国盟信息安全通报

2019 年 4 月 15 日第 190 期

国盟信息安全通报

（第 190 期）

国际信息安全学习联盟

2019 年 4 月 15 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 180 个，其中高危漏洞 71 个、中危漏洞 78 个、低危漏洞 31 个。漏洞平均分值为 5.99。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 47%），其中互联网上出现“BigTreeCMS 'parent' SQL 注入漏洞、WordPress 插件 WordPress-Feed-Statistics 开放重定向漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1599 与上周（1960 个）环比下降 18%。

主要内容

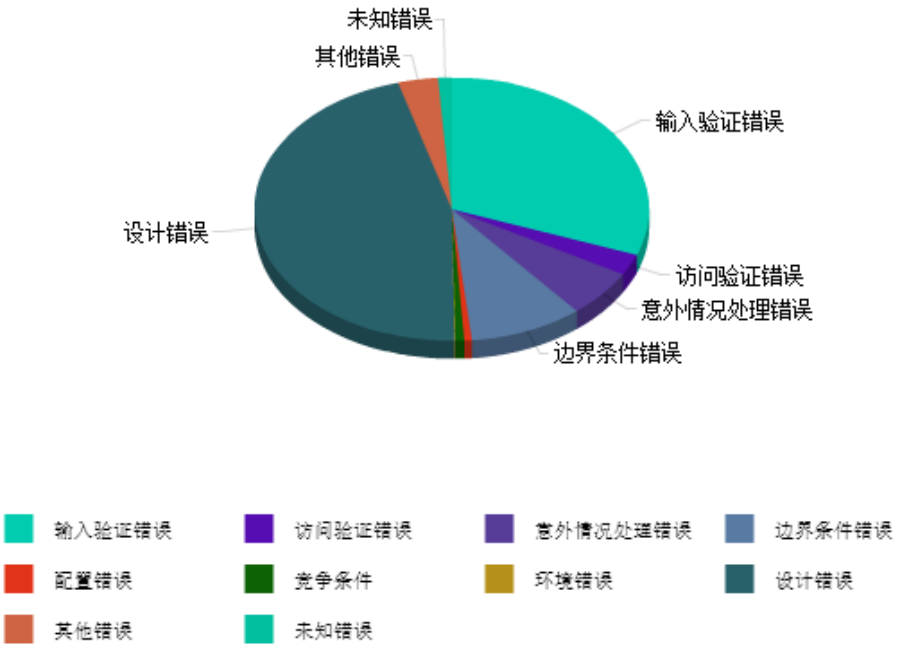
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

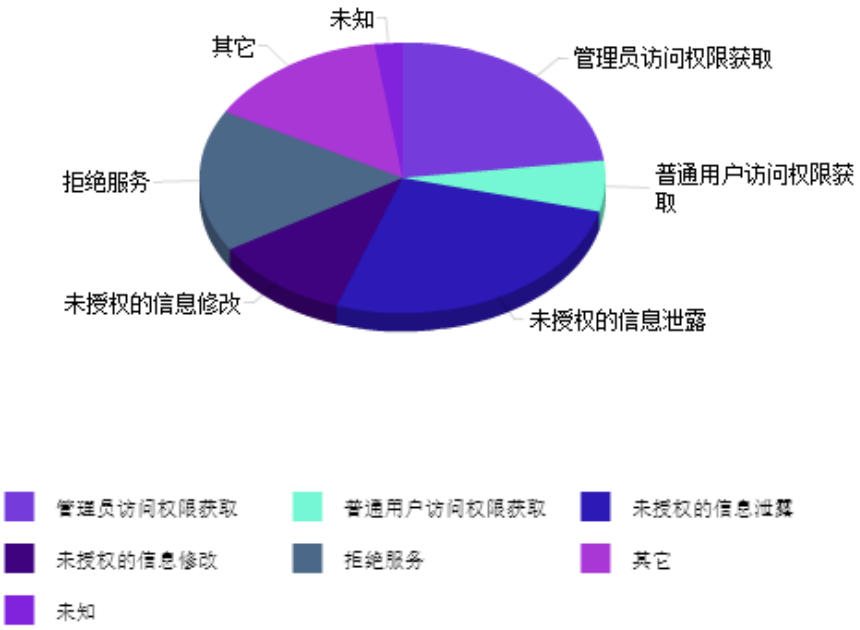
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 180 个，其中高危漏洞 71 个、中危漏洞 78 个、低危漏洞 31 个。漏洞平均分值为 5.99。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 47%），其中互联网上出现“BigTreeCMS 'parent' SQL 注入漏洞、WordPress 插件 WordPress-Feed-Statistics 开放重定向漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1599 与上周（1960 个）环比下降 18%。

二、安全漏洞增长数量及种类分布情况

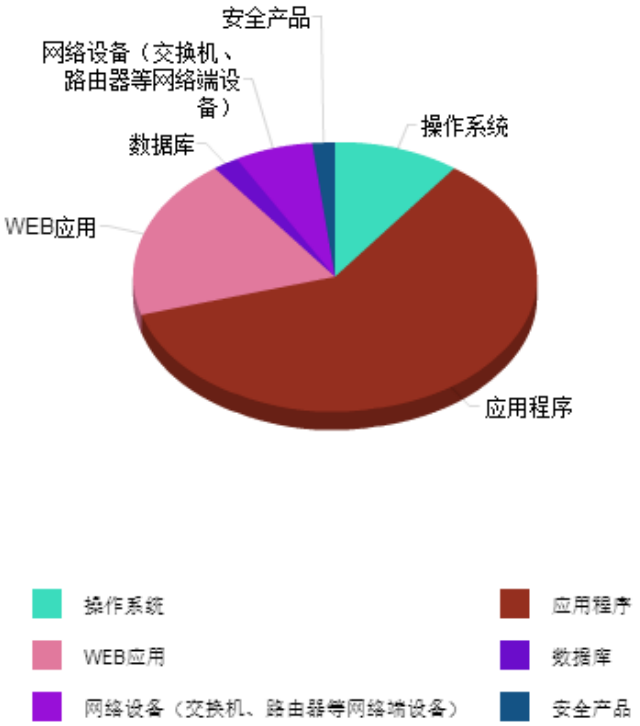
➢ 漏洞产生原因（2019 年 4 月 1 日—2019 年 4 月 15 日）



➢ 漏洞引发的威胁（2019 年 4 月 1 日—2019 年 4 月 15 日）



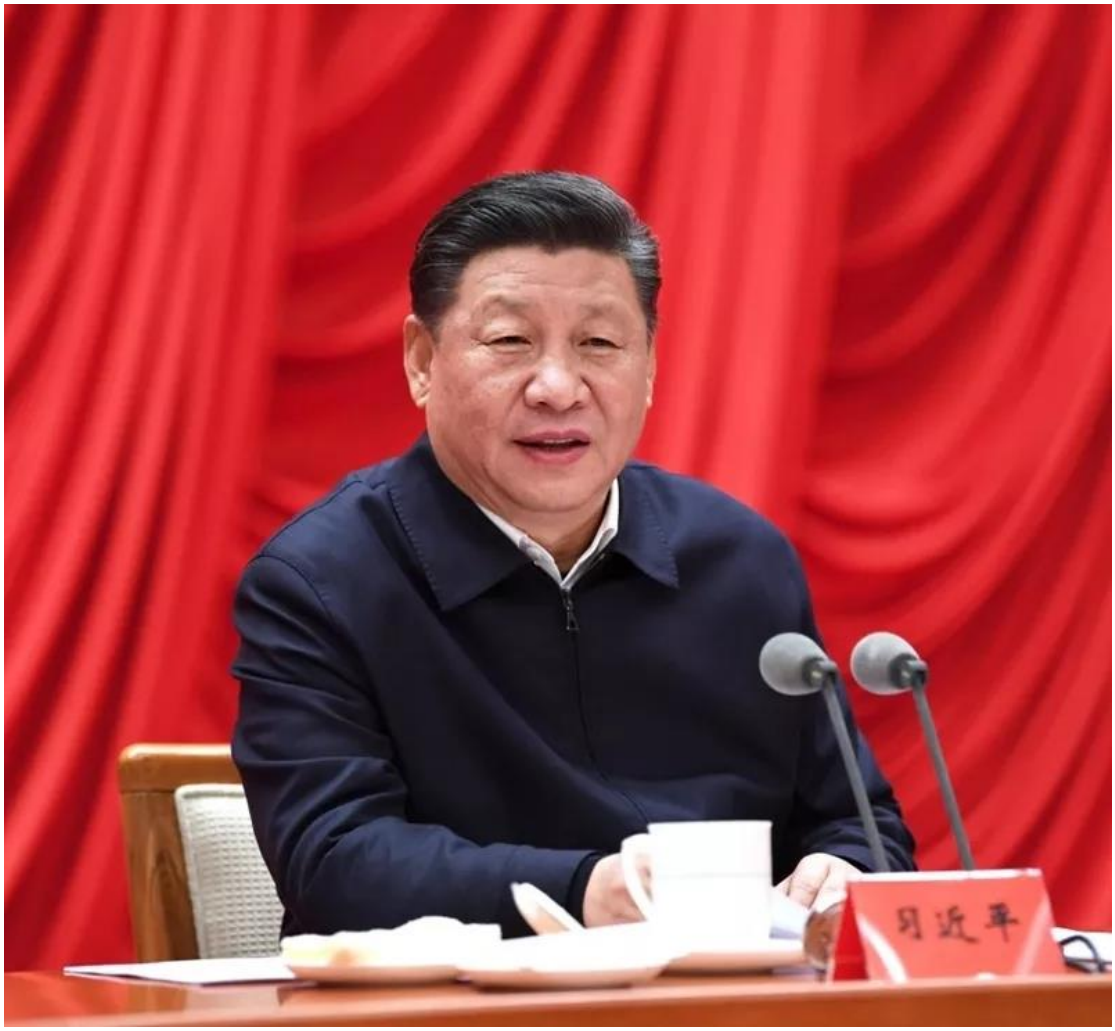
➢ 漏洞影响对象类型（2019 年 4 月 1 日—2019 年 4 月 15 日）



