue，Lord&Taylor 的实体店整个网络同样遭攻陷。而黑客组织 Fin7 炫耀称其攻陷了 Saks 的计算机系统。

GeminiAdvisory 指出，由于 Saks 的客户是高收入群体，因此被盗的银行卡对于欺诈者而言价值尤高，因为高收入群体的支付卡盗用情况难以检测。

（十） 美国线上旅行社 Orbitz 遭遇黑客攻击，88 万客户个人资料或已泄露

2018 年 3 月 22 日，据国外综合新闻平台 PhocusWire 的报道，美国在线旅游巨头 Expedia 旗下的在线旅行社 Orbitz 公司在本周二公开宣布称，其在线旅游预定平台存在一个严重的安全漏洞，而这个漏洞可能会使得大约 88 万名 Orbitz 客户面临数据泄露风险。

信息泄露所涉及到的客户是那些于 2016 年上半年在 Orbitz 预定平台以及于 2016 年至 2017 年在 Orbitz 商业合作伙伴平台进行订单交易的客户，存在泄露风险的信息可能包括姓名、支付卡信息、出生日期、电话号码、电子邮件地址、帐单地址和性别等。

根据 Expedia 的说法，这个漏洞是该公在司对 Orbitz 的商业合作伙伴 Travelocity 运行的平台进行调查时发现的，而 Orbitz 平台和该平台处于相同的环境中。

（十一） 美国最大面包连锁店 Panerabread 泄露数百万顾客隐私长达八个月

2018 年 4 月 4 日，网络安全公司 KrebsOnSecurity 在本周一发表的文章中指出，美国最大面包连锁店 Panerabread 旗下网站 panerabread.com 泄露了数百万顾客记录，包括姓名、生日、电子邮箱地址、家庭住址以及信用卡号码的最后四位数字。

KrebsOnSecurity 还表示，在他们与该公司取得联系后，该网站已在周一早些时候离线。而截止到这个时间，这起数据泄露事件至少已经持续了长达八个月的时间。

安全研究人员已在去年 8 月通知了该公司。当被问及到在 2017 年 8 月进行通报后直到现在以来，是否看到有任何迹象表明 Panerabread 曾试图解决这个问题时，Houlihan 表示“从来没有”。目前尚不清楚该公司的网站到底暴露了多少顾客记录，但该网站索引的增量客户数据表明，这个数字可能高于 700 万。

（十二） 内鬼作祟！可口可乐承认 8000 名员工的个人信息被泄漏

2018 年 5 月 25 日，据外媒 BleepingComputer 报道，可口可乐公司本周对外宣布了一起数据泄露事件，他们在前员工的个人硬盘中，发现了大量现有员工的个人数据，而这些数据，是该前员工从可口可乐违规挪用的。

这起泄漏时间从去年 9 月被发现，直到本周才对外宣布。事件影响 8000 可口可乐员工。目前，可口可乐正通过第三方供应商向受影响的员工提供一年的免费身份监测。

（十三） 纽约 9 家 B&BHG 餐厅遭恶意软件感染，顾客支付卡数据泄漏

2018 年 7 月，据多家国外媒体报道，B&BHG 酒店集团（B＆BHospitalityGroup）证实该集团在纽约市运营的 9 家餐厅所配备的销售终端（POS）被发现感染了恶意软件。初步调查结果显示，此次黑客入侵发生在 2017 年 3 月 1 日至 2018 年 5 月 8 日之间，黑客可能已经偷走了支付卡号码、持卡人姓名、支付卡有效日期、内部验证码以及其他一些付款信息。

第三方网络风险管理平台公司 CyberGRX 的首席执行官 FredKneip 表示：“一个企业数字生态系统中的所有第三方都需要不断评估他们引入的风险水平，这一点对于销售终端解决方案提供商来说尤其重要，因为他们能够访问所有的支付数据。”

（十四） 新西兰网盘 Mega 上万帐号密码遭泄露，被公开在 VirusTotal 上

2018 年 7 月 17 日，据外媒 ZDNet 报道，Mega——这家于新西兰成立并提供在线云存储和文件托管服务的公司，目前被发现其平台中有成千上万的帐号凭证信息已在网上被公开

发布。被泄露的信息以文本文件形式提供，涉及超过 15,500 条用户名、密码和文件名的数据。

这份文本文件最早由 DigitaSecurity 公司的首席研究官和联合创始人 PatrickWardle 于 6 月份在恶意软件分析 VirusTotal 上发现，而这份文件是在几个月前由一名据称在越南的用户上传的。

（十五） 云泄露最前线：巴西订阅视频服务 SkyBrasil 暴露 32.7 万用户信息

2018 年 12 月 4 日，独立研究员 FabioCastro 发现，巴西最大的订阅电视服务公司 SkyBrasil 泄露了 32.7 万用户的信息，包括 28.7GB 的日志文件和 429.1GB 的 API 数据，这些数据涉及姓名，家庭住址，电话号码，出生日期，客户端 IP 地址，付款方式和加密密码。

虽然 Castro 发现了这一事件后通知了 SkyBrasil，公司随后也对数据库进行了密码保护；但其服务器至少从 10 月中旬就开始在 Shodan 上被编入索引，目前还不清楚数据库的访问者数量。

（十六） 知名运动品牌 UnderArmour1.5 亿用户数据被泄露，称不涉及敏感信息

2018 年 3 月 30 日，据报道，本周四，美国著名运动装备品牌 UnderArmour 称有 1.5 亿 MyFitnessPal 用户数据在上个月被泄露了，MyFitnessPal 是一款 UnderArmour 旗下的食物和营养主题应用。

此次关于用户数据泄露的声明使得该公司的股票价格下跌了 2.4%。据该公司称，此次数据泄露事件影响到的用户数据包括用户名、邮箱地址、和加密的密码。该运动装备制造商称，是在 3 月 25 日才发现的此次数据泄露事件，并从那时就开始通知受影响用户。

（十七） 珠宝电商 MBM 公司 130 万客户信息泄漏，内含明文密码

2018 年 3 月 18 日，据雷锋网报道，MBM 公司被德国安全公司 KromtechSecurity 的研究人员抓住了小辫子。研究人员在不安全的亚马逊 S3 存储桶中发现了该公司的 MSSQL 数据库备份文件。

最初，研究者怀疑这些数据归沃尔玛所有，因为这个存储桶被命名为“walmartsql”，不过后来他们通过分析后发现，这些数据的主人其实是 MBM 公司。在对泄露文档作了进一步评估后他们发现，这里容纳了超过 130 万人（准确来说是 1314193 人）的私人敏感数据。这些数据包含个人住址、email 地址、IP 地址和邮政编码，许多客户的密码甚至直接用明文显示，毫无安全性可言。

安全专家支招称，直接把敏感信息存入一个向公众开放的存储桶可不是什么高明的决定，没有对密码进行加密更是不可饶恕。

（十八） 英国电商软件 FashionNexus 爆漏洞，多个品牌网站 140 万购物者隐私泄露

2018 年 8 月，许多在英国服饰和配饰在线购物网站上消费的购物者发现他们的个人信息已经被确认遭到了泄露。此次数据泄露事件涉及多个英国时尚品牌，而导致时间发生的根源来自于他们共同的 IT 服务提供商 FashionNexus。

由于 FashionNexus 及其姊妹公司 WhiteRoomSolutions 在安全管理方面的问题，导致一

台服务器能够被公开访问。安全研究员 TaylorRalston 指出，在这台服务器上包含有一个共享数据库，其中涉及众多在线购物网站消费者的个人详细信息。总的来说，在线暴露的信息包含了大约 140 万消费者的个人信息，包括 md5 哈希密码、密码、Salt 值、姓名、电子邮件地址、电话号码和其他一些数据。值得庆幸的是，并不涉及明支付卡信息。

（十九） 上万印度板球球员个人信息泄露

2018 年 5 月，Kromtech 安全中心的研究人员再次发现了两个因配置错误而在线暴露的 AmazonS3 存储桶。从数据的内容来看，它们似乎归属于印度板球管理委员会（BoardofControlforCricketinIndia，BCCI）。

暴露的 S3 存储桶包含有大量的敏感数据，涉及从 2015 年至今向 BCCI 提交赛季参赛申请的约 1.5 万~2 万印度人。泄漏的信息包括：注册过球员的登记表、选票、银行单据等扫描件及其亲属的姓名、出生日期、出生地、永久地址、电子邮箱地址、手机号码/固定号码、医疗记录、出生证明号码、护照号码、SSC 证书号码、PAN 卡号码及各种扫描件等。

十二、 医疗卫生

（一） 问题综述

2018 年医疗卫生领域的数据安全形势也不同乐观，医疗机构涉及大量隐患及疾患信息，如果保护不当，将严重侵害民众隐私，相当于对医院患者的二次伤害及广泛。一方面医疗机构需要在自身的安全建设上补课，提升自身信息化系统的“免疫”能力；另一方面，今年的一些数据被盗事件，是患者家属等发现的，说明医疗机构应重视社会的反馈，及时发现问题，防范风险。

（二） MongoDB 数据库意外暴露两百多万墨西哥公民的医疗健康数据

2018 年 8 月，据 BleepingComputer 报道，一个 MongoDB 数据库被发现可以通过互联网公开访问，其中包含了超过 200 万（2,373,764）墨西哥公民的医疗健康数据。这些数据包括个人的全名、性别、出生日期、保险信息、残疾状况和家庭住址等信息。

这个数据库是由安全研究员 BobDiachenko 通过 Shodan 发现的，Shodan 是一个搜索引擎，可以搜索所有联网设备，而不仅限于 Web 服务器。当被发现时，这个数据库完全暴露在互联网上，任何人都可以对其访问和编辑，因为它没有设置密码。“MongoDB 的安全隐患问题至少从 2013 年 3 月开始被人们所知道，从那以后就开始被广泛报道……不安全的数据库仍然大量暴露在互联网上，此类数据库至少有 54,000 个。”

（三） 澳大利亚 SAHealth 医院意外暴露 7200 名儿童个人资料

2018 年 8 月 7 日，据报道，澳大利亚 SAHealth 在其官方网站上发布了一篇新闻稿，称旗下位于澳大利亚第五大城市阿德莱德的妇女儿童医院（WomensandChildrensHospital）因工作人员操作失误，意外暴露了约 7200 名儿童的医疗记录和个人资料。其中，包括 1996 年至 2005 年期间在该医院接受百日咳、胃肠和呼吸道感染治疗的患者的详细资料。

根据 SAHealth 的说法，这些数据早在 2005 年就已经可以被公众通过互联网访问，直到

在上周三有患者的父母在线注意到这些数据后，医院方面才得知了这一事件。这也意味着，这些数据已经在线暴露近 13 年！

（四） 美国医疗保健公司 BlueSpringsFamilyCare 近 4.5 万条患者记录遭泄露

2018 年 7 月 31 日，最近的新闻报道显示，BlueSpringsFamilyCare 遭遇了勒索软件攻击，而被落入攻击者手里的数据达到了近 4.5（44,979）万条。

在该公司的一封公开信中指出，攻击者可能获得了各种患者记录信息，这至少包括：患者的全名、住址和出生日期、帐号、社会保险号、残疾等级、医疗诊断和驾驶执照/身份证号码。

公开信还透露，2018 年 5 月公司曾遭受勒索软件攻击。BlueSpringsFamilyCare 表示，他们已经与另一家电子健康记录提供商达成合作协议，而这个新的合作伙伴会对所有健康数据进行加密保护。

（五） 美国医疗公司 LifeBridgeHealth 泄露近 50 万患者个人信息

2018 年 5 月 22 日，根据《巴尔的摩太阳报（BaltimoreSun）》在本周二刊登的一则报道，LifeBridgeHealth 公司日前向近 50 万位患者发出通知称，他们的个人信息可能会因为网络黑客攻击事件而遭到暴露。

根据 LifeBridgeHealth 官方的说法，这一事件最初是在今年 3 月份被发现的，当时他们在一台服务器上发现了恶意软件，而该服务器被用于为医疗系统的附属医师小组以及共享注册和计费系统提供电子医疗记录数据。

LifeBridgeHealth 通过电子邮件告知患者，根据第三方安全公司的调查结果来看，数据泄露最初开始于 2016 年 9 月 27 日，遭泄露的信息包括患者的姓名、家庭住址、出生日期、保险信息和社会安全号码。