三、安全产业动态

➢ 提升网络意识形态领域风险防范化解能力

习近平总书记在省部级主要领导干部坚持底线思维着力防范化解重大风险专题研讨班开班式上的重要讲话，从维护总体国家安全的战略高度和全局视野，深刻分析了需要着力防范化解的各领域重大风险，对领导干部提出明确要求，强调要“深刻认识和准确把握外部环境的深刻变化和我国改革发展稳定面临的新情况新问题新挑战，坚持底线思维，增强忧患意识，提高防控能力，着力防范化解重大风险”。提升网络意识形态领域风险防范化解能力，是贯彻落实习近平总书记重要讲话精神、切实维护我国政治安全的重要举措。



1 月 21 日，省部级主要领导干部坚持底线思维着力防范化解重大风险专题研讨班在中央党校开班。中共中央总书记、国家主席、中央军委主席习近平在开班式上发表重要讲话。

一、提升网络意识形态领域风险防范化解能力，关乎国家安全

近年来，受网络信息技术突飞猛进式发展的影响，全球经济社会进入被互联网全面深度“渗透”的新阶段。据报道，截至 2018 年末，全球互联网用户规模已达 41 亿，互联网用户日均上网时长接近 7 小时。数据显示，我国以超 8 亿的网民规模和高达近 60%的互联网普及率强势“领跑”全球。互联网在渗透式影响全球经济社会发展和人类生产生活方式的同时，也在深刻改变全球传播秩序和国际舆论格局。在这个全球互联、技术赋能的时代，意识形态领域的斗争呈现出前所未有的复杂性：传统现实场域向网络虚拟场域的延伸，“线下战”与“线上战”的交织，“明争”向“暗斗”的转向，阶段化斗争向常态化斗争的转变……当前，互联网已成为世界各国竞相抢占的意识形态主战场，较之传统意识形态领域，安全风险发生的概率更大、能级更高。在互联网这个战场上能否顶得住、打得赢，直接关系我国意识形态安全和政权安全。因此，要从总体国家安全观的战略高度来审视提升网络意识形态领域风险防范化解能力的紧迫性和重要性。

我国积极推进基层融媒体中心建设，主动抢占网络意识形态斗争的战略制高点。图为浙江省湖州市长兴县融媒体中心。光明图片/视觉中国

二、提升网络意识形态领域风险防范化解能力，重在科学预判

防范化解重大风险重在“防”，要强化“治未病”的预防意识，加强对重大风险发生的及时预判。加强风险预判，首要在提高政治站位，时刻绷紧网络意识形态安全事关总体国家安全这根弦不放松，始终保持意识形态无小事的警惕心和警觉性，以高度的使命感和责任心守好网络空间主阵地。其次，要在提高前瞻性和预测力上下功夫，做到观大局、察大势，耳聪目明、心若明镜，准确把握网络意识形态领域风险发生的规律和特点，并紧跟大数据、人工智能等互联网信息技术发展前沿，持续加大对网络核心技术的自主研发，充分运用先进技术手段提升洞察网络意识形态领域风险的及时性、精准性，确保早发现、早预警、早行动。最后，还要加强科学研判，确保对网络意识形态领域潜在性、苗头性的风险有防范的先手，一经发现风险，即能够对其性质、特点、影响范围、危害程度等及时把脉、科学诊断、因“险”施“诊”，切实控制风险的发生频次和影响范围，努力将风险消灭在萌芽状态和早期阶段。

三、提升网络意识形态领域风险防范化解能力，重在有效治理

当前，互联网无疑是海量信息的第一集聚地和分发地，网民人数的持续攀升和网民群体结构的多样化也意味着网络空间还汇集着海量多元的民意。较之于传统舆论场，网络舆论场中的意识形态斗争形势更加纷繁复杂，更加暗流涌动，网络意识形态领域的风险防控难度更大。习近平总书记强调指出：“既要有防范风险的先手，也要有应对和化解风险挑战的高招。”因此，在严把网络意识形态领域风险预判关口、力求防患于未然的同时，还要做到有备无患，

加强应对，切实提高风险处置力。具体来说，一是要做到分而治之。面对网络意识形态领域多发、复杂的风险，要能够拨云见日、化繁为简，根据内容、性质、特点、影响等因素对网络意识形态领域出现的风险进行分类分级，找准引发风险的核心问题，再先后和分别采取有针对性、切中要害的处置措施。要注意合理区分境内外敌对势力挑衅攻击、错误社会思潮影响、民生问题和社会事件泛政治化等不同类型、不同程度的网络意识形态风险根源，有的放矢地破解难题，并在风险处置过程中切实避免简单问题复杂化、原则问题简单化。二是要做到依法治之。党的十九大报告明确提出，建立网络综合治理体系，营造清朗的网络空间。习近平总书记在省部级主要领导干部坚持底线思维着力防范化解重大风险专题研讨班开班式上也指出，加快建立网络综合治理体系，推进依法治网。防范化解网络意识形态领域风险是建立网络综合治理体系的重要组成，在风险处置的过程中必须牢固树立法治思维，坚持“管得住是硬道理”的工作理念和依法依规管网治网的工作原则，一方面要着力建立健全网络综合治理法律法规，加强总体指导；另一方面要针对网络意识形态领域风险防控研究出台更加专门化、细化和更加具有操作性的治理方案，切实提高网络意识形态领域的违法违规“成本”，探索建立多部门联动监管、联合执法等工作机制，加大惩治力度，以更好发挥直击要害的威慑作用。

四、提升网络意识形态领域风险防范化解能力，重在主动出击

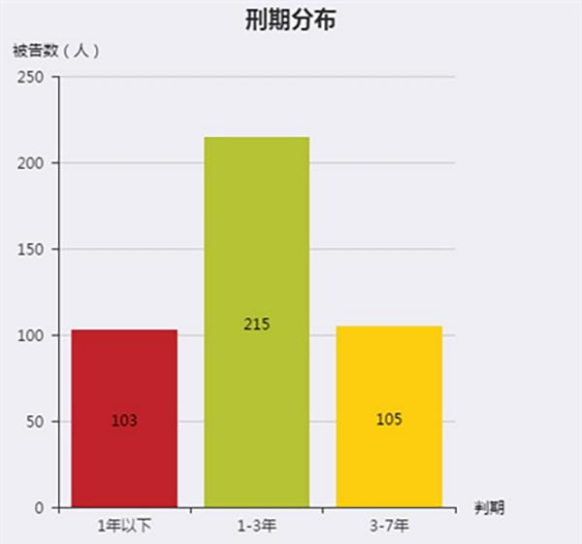
对网络意识形态领域风险做到科学预判、有效治理，是不打无准备之战，以防范和应对为主，从某种意义上讲更多属于防御战。要切实提升网络意识形态领域风险防范化解能力，还要打好习近平总书记所强调的“战略主动战”。打好战略主动战，一是要加强顶层战略规划。要善于总结防御战经验，深入分析网络意识形态领域各级各类风险的发生机理、演变规律和深层原因，追溯风险源头，将以往一个个相对零散、独立的应对处置措施加以整合，有效转化为指导主动作战的整体性战略指导方案。二是要积极抢占工作阵地。网络意识形态领域风险具有的多发性特点，与作为信息和思想舆论载体的网络媒介的持续快速迭代更新不无关系。就国内而言，从传统媒体到新媒体，网络意识形态的“战场”不断延伸、扩展、更迭，这就要求我们要紧跟技术发展前沿，坚持创新引领，主动抢占网络意识形态斗争的战略制高点，牢牢把握网络意识形态工作领导权，不断壮大网络意识形态工作阵地，做到网络意识形态领域风险防控多点联防、协同发力。三是要切实增强对象意识。人在哪里，意识形态争夺就在哪里，意识形态风险就会出现在哪里，风险防控的“战旗”就要插在哪里。打好网络意识形态领域风险防控战略主动战，颇为重要的是做到眼中有人、脑中有人、心中有人，要切实增强对作为网络意识形态争夺主体的互联网用户，特别是青年网民的思想和行为的深入研

究，尊重互联网用户特有的群体特征和个体特性，不断优化主流意识形态的内容建设和手段创新，切实提高网络意识形态工作的亲和力和可接受度，让主旋律为更多人传唱、唱得更加响亮，让正能量在更大范围内传播，在消解网络意识形态领域潜在风险等方面发挥更为深远的作用。（来源：光明日报）

➢ 是谁偷走你的个人信息？有“内鬼”也有“侦探”

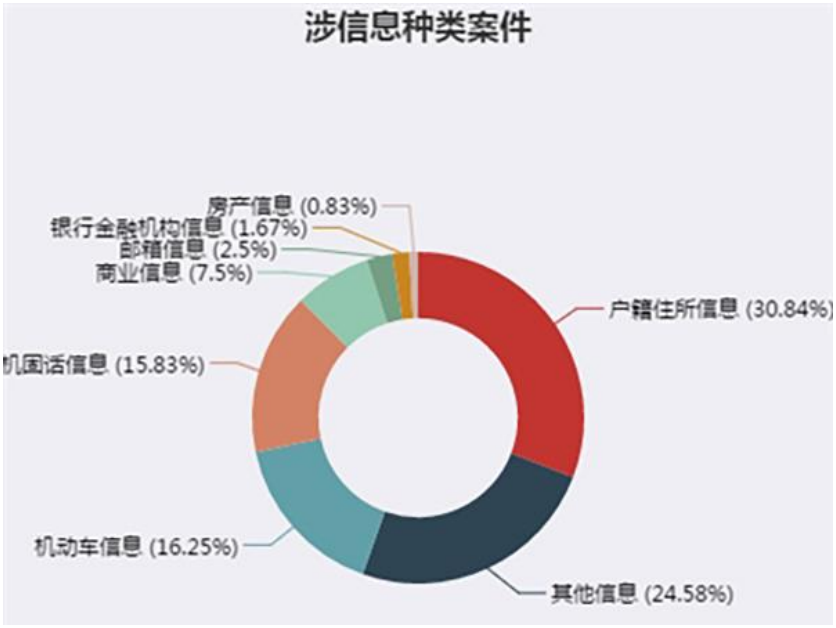
我家的智能机器人会不会一直在偷听我说话？当你看了央视今年“3·15”晚会——一些科技公司侵犯消费者隐私的事件曝光后，会不会用这样的眼光打量家里的扫地机器人、摄像头、指纹锁等智能家居？随着移动互联网与大数据时代的到来，骚扰电话、诈骗电话层出不穷，公民个人信息被泄露、个人隐私被侵犯等问题越来越受到社会关注。

记者对近年来浙江法院审理的侵犯公民个人信息案件进行调查后发现，此类案件上升趋势明显，2015 年，全省法院共受理此类案件 30 起，2016 年 36 起，2017 年 141 起，2018 年 198 起。**到底是谁偷走了你的个人信息？犯罪分子又把这些信息用于何处？**



你的哪些信息被盯上了？

从浙江法院 2018 年度侵犯个人信息罪数据看，公民户籍住所信息是不法分子的关注热点，占比 30.84%。其次是机动车信息、个人联系方式，分别占比 16.25%和 15.83%。电子邮箱信息、银行金融信息和房产信息等，也都榜上有名。



有些信息泄露会被人骚扰，有些信息泄漏就直接影响财产、人身安全了。在杭州市江干区人民法院审理的一起案件中，被告人林某非法获取他人信息用来牟利：通过编写程序破解证券公司客户的账户、密码，然后使用该账户原有市值申购新股。2017 年 1 月至 12 月，林某共非法获取三家证券公司的客户账户财产信息，共计 6609 条。

江干法院审理后认为，林某行为非法获取他人的证券账户信息达 6609 条，且可对掌握的相关账户进行实际操控，社会危害性极大，已构成侵犯公民个人信息罪，故对其判处有期徒刑三年三个月，并处罚金 2000 元。

更让人坐卧不安的是，你的定位信息等可能被 APP 软件“偷”走并被违法出售。被告人裴某，大学文化，是一家网络科技公司老板。2017 年 4 月，裴某伙同他人，通过网络发布推广“云上寻亲宝”应用软件，利用该软件可以获取他人位置信息的特点，吸引用户注册缴费并通过消费积分来获取被定位人的位置信息，从中牟利。

嘉兴市南湖区人民法院审理后认为，裴某违反国家有关规定，向他人出售公民个人信息，违法所得 6.7 万余元，情节特别严重，其行为已构成侵犯公民个人信息罪。

有“内鬼”也有“侦探”

从犯罪手段上看，198 起案件中，向他人索要购买信息的 67 起，利用职务便利窃取个人信息的 23 起，通过网站软件窃取 12 起。

分析被告人在履行职责或者提供服务过程中获取信息的案件，所涉信息主要是驾驶员身份信息、实时交通事故信息以及金融、电信、教育、订单等信息。

黄某是一家物流公司打单员，2017 年 1 月至 3 月，他利用职务便利，在公司电脑利用公司账户非法下载淘宝买家信息共计 111 万余条（内含淘宝买家姓名、电话及收货地址等信

息），并储存在其 QQ 微云内。之后多次出售，非法获利 3.5 万元。为扩大手中信息，黄某还用其中的 10 万余条淘宝买家信息与其他人交换了 13 万余条买家个人信息，最终被杭州市萧山区人民法院判处有期徒刑三年八个月，并处罚金 10 万元。

除了网络购买信息、利用计算机技术或者网络资源共享获取信息外，还包括跟踪、偷拍、监控等非法手段。2016 年 12 月，被告人马某和金某成立一家公司，专司调查业务。2016 年 12 月至 2017 年 8 月，该公司以调查公司、调查事务所等名义，以擅长“寻人寻址服务”“婚姻取证调查”“个人背景咨询”等业务吸引委托人签订调查服务合同，并由金某指派员工通过安装定位器非法定位、购买被调查人个人信息等方式，跟踪、盯梢、偷拍被调查对象及与其接触的关系人，非法拍摄公民个人活动视频片段 527 段，向委托人提供内含公民行踪轨迹信息的日常文字报告 28 份，出具调查工作总结报告 9 份，以及以购买、收受的方式非法获取公民住宿、住址、户籍、银行开户、宽带开户、车辆信息等公民个人信息 66 条，随后该公司将部分信息出售给相应委托人，违法所得共计 12.45 万元。最终，两人都被杭州市西湖区人民法院追究刑事责任。

将信息出售牟利的占绝大多数

在 2018 年 198 起侵犯个人信息犯罪案件中，出售并牟利的占绝大多数，有 125 起。但也有购买来用于业务推广和营销的，计 31 起。

2016 年 10 月，被告人蔡某、罗某合伙成立一家网络科技公司，主要运营模式是通过与某平台合作，对淘宝店产品进行推广，即向客户推荐合作的淘宝商家的优惠链接，客户如果通过优惠链接购买了商家的相关产品，公司便可以获得该平台提成。为此，该网络科技公司成立数据团队，与淘宝店家购买或者交换客户个人信息，非法获取 2000 余万条信息，获取了巨额收益。2018 年，两人被宁波市鄞州区人民法院追究刑事责任。

对于非法获取的个人信息，还有相当比例用于犯罪，在 198 起案件中有 39 起，其中，温州市龙湾区人民法院审理的一起案件比较典型。

2017 年 2 月至 5 月，被告人赵某从张某等人处购买大量的 iphone 设备 ID 账号和密码等数据，并雇佣其小舅子叶某帮忙操作。赵某伙同叶某利用购买的数据，登陆 iphone 官方网站，更改机主的 ID 密码并替换救援邮箱，再通过 icloud“查找我的 iphone”功能将苹果设备设置成丢失状态或抹除数据，致使机主的苹果设备无法正常使用。之后，赵某向被害人发送电子邮件，以解锁费用的名义索取财物，待被害人多次支付费用后才将苹果设备予以解锁。

经查，两人共远程锁定或抹除 iphone 设备 70 台，通过锁机行为向被害人索取解锁费用共计 2.1 万余元。

最终，被告人赵某因犯破坏计算机信息系统罪，被判处有期徒刑六年六个月；被告人张某犯侵犯公民个人信息罪，被判处有期徒刑三年二个月，并处罚金 8 万元。（来源：人民法院报）

➢ App 违法违规收集使用个人信息的分析与解读

目前，一些手机 App 越界获取隐私的问题愈发严重，例如，有的输入法 App、手电筒 App 要求位置权限；有的 App 在用户对 App 的权限请求默许的情况下，在后台记录用户的通话记录、短信、通讯录、位置信息、设备信息等，上传到服务器端；有的 App 开发者为了牟利，甚至将用户隐私出售或利用获取的权限推送广告获利。本文从 App 信息泄露形势、数据采集制度、如何保护隐私等方面进行分析和解读。