（六） 美国医疗转录公司 MEDantex 意外暴露数千名医生提交的患者记录

2018 年 4 月，KrebsOnSecurity 在上周五（4 月 20 日）了解到，MEDantex 旗下的一个门户网站存在泄露患者医疗记录的安全隐患。该网站允许医生上传音频文件。这个功能页面原本是应该得到加密保护的，但事实证明任何互联网用户都可以对其进行访问。

MEDantex 是一家总部位于美国堪萨斯州的医疗转录公司，它的主要业务即是为医院、诊所和私人医生提供定制的转录解决方案。KrebsOnSecurity 表示，他们目前尚不清楚在 MEDantex 网站上具体有多少患者的医疗记录遭到了暴露，但其中一个被命名为“/documents/userdoc”的目录包含了与 2300 多名医生相关的文件。目录以按字母顺序排列，每一个目录中都包含有不同数量的患者医疗记录，其中的 MicrosoftWord 文档和原始音频文件都可以被下载。

（七） 挪威过半人口医疗数据疑遭泄漏，攻击者“高阶且专业”

2018 年 1 月 19 日，挪威当地媒体报道称，负责管理挪威东南部地区医院的机构 HealthSouth-EastRHF 宣布网站遭泄露事件，超过 290 万用户，超过挪威（总人口 520 万）一半的人口可能受影响。该组织表示，挪威医疗部门的计算机紧急响应中心 HelseCERT 发现来自 HealthSouth-East 计算机网络的可疑流量；一名黑客或黑客组织可能已经盗取了上述人口的医疗数据。

HealthSouth-EastRHF 和其母公司 SykehuspartnerHF 发布联合声明称，“情况严重，并已采取措施限制该事件造成的损害。”HealthSouth-EastRHF 将攻击者描述为“高阶且专业”。另外已将该事件通知挪威 CERT 团队即 NorCERT。

（八） 为防止再次发生泄漏事件，新加坡公共医疗领域电脑暂时“断网”

2018 年 7 月 23 日，新加坡卫生部称，公共医疗机构使用的电脑已暂停接入互联网，防止类似新加坡保健服务集团（新保集团）数据库遭网络攻击事件再度发生。

新加坡公共医疗机构多项服务依靠互联网，切断工作人员所用电脑与互联网的连接可能延长等待时间，给病人带来不便。

据了解，新保集团数据库 6 月底开始遭网络攻击，大约 150 万名病人个人资料失窃，新加坡总理李显龙、荣誉国务资政吴作栋及多名部长的个人资料和门诊记录也被窃取，新加坡政府已成立独立调查委员会调查此事。

（九） 英国知名药妆店 Superdrug 近 2 万名顾客个人信息遭泄露

2018 年 8 月 24 日，据报道，有黑客在本周一（8 月 20 日）联系了英国知名药妆店 Superdrug，称他们已经获得了大约 2 万名 Superdrug 顾客的详细个人信息。作为证据，黑客还向 Superdrug 展示了 386 名顾客的个人信息记录。

Superdrug 号称英国第二大美容和健康零售商，占据英国 30%市场份额。经过 Superdrug 的确认，被窃取的个人信息包括顾客的姓名、住址，以及部分顾客的出生日期、电话和积分余额。不过，Superdrug 坚称被黑客窃取的凭证是从入侵第三方得来的，而并非通过入侵 Superdrug 的系统。之所以能够进一步获取到 Superdrug 顾客的详细个人信息，这是因为黑客

利用了人们有在各种在线服务使用相同密码的习惯。

（十） 遭遇网络钓鱼攻击，美国奥古斯塔大学医疗中心泄露 41.7 万份记录

2018 年 8 月 21 日，据报道，奥古斯塔大学医疗中心在去年曾遭遇了一次网络钓鱼攻击。最新调查显示这次攻击导致约 41.7 万份记录遭泄露。遭泄露的数据包含了患者个人信息，以及他们的医疗和健康记录。对于其中一些受害者来说，遭泄露的数据还可能包含财务记录和社会安全号码。

根据该校网站上最新发布的安全通知来看，攻击发生在 2017 年 9 月 10 日至 11 日。最初，该校认为攻击仅暴露了“少量的内部电子邮件帐户”。然而，在今年，他们意识到约有 41.7 万份记录因此遭到泄露。

奥古斯塔大学已经准备向每一名受害者发送个人电子邮件，以通知他们有关此次事件，并为社会安全号码遭到泄露的人提供为期一年的免费信用监控服务。

（十一） 优步 270 万用户信息被黑客盗取，遭英国监管机构罚款 38.5 万英镑

2018 年 11 月 27 日，优步（Uber）近日被英国媒体曝光：旗下约 270 万英国用户个人信息在 2016 年被黑客盗取，而最夸张的是优步为了“息事宁人”居然支付了 10 万美元给黑客，因此被英国监管机构重罚 38.5 万英镑。

据报道，英国政府 InformationCommissioner'sOffice（ICO）表示，优步在遭遇黑客攻击后，没有第一时间告知被泄露的用户有关细节，反而支付赎金，这一做法是对用户和优步司机信息安全性的漠视。ICO 将这次的黑客行为定义为“严重违法行为”。

目前，ICO 正在对案件进行进一步的调查。该办公室还指出，已经在优步的系统中发现了一系列可获得数据的安全漏洞，黑客从一个优步运营的云储存系统中可以下载数以百万计的客户的敏感信息，已掌握了 2016 年 10 月和 11 月被攻击的犯罪事实。

十三、 制造业

（一） 本田汽车泄露敏感数据

2018 年 5 月 30 日，Kromtech 安全中心再次披露了本田汽车公司（HONDA）在印度的子公司——本田印度（HondaIndia）因不安全 AWSS3 存储桶泄露了超过 5 万名客户的个人详细信息。

由于公司意外的将超过 5 万名 HondaCONNECT 移动应用程序用户的个人详细信息存储在了两个可公开访问的 AmazonS3 存储桶中，这使得黑客窃取这些数据成为了可能。Kromtech 安全中心的研究人员 BobDiachenko 发现，能够被公开访问的信息包括用户及其可信联系人的姓名、电话号码、密码、性别和电子邮箱地址，以及有关他们汽车的信息，包括 VIN、ConnectID 等。