一、App 信息泄露形势严峻

信息泄露的危害不言而喻。如果个人信息、地址位置、身份、财产及银行卡信息等被不法分子掌握，轻则饱受广告推销烦恼，重则导致隐私泄露。而且，个人信息一旦被非法获取后，便会通过直接或间接的方式被出售给下游犯罪产业，导致犯罪团伙能够更“精准”地实施犯罪行为，包括但不限于广告推销、恶意营销、网络盗窃、电信诈骗、敲诈勒索、骗贷、洗钱、绑架等。

根据 2019 年 1 月腾讯发布的《2018 网络隐私及网络欺诈行为分析报告》，在被收集的样本中，100%的安卓手机 App 会不同程度获取手机隐私权限，90%发 iOS 手机 App 获取用户隐私权限。报告显示，新技术的发展也让隐私的外延进一步扩大，很多 App 都收集用户的

指纹、虹膜等生物信息。2018 年下半年，有 24.9%的安卓 App 已经通过用户使用身体传感器收集用户的生物信息。

此外，从安卓端恶意获取信息的手法看，恶意开发者已经从开发恶意 App 向开发恶意软件开发工具包（SDK）转移，恶意 SDK 开发者通过提供 SDK 给其他 App 使用，以达到快速传播的目的。同时，恶意 SDK 开发者通过使用代码分离和动态代码加载技术，可完全从云端控制 SDK 中实际执行的代码，具有很强的隐蔽性和对抗杀毒软件的能力。

近些年，个人信息保护已经获得政府及社会各界的高度关注，腾讯已经协助公安机关破获了多起涉及公民个人信息的案件。然而，对于侵犯公民信息的黑灰产治理还存在一些困难，一方面，不法分子行为难以察觉，例如，其沟通的方式更为隐蔽，跨平台作案，通过 A 渠道勾连，B 渠道传输信息，C 渠道交易资金，D 渠道贩卖，很难通过单方面的力量进行遏制，需要更多政府、企业联合起来共同对抗。另外，犯罪团伙的中上游为了逃避打击，开始逐渐转向在境外作案。另一方面，对于新兴的互联网数据是否属于公民个人信息在认定上，存在争议。

个人信息安全保护是一项长期而又艰巨的任务，无论是监管部门、企业和个人，都应积极采取各项措施维护用户的个人信息安全。2019 年 1 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，在全国范围内组织开展 App 违法违规收集使用个人信息专项治理行动，该专项治理行动将贯穿 2019 年全年。

二、现有数据采集制度的相关规定

通过 App 的数据泄露事件增多，更重要的原因是用户 App 隐私签署形同虚设，一是自动默认勾选为同意企业用户协议和隐私政策，二是不同意就不能使用 App，用户没有其他选择，三是在隐私条例里面设置霸王条款或者偷换概念的情况存在，以恶意规避法律责任。

2012 年的《全国人大常委会关于加强网络信息保护的决定》、2016 年的《中华人民共和国网络安全法》和 2018 年 5 月 1 日开始实施的 GB/T 35273-2017《信息安全技术 个人信息安全规范》（以下简称《规范》）共同建立了在非基于公共职权数据采集领域的以数据主体同意为唯一合法依据的个人数据采集制度。

其中，《全国人大常委会关于加强网络信息保护的决定》首次制定了我国个人数据保护“法律”层面的框架性规范，奠定了我国数据采集制度的基调，明确了数据控制者采集个人数据应当遵循合法、正当和必要的原则，应当向数据主体明示采集的目的、方式和范围，并征得数据主体的同意。

从上述法律法规可见，我国目前仅以告知同意作为数据采集的唯一合法依据。无论是何种情况下的数据采集行为，都必须经过数据主体的同意，否则将被视为非法采集相关数据。

我国在法律层面并未予以明确规定“同意的方式”，但是，根据 2012 年 11 月，原国家质量监督检验检疫总局和国家标准化管理委员会联合发布的我国首个个人信息保护国家标准 GB/Z 28828-2012《信息安全技术 公共及商用服务信息系统个人信息保护指南》，我国在同意的方式上并未强调必须明示同意，在一定程度上同样接受默示同意的方式。

《规范》阐明了个人信息安全保护领域的诸多重要问题。例如，《规范》中定义个人信息为电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，即可被用于识别自然人（数据主体），或者与识别个人相关用于影响个人的信息（且不包括匿名化数据，但是，匿名化数据有可能被用于重新识别或影响该个人，则应属于个人数据）。《规范》规定了个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节的相关行为。这些对于遏制个人信息非法收集、滥用、泄露等乱象，最大程度保障个人的合法权益和社会公共利益，起到积极的作用。

《规范》不仅规范了数据收集企业、组织的行为，保障了个人的信息权益，还为有关机关提供了判断企业是否违反《网络安全法》甚至构成刑事犯罪的依据。在个人信息收集这一重要环节，《规范》严格界定了个人信息控制者的权利并明确了其义务，规定在收集个人信息前，应当向信息主体明示相关内容并取得同意；涉及间接获取方式以及个人敏感信息时，应当做出必要说明或取得明示同意且遵守有关法律、行政法规关于个人信息保护的规定。

在信息收集方面，《规范》就个人信息控制者的义务提出了以下几点意见：首先，合法性。要求个人信息控制者在法律法规规定的范围内采用合法的手段和获取信息的渠道，在征得个人信息主体同意的前提下收集个人信息或要求信息主体提供个人信息。其次，最小化。

要求个人信息的收集类型、频率和数量应在必要性的最小要求之内，即符合最少够用原则。不仅要求信息收集者在最小范围内收集个人信息，而且尽量保证信息收集者至少能够实现其收集的目的，“收集和处理个人信息的行为与目的相关且适当：在行使信息形成权和为公众带来的负担之间平衡”。最后，授权同意。要求个人信息控制者处理个人信息时的目的、方式、范围以及相关规则，均要经过个人信息主体的授权同意。事实上，这一要求贯穿《规范》勾勒的个人信息处理全链条，也涵盖对个人信息的保存、使用以及委托处理、共享、转让、公开披露等。

对于个人敏感信息，《规范》根据敏感程度的不同，考虑到敏感度较高的个人信息的收集与提供对个人信息主体带来的不同范围的利害影响，要求个人信息控制者要在个人信息主体完全知情的基础上给出自愿的、具体的、清晰明确的同意的意思表示。同时，若涉及产品或服务的核心功能以及附加功能，应明确告知个人信息主体对此享有的同意与拒绝提供或被收集信息的权利以及由此带来的不利影响。

值得注意的是，《规范》加强了个人信息主体对其个人信息的控制权，在个人信息主体明确表示同意的前提下，才可以进行相关的个人信息处理活动。其要求个人信息控制者制定相关的隐私政策，说明其自身的基本情况，并对收集行为做出目的性解释。在后续的共享、转让、公开披露等环节，需要提供行为目的、被处理的信息类型乃至与此相关的第三方主体、涉及的法律责任等情况说明。在隐私政策的相关内容中，特别强调个人信息主体的权利实现机制，隐私政策的发布方式要以最基本的法律法规以及相关规范作为基准，以真实易懂的信息内容，采取公开发布或易于访问的方式逐一送达或公告送达相关个人信息主体。

针对个人信息的保存问题，《规范》确定了个人信息保存时间最小化与个人信息去标识化处理标准，采取技术措施处理敏感性较高的信息，与信息控制者停止运营后也应停止继续收集的行为。“以逐一送达或公告的形式通知个人信息主体，并对已经收集到的个人信息进行删除或匿名化处理：时间最小化，要求信息的保存时间应与使用目的保持程度上的一致，应满足一定的必要性，在超过保存期限后，即应对信息作出删除或匿名化处理；去标识化处理，是对信息主体的技术性保护，要求将收集到的信息去除识别性特征，并避免该数据二次复原重新识别，妥善地保管信息控制者收集到的各类数据”。

三、亟需各方协同保护个人隐私

用户作为隐私信息的源头和最终受害者，需要加强网络安全意识和知识，了解隐私保护手段。用户可以参考以下手机隐私安全保护措施：1.下载：尽量选择官方渠道，特别是投资理财、银行类 App，不要下载来历不明的山寨 App；2.授予权限：谨慎授予 App“发送短信”

“读取短信”“读取联系人”“读取位置信息”等权限；3.流量使用：观察 App 流量使用情况，对一些使用大量流量且没有告知的 App，及时检查和删除；4.自动登录：不要把手机中的 App 设置为“自动登录”，密码最好定期更换；5.退出不彻底：不再使用 App 时应彻底退出，如果退出不彻底会给后台运行的恶意程序以可乘之机；6.自启动：某些 App 即使用户没有打开过，也会自己启动常驻后台，最好想办法关闭其自启动功能。如果仍然自启动，则建议卸载；7.安全软件：安装手机管家等安全软件，保障设备安全。

对于新型通过恶意 SDK 获取用户个人隐私的情况，建议 SDK 开发者、应用开发者和应用市场做到：1.SDK 开发者避免使用云控、热补丁等动态代码加载技术；2.应用开发者在集成使用第三方提供的 SDK 时要谨慎连接具有动态更新能力的 SDK；3.应用市场要加强管理，增强对恶意应用和恶意 SDK 的识别能力。