（二） 特斯拉起诉前员工：黑进内部生产系统盗取并泄露机密数据

2018 年 6 月，据美国内华达州联邦法庭公布的诉讼文件显示，特斯拉起诉了一名该州 TeslaGigafactory 超级工厂的一名前员工马丁·特里普（MartinTripp），称其盗取了该公司的商业机密并向第三方泄露了大量公司内部数据。

据诉讼文件显示，该名员工承认曾开发恶意软件进入特斯拉内部生产操作系统，偷取大量数据并交给第三方，还向媒体发表不实言论。这些被泄露的数据包括“数十份有关特斯拉的生产制造系统的机密照片和视频”。

特里普开发的恶意软件安装在了三台不同员工的电脑上，所以在他离开特斯拉后，还能继续从该公司传输数据到第三方。而电脑被安装该恶意软件的员工也将受到牵连。

（三） 史上最严重数据车祸：100+车厂机密全曝光，通用丰田特斯拉统统中招

2018 年 7 月 22 日，据报道，加拿大汽车供应商 LevelOne 被 UpGuard 的研究员 ChrisVickery 发现，该厂商的数据后门大开，黑客可轻松访问其 100 多家合作伙伴车厂的机密文件。这 100 多家车厂，从通用汽车、菲亚特克莱斯勒、福特、丰田，大众到特斯拉，都名列其中。

而被泄露的数据，从车厂发展蓝图规划、工厂原理、制造细节，到客户合同材料、工作计划，再到各种保密协议文件，甚至员工的驾驶证和护照的扫描件等隐私信息，共计 157 千兆字节，包含近 47,000 个文件。在反复检查过程中，ChrisVickery 确认，通过 LevelOne 的文件传输协议 rsync，可以无障碍访问上述所有隐私数据。

（四） 巴西最大工业协会被指数据泄露，数千万个人信息可互联网访问

2018 年 11 月，据报道，白帽黑客生态系统 HackenProof 的安全研究员鲍勃·迪亚琴科（BobDiachenko）称其发现了三个包含个人记录的数据库，可通过 Elasticsearch 搜索引擎访问这些记录。最大的数据源包含 3480 万个条目。据迪亚琴科称这些数据已在网上暴露数日。

而被指控泄露上述数据的主体是巴西圣保罗州工业联合会（简称 FIESP），FIESP 代表了约 13 万家公司，是巴西工业部门的最大企业实体。这些外泄记录包括：姓名、ID 与社会安全号码、完整住址信息以及电子邮件与电话号码。

关于该数据泄露事件，该研究员称其已试图警告 FIESP，但无济于事。HackenProof 在推特上首次公开该泄露事件后，一位巴西粉丝将该数据泄露事件告知了企业，企业这时才离线了数据库。

十四、 物联网

（一） 神乎其神！北美某赌场因联网鱼缸漏洞被黑，客户信息全泄露

2018 年 4 月 17 日，据报道，网络安全公司 Darktrace 的首席执行官 NicoleEgan 在上周四于伦敦举办的一次会议上演示了黑客如何通过入侵赌场走廊上水族馆中的联网恒温器黑掉一个名称未被透露的赌场。

黑客利用了恒温器中存在的一个漏洞在网络中站稳脚跟，随后，其设法访问了赌徒中豪掷重金的人的数据库，“然后在网上拉回来拉出恒温器并拉向云。”尽管 Eagan 并未透露这家赌场的身份信息，但她分享的这次安全事件可能发生在去年。当时 Darktrace 公司发布了一份报告，说明了位于北美的一家赌场遭到了这类恒温器攻击。

（二） 俄罗斯视频监控公司 iVideon 数据泄露，涉及超过 82 万名用户个人信息

2018 年 5 月 14 日，Kromtech 安全中心的研究人员在最近发现，一个归属于俄罗斯视频

监控公司 iVideon 的 MongoDB 数据库并没有得到保护，并向公众开放。

从数据库的内容来看，它似乎涵盖了 iVideon 公司的整个用户群，包括其用户和合作伙伴的登录名、电子邮箱地址、密码哈希值、服务器名称、域名、IP 地址、子帐户以及软件设置和付款设置信息（并不包括任何信用卡数据）。有超过 82 万（825388）名用户以及 132 家合作伙伴受到影响。

十五、 其他

除了金融、交通、教育、医疗等热点领域的数据泄露事件，工业系统、物联网、咨询营销公司等其他领域的数据安全隐患也助推了 2018 年数据不安全形势。这些事件，有的关乎选民、有的涉及隐私、有的威胁企业商业机密，同样应该收到重视，从中吸取教训，及时改进。

（一） MongoDB 数据库配置不当，数万 Bezop 代币用户个人信息泄露

2018 年 4 月，据报道，网络安全公司 Kromtech 偶然发现了一个未加密的 MongoDB 数据库，其中包含了超过 25,000 名 Bezop 用户的详细个人信息，其中一部分是 6,500 名 Bezop（BEZ）加密货币的投资者，剩余部分则单单只是 Bezop 代币的接收者。

安全研究人员称，这个向公众开放的数据库包含了姓名、家庭住址、电子邮箱地址、加密密码、钱包信息以及护照、驾驶执照或身份证的扫描件等敏感信息。

数据库所存储的这些信息与 Bezop 团队在年初开始运行的“赏金计划”有关。在此期间，该团队将 Bezop 代币分发了给在其社交媒体帐户上推广该货币的用户。

（二） MongoDB 可公开访问，美国慈善机构 Kars4Kids 泄露上万名捐赠者个人信息

2018 年 11 月 3 日，网络安全咨询公司 Hacken 的网络风险研究主管 BobDiachenko 发现了一个似乎是可公开访问的 MongoDB 数据库。经过进一步调查，这些数据似乎包含了 21,612 名 Kars4Kids 捐赠者的电子邮箱地址和其他个人信息，以及超级管理员用户名和密码。

Kars4Kids 是一家成立于 1994 年的慈善机构，总部设在美国新泽西州莱克伍德，将其大部分收益都捐赠给了 Oorah，一个以解决“犹太儿童及其家庭的教育、物质、情感和精神需求”为目标的国家组织。

据分析，有网络犯罪分子可能已经使用这些用户名和密码访问了 Kars4Kids 仪表板的内部帐户，这将使得他们能够访问更敏感的数据。例如，度假券（向捐赠者提供的免费假期）和收据，以及包括电子邮箱地址、家庭住址和电话号码等在内的个人信息。

（三） MongoDB 配置不当，近 70 万美国运通印度分公司客户联系信息遭泄露

2018 年 11 月，据外媒 ZDNet 报道，近 70 万名美国运通（Amex）印度分公司客户的个人详细信息在最近被一名安全研究人员发现通过一台存在配置错误的 MongoDB 服务器暴露在了网上。

大约在三个星期以前，国际网络安全咨询公司 Hacken 的网络风险研究主管 BobDiachenko 发现了这台漏洞百出的服务器。该服务器不仅能够被公开访问，而且没有设置密码。

据研究员表示，这些以明文形式存储的记录包含了美国运通印度分公司客户的个人详细信息，如电话号码、全名、电子邮箱地址和支付卡类型等。虽然这些数据似乎并不过于敏感，但很可能会对垃圾电子邮件活动起到推动作用。

（四） 开发者安全预警：数万 Jenkins 暴露在网上，已发现大量敏感数据

2018 年 1 月 23 日，研究人员表示，没有利用任何漏洞，就在互联网上发现了暴露 2.5 万个 Jenkins 实例，从这些实例中发现了不少大型公司泄露了敏感证书和日志文件，这都可能会引发数据泄露事件。

Jenkins 是最受欢迎的开源自动化服务器，由 CloudBees 和 Jenkins 社区维护。自动化服务器支持开发人员构建，测试和部署其应用程序，在全球拥有超过 133,000 个活跃安装实例，用户超过 100 万。

上述 2.5 万个实例中，10-20％的实例存在配置错误，这些错误配置的实例，大多也都泄露了敏感信息，包括专用源代码库的证书，部署环境的证书（例如用户名、密码、私钥和 AWS 令牌）以及包括凭证和其他信息的作业日志文件敏感数据。

（五） 澳大利亚国家绝密文件被卖二手店

2018 年 2 月 1 日，澳大利亚政府的某人决定卖掉两个尘封已久的文件柜卖掉，因为他们丢掉了文件柜钥匙；随后买家用一把电钻打开了柜——连续五届政府在储藏柜放着的文件。

最终，这些文件辗转到达澳大利亚广播公司（ABC）的手中，这家媒体目前正在发布他们认为安全的资料。ABC 披露的文档中包括 Rudd 政府如何计划资助澳大利亚已引发争议的国家宽带网络（NBN）的机密简讯。该公司播报人员表示“不会发布涉及国家安全、或者信息已公开、或涉及公务员的隐私的文档”。

（六） 半年 186 家！日企机密文件大量被“晒”百度文库

2018 年 3 月，据调查企业信息泄露情况的相关公司的统计，最近半年多时间，186 家日企的文件被发布到文档分享网站上。这可能导致专利信息的泄露等，专家呼吁日本企业加强内部管理。

发布日本企业内部文件的是中国百度运营的文档分享网站“百度文库”。日本 IT 相关公司“CROSSWARP”调查显示，仅 2017 年 6 月～2018 年 2 月期间，上述近 200 家日企的文件被发布到百度文库上。这些资料上均标有注意字样，意味着属于“机密”文件。

熟悉中国法律的律师分部悠介表示，在中国泄露企业营业机密也属于违法行为，不过只有受害金额较大等情况下才会适用刑事处罚。另外，由于要证明网上的投稿使企业蒙受严重损失十分困难，因此很难通过刑事处罚来遏制这种行为。

（七） 环球唱片被爆泄露敏感数据

2018 年 5 月 30 日，Kromtech 安全中心披露了成立于 1912 年的全球音乐巨头——环球唱片（UniversalMusicGroup，UMG）因为受到其承包商的牵连，暴露了自己的内部 FTP 凭证、数据库跟密码和 AWS 配置详细信息，包括访问密钥和密码。

在与环球唱片取得联系后，该公司迅速进行了回应并解决了问题。

（八） GoogleGroups 配置不当，一大波财富 500 强公司敏感信息遭泄露

2018 年 6 月，KennaSecurity 公司研究员指出，由于 GoogleGroup 配置出错，导致数千家组织机构的某些敏感信息被泄露。这些受影响组织机构包括财富 500 强公司、医院、高等院校、报纸和电视台以及美国政府机构等。根据样本统计，约 31%的 GoogleGroups 会导致泄露数据。

独立研究员 BrainKrebs 上周五发布分析结果表示，除了泄露个人信息和金融数据外，配置错误的 GoogleGroups 账户有时候还公开检索关于组织机构本身的大量信息，包括员工使用手册链接、人员配备计划、宕机和应用 bug 报告以及其他内部资源。

研究人员指出，“鉴于这种信息的敏感特征，可能会引发鱼叉式钓鱼攻击、账户接管和多种特定案例的欺诈和滥用情况。”

（九） 美国大数据营销公司因失误泄露 2TB 隐私信息，涉 2.3 亿人

2018 年 6 月 28 日，据 Wired 报道，本月初曝光的市场和数据汇总公司 Exactis 服务器信息暴露的事情经调查为实。Exactis 此次的信息泄露并不是黑客撞库引起或者其它恶意攻击，而是他们自己的服务器没有防火墙加密，直接暴露在公共的数据库查找范围内。

据了解，Exactis 采集了大约 3.4 亿条记录，大小 2TB，可能涵盖 2.3 亿人，几乎是全美的上网人口。虽然上述信息中不包含信用卡号、社会保障号码等敏感的金融信息，但是隐私深度却超乎想象，包括一个人是否吸烟，他们的宗教信仰，他们是否养狗或养猫，以及各种兴趣，如潜水和大码服装，这几乎可以帮助构建一个人的几乎完整“社会肖像”。

（十） 3500 万美国选民记录黑客论坛有售

2018 年 10 月 24 日，美国 11 月中期选举临近，AnomaliLabs 和 Intel471 的研究人员发现某黑客论坛上竟然在售卖 3500 万条美国选民的记录，牌出售的选民记录来自美国 19 个州的 2018 选民登记，包括威斯康辛、得克萨斯和佐治亚州。据称该选民数据记录包含全名、电话号码、住址、选举历史和其他未明确的选举数据。