对于互联网企业来说，用户个人信息和数据安全关系用户权利与企业生存，企业应严格遵循《网络安全法》确立的收集、使用个人信息合法、正当、必要的三原则。收集的信息仅用于为给用户提供必要而良好服务，保障用户知情权，给予用户选择权，以严格的标准保护数据存储的安全性，防止数据泄露与不当使用，尊重用户对个人信息的合法权利。

从技术层面讲，没有什么是绝对安全的。每个应用在互联网服务中，都涉及数据库、服务器、网络运营商、软件客户端、用户终端（PC/Pad/手机），每个环节或参与者，都有可能被攻击导致个人隐私数据泄露。企业能做的是通过不断地完善保护策略，增加黑客窃取信息的难度，降低个人隐私泄露的风险。例如，根据不同的数据库分散管理员权限，数据库的访问权限应该只开放给对应局域网的服务器使用，禁止连接公网，并且修改数据库的默认密码及要求设置密码的复杂度。再如，提升黑客撞库攻击的难度；部署通向服务器的防火墙，对连接数、端口、协议做统一的规范和部署等。（来源：《中国信息安全》杂志 2019 年第 3 期）

➢ 数据跨境流动的风险与隐忧

上世纪 80 年代，经济合作与发展组织（Organization for Economic Co-operation and Development，OECD）将数据跨境流动定义为个人数据跨国界的传输。然而，随着世界多极化、经济全球化和社会信息化的大潮到来，全球经贸交易、技术交流、资源分享等跨国合作日益频繁，商品流、人员流、数据流不断涌动，数据跨境流动已不仅限于个人数据。

当前，对数据跨境流动的普遍理解是数据跨越国界的传输、访问或处理。数据有序跨境流动，有利于全球数据资源的开发利用和开放共享，有利于信息化产品和服务跨境运营和商业拓展，有利于推动信息网络技术、产品和服务的创新发展，进一步提升经济效率和社会福祉。如何辨识和管理数据跨境流动中的潜在风险，逐渐成为新时代数字经济发展与治理的关键环节。

整体看，数据跨境流动风险与隐忧主要集中于数据的传输、存储和应用三个环节。传输上，数据跨境过程环节多、路径广、溯源难，传输过程中可能被中断，数据也面临被截获、篡改、伪造等风险；存储上，受限于数据跨域存储当地的防护水平等因素，容易出现数据泄露等问题；应用上，跨境数据的承载介质多样、呈现形态各异、应用广泛，数据所在国政策和法律存在差异、甚至冲突，导致数据所有和使用者权限模糊，数据应用开发存在数据被滥用和数据合规等风险。

数据跨境流动涉及个人、企业和国家，影响重大，具体来看：

第一，数据跨境流动可能会引发用户数据易被泄露、滥用等问题。个人数据跨境流动中，可能出现经由移动设备的 GPS 等定位服务跟踪用户行踪的情况，甚至通过蜂窝基站、Wi-Fi、热点、蓝牙、麦克风、摄像头等设备收集未经授权的离线数据，还可能利用应用程序的访问权限漏洞擅自收集用户数据。这些数据包括用户个人信息、银行卡、信用卡、购物历史和网上访问记录等隐私，若被不法分子泄露或滥用，会给用户带来经济损失甚至人身伤害。如近期，亚洲某厂商被爆出利用境外销售的手机，收集用户信息并传送到合作伙伴服务器上共享。如果该服务器遭到黑客入侵，泄露的敏感数据落入不法分子之手，将成为电信网络诈骗“精准投放”的信息来源。

第二，数据跨境流动可能会给企业带来技术管理、资产管理和组织管理上的问题。技术管理上，跨国企业使用境外数据中心或云平台，由于大量数据向这些平台汇集，易成为黑客攻击的目标。如黑客通过恶意入侵云平台，常驻用户网络，长期进行盗取、篡改数据等活动。资产管理上，受到数据所在国政策、法律等限制，跨国企业的境外分支机构存在商业信息被披露的风险。如有跨国会计师事务所被境外证监会起诉、要求提供审计底稿等文件配合相关调查。组织管理上，跨国企业利用境外政策和制度上的漏洞发展灰色业务，给行业管理带来新挑战。例如，企业通过线上载体扩展境外线下灰色业务，来规避跨境业务的准入政策。

第三，海量数据跨境流动会使他国更容易分析挖掘国家重要战略信息。全球网络互联、信息互通，国际经贸、技术等多领域合作使跨境服务和数据流动日益频繁，数据留存境外时间更长、体量更大、涉及范围更广。这些数据经分析处理，能反映国家相关行业和领域的情况，例如，可通过海量手机位置反向绘制出移动通信基站分布图，再如，根据跨国电商的订单等相关数据推测用户群体的消费情况以及对应行业的宏观经济运行情况。当前，大数据已成为决定未来发展潜力的战略性资产，各方对数据跨境流动、海量采集和控制挖掘都高度重视。美国主张全球数据自由流动，意图通过遍布世界各地的美属企业分支机构，利用其信息通信技术、产业、政策上的优势，占领数据主权的制高点。欧盟设定了《通用数据保护条例》《非个人数据自由流动框架条例》等高标准的数据保护条例，在全球大力推广欧盟标准，通过延伸数据控制者在数据跨境流动中的权利范畴，最大程度上维护欧盟企业的权益。

随着数据价值与安全风险凸显，数据跨境流动安全和管理，已成为各国学术科研和政府管理共同关注的焦点。这就需要我们在保证跨境数据合法性、正当性、必要性的前提下，一方面，要加快推动数据存储、传输和分析等技术研发，提升数据防护水平，实现数据跨境流动全环节安全，即数据系统攻进不去，数据传输切不断，数据资产窃不走、数据滥用行为赖不掉；另一方面，要建立健全行业数据分级分类制度，加强数据出境的使用规范和安全保障，推动制定数据跨境流动的国际管理规则，通过经济、法律、技术、管理、国际规则等多种手段，建立健全数据跨境取证、域外管辖等的国际协调机制。（来源：中国信息通信研究院）

四、政府之声

➢ 国家广电总局发布《未成年人节目管理规定》

2019 年 4 月 3 日，国家广播电视总局颁布第 3 号令：《未成年人节目管理规定》，要求不得制作、传播利用未成年人或者未成年人角色进行商业宣传的非广告类节目。邀请未成年人参与节目制作，其服饰、表演应当符合未成年人年龄特征和时代特点，不得诱导未成年人谈论名利、情爱等话题。未成年人节目不得宣扬童星效应或者包装、炒作明星子女。

此次规定按照“网上网下统一标准”的要求，规范调整的未成年人节目包括未成年人作为主要参与者或者以未成年人为主要接收对象的广播电视节目和网络视听节目，短视频和直播平台也在其中。

本次国家广播电视总局颁布的第 3 号令《未成年人节目管理规定》已在 2019 年 2 月 14 日国家广播电视总局局务会议通过审议，并将于 2019 年 4 月 30 日全面实施。

当下短视频和直播平台的迅猛发展，大批主播及平台唯流量论，存在着大量对未成年人进行各类炒作包装的现象。如“全网最小二胎妈妈”，自称 17 岁的炫富红人温婉等，以及通过包装未成年人成为小模特小童星，获取商业利益，这些行为都极大地悖逆了未成年人身心健康发展的规律，严重破坏网络和社会风气。相信随着新规的发布和实施，侵犯未成年人合法权益的现象，以及一些未成年人“商业化、成人化和过度娱乐化”的现象都将被列入监管和处罚的范畴，网络未成年人内容乱象将得到有效遏制。

同时随着“全国网络节目主持人职业素养能力培训”等专业培训项目的开展，互联网平台的运营管理、网络主播的综合素质都将得到有效提升。（来源：国家广播电视总局）

- **国家广播电视总局《未成年人节目管理规定》**
- **全文：**http://www.gov.cn/xinwen/2019-04/06/content_5380015.htm

➢ 国家市场监管总局开展“守护消费”行动打击侵害消费者个人信息违法行为

2019 年 3 月 29 日，国家市场监管总局办公厅印发《市场监管总局办公厅关于开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动的通知》，通知决定于 4 月 1 日至 9 月 30 日，在全国范围内部署开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动，重点打击侵害消费者个人信息违法行为。

在日常生活中，消费者经常会遇到买房没多久接到装修、家具商家的电话、短信，或者买车后接到推销车险的电话，特别是每年保险快到期的时候，会被不同保险公司反复骚扰。市场监管总局执法稽查局相关负责人表示，这些现象的背后其实是消费者个人信息被泄露，不仅威胁消费者的人身财产安全，也影响经济社会的健康发展。为了更好地保护消费者合法权益，营造安全放心消费环境，市场监管总局决定组织开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动。本次行动重点关注违法行为多发的房产租售、小贷金融、教育培训、保险经纪、美容健身、装饰装修、旅游住宿、快递、电话营销、网站或 APP 运营等行业和领域。本次行动主要查处 3 类违法行为：一是未经消费者同意，收集、使用消费者个人信息;二是泄露、出售或者非法向他人提供所收集的消费者个人信息;三是未经消费者同意或者请求，或者消费者明确表示拒绝的，向其发送商业性信息。