号称有 600 万选民的威斯康辛州，选民记录价格为 1.25 万美元。其他州的选民信息报价在几千美元，到几百美元不等。卖家承诺，每周都会在从州政府线人处收到信息时更新选民登记数据。令人匪夷所思的是，售卖信息刚贴出来几小时后，论坛上就出现了众筹购买该选民记录的活动。

（十一） 国泰航空 940 万名乘客个人数据被盗，包含出行地点数据

2018 年 10 月 25 日，据外媒报道，大型国际航空公司国泰航空披露，在今年 3 月发生的一次数据泄露事件中，该公司的 940 万名乘客的记录被盗，另外含有姓名、出生日期、住址等个人信息的护照信息也可能已经泄露。据悉，此次事件还涉及到了每位乘客的具体出行地点以及客户服务代表的评论等等。

另外，国泰航空还指出，有 403 个过期信用卡卡号、27 个没有 CVV 号码的信用卡卡号遭到访问。但是，没有密码遭到泄露。

这家公司选择在 6 个月后公布数据泄露事件的做法也许会在欧洲市场遇到阻碍，因为那边最新通过的通用数据保护条例要求公司在发现违规情况三天后就要告知客户和执法部门。

（十二） 咨询公司 RiceConsulting 云泄露大量敏感数据：曾为美国民主党筹款 432 万美元

2018 年 10 月 30 日，Hacken 网络风险研究主管 BobDiachenko 在本月 17 日通过 Shodan 搜索引擎发现了一台因配置错误而公开暴露在互联网上的 BuffaloTeraStationNAS 网络附加存储器，所有者是总部位于美国马里兰州的 RiceConsulting 咨询公司。

根据 RiceConsulting 官方网站所展示的信息来看，该公司曾在 2017 年与美国民主党合作（DemocraticPartyUS），为其筹集资金超过 432 万美元。NAS 包含了有关 RiceConsulting 过去数千次筹款活动的详细信息，如姓名、电话号码、电子邮箱地址、地址、公司、合同、会议记录、桌面备份、员工详细信息等。

Diachenko 表示，他在 NAS 上发现的“最重要的资产”是 NGP 的用户名和密码组合。但遗憾的是，所有这些用户名和密码都被存储在一个没有设置密码的 Excel 文件中。

（十三） 丽笙酒店集团遭遇数据泄露，官方称受影响会员不足 10%

2018 年 11 月 2 日，据英国 TheRegister 报道，丽笙酒店集团（RadissonhotelGroup，以下简称“丽笙”）已经于 10 月 30 日开始向参与其奖励计划的会员发出电子邮件，确认了一起黑客攻击。丽笙在其声明中没有提到黑客侵入了哪个系统，也没有提供其他技术细节。其发言人表示，此次事件只影响不足 10%的丽笙奖励计划会员账户。

丽笙在其发出的电子邮件中表示，此次数据事件并不涉及任何信用卡或密码信息，目前已经被确认能够被黑客访问的信息仅限于会员的姓名、住址（包括居住国）、电子邮箱地址，以及一部分会员的公司名称、电话号码、丽笙奖励计划会员编号等信息等。

附录 3 暗网上重大数据交易事件

本章主要梳理了 2018 年被爆出的一系列暗网重大数据交易事件，涉及军事、政府、互联网等多个行业。

一、 军政及事业单位在暗网的重大数据交易事件

（一） 问题综述

2018 年，发生多起与军事单位，政府机构和事业单位相关的暗网交易事件。这些事件背后的影响都非常严重，如 3500 万的选民数据被泄露势必会造成大规模地身份泄露，干预到美国总统大选；FBI 的特工包含职务在内的个人信息被泄露，势必给了相关人员一个新的突破口。

一般来讲，军政相关的机构，更应该做好安全相关的工作，因这些信息一旦被泄露，将会造成非常大的影响，然而事实表明，在目前阶段各国在安全方面还未能做到牢不可破的程度，存在着很多安全问题。在下列列出的重大事件中，有针对 FBI 等情报机构的反击活动，也有简单因内鬼或内部人员账号泄露而导致的信息售卖活动，可以看出，到目前为止，相关机构易受到的攻击同时包含内部和外部两个方面。

（二） 某省 1000 万学籍数据在暗网出售

2018 年 8 月 1 日晚，“威胁猎人”微信公众号披露称，监测到有人在暗网出售某省 1000 万学籍数据。从卖家放出来的测试数据来看，这些被售卖的学籍数据覆盖了某省的大部分市区，年龄主要分布在 95 年~06 年之间，即 12 岁到 23 岁之间。泄露的数据涉及到多个维度：学生姓名、身份证、学籍号、户籍位置、监护人号码、居住地址、出生地和学校名称等。此外，被出售的数据还提供 100G 照片链接。出售者表示，这些数据可以分开购买：500 万条数据 0.01 个比特币；1000 万条数据 0.02 个比特币

根据分析，这些被售卖的数据主要为小学生的信息，几乎不包含大学生的信息。根据合理推测，该数据来源应该是该省中小学生的信息管理系统被拖库，并且该“拖库”事件很有可能是内部人员泄露或者内部人员的账号被泄露而导致的。

（三） 11 月中期选举临近，3500 万美国选民数据通过暗网出售

AnomaliLabs 和 Intel471 的安全研究人员追踪到有人在暗网兜售 2018 年美国选民登记记录。这些选民数据来自以下 19 个州：格鲁吉亚、爱达荷州、爱荷华州、堪萨斯、肯塔基、路易斯安那州、明尼苏达、密西西比州、蒙大拿、新墨西哥、俄勒冈、南卡罗来纳、南达科他州、田纳西、德州、犹他州、西弗吉尼亚、威斯康星、怀俄明。被售卖的信息包含选民的全名、电话号码、真实地址、历史投票和其他暂未明确的投票数据。而每个选民的信息以 150~12,500 美元的价格出售。售卖者还声称，一旦购买这些数据，他们将每周都为购买者提供定期的更新。

AnomaliLabs 声称这是第一次发现有人售卖 2018 年的选民登记数据。此次美国选民的数据在暗网被出售发生在 2018 年 10 月 5 日，距离 11 月中期大选大约才一个月的时间。而出售选民记录的帖子在贴出的几个小时内，就有人在论坛上发起了众筹购买选民记录的活

动。根据以往的 Facebook5000 万用户数据被泄露且用于干涉选举的事件来看，在美国中期大选中，很有可能会出现大规模的出于恶意的身份盗用。

（四） FBI 数万名特工信息在暗网遭披露，国外多家情报机构均受影响

2018 年 12 月，Twitter 上 ID 为 AnonymousUnity 的用户表示在暗网公开了 FBI 数万名特工以及法国警察的个人信息，并且附上了暗网链接。进入该暗网链接，可以看到 2 万余名 FBI 特工及法国警察的个人信息。被公布 FBI 特工的个人信息包含：姓名、职务、电话、邮箱等；被公开的法国警察的个人信息同样包含：姓名、电话和邮箱地址。此外，此份在暗网被公开的信息，还包括法国对外安全局 DGSE、美国 FBI、CIA、英国军情六处下的各级网站域名和对应的 IP。

因任何黑客都可以通过 Anonymous 组织的名义发布活动，对于在暗网直接披露这些信息所使用的 Anonymous 这个身份我们暂且无法考证。据披露者展示的“圣战宣言”，表明了此次的 FBI 特工个人信息披露活动的目的：对情报机构监视和逮捕多人的反击。而对应暗网页面的“Part1”显然意味着还有后续的数据披露。

一、 IT 互联网企业在暗网的重大信息交易事件

（一） 问题综述

2018 年 6 月 13 日左右的一周内，发生了多起大型企业的数据在暗网被售卖的事件，除去某知名动漫网站发布过通告承认有近千万用户的数据被盗外，我们目前无法确认其他同期售卖的数据是否为对应的官方数据，因为也有很大可能为利用其他数据撞库而得。但是经过测试，可以确定的是，这些数据都是真实有效的。

从暗网中哪些出售的帖子来看，数据的来源主要涉及以下黑客攻击和撞库两个方面。因互联网大型公司一般都有数据量大和日流量高的特点，所有有些黑客出来出售相关的数据外，还会出售大型网站的 shell 和内网权限。此外由于很多人在不同的网站也使用同样的账号和密码，导致有心人会拿着已有的账户和密码去撞库，以求获得更多的信息，在下列被列出的事件中，就有不少数据为撞库所得。

此外，近年来区块链越来越火热，针对区块链的攻击和数据泄露也越来越多。根据以往经验，针对区块链的攻击活动的背后，一般都不是个人而是团队，且多利用恶意软件盗取信息和货币。

（二） 某动漫网站以及某共享单车平台近千万用户信息在暗网出售

2018 年 6 月 13 日，某动漫网站发布公告称近千万用户数据被盗，被盗的数据包含：用户的 ID、用户昵称和加密存储的密码等数据。而这些数据早在 3 月 8 日就已经在暗网被出售。出售数据被分为 3 组，其中一组为 800 万条该视频网站数据，以 12,000 元，即 1 元 800 条的价格出售。而另外两组的数据也分别达到了 70 万和 600 万条，以 7,000 和 12,000 元的价格出售。这些被出售的数据均包含：用户名、手机号码和密码，且均为一手数据，一整份价格约为 0.49 个比特币。

此外，暗网中还有人在兜售该视频网站的 Shell 和内网权限，据称主要卖点为：数据量大以及日流量高。

（三） 某知名招聘网站近 200 万条用户数据在暗网公开出售

2018 年 6 月 14 日，某知名动漫网站公开声明表示近千万用数据被泄露且在暗网被出售的第二天，就有人在暗网发帖公开出售另一家大型招聘网站的用户数据。卖家声称拥有近 200 万条相关数据，至少包含用户的账户、密码和邮箱。

有人表示这些数据可能为卖家从别处整理，伪装成招聘网站的数据。但据测试，卖家所展示数据同样真实有效，可能为撞库所得。

（四） 暗网最大的托管商被黑客攻击，6500+网站被删

2018 年 11 号 15 号，暗网最大的托管商发出公告声称，有黑客攻击了他们的服务器，托管在他们服务器上的多达 6500+个网站被删除。一直以来暗网都是都是各种非法分子的集中地，充满了毒品、枪支、色情等交易，是很多人眼中的法外之地。此次暗网最大托管商被黑客攻击事件，目前尚不清楚缘由。但根据该公司的公告可以肯定，此次事件绝非临时起意，而是筹备了很久。

事实上，这并不是暗网第一次发生黑吃黑的事件了，早在去年 2 月份左右当时暗网最大的服务托管商就曾因托管儿童色情网站被一开始只想搞到数据读取权限的黑客删库。

不管此次暗网托管商是被何人以何种目的攻击，6500+暗网网站被删除，无疑从一定程度上打击了暗网上违法犯罪活动，给了相关产业一个重大的打击。

（五） 某社交平台 3000 万用户数据以仅仅 50 美元的价格在暗网抛售

2018 年 11 月 30 日，有人在暗网中出售某社交平台的 3000 万用户数据，包含：手机号和密码。卖家声称这些数据共 31,613,301 条数据，其中有仅有不到 1%的用户密码为空，也就说至少有 3000 万用户的被出售的数据同时包含手机号和密码。这些数据应该为 2015 年 7 月 17 日之前的数据，一直到今年 11 月份才在暗网出售，且出售的价格非常低，仅仅只需 50 美元，折合人民币不到 350 元。

根据卖家泄露，这些数据为 3 年前撞库所得，因此无法保障数据的时效性。但是如此大规模地数据，仍然适合用来制作字典和撞库。

（六） 某比特币网站数据库以及网站源码在暗网被出售

2018 年 12 月 17 日，某比特币网站最新数据库以及网站源码在暗网被出售。源码售价为 0.5 个比特币，数据售价为 4 个比特币。其中源码内含接口 API 等信息，而数据涉及到 14 万会员的信息，包含用户的账号、密码、联系方式等，并且据卖家声称，这些数据均为原始数据库数据，而非整理后的数据。