据悉，本次行动依照《消费者权益保护法》《电子商务法》《网络安全法》《侵害消费者权益行为处罚办法》等法律法规的相关规定，主要从 3 个方面开展工作：一是深挖案件线索，通过畅通投诉渠道、关注舆情动态、充分运用大数据等，收集案件线索;二是加强执法联动，在扎实推进案件查办的同时，做好统筹协调，及时通报信息、互相支持配合、开展联合行动，加强行政与司法衔接;三是广泛开展宣传，宣传行动成果、典型案件以及消费者个人信息保护相关的法律法规和消费知识，提高经营者守法经营意识，树立保护消费者个人信息的理念，并教育和引导消费者主动保护个人信息。（来源：国家市场监管总局）

- **市场监管总局办公厅关于开展“守护消费”暨打击侵害消费者个人信息违法行为专项执**

法行动的通知

- 全文：http://www.samr.gov.cn/zfjcj/tzgg/201903/t20190329_292443.html

➢ 国家版权局：图片版权保护将纳入“剑网 2019”专项行动

2018 年 4 月 12 日电 12 日上午，国家版权局发布公告称，国家版权局将把图片版权保护纳入即将开展的“剑网 2019”专项行动，进一步规范图片市场版权秩序。近日，“黑洞图片”版权问题引发关注。国家版权局称，重视图片版权保护，依法维护著作权人合法权益。各图片公司要健全版权管理机制，规范版权运营，合法合理维权，不得滥用权利。（来源：国家版权局）

➢ 国家网信办持续推进 APP 乱象专项整治关停清理违法 APP3 万余个

2019 年 4 月 12 日，国家网信办报道：2018 年 12 月以来，国家网信办会同有关部门，针对涉黄涉赌、恶意程序、违规游戏、不良学习类移动 APP 开展专项整治行动，关停下架违法违规 APP 33638 款，拦截恶意网站链接 234 万余个，社交平台清理低俗不良信息 2474 万余条、封禁违规账号 364 万余个，APP 乱象得到有效遏制，网络生态持续向好。

国家网信办会同相关部门对违法违规 APP 开展全环节全链条治理。在入口环节，约谈有关云基础设施提供者，要求全面开展自查自纠，屏蔽恶意链接，清查接入服务。在分发环节，集体约谈 20 家主要应用商店相关负责人，责成企业认真履行主体责任，完善应用程序上架审核流程，提升安全检测技术能力，及时清理违法违规移动应用程序。在传播环节，督促微信、QQ、微博、论坛、贴吧等主要社交平台加强管理力量，针对群组传播特点，强化对群组中的站外链接、二维码的审核力度。

有关负责人表示，国家网信办将进一步加强与行业主管部门之间协同配合，共同压实网络接入服务商、应用分发平台、社交平台的企业主体责任，切断违法违规 APP 传播链条，构建全环节管理的综合治理模式，持续深入推进违法违规 APP 乱象专项治理工作，营造正能量充沛、风清气正的网络空间。（来源：国家网信办）

五、本期重要漏洞实例

➢ Adobe Flash Player 越界读取信息泄露漏洞

发布日期：2019-04-09
更新日期：2019-04-09
受影响系统：
Adobe Flash Player < 32.0.0.171
描述：

BUGTRAQ ID: 107814
CVE(CAN) ID: CVE-2019-7108
Adobe Flash Player 含有一个信息泄露漏洞。
利用这个漏洞，攻击者可以获取可能导致进一步攻击的敏感信息。
Adobe Flash Player 32.0.0.171 之前的版本都收到影响。

<*链接：https://helpx.adobe.com/security/products/flash-player/apsb19-19.html
*>

建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB19-19）以及相应补丁:
APSB19-19：Updates available for Adobe Flash Player | APSB19-19
链接：https://helpx.adobe.com/security/products/flash-player/apsb19-19.html
补丁下载：
Adobe Flash Player Desktop Runtime （Windows 和 MAC）
https://get.adobe.com/flashplayer/
https://www.adobe.com/products/players/flash-player-distribution.html

Adobe Flash Player for Google Chrome （Windows, macOS, Linux, 和 Chrome OS ）
https://chromereleases.googleblog.com/

Adobe Flash Player for Microsoft Edge and Internet Explorer 11 （Windows 10 和 8.1）
https://portal.msrc.microsoft.com/en-US/security-guidance

Adobe Flash Player Desktop Runtime （Linux）
https://get.adobe.com/flashplayer/

➢ D-Link DSL-3782 跨站脚本漏洞

发布日期：2019-04-01
更新日期：2019-04-03
受影响系统：
D-Link DSL-3782 EU 1.01
描述：

CVE(CAN) ID: CVE-2018-17989

D-Link DSL-3782 是一款无线路由器。
D-Link DSL-3782 设备(1.01 版本固件)，在 Web 界面中存在跨站脚本漏洞，成功利用后可使攻击者在 ACL 页中注入 JS 或 HTML 负载，请求"/cgi-bin/New_GUI/Acl.asp"时，利用该漏洞在用户浏览器中执行代码。

<*来源：vendor
*>

建议：

厂商补丁：

D-Link

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：https://c0mix.github.io/2019/D-Link-DIR-3782-SecAdvisory-OS-Command-Injection-and-Stored-XSS/

➢ WordPress W3 Total Cache 插件信息泄露安全漏洞

发布日期：2019-04-01
更新日期：2019-04-03
受影响系统：
WordPress W3 Total Cache < 0.9.4
描述：

CVE(CAN) ID: CVE-2019-6715

WordPress 是一套使用 PHP 语言开发的博客平台。W3 Total Cache plugin 是使用在其中的一个 SEO（搜索引擎优化）插件。
WordPress W3 Total Cache 插件 0.9.4 之前版本，pub/sns.php 文件存在任意文件读取漏洞，可使远程攻击者通过 SubscribeURL 字段，读取任意文件。

<*来源：vendor
*>

建议：

厂商补丁：
WordPress

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://wordpress.org/plugins/w3-total-cache/#developers

➢ IBM InfoSphere Information Server 信息泄露漏洞

发布日期：2019-03-30
更新日期：2019-04-02
受影响系统：
IBM InfoSphere Information Server 11.7
IBM InfoSphere Information Server 11.5
IBM InfoSphere Information Server 11.3
IBM InfoSphere Information Server on Cloud 11.7
IBM InfoSphere Information Server on Cloud 11.5
描述：

CVE(CAN) ID: CVE-2018-1917

IBM InfoSphere Information Server 是一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。

IBM InfoSphere Information Server 在配置实现中存在信息泄露漏洞，攻击者可利用漏洞访问 JSP 文件，获取受影响组件敏感信息。

<*来源：IBM （ncsupp@ca.ibm.com）
*>

建议：

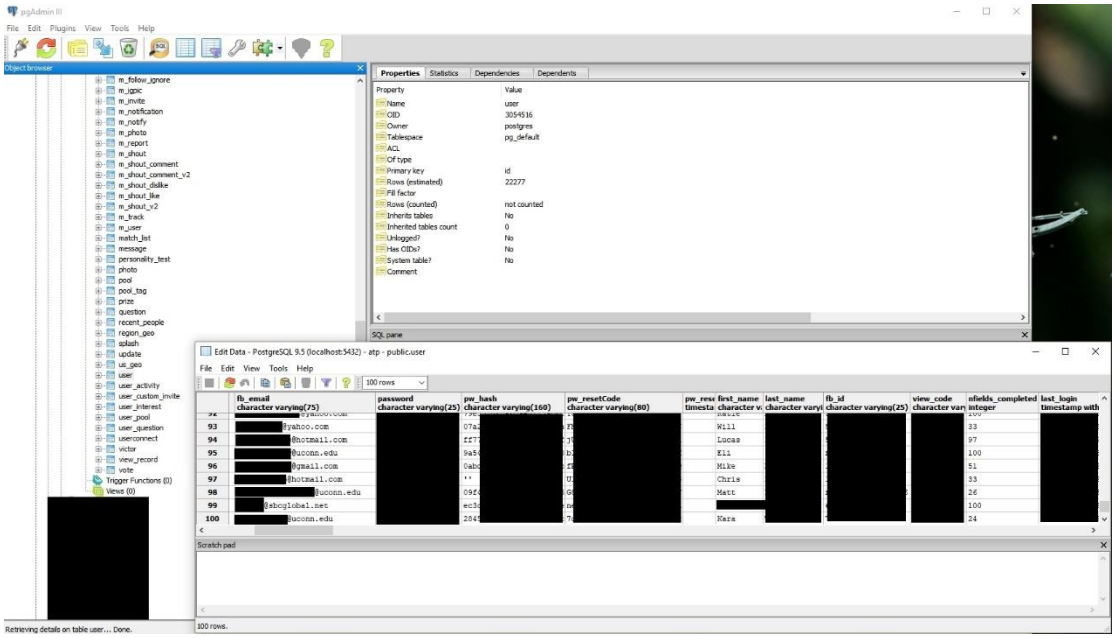
厂商补丁：
IBM

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://www-01.ibm.com/support/docview.wss?uid=ibm10872274