近年来随着区块链的火热，很多黑产从业人员纷纷转向了区块链行业。此次该网站的数据以及网站源码在暗网被出售，背后的攻击者应该为一个团队而非个人。

二、 出行、酒店及餐饮行业在暗网的重大信息交易事件

（一） 问题综述

出行、酒店等行业是与我们日常息息相关的行业，而因实名制等相关政策以及行业本身的特性，这些行业的相关企业和机构往往拥有着非常详细的信息，如姓名、省份证号等，从而驱使着黑客或者内部人员去窃取相关的信息。在今年发生的几起相关行业的大型数据买卖事件中，数据的来源多为黑客攻击窃取。同互联网行业一样，因这些企业数据量大和日流量

高以及即时价值大等特点，黑客还公开在暗网出售相关企业的 shell 和内网权限。

（二） 疑似某官方火车票购买平台 3000 万条数据在暗网兜售

2018 年 6 月 13 日下午，网传有在暗网有人出售某官方火车票平台的 3000 万条相关数据。被泄露的数据包含手机号、密码、支付密码、姓名、身份证号码和验证答案等。传言这些信息在暗网以 10 个比特币的价格出售，而当时的比特币价格折合人民币超过 4 万元。

今年的 6 月份发生过多起大型企业数据在暗网出售的事件，且集中在 6 月 13 号左右。如，6 月 14 日招聘平台近 200 万用户数据在暗网被兜售，6 月 13 日，动漫网站近千名数据被爆在暗网出售长达 3 个月之久，同时被出售的还有疑似共享单车平台等公司的一手数据。除了出售用户数据，卖家还出售了相关 shell 和内网权限。

因多起事件发生的时间点非常的接近，很难判别这些数据是否为对应官方的一手数据，哪怕经过测试这些数据都是真实有效的，因为这些都可以在已有的数据上，经过撞库所得。

（三） 某酒店数据在暗网出售，涉及 1.3 亿用户开房记录

2018 年 8 月 28 日，某集团旗下多家连锁酒店的数据在中文暗网市场交易网站出售。卖家声称，这些数据涉及到多个知名酒店，共 1.3 亿人的个人信息以约五亿余条的开房记录。出售的数据包含三个部分，官网的注册资料，如：姓名、手机号、邮箱、身份证号和登录密码等；酒店入住时登记的登录信息，包含姓名、身份证、家庭住址、生日和内部 ID；酒店开房记录包含同房间关联号、姓名、卡号、手机号、邮箱、入住时间、离开时间等。

在卖家提供的附件中，包含了 10,000 余条的用于买家验证数据证实性的测试数据。经过验证这些数据大多都真实有效。并且据卖家透露，此次出售的数据库为 8 月 14 号拖库所得，以 5 个比特币或 520 个门罗币的价格打包出售。且卖家承诺只要权限不丢失，后续的数据可以免费提供给买家。

这次事件涉及到的数据量非常巨大，大致为史上之最。

三、 快递行业在暗网的重大数据交易事件

（一） 问题综述

快递相关行业因企业下属一般有很多代理商和临时工，快递信息一直都存在着很大的安全隐患。今年发生的两起重大快递行业相关信息买卖事件，涉及到的数据量均以亿为单位，如此可怕的数据量的数据，远非一个普通员工可以轻易得到的。实时上这两起事件中，有一起为几年前的数据，而另一起疑似为去年快递代理商和内部员工泄露。

值得注意的是，因快递信息的特殊性，哪怕多年前的数据，很多信息到今年依旧邮箱，尤其是姓名和家庭地址等。

（二） 某快递公司数 10 亿条数据在暗网以 1 个比特币的价格出售

2018 年 6 月 19 日，有人在暗网公开出售某快递公司近 10 亿条数据。这份数据并不是最新的数据，而是 2014 年以前的数据，被售卖的数据包含寄件人和收件人的姓名、电话、地址等快递必有的基本详细信息。卖家表示，这些信息已经做了去重处理，目前的重复率低于 20%，所有的数据打包后以一个比特币的价格出售。

（三） 某快递公司 3 亿用户的数据在暗网被兜售，仅售 2 个比特币

2018 年 7 月 18 日，某快递公司近 3 亿条信息在暗网以 2 个比特币的价格在暗网出售。这些数据为快递物流的详细信息，包含收寄件人的姓名、地址和电话等。据卖家透露这些数据均为一手数据，且可以在 3 亿条信息中随机抽取出 10 万条数据用于验货，但需要支付 0.01 个比特币。

虽然实际的验货数据只给出 6 万余条，但经过验证，这些信息基本上真实有效。在这名卖家出售该份涉及 3 亿条数据的 10 多天后，他曾再度发贴出售 2000w 条该公司在 2017 年泄露的数据。

有关证据表明，到目前为止，至少有近 3200 万条数据流入市场。

四、 医疗卫生机构在暗网的重大数据交易事件

（一） 新加坡 150 万公民医保资料以每份 35 元起步的价格在暗网出售

2018 年 7 月 27 日，新加坡近 150 万公民的医保资料遭泄露，并以每份 35 元起的价格在暗网出售。这些被出售的数据包含患者的姓名、国际、地址、性别、种族和出生日期等，而受害者甚至包括新加坡的总理李显龙。

近年来，医疗机构一直呈现着加速数字化的转变趋势，然而，相应的网络安全能力却依然很匮乏，因此被很多心怀不轨的攻击者盯上。而医疗相关的数据在暗网非常的受欢迎，一份资料一般以 35 元起步，这又不断的驱使着黑客去窃取医疗相关的数据。此次新加坡的事件绝不是孤立，在国内，某部委的医疗服务信息系统就曾遭到黑客入侵，大量孕检信息遭到泄露甚至是买卖。

五、 金融行业重大数据泄露事件交易事件

（一） 某金融网 30 万用户数据被挂暗网，以一个比特币的价格出售

今年 11 月份，一本财经的记者发现有人黑客盗取了汽车金融平台的后台权限，并在暗网公开出售该平台上的价值 30 万的用户数据。该被出售的数据共包含 65 个维度，如：身份证、银行卡、住址和电话等基本信息、工作单位、月薪、车型号和担保人手机号码等。这些数据被卖家以一个比特币的价格在暗网出售。