六、本期网络安全事件

➢ 亚马逊云服务器泄露上百万份用户资料脸书背锅

2019 年 4 月 4 日，据彭博社报道，来自 UpGuard 的研究人员发现在亚马逊的公共云服务器上竟然可以访问数百万用户的脸书记录，据称数据是由与 Facebook 合作的第三方公司上传至该服务器的。惹祸的是一款名为 At the Pool 的应用（已失效），错误地将 22000 名 Facebook 用户的敏感数据（比如姓名和邮件地址）分享出去。



虽然 Facebook 本身没有泄露数据，但确实是该公司将这些数据提供给了第三方公司，而后者却未能妥善保管这些数据，因此 Facebook 也有不可推卸的缺乏监管的责任。

UpGuard 的网络风险调查总监 Chris Vickery 表示，“公众还没有意识到这些保管数据的高级系统管理人员、开发人员有多么失职，他们要么缺乏风险意识、要么消极怠工，对大数据的安全方面缺少足够的关注。”

作为对 UpGuard 的发现的回应，Facebook 的发言人通过彭博社表示，该公司目前的政策是严禁将 Facebook 的信息存储在公共数据库中，显然 Facebook 在这方面缺少监管。被 UpGuard 发现后，Facebook 已经与亚马逊合作撤下了那些数据库。（来源：MacX）

➢ 丰田汽车服务器再遭黑客入侵 310 万名用户信息存忧

2019 年 4 月 1 日，据美国科技媒体 ZDNet 报道，丰田汽车今日公布了第二起数据泄露事件，这也是该公司在过去五周内承认的第二起网络安全事件。第一起安全事件发生在其澳大利亚子公司，而今日公布的第二起事件发生在丰田汽车的日本主办事处。

丰田汽车表示，黑客入侵了其 IT 系统，并访问了几家销售子公司的数据。这些子公司包括丰田东京销售控股公司、东京汽车、东京丰田、丰田东京卡罗拉、丰田东京销售网络、雷克萨斯 Koishikawa Sales 公司、Jamil Shoji（雷克萨斯 Nerima）和丰田西东京卡罗拉。

该公司表示，黑客访问的服务器存储了多达 310 万名客户的销售信息。丰田汽车称，目前正在调查此事，以确定黑客是否泄露了他们可以访问的任何数据。

丰田汽车强调，客户的财务细节并未存储在被黑客攻击的服务器上。至于黑客可能访问了哪些类型的数据，丰田汽车并未披露。

丰田汽车发言人今日向媒体表示：“我们向所有使用丰田和雷克萨斯汽车的客户表示歉意。我们认真对待这一问题，并将在经销商和整个丰田集团中彻底实施信息安全措施。”

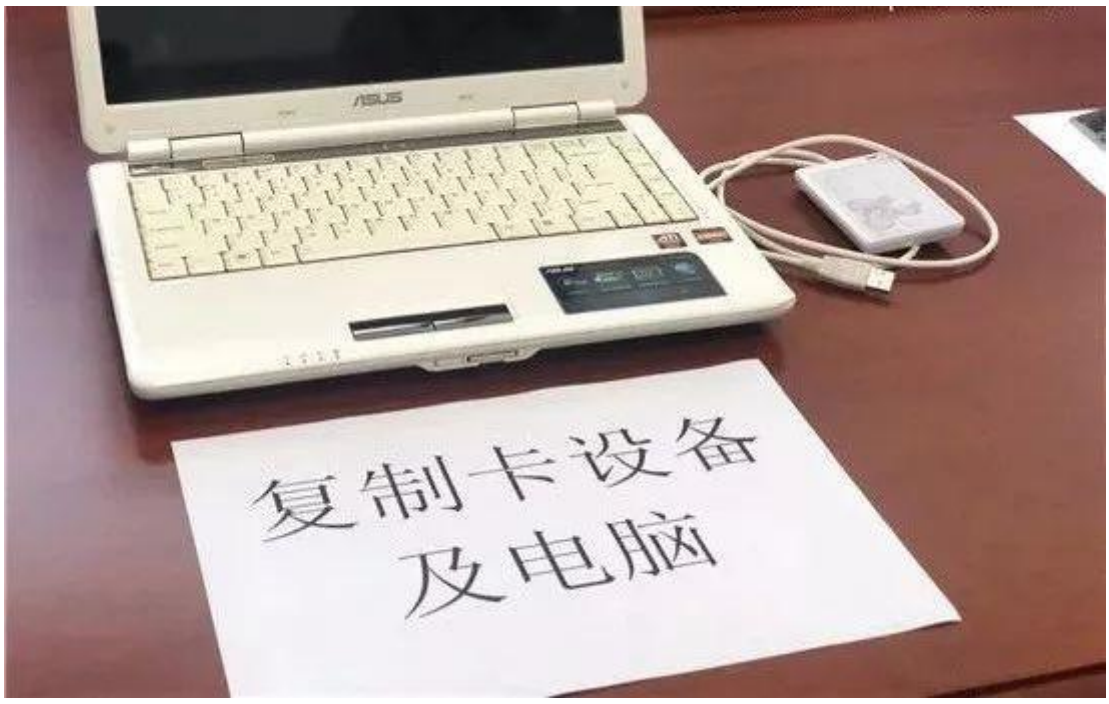
这已是该公司今年宣布的第二起网络安全事件。2 月底，丰田汽车曾披露了一起类似的事件，影响其澳大利亚分公司。

而在丰田日本公布数据泄露事件的同时，丰田位于越南的子公司也发生类似事故，但目前没有细节公布，也不能确定其与丰田日本的事故是否有关。（来源：新浪科技）

➢ 大学生自学复制假饭卡:2 个月销售 3 千张获利 10 万元被抓!

随着社会的进步,网络的普及,人们在越来越多地享受高科技给社会带来财富和好处的同时,利用高科技手段进行高智能犯罪活动也越来越多,令人深思的是大学生高智能犯罪成逐年上升的趋势。然而，一些被人们视为高智商、高素质、高层次的大学生却因触犯刑律而银铛当入狱，断送了自己的美好前程。

2019 年 4 月 7 日据微辣 Video 消息：山东淄博在校一大学生刘某，在网上无意之间从某软件上看到了一则复制饭卡的“技术贴”。便想自己制作饭卡，不久就来到这家非法贩卖读卡器的网店。花费 1500 元购买了一台复制饭卡的设备，经过多次失败后最终学会了复制饭卡。



最初，刘某只是想要把复制的饭卡拿来自己用，可能觉得复制饭卡也需要本钱于是便想着把复制来的饭卡用以售卖从中获取利益。他在陆续收到“利益”后，便开始膨胀起来。由于他卖的饭卡便宜。所以购买的同学也很多。为了从中谋取更多的利益，他在自己学校寻找同伙发展“业务”，很快就扩展到了别的学校，他开始去其他学校办饭卡。很快刘某就复制了山东十多所学校的饭卡。

今年 1 月初，山东淄博一高校的一位食堂管理人员发现了这个事件，起初有充值饭卡时电脑反映学生饭卡里面余额出现了负数，管理人员以为是系统出了问题，就没有多加留意，不久饭卡里呈现负数的学生越来越多，资金统计的时候，发现饭卡充值的金额也对不上。管

理人员意识到了问题，开始通过学校平台对这件事情进行彻查，最终怀疑学校饭卡有可能被复制了。

报警后，警方很快就锁定了犯罪嫌疑人刘某。被抓获之后，刘某对自己的犯罪事实供认不讳。仅仅从去年 12 月份到今年 1 月初，短短不到 2 个月的时间里，刘某就复制了十余所高校的饭卡 3000 多张，期间通过出售总共获利 10 万元，目前这名在校大学生已经被刑事拘留，等待他的也将是法律的严惩。

检察提醒：随着互联网技术的普及和发展，网络案件呈现出犯罪主体低龄化的趋势。君子爱财取之有道，自己有技能学到的多是好事，但是也要用于正途，大家在学习专业知识的同时也不要忽略思想道德与法律知识，合理合法创造自身价值才是正确解答。（来源：安全学习那些事）

➢ 雅虎就数据泄露案达成和解协议：金额达 1.175 亿美元

2019 年 4 月 10 日，据路透社报道由于遭遇史上最大数据泄密事件，雅虎接受了一项修改后的 1.175 亿美元和解协议，与本案的数百万受害者达成和解。这项周二披露的集体诉讼和解是为了解决美国加州圣何塞地区法院法官高兰惠（Lucy Koh）之前的批评。她在 1 月 28 日驳回了之前的和解协议，此次和解协议仍然需要获得她的批准。

高兰惠表示，最初的和解协议“不够公平、充分和合理”，因为没有列出整体金额，也没有说明每个受害者具体有望获得多少赔偿。她还表示，本案的法律费用似乎过高。

这起案件在 2013 至 2016 年间导致大约 30 亿帐号受到影响，而雅虎则被控在披露此事的过程中反应过慢。雅虎目前已经成为 Verizon 电信旗下的一家公司。

这份新的和解协议包含至少 5500 万美元支付给受害者的实付费用和其它成本，2400 万美元的两年信用监控费用，和高达 3000 万美元的法律费用，另有最多 850 万美元的其他费用。

本案涵盖 1.94 亿美国人和以色列人，大约涉及 8.96 亿帐号。

本案原告律师在法庭文件中称，1.175 亿美元是数据泄密案有史以来获得的最大赔偿。他尚未发表进一步评论。Verizon 也同意在 2019 至 2022 年间投入 3.06 亿美元信息安全费用，达到雅虎 2013 至 2016 年投入的 5 倍。该公司还承诺把雅虎在这一领域的人员数量增加到原先的 4 倍。

Verizon 在声明中说：“这份和解协议证明了我们对安全的重大承诺。”雅虎在 2016 年 7 月同意将其互联网业务作价 48.3 亿美元出售给 Verizon。不久后才披露此次数据泄密事件，导致收购价格降至 44.8 亿美元。Verizon 去年 12 月减记了雅虎的大量商誉价值。（来源：新浪科技）

➢ 研究人员发现中国企业简历信息泄露：涉 5.9 亿份简历

2019 年 4 月 8 日，据美国科技媒体 ZDNet 报道，有研究人员发现，中国企业今年前 3 个月出现数起简历信息泄漏事故，涉及 5.9 亿份简历。大多数简历之所以泄露，主要是因为 MongoDB 和 ElasticSearch 服务器安全措施不到位，不需要密码就能在网上看到信息，或者是因为防火墙出现错误导致。

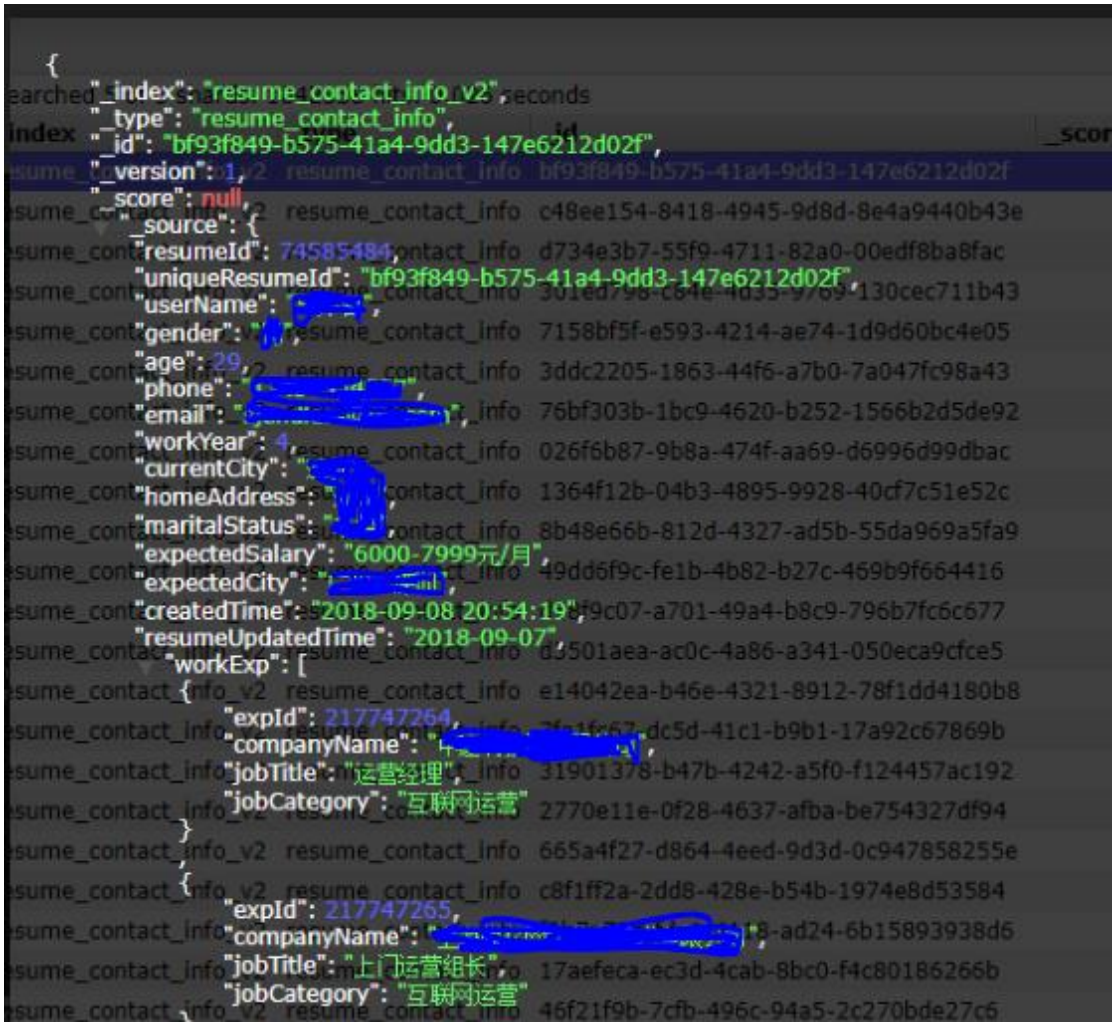
在过去几个月，尤其是过去几周，ZDNet 收到一些服务器泄露信息的相关消息，这些服务器属于中国 HR 企业。发现信息泄露的安全研究者叫山亚·简恩（Sanyam Jain）。单是在过去一个月，简恩就发现并汇报了 7 宗泄露事件，其中已经有 4 起泄露事故得到修复。

例如，3 月 10 日，简恩发现有一台 ElasticSearch 不安全，里面存放 3300 万中国用户的简历。他将问题报告给中国国家计算机应急响应小组（CNCERT），4 天之后数据库修正了问题。

3 月 13 日，简恩又发现一台 ElasticSearch 不安全，里面存放 8480 万份简历，在 CNCERT 的帮助下，问题也得到解决。

3 月 15 日，简恩又找到一台问题 ElasticSearch 服务器，里面存放 9300 万份简历。简恩说：“数据库意外离线，我向 CNCERT 汇报，还没有收到回应。”

第四台服务器存放来自中国企业的简历数据，里面有 900 万份简历，服务器同样来自 ElasticSearch。



还有第五个泄露点，这是一个 ElasticSearch 服务器集群，里面存放的简历超过 1.29 亿份。简恩无法确认所有者，目前数据库仍然门户大开。

简恩还发现另外两个泄露点，只是规模较小。一台 ElasticSearch 服务器存放 18 万份简历，一台存放 17000 份简历。

简单统计，中国企业在过去 3 个月泄露的简历达以 5.90497 亿份。（来源：新浪科技）

➢ 东莞通报医院候诊区播放不雅视频：初步分析系设备被入侵控制

2019 年 4 月 11 日中午，长安医院一处于待机状态的智能电视机自动播放不雅视频，后被医院护士发现后关闭。事件发生后，长安医院第一时间向公安机关报案，长安警方已介入调查。

收到事件信息后，长安镇、市卫生健康局高度重视。长安镇组织工作组到长安医院指导调查工作，并要求长安医院全面做好隐患排查工作，堵塞网络安全漏洞，保障医院网络安全，同时配合公安部门迅速开展侦查工作，查明事件真相。

目前，长安警方正在组织警力对电视播放源及现场人员进行全面排查，传播源仍在进一步调查当中。接下来，长安医院将全力配合公安部门做好案件侦办工作。

针对此次事件暴露出来的问题，市卫生健康局昨晚下发紧急通知，要求全市医疗机构组织自纠自查，加强设备管理，彻底关闭显示屏的自动投屏功能和 WiFi 连接功能。同时深刻吸取教训，深入排查整改，确保信息安全。（东莞市长安镇人民政府）

4 月 12 日市委网信办相关负责人介绍，这个事件从目前掌握的情况，初步分析是信息设备管理出现了漏洞，智能电视没有设置管理员密码或者使用弱口令，导致设备被入侵控制。“这个事件比较典型，类似的事件也比较多。比如近期有媒体报道，今年 1 月在武汉一家海底捞店发生的播放淫秽视频事件，就是涉案嫌疑人梁某破解电视接入密码后投屏播放导致。”

市委网信办提醒：随着智能家电、智能家居和公共 WIFI 的普及，互联网+生活日益便利，但网络安全隐患和风险也显著增加，社会大众在关注产品的功能和使用的便利性的同时，也应增强智能设备使用的安全意识。

在这里，分享一些简单易行的安全措施，比如增加访问权限设置，避免使用简单或初

始密码，定期更改密码以及限制网络上的设备数量,关闭不必要的功能等，这些都可在一定程度上防御网络安全风险。

对于消费者来说，在使用智能家电、家居的过程中应注意以下几点：

第一，智能家电、家居尽量使用有线连接

第二，不连接陌生 WiFi

第三，用户要使用强密码，密码要使用数字、特殊符号和大小写字母组合

第四，向云端传输数据的时候，使用安全的网络连接，不要在手机等控制设备上存储账号密码等敏感数据，以免手机被恶意入侵后导致住宅风险。（来源：澎湃新闻